Privacy-Handbuch

Spurenarm Surfen mit Mozilla Firefox,
E-Mail mit Thunderbird,
chatten und verschlüsselt telefonieren,
Anonymisierungsdienste nutzen
und Daten verschlüsseln
für WINDOWS + Linux

8. Juni 2021
Inhaltsverzeichnis

1 Scroogled 7

2 Angriffe auf die Privatsphäre 17
   2.1 Big Data - Kunde ist der, der bezahlt 18
   2.1.1 Google 18
   2.1.2 Weitere Datensammler 24
   2.2 Techniken der Datensammler 26
   2.3 Tendenzen auf dem Gebiet des Tracking 31
   2.4 Crypto War 3.0 34
   2.5 Fake News Debatte 37
   2.5.1 Der Kampf gegen Fake News 38
   2.5.2 Fake News Beispiele 39
   2.5.3 Medienkompetenztraining 43
   2.5.4 Fake News oder Propaganda - was ist der Unterschied? 44
   2.6 Geotagging 44
   2.7 Kommunikationsanalyse 47
   2.8 Überwachungen im Internet 49
   2.9 Terrorismus und der Ausbau der Überwachung 55
   2.10 Ich habe doch nichts zu verbergen 59

3 Digitales Aikido 63
   3.1 Nachdenken 64
   3.2 Ein Beispiel 67
   3.3 Schattenseiten der Anonymität 68
   3.4 Wirkungsvoller Einsatz von Kryptografie 69

4 Spurenarm Surfen 72
   4.1 Auswahl des Webbrowsers 73
   4.2 Datensparsame Suchmaschinen 75
   4.3 Cookies und EverCookies 80
   4.4 Surf-Container 84
   4.5 JavaScript 85
   4.5.1 NoScript für Mozilla Firefox 86
   4.6 iFrames 88
   4.7 Werbung, HTML-Wanzen und Social Media 90
   4.7.1 Tracking-Filter für Firefox 91
   4.7.2 Tracking Protection in Firefox 92
   4.7.3 uBlock Origin für Firefox 94
   4.8 Firefox activity-stream 95
   4.9 Contextual Feature Recommender (CFR) 98
   4.10 Browsercache und Surf-Chronik 99
   4.11 Referer 102
   4.12 URL-Parameter 103
   4.13 Risiko Plugins 104
   4.13.1 Media Plug-ins für Video und Audio 104
   4.13.2 Anzeige von PDF Dokumenten 105
INHALTSVERZEICHNIS

3

4.14 HTTPS-Verschlüsselung erzwingen und härten .......................... 106
  4.14.1 Anzeige der HTTPS Verschlüsselung .................................. 108
  4.14.2 Vertrauenswürdigkeit von HTTPS ...................................... 109
  4.14.3 SSL-Zertifikate via OCSP validieren .................................. 110
  4.14.4 Tracking via TLS Session .................................................. 111
  4.14.5 Tracking via HTTP Strict Transport Security (HSTS) .................. 112
  4.14.6 SSL/TLS Konfiguration ..................................................... 113

4.15 Installierte Schriftarten verstecken ......................................... 114

4.16 HTML5 Canvas Elemente .......................................................... 116

4.17 Zugriff auf lokale URLs blockieren ......................................... 118

4.18 Der Unsinn vom Spoofen der User-Agent Kennung ........................ 119

4.19 Hardware Fingerprinting .......................................................... 121

4.20 WebRTC mit Firefox ................................................................. 123

4.21 DNS-over-HTTPS mit Firefox .................................................... 126

4.22 Sonstige Maßnahmen ............................................................... 129

4.23 Zusammenfassung der Einstellungen ......................................... 135

4.24 Snakeoil für Firefox (überflüssiges) ........................................ 136

5 Passwörter und 2-Faktor-Authentifizierung ................................. 139
  5.1 Hinweise für Passwörter .......................................................... 140
  5.1.1 Firefox build-in Passwortspeicher ....................................... 142
  5.1.2 Passwortspeicher .............................................................. 143
  5.2 Zwei-Faktor-Authentifizierung ............................................... 145
  5.3 Phishing Angriffe ................................................................. 150

6 Bezahlen im Netz ........................................................................... 152
  6.1 Anonyme Online-Zahlungen vor dem Aus? .................................... 155
  6.2 Bargeld ....................................................................................... 156
  6.3 Bitcoin ....................................................................................... 158

7 E-Mail Kommunikation ................................................................. 160
  7.1 E-Mail Provider ......................................................................... 160
  7.2 ProtonMail und Tutanota ............................................................ 162
  7.3 Mozilla Thunderbird ................................................................. 164
    7.3.1 Account erstellen ............................................................... 165
    7.3.2 Sichere Optionen für TLS-Verschlüsselung .............................. 168
    7.3.3 Sichere Konfiguration des E-Mail Client ................................. 170
    7.3.4 Datenverluste vermeiden ..................................................... 174
    7.3.5 Wörterbücher installieren .................................................... 174
    7.3.6 Spam-Filter aktivieren ......................................................... 175
    7.3.7 Spam vermeiden ................................................................. 175
    7.3.8 RSS-Feeds ......................................................................... 179
    7.3.9 Filelink ............................................................................. 180
  7.4 Private Note ................................................................................ 181

8 E-Mails verschlüsseln ................................................................. 183
  8.1 E-Mails verschlüsseln mit Thunderbird ....................................... 185
  8.1.1 Eigenen OpenPGP Schlüssel erstellen oder importieren ............... 186
  8.1.2 Eigenen OpenPGP Schlüssel mit GnuPG verwenden .................... 186
  8.1.3 Den eigenen öffentlichen Schlüssel verteilen ............................... 187
  8.1.4 Fremde Schlüssel importieren ............................................... 188
  8.1.5 Fremde Schlüssel akzeptieren bzw. verifizieren ......................... 189
  8.2 Gedanken zum Mailvelope Browser Add-on ................................... 189
    8.2.1 Mailvelope mit GnuPG nutzen ............................................. 191
    8.2.2 Mailvelope und Autocrypt ................................................. 191
  8.3 Einige Ergänzungen zum Thema GnuPG ....................................... 192
    8.3.1 Gedanken zur Auswahl und Stärke von Schlüsseln .................... 194
    8.3.2 GnuPG Smartcards nutzen .................................................. 194
8.3.3 Adele - der freundliche OpenPGP E-Mail-Roboter ........................................ 197
8.3.4 Memory Hole Project .................................................................................. 198
8.3.5 Autocrypt .................................................................................................. 199
8.3.6 Verschlüsselung in Webformularen ............................................................ 200
8.3.7 OpenPGP-Verschlüsselung für Kontaktformulare ....................................... 201
8.3.8 OpenPGP Keyserver .................................................................................. 204
8.3.9 Web des Vertrauens (WoT) ........................................................................ 205
8.4 Verschlüsselte Dokumente per E-Mail senden .................................................. 208

9 Instant Messaging und Telefonie ................................................................. 209
9.1 Verschlüsselte Telefonie ................................................................................ 212
  9.1.1 SRTP/ZRTP Verschlüsselung ..................................................................... 213
  9.1.2 Verschlüsselt chatten und telefonieren mit qTox ...................................... 213
  9.1.3 Skype?? ................................................................................................ 217
9.2 Instant Messaging ........................................................................................ 218
  9.2.1 Messenger Threema ................................................................................ 224
  9.2.2 Messenger Signal App ............................................................................. 226
  9.2.3 Messenger Telegram .............................................................................. 230
  9.2.4 Messenger basierend auf [matrix] ............................................................... 236
  9.2.5 Chatten mit Jabber/XMPP ......................................................................... 238
  9.2.6 Messenger Wire ....................................................................................... 240
  9.2.7 Einige weitere Messenger (unvollständig) ................................................ 241
9.3 Videokonferenzen mit Jitsi Meet ................................................................. 242

10 Anonymisierungsdienste .............................................................................. 244
10.1 Warum sollte man diese Dienste nutzen? .................................................... 244
10.2 Tor Onion Router ......................................................................................... 246
  10.2.1 Security Notes ........................................................................................ 249
  10.2.2 Anonym Surfen mit dem TorBrowserBundle ......................................... 250
  10.2.3 TorBrowser für Android Smartphones .................................................... 257
  10.2.4 OnionBrowser für iPhones ....................................................................... 257
  10.2.5 Sicherheitskonzept für hohe Ansprüche ................................................... 258
  10.2.6 Anonyme E-Mail Accounts .................................................................... 261
  10.2.7 Anonym Bloggen ................................................................................... 264
  10.2.8 Anonymes Instant-Messaging ................................................................. 264
  10.2.9 Gajim (Linux) und Tor Onion Router ...................................................... 266
  10.2.10 Dateien anonym tauschen via Tor ............................................................ 267
  10.2.11 Tor Onion Services ............................................................................... 269
  10.2.12 Tor Bad Exit Nodes ............................................................................. 274
  10.2.13 Tor Good Exit Nodes ........................................................................... 276
10.3 Finger weg von unseriösen Angeboten ....................................................... 278

11 Anonyme Peer-2-Peer Netzwerke .............................................................. 280
11.1 Invisible Internet Project (I2P) ................................................................... 282
  11.1.1 Installation des I2P-Routers .................................................................... 282
  11.1.2 Konfiguration des I2P-Router ................................................................ 284
  11.1.3 Anonym Surfen mit I2P ......................................................................... 285
  11.1.4 I2P Mail 1 (Susimail) ............................................................................ 287
  11.1.5 I2P Mail 2 (Bote) .................................................................................. 289
  11.1.6 I2P IRC .................................................................................................. 292
  11.1.7 I2P BitTorrent ....................................................................................... 293
11.2 DSL-Router und Computer vorbereiten ..................................................... 295
12 Virtual Private Networks (VPNs) 296
  12.1 VPN Dienste als Billig-Anonymisierer .................................. 297
  12.2 Empfehlenswerte VPN-Provider ........................................... 298
  12.3 Verschiedene VPN Lösungen für Linux .................................... 299
    12.3.1 OpenVPN mit Linux .................................................. 299
  12.4 IPsec/IKEv2 VPN Client mit Windows 10 ................................ 300
  12.5 Das VPN Exploitation Team der NSA .................................... 301

13 Domain Name Service (DNS) 304
  13.1 DNSSEC Validierung ......................................................... 305
  13.2 Verschlüsselung des DNS Datenverkehr .................................. 305
  13.3 Vertrauenswürdige DNS-Server ............................................ 307
  13.4 DNS-Server der Big Player der IT Branche ............................. 308
  13.5 Konfiguration der DNS-Server ............................................ 309

14 Daten verschlüsseln 313
  14.1 Konzepte der vorgestellten Tools ......................................... 314
  14.2 Gedanken zur Passphrase .................................................. 315
  14.3 Dokumente verschlüsselt speichern ..................................... 318
  14.4 Quick and Dirty mit GnuPG ............................................... 319
  14.5 dm-crypt/LUKS für Linux ................................................. 320
    14.5.1 Linux System komplett verschlüsseln ................................ 320
    14.5.2 Für Genießer in der Konsole mit cryptsetup ....................... 321
    14.5.3 Hardware Token verwenden (Nitrokey, Yubikey) .................... 325
    14.5.4 LUKS-Nuke - hinterhältige Datenzerstörung ........................ 328
  14.6 zuluCrypt für Linux ...................................................... 329
  14.7 Backups verschlüsseln ..................................................... 330
    14.7.1 Schnell mal auf den USB-Stick ...................................... 330
    14.7.2 Online Backups ....................................................... 332

15 Daten löschen 336
  15.1 Dateien in den Papierkorb werfen ....................................... 336
  15.2 Dateien sicher löschen (Festplatten) ................................... 336
  15.3 Dateierste nachträglich beseitigen ..................................... 337
  15.4 Dateien sicher löschen (SSDs) .......................................... 338
  15.5 Gesamten Datenträger säubern (Festplatten) .......................... 339
  15.6 Gesamten Datenträger säubern (SSDs) ................................ 339
  15.7 Datenträger zerstören ..................................................... 340

16 Daten anonymisieren 341
  16.1 Fotos und Bilddateien anonymisieren .................................. 342
  16.2 PDF-Dokumente säubern .................................................. 342

17 Daten verstecken 345
  17.1 Allgemeine Hinweise ....................................................... 346
  17.2 steghide .......................................................................... 346
  17.3 stegdetect ................................................................. 347

18 Betriebssysteme 349
  18.1 Microsoft Windows .......................................................... 349
    18.1.1 Telemetrie in Windows 10 ........................................... 350
    18.1.2 Virescanner sind Snakeoil .......................................... 352
  18.2 Apple MacOS ................................................................. 353
  18.3 Linux Distributionen ........................................................ 354
  18.4 Linux-taugliche Hardware ................................................ 357
  18.5 NetBSD und OpenBSD ...................................................... 358
  18.6 Risiko USB, Firewire und Thunderbolt .................................. 358
  18.7 Linux Firewall konfigurieren ............................................. 362
<table>
<thead>
<tr>
<th>Kapitel</th>
<th>Unterkapitel</th>
<th>Seitenzahl</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.7.1</td>
<td>Uncomplicated Firewall (UFW)</td>
<td>362</td>
</tr>
<tr>
<td>18.7.2</td>
<td>RHEL Firewall</td>
<td>363</td>
</tr>
<tr>
<td>18.7.3</td>
<td>QubesOS Firewall</td>
<td>364</td>
</tr>
<tr>
<td>18.8</td>
<td>WLAN Privacy Leaks</td>
<td>364</td>
</tr>
<tr>
<td>18.8.1</td>
<td>MAC-Adresse faken (Windows 10)</td>
<td>366</td>
</tr>
<tr>
<td>18.8.2</td>
<td>MAC-Adresse faken (Linux)</td>
<td>366</td>
</tr>
<tr>
<td>18.8.3</td>
<td>Automatische Anmeldung für bevorzugte WLANs deaktivieren</td>
<td>367</td>
</tr>
<tr>
<td>18.8.4</td>
<td>Hostname und DNS-Domain konfigurieren</td>
<td>368</td>
</tr>
<tr>
<td>19</td>
<td>Smartphones</td>
<td>369</td>
</tr>
<tr>
<td>19.1</td>
<td>Kommerzielle Datensammlungen</td>
<td>370</td>
</tr>
<tr>
<td>19.1.1</td>
<td>Datensammlungen der Smartphone Hersteller</td>
<td>370</td>
</tr>
<tr>
<td>19.1.2</td>
<td>Datensammlungen mit Smartphone Apps</td>
<td>372</td>
</tr>
<tr>
<td>19.2</td>
<td>Überwachung</td>
<td>376</td>
</tr>
<tr>
<td>19.3</td>
<td>Aktivierung als Abhörwanze</td>
<td>377</td>
</tr>
<tr>
<td>19.4</td>
<td>WLAN ausschalten, wenn nicht genutzt</td>
<td>378</td>
</tr>
<tr>
<td>19.5</td>
<td>Tracking blockieren</td>
<td>381</td>
</tr>
<tr>
<td>19.6</td>
<td>Zugriff auf Standortdaten einschränken</td>
<td>382</td>
</tr>
<tr>
<td>19.7</td>
<td>Krypto-Apps</td>
<td>383</td>
</tr>
<tr>
<td>19.8</td>
<td>Stille SMS ind IMSI-Catcher erkennen</td>
<td>384</td>
</tr>
<tr>
<td>19.9</td>
<td>Juice Jacking Angriffe</td>
<td>385</td>
</tr>
<tr>
<td>19.10</td>
<td>Das Hidden OS im Smartphone</td>
<td>385</td>
</tr>
</tbody>
</table>
Kapitel 1

Scroogled

Greg landete abends um acht auf dem internationalen Flughafen von San Francisco, doch bis er in der Schlange am Zoll ganz vorn ankam, war es nach Mitternacht. Er war der ersten Klasse nussbraun, unrasiert und drahtig entstiegen, nachdem er einen Monat am Strand von Cabo verbracht hatte, um drei Tage pro Woche zu tauchen und sich in der übrigen Zeit mit der Verführung französischer Studentinnen zu beschäftigen. Vor vier Wochen hatte er die Stadt als hängeschulteriges, kullerbäuchiges Wrack verlassen. Nun war er ein bronzener Gott, der bewundernde Blicke der Stewardessen vorn in der Kabine auf sich zog.

Vier Stunden später war in der Schlange am Zoll aus dem Gott wieder ein Mensch geworden. Sein Elan war ermattet, Schweiß rann ihm bis hinunter zum Po, und Schultern und Nacken waren so verspannt, dass sein Rücken sich anfühlte wie ein Tennisschläger. Sein iPod-Akku hatte schon längst den Geist aufgegeben, sodass ihm keine andere Ablenkung blieb, als dem Gespräch des Pärchens mittleren Alters vor ihm zu lauschen.


“Ich dachte, das sollte erst nächsten Monat losgehen?” Der Mann setzte seinen Riesen-Sombrero immer wieder auf und ab.

Googeln an der Grenze - Allmächtiger. Greg hatte sich vor sechs Monaten von Google verabschiedet, nachdem er seine Aktienoptionen zu Barem gemacht hatte, um sich eine Auszeit zu gönnen, die dann allerdings nicht so befriedigend wurde wie erhofft. Denn während der ersten fünf Monate hatte er kaum etwas anderes getan, als die Rechner seiner Freunde zu reparieren, tagsüber vorm Fernseher zu sitzen und zehn Pfund zuzunehmen - was wohl darauf zurückzuführen war, dass er nun daheim herumsaß statt im Googleplex mit seinem gut ausgestatteten 24-Stunden-Fitnessclub.


“Möchten Sie mir was über Juni 1998 erzählen?”

Greg blickte vom Abflugplan hoch. “Pardon?”

“Sie haben am 17. Juni 1998 eine Nachricht auf alt.burningman über Ihre Absicht geschrieben, ein Festival zu besuchen. Und da fragten Sie: Sind Psychopilze wirklich so eine schlechte Idee?”

Der Interviewer im zweiten Befragungsraum war ein älterer Mann, nur Haut und Knochen, als sei er aus Holz geschnitzt. Seine Fragen gingen sehr viel tiefer als Psychopilze.

“Berichten Sie von Ihren Hobbys. Befassen Sie sich mit Raketenmodellen?”

“Womit?”

“Mit Raketenmodellen.”


Der Mann machte eine Notiz und klickte ein paarmal. “Ich frage nur, weil bei Ihren Suchanfragen und Ihrer Google-Mail ne Menge Werbung für Raketenzubehör auftaucht.”

Greg schluckte. “Sie blättern durch meine Suchanfragen und Mails?” Er hatte nun seit einem Monat keine Tastatur angefasst, aber er wusste: Was er in die Suchleiste eintippte, war wahrscheinlich aussagekräftiger als alles, was er seinem Psychiater erzählte.


Der Mann nickte. “Ich verstehe, Sir. Und genau deshalb spreche ich jetzt hier mit Ihnen. Können Sie sich erklären, weshalb bei Ihnen so häufig Modellraketen-Werbung erscheint?”


Die Sache schien gerade ausgestanden zu sein, als der geschnitzte Mann die Halloween-Fotos entdeckte - tief vergraben auf der dritten Seite der Suchergebnisse für Greg Lupinski.

“Es war eine Golfkriegs-Themenparty im Castro”, sagte er.

“Und Sie sind verkleidet als . . .?”

“Selbstmordattentäter”, erwiderte er kläglich. Das Wort nur auszusprechen verursachte ihm Übelkeit.

“Kommen Sie mit, Mr. Lupinski”, sagte der Mann.
Als er endlich gehen durfte, war es nach drei Uhr. Seine Koffer standen verloren am Gepäckkarussell. Er nahm sie und sah, dass sie geöffnet und nachlässig wieder geschlossen worden waren; hier und da lugten Kleidungsstücke heraus.

Daheim stellte er fest, dass all seine pseudopräkolumbianischen Statuen zerbrochen worden waren und dass mitten auf seinem brandneuen weißen mexikanischen Baumwollhemd ein ominöser Stiefelabdruck prangte. Seine Kleidung roch nun nicht mehr nach Mexiko - sie roch nach Flughafen.

An Schlaf war jetzt nicht mehr zu denken, er musste über die Sache reden. Es gab nur eine einzige Person, die all das begreifen würde. Zum Glück war sie normalerweise um diese Zeit noch wach.

Maya war zwei Jahre nach Greg zu Google gekommen. Sie war es, die ihn überzeugt hatte, nach dem Einlösen der Optionen nach Mexiko zu gehen: Wohin auch immer, hatte sie gesagt, solange er nur seinem Dasein einen Neustart verpasste.

Maya hatte zwei riesige schokobraune Labradore und eine überaus geduldige Freundin, Laurie, die mit allem einverstanden war, solange es nicht bedeutete, dass sie selbst morgens um sechs von 350 Pfund sabbernder Caniden durch Dolores Park geschleift wurde.

Maya griff nach ihrem Tränengas, als Greg auf sie zugelaufen kam; dann blickte sie ihn erstaunt an und breitete ihre Arme aus, während sie die Leinen fallen ließ und mit dem Schuh festhielt. "Wo ist der Rest von dir? Mann, siehst du heiß aus!"

Er erwiderte die Umarmung, plötzlich seines Aromas nach einer Nacht invasiven Googelns bewusst. "Maya", sagte er, "was weißt du über Google und das DHS?"


Letztlich war es für Google gar nicht teuer gewesen, die Stadt mit Webcams zu überziehen - vor allem, wenn man bedachte, welche Möglichkeiten es bot, Menschen die passende Werbung zu ihrem jeweiligen Aufenthaltsort liefern zu können. Greg hatte seinerzeit kaum Notiz davon genommen, als die Kameras auf all den Hotspots ihren öffentlichen Betrieb aufnahmen; es hatte einen Tag lang Aufruhr in der Blogosphäre gegeben, während die Leute mit dem neuen Allesseher zu spielen begannen und an diverse Rotlichtviertel heranzoomten, doch nach einer Weile war die Aufregung abgeebbt.

Greg kam sich albern vor, er murmelte: "Du machst Witze."

"Komm mit", erwiderte sie, nicht ohne sich dabei vom Laternenpfahl abzuwenden.

Die Hunde waren nicht einverstanden damit, den Spaziergang abzukürzen, und taten ihren Unmut in der Küche kund, wo Maya Kaffee zubereitete.

"Wir haben einen Kompromiss mit dem DHS ausgehandelt", sagte sie und griff nach der Milch. "Sie haben sich damit einverstanden erklärt, nicht mehr unsere Suchprotokolle zu durchwühlen, und wir lassen sie im Gegenzug sehen, welcher Nutzer welche Anzeigen zu sehen bekommt."

Greg fühlte sich elend. "Warum? Sag nicht, dass Yahoo es schon vorher gemacht hat…"

"N-nein. Doch, ja sicher, Yahoo war schon dabei. Aber das war nicht der Grund
für Google mitzumachen. Du weißt doch, die Republikaner hassen Google. Wir sind größtenteils als Demokraten registriert, also tun wir unser Bestes, mit ihnen Frieden zu schließen, bevor sie anfangen, sich auf uns einzuschießen. Es geht ja auch nicht um P.I.I. - persönlich identifizierende Information, der toxische Smog der Informationsära - sondern bloß um Metadaten. Also ist es bloß ein bisschen böse."

"Warum dann all die Heimlichtuerei?"


Greg fühlte sich sehr müde. "Na, da kann ich von Glück reden, dass ich lebend aus dem Flughafen herausgekommen bin. Mit Pech wäre ich jetzt eine Vermisstenmeldung, was?"

Maya blickte ihn nachdenklich an. Er wartete auf eine Antwort.

"Was ist denn?"

"Ich werde dir jetzt was erzählen, aber du darfst es niemals weitergeben, o.k.?"

"Ähm, du bist nicht zufällig in einer terroristischen Vereinigung?"

"Wenn es so einfach wäre ... Die Sache ist die: Was das DHS am Flughafen treibt, ist eine Art Vorsortierung, die es den Schlapphüten erlaubt, ihre Suchkriterien enger zu fassen. Sobald du an der Grenze ins zweite Zimmerchen gebeten wirst, bist du eine Person von Interesse - und dann haben sie dich im Griff. Sie suchen über Webcams nach deinem Gesicht und Gang, lesen deine Mail, überwachen deine Suchanfragen."

"Sagtest du nicht, die Gerichte würden das nicht erlauben?"


Greg fühlte Übelkeit in sich aufsteigen. "Wie zum Teufel konnte das passieren? Google war ein guter Ort. Tu nichts Böses, war da nicht was?" Das war das Firmenmotto, und für Greg war es ein Hauptgrund dafür gewesen, seinen Stanford-Abschluss in Computerwissenschaften direkten Wegs nach Mountain View zu tragen.


Sie schwiegen eine Minute lang.

"Es ging in China los", sagte sie schließlich. "Als wir unsere Server aufs Festland brachten, unterstellten wir sie damit chinesischem Recht."


Greg schüttelte den Kopf. “Und warum mussten die Server in China stehen?”

“Die Regierung sagte, sie würde uns sonst blocken. Und Yahoo war schon da.” Sie schnitten beide Grimassen. Irgendwann hatten die Google-Mitarbeiter eine Obsession für Yahoo entwickelt und sich mehr darum gekümmert, was die Konkurrenz trieb, als darum, wie es um das eigene Unternehmen stand. “Also taten wir es - obwohl viele von uns es nicht für eine gute Idee hielten.”

Maya schlürfte ihren Kaffee und senkte die Stimme. Einer ihrer Hunde schnupperte unablässig unter Gregs Stuhl.


“Und jetzt?” Greg schubste einen Hund beiseite. Maya wirkte gekränkt.


“…verratet und vergoogelt.”

“Voll und ganz”, nickte sie.

Maya brachte beide Labradors zum Schlafzimmer. Eine gedämpfte Diskussion mit ihrer Freundin war zu hören, dann kam sie allein zurück.


“Ich will nicht, dass du meinetwegen Ärger bekommst.”

Sie schüttelte den Kopf. “Ich bin ohnehin schon geliefert. Jeder Tag, seit ich das
verdammte Ding programmiert habe, ist geschenkte Zeit. Ich warte bloß noch drauf, dass jemand dem DHS meinen Background steckt, und dann ... tja, ich weiß auch nicht. Was auch immer sie mit Menschen wie mir machen in ihrem Krieg gegen abstrakte Begriffe."

Greg dachte an den Flughafen, an die Durchsuchung, an sein Hemd mit dem Stiefelabdruck.

"Tu es", sagte er.


Nun gut, das sollte ihm recht sein.

Dann klickte er sein Adressbuch an und stellte fest, dass die Hälfte seiner Kontakte fehlte. Sein Gmail-Posteingang war wie von Termiten ausgehöhlt, sein Orkut-Profil normalisiert. Sein Kalender, Familienfotos, Lesezeichen: alles leer. Bis zu diesem Moment war ihm nicht klar gewesen, wie viel seiner selbst ins Web migriert war und seinen Platz in Googles Serverfarmen gefunden hatte - seine gesamte Online-Identität. Maya hatte ihn auf Hochglanz poliert; er war jetzt Der Unsichtbare.

Greg tippte schläfrig auf die Tastatur seines Laptops neben dem Bett und erweckte den Monitor zum Leben. Er blinzelte die Uhr in der Toolbar an. 4:13 Uhr morgens! Allmächtiger, wer hämmerte denn um diese Zeit gegen seine Tür?

Er rief mit nuscheliger Stimme "Komm ja schon" und schlüpfte in Morgenmantel und Pantoffeln. Dann schlurfte er den Flur entlang und knipste unterwegs die Lichter an. Durch den Türspion blickte ihm düster Maya entgegen.

Er entfernte Kette und Riegel und öffnete die Tür. Maya huschte an ihm vorbei, gefolgt von den Hunden und ihrer Freundin. Sie war schweißüberströmt, ihr normalerweise gekämmtes Haar hing strähnig in die Stirn. Sie rieb sich die roten, geränderten Augen.

"Pack deine Sachen", stieß sie heiser hervor.

"Was?"


"Wohin willst ..."


"Maya", sagte er scharf, "ich gehe nirgendwohin, solange du mir nicht sagst, was los ist."

“Googler frisieren die Profile von Senatoren?”


“Du schnüffelst in Gmail-Konten?”


“Sie kamen heute zu Besuch”, entgegnete sie. “Zwei politische Beamte vom DHS. Blieben stundenlang und stellten eine Menge verdammt harter Fragen.”

“Über den Googleputzer?”

“Über meine Freunde und Familie. Meine Such-Geschichte. Meine persönliche Geschichte.”

“Jesus.”

“Das war eine Botschaft für mich. Die beobachten mich - jeden Klick, jede Suche. Zeit zu verschwinden, jedenfalls aus ihrer Reichweite.”

“In Mexiko gibt es auch eine Google-Niederlassung.”

“Wir müssen jetzt los”, beharrte sie.

“Laurie, was hältst du davon?”, fragte Greg.


“Greg, kommst du nun?”


Maya zog ein Gesicht, als wolle sie ihm eine runterhauen. Dann entspannte sie sich und umarmte ihn heftig.
“Pass du auf dich auf”, flüsterte sie ihm ins Ohr.

Eine Woche später kamen sie zu ihm. Nach Hause, mitten in der Nacht, genau wie er es sich vorgestellt hatte. Es war kurz nach zwei Uhr morgens, als zwei Männer vor seiner Tür standen.

Einer blieb schweigend dort stehen. Der andere war ein Lächler, klein und faltig, mit einem Fleck auf dem einen Mantelrevers und einer amerikanischen Flagge auf dem anderen. “Greg Lupinski, es besteht der begründete Verdacht, dass Sie gegen das Gesetz über Computerbetrug und -missbrauch verstoßen haben”, sagte er, ohne sich vorzustellen. “Insbesondere, dass Sie Bereiche autorisierten Zugangs überschritten und sich dadurch Informationen verschafft haben. Zehn Jahre für Ersttäter. Außerdem gilt das, was Sie und Ihre Freundin mit Ihren Google-Daten gemacht haben, als schweres Verbrechen. Und was dann noch in der Verhandlung zutage kommen wird … angefangen mit all den Dingen, um die Sie Ihr Profil bereinigt haben.”

Greg hatte diese Szene eine Woche lang im Geist durchgespielt, und er hatte sich allerlei mutige Dinge zurechtgelegt, die er hätte sagen wollen. Es war eine willkommene Beschäftigung gewesen, während er auf Mayas Anruf wartete. Der Anruf war nie gekommen.

“Ich möchte einen Anwalt sprechen”, war alles, was er herausbrachte.

“Das können Sie tun”, sagte der kleine Mann. “Aber vielleicht können wir zu einer besseren Einigung kommen.”

Greg fand seine Stimme wieder. “Darf ich mal Ihre Marke sehen?”


Greg wandte sich der Kaffeemaschine zu und entsorgte den alten Filter.

“Ich gehe zur Presse”, sagte er.

Der Mann nickte, als ob er darüber nachdenken müsse. “Na klar. Sie gehen eines Morgens zum Chronicle und breiten alles aus. Dort sucht man nach einer Quelle, die Ihre Story stützt; man wird aber keine finden. Und wenn sie danach suchen, werden wir sie finden. Also lassen Sie mich doch erst mal ausreden, Kumpel. Ich bin im Win-Win-Geschäft, und ich bin sehr gut darin.”

Er pausierte. “Sie haben da übrigens hervorragende Bohnen, aber wollen Sie sie nicht erst eine Weile wässern? Dann sind sie nicht mehr so bitter, und die Öle kommen besser zur Geltung. Reichen Sie mir mal ein Sieb?”

Greg beobachtete den Mann dabei, wie er schweigend seinen Mantel auszog und über den Küchenstuhl hängte, die Manschetten öffnete, die Ärmel sorgfältig hochrollte und eine billige Digitaluhr in die Tasche steckte. Er kippte die Bohnen aus der Mühle in Gregs Sieb und wässerte sie in der Spüle.

Er war ein wenig untersetzt und sehr bleich, mit all der sozialen Anmut eines Elektroingenieurs. Wie ein echter Googler auf seine Art, besessen von Kleinigkeiten. Mit Kaffeemühlen kannte er sich also auch aus.
Wir stellen ein Team für Haus 49 zusammen …”

”Es gibt kein Haus 49”, sagte Greg automatisch.

”Schon klar”, entgegnete der andere mit verkniffenem Lächeln. “Es gibt kein Haus 49. Aber wir bauen ein Team auf, das den Googleputzer überarbeiten soll. Mayas Code war nicht sonderlich schlank und steckt voller Fehler. Wir brauchen ein Upgrade. Sie wären der Richtige; und was Sie wissen, würde keine Rolle spielen, wenn Sie wieder an Bord sind.”

”Unglaublich”, sagte Greg spöttisch. ”Wenn Sie denken, dass ich Ihnen helfe, im Austausch für Gefälligkeiten politische Kandidaten anzuschwärzen, sind Sie noch wahnsinniger, als ich dachte.”


”Wir tun für unsere Freunde das Gleiche, was Maya für Sie getan hat. Nur ein wenig aufräumen. Nur ihre Privatsphäre schützen - mehr nicht.”

Greg nippte am Kaffee. ”Was geschieht mit den Kandidaten, die Sie nicht putzen?”

”Na ja”, sagte Gregs Gegenüber mit dünnem Grinsen, ”tja, Sie haben Recht, für die wird es ein bisschen schwierig.” Er kramte in der Innentasche seines Mantels und zog einige gefaltete Blätter Papier hervor, strich sie glatt und legte sie auf den Tisch. ”Hier ist einer der Guten, der unsere Hilfe braucht.” Es war das ausgedruckte Suchprotokoll eines Kandidaten, dessen Kampagne Greg während der letzten drei Wahlen unterstützt hatte.

”Der Typ kommt also nach einem brutalen Wahlkampf-Tag voller Klinkenputzen ins Hotel, fährt den Laptop hoch und tippt knackige Ärsche in die Suchleiste. Ist doch kein Drama, oder? Wir sehen es so: Wenn man wegen so was einen guten Mann daran hindert, weiterhin seinem Land zu dienen, wäre das schlichtweg unamerikanisch.”

Greg nickte langsam.

”Sie werden ihm also helfen?”, fragte der Mann.

”Ja.”

”Gut. Da wäre dann noch was: Sie müssen uns helfen, Maya zu finden. Sie hat überhaupt nicht verstanden, worum es uns geht, und jetzt scheint sie sich verdrückt zu haben. Wenn sie uns bloß mal zuhört, kommt sie bestimmt wieder rum.”

Er betrachtete das Suchprofil des Kandidaten.

”Denke ich auch”, erwiderte Greg.

Der neue Kongress benötigte elf Tage, um das Gesetz zur Sicherung und Erfassung von Amerikas Kommunikation und Hypertext zu verabschieden. Es erlaubte dem DHS und der NSA, bis zu 80 Prozent der Aufklärungs- und Analysearbeit an Fremdfirmen auszulagern. Theoretisch wurden die Aufträge über offene Bietverfahren vergeben, aber in den sicheren Mauern von Googles Haus 49 zweifelte niemand daran, wer den Zuschlag erhalten würde. Wenn Google 15 Milliarden Dollar für ein Programm ausgegeben hätte,
Übeltäter an den Grenzen abzufangen, dann hätte es sie garantiert erwischt - Regierungen sind einfach nicht in der Lage, richtig zu suchen.

Am Morgen darauf betrachtete Greg sich prüfend im Rasierspiegel (das Wachpersonal mochte keine Hacker-Stoppelbärte und hatte auch keine Hemmungen, das deutlich zu sagen), als ihm klar wurde, dass heute sein erster Arbeitstag als De-facto-Agent der US-Regierung begann. Wie schlimm mochte es werden? Und war es nicht besser, dass Google die Sache machte, als irgendein ungeschickter DHS-Schreibtischtäter?


Ziehen, ziehen, ziehen. Plötzlich hörte er eine Stimme neben sich. “Greg, kann ich Sie bitte sprechen?”

Der verschrumpelte Mann legte einen Arm um seine Schulter, und Greg atmete den Duft seines Zitrus-Rasierwassers ein. So hatte sein Tauchlehrer in Baja geduftet, wenn sie abends durch die Kneipen zogen. Greg konnte sich nicht an seinen Namen erinnern: Juan Carlos? Juan Luis?

Der Mann hielt seine Schulter fest im Griff, lotste ihn weg von der Tür, über den tadellos getrimmten Rasen und vorbei am Kräutergarten vor der Küche. “Wir geben Ihnen ein paar Tage frei”, sagte er.

Greg durchschoss eine Panikattacke. “Warum?” Hatte er irgendetwas falsch gemacht? Würden sie ihn einbuchten?


Greg spürte, wie der Boden unter seinen Füßen verschwand und wie er meilenweit emporgezogen wurde. In einer Google-Earth-Ansicht des Googleplex sah er sich und den verschumpelten Mann als Punktepaar, zwei Pixel, winzig und belanglos. Er wünschte, er könnte sich die Haare ausreißen, auf die Knie fallen und weinen.

Von weit, weit weg hörte er sich sagen: “Ich brauche keine Auszeit. Ich bin okay.”

Von weit, weit weg hörte er den verschumpelten Mann darauf bestehen.

Die Diskussion dauerte eine ganze Weile, dann gingen die beiden Pixel in Haus 49 hinein, und die Tür schloss sich hinter ihnen.

Ich danke dem Autor Cory Doctorow und dem Übersetzer Christian Wöhrl dafür, dass sie den Text unter einer Creative Commons Lizenz zur Nutzung durch Dritte bereitstellen.
Kapitel 2

Angriffe auf die Privatsphäre

Im realen Leben ist Anonymität die tagtäglich erlebte Erfahrung. Wir gehen eine Straße enlang, kaufen eine Zeitung, ohne uns ausweisen zu müssen, beim Lesen der Zeitung schaut uns niemand zu. Das Aufgeben von Anonymität (z. B. mit Rabattkarten) ist eine aktive Entscheidung.

Im Internet ist es umgekehrt. Von jedem Nutzer werden Profile erstellt. Webseitenbetreiber sammeln Informationen (Surfverhalten, E-Mail-Adressen), um mit dem Verkauf der gesammelten Daten ihr Angebot zu finanzieren. Betreiber von Werbe-Servern nutzen die Möglichkeiten, das Surfverhalten webseitenübergreifend zu erfassen.


2.1 Big Data - Kunde ist der, der bezahlt


2.1.1 Google

Das Beispiel Google wurde aufgrund der Bekanntheit gewählt. Auch andere Firmen gehören zu den Big Data Companies und versuchen mit ähnlichen Geschäftsmodellen Gewinne zu erzielen. Im Gegensatz zu Facebook, Twitter... usw. verkauft Google die gesammelten Informationen über Nutzer nicht an Dritte sondern verwendet sie intern für Optimierung der Werbung. Nur an die NSA werden nach Informationen des Whistleblowers W. Binney zukünftig Daten weitergegeben.

**Wirtschaftliche Zahlen**


**Google Web Search**

Googles Websuche ist in Deutschland die Nummer Eins. 89% der Suchanfragen gehen direkt an google.de. Mit den ersten wie Ixquick, Metager2, Web.de... die indirekt Anfragen an Google weiterleiten, beantwortet der Primus ca. 95% der deutschen Suchanfragen (2008).


Die entwickelten Bewertungsverfahren werden zur Beobachtung der Trends im Web eingesetzt. Der Primus unter den Suchmaschinen ist damit in der Lage, erfolgversprechende Ideen und Angebote schneller als andere Mitbewerber zu erkennen und
2.1. BIG DATA - KUNDE IST DER, DER BEZAHLT

Darauf zu reagieren. Die Ideen werden nicht mehr selbst entwickelt, sondern aufgekauft und in das Imperium integriert. Seit 2004 wurden 60 Firmen übernommen, welche zuvor die Basis für die meisten aktuellen Angebote von Google entwickelt hatten: Youtube, Google Docs, Google Maps, Google Earth, Google Analytics, Picasa, SketchUp, die Blogger-Plattformen...

Das weitere Wachstum des Imperiums scheint langfristig gesichert.


Adsense, DoubleClick, Analytics & Co.


Inzwischen lehnen 84% der Internetnutzer dieses Behavioral Tracking ab. Von den Unternehmen im Internet wird es aber stetig ausgebaut. Google ist auf diesem Gebiet führend und wird dabei (unwissentlich?) von vielen Websitebetreibern unterstützt.


Die Grafik in Abb. 2.2 zur Besucherstatistik wurde vom Google Ad-Planner für eine (hier nicht genannte) Website erstellt. Man erkennt, dass der überwiegende Anteil der Besucher männlich und zwischen 35-44 Jahre alt ist. Die Informationen zu Bildung und Haushaltsseinkommen müssen im Vergleich zu allgemeinen Statistiken der Bevölkerung bewertet werden, was hier mal entfällt.


Google Attribution
Der Dienst Google Attribution wurde im Frühjahr 2017 gestartet. Mit diesem Dienst möchte Google Werbetreibenden Informationen liefern, wie sich personalisierte Online Werbekampagnen auf Einkäufe in der realen Welt auswirken.


- Die Ladenbesuchmessung basiert auf der genauen Lokalisierung von Android Smartphones und liefert Informationen, welche Geschäfte der Besitzer eines Smartphones besucht.
- Durch Partnerschaften hat Google in den USA Zugriff auf 70% der Kreditkartenzahlungen. Für Europa sind ähnliche Partnerschaften in Vorbereitung.
- Außerdem wird viel Voodoo Magic (KI) für die Auswertung genutzt.
2.1. BIG DATA - KUNDE IST DER, DER BEZAHLT

Google hat errechnet, dass Kunden bei dem Besuch eines Geschäftes in der realen Welt mit 25% höherer Wahrscheinlichkeit etwas kaufen und 10% mehr ausgeben, wenn sie zuvor Online Werbung zu dessen Angebot gesehen haben.

Google Mail, Talk, News... und Google+ (personalisierte Dienste)

Mit einem einheitlichem Google-Konto können verschiedene personalisierte Angebote genutzt werden. (Google Mail, News, Talk, Calendar, Alert, Youtube, Börsennachrichten...)


Patente aus dem Umfeld von Google Mail zeigen, dass dabei nicht nur Profile über die Inhaber der Accounts erstellt werden, sondern auch die Kommunikationspartner unter die Lupe genommen werden. Wer an einen Google Mail Account eine E-Mail sendet, landet in der Falle des Datenkrakens.

Die Einrichtung eines Google-Accounts ermöglicht es aber auch, gezielt die gesammelten Daten in gewissem Umfang zu beeinflussen. Man kann Einträge aus der Such- und Surf-Historie löschen u.ä. (Besser ist es sicher, die Einträge von vornherein zu vermeiden.)

Smartphones und Android


Bei der Nutzung von Android Smartphones sollen alle E-Mails über Google Mail laufen, Termine mit dem Google Calendar abgeglichen werden, die Kontaktdaten sollen bei Google landen... Die Standortdaten werden ständig an Google übertragen, um sogenannte Mehrwertdienste bereit zu stellen (genau wie das iPhone die Standortdaten an Apple sendet). Smartphones sind als Lifestyle-Gadget getarnte Tracking Devices.

Wir wissen, wo u bist. Wir wissen, wo du warst. Wir können mehr oder weniger wissen, was du gerade denkst. (Google-Chef Eric Schmidt, 2010)

Mozilla Firefox


- Sollte die Startseite modifiziert worden sein, erfolgt die “Personalisierung” des Browsers wenige Minuten später durch Aktualisierung der Phishing-Datenbank.
• Diese “Personalisierung” ermöglicht es Google, den Nutzer auf allen Webseiten zu erkennen, die mit Werbeanzeigen aus dem Imperium oder Google-Analytics verschmutzt sind. Im deutschsprachigen Web hat sich diese Verschmutzung auf 4/5 der relevanten Webseiten ausgebreitet.

(Trotzdem ist Mozilla Firefox ein guter Browser. Mit wenigen Anpassungen und Erweiterungen von unabhängigen Entwicklern kann man ihm die Macken austreiben und spurenarm durchs Web surfen.)

**Google DNS**

Mit dem DNS-Service versucht Google, die Digital Natives zu erreichen. Der Service spricht Nerds an, die in der Lage sind, Cookies zu blockieren, Werbung auszublenden und die natürlich einen DNS-Server konfigurieren können.

Google verspricht, dass die DNS-Server unter den IP-Adressen 8.8.8.8 und 8.8.4.4 nicht kompromittiert oder zensiert werden und bemüht sich erfolgreich um schnelle DNS-Antworten. Die Google-Server sind etwa 1/10 sec bis 1/100 sec schneller als andere unzensierte DNS-Server.


**Kooperation mit Geheimdiensten (NSA, CIA)**

Es wäre verwunderlich, wenn die gesammelten Datenbestände nicht das Interesse der Geheimdienste wecken würden. Das EPIC bemühte sich jahrelang auf Basis des Freedom of Information Act, Licht in diese Kooperation zu bringen. Die Anfragen wurden nicht beantwortet.¹


> *It will store all Google search queries, e-mail and fax traffic.*

Wenn Googles Verwaltungsratschef Eric Schmidt auf der SXSW-Konferenz 2014 behauptet, durch Einführung der SSL-Verschlüsselung zwischen Datenzentern seien die Daten der Google-Nutzer jetzt vor der NSA sicher³, dann kann man es als PR-Gag

² http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/google-yahoo-co-nsa-anwalt-internetfirmen-wussten-von-ausspaehaktionen-12855553.html
³ https://www.heise.de/-2138499
2.1. BIG DATA - KUNDE IST DER, DER BEZAHLT

Abbildung 2.3: NSA-Folie zu den PRISM-Partnern

abtun. Google ist aufgrund geltender Gesetze zur Kooperation mit den weitreichenden Späh-Programmen der NSA verpflichtet.

Außerdem kooperiert Google mit der CIA bei der Auswertung der Datenbestände im Rahmen des Projektes Future of Web Monitoring, um Trends zu erkennen und für die Geheimdienste der USA zu erschließen.

Kooperation mit Behörden

Auf Anfrage stellt Google den Behörden der Länder die angeforderten Daten zur Verfügung. Dabei agiert Google auf Grundlage der nationalen Gesetze. Bei daten-speicherung.de findet man Zahlen zur Kooperationswilligkeit des Imperiums. Durchschnittlich antwortet Google Anfragen mit folgender Häufigkeit:

- 3mal täglich von deutschen Stellen
- 20mal täglich von US-amerikanischen Stellen
- 6mal täglich von britischen Stellen

In den drei Jahren von 2009-2012 haben sich die Auskünfte von Google an staatliche Behörden und Geheimdienste verdoppelt, wie die Grafik Bild 2.4 der EFF.org zeigt.

Abbildung 2.4: Steigerung der Auskünfte von Google an Behörden
Die (virtuelle) Welt ist eine “Google” - oder?


Experten schätzen, dass ca. 1 Mio. PCs in den Rechenzentren für Google laufen (Stand 2007). Alle drei Monate kommen etwa 100.000 weitere PCs hinzu. Es werden billige Standard-Komponenten verwendet, die zu Clustern zusammengefasst und global mit dem Google File System (GFS) vernetzt werden. Das GFS gewährleistet dreifache Redundanz bei der Datenspeicherung.

Die Kosten für diese Infrastruktur belaufen sich auf mehr als zwei Milliarden Dollar jährlich. (2007)

Die Videos von Youtube sollen für 10% des gesamten Traffics im Internet verantwortlich sein. Über den Anteil aller Dienste des Imperiums am Internet-Traffic kann man nur spekulieren.

Google dominiert unser (virtuelles) Leben.

Dabei geht es nicht um ein paar Cookies sondern um eine riesige Maschinerie.

2.1.2 Weitere Datensammler

Die Datensammler (Facebook, Amazon, Twitter, Onlineshops...) verkaufen Informationen über Nutzer an Datenhändler (z. B. Acxiom, KaiBlue, RapLeaf...), welche die Daten anreichern, zusammenfassen und umfassende Profile den eigentlichen Endnutzern wie Kreditkartenfirmen, Personalabteilungen großer Unternehmen und Marketingabteilungen von Microsoft bis Blockbuster verkaufen.


*Sie können sich Acxiom wie eine automatisierte Fabrik vorstellen, wobei das Produkt, das wir herstellen, Daten sind.* (Aussage eines Technikers von Acxiom)
**Oracle** ist eine ehemalige IT-Firma. Früher wurde Software entwickelt und neuerdings wird das Sammeln und Verknüpfen von Daten als profitabler Geschäftszweig entdeckt. Oracle wirbt mit folgenden Datenbeständen:

3 Milliarden Verbraucherprofile aus 700 Millionen täglichen Social-Media-Nachrichten, Daten über die Nutzung von 15 Millionen Webseiten und Einkäufe bei 1 500 Händlern.

Das Tracking des Surfverhaltens wird mit der Auswertung des tagtäglichen Social-Media-Gedöhnis und den Einkäufen in Online-Shops kombiniert.

**BlueKai** ist seit 2014 eine Tochterfirma von Oracle. Ein Datenleck im Juni 2020 zeigte, wie gigantisch und detailiert die Datenbestände von Bluekai sind. Die personenbezogenen Datensätze enthalten folgende Angaben:

- realen Namen, genutzte E-Mail Adressen, Telefonnummern und Kreditkarten
- Historie von online und offline Einkäufen
- Historie des Surfverhaltens im Internet


Gemäß Eigenwerbung kann BlueKai 1,2% des Internettraffics beobachten, inklusive der Besucher bekannter Porno-Webseiten. Daten von offline Einkäufen werden von Firmen gekauft, die als Payment Processoren Kreditkarten Transaktionen abwickeln.

**Match Group** monopolisiert den Online-Datingmarkt. Zur Match Group gehören die Dating Portale Tinder, OkCupid, Plenty of Fish, Meetic, LoveScout24, OurTimes, Pairs, Meetic, Match, Twoo, Neu.de und weitere Partnerportale. In den Datenschutzpolicies der Portale kann man nachlesen, dass die sensiblen Persönlichkeitsdaten der Nutzen innerhalb der Match Group zwischen Portalen ausgetauscht werden.

Ein Beispiel: laut Tinder Datenschutz Policy\(^4\) werden folgende Daten gesammelt:

- Informationen, die Nutzer selbst angibt über Name, Ort, Alter, Geschlecht, sexuelle Vorlieben, Fotos, Videos…
- Informationen über die Nutzung des Dienstes wie Login/Logout Zeitpunkt, Suchanfragen, Klicks auf interne Seiten und auf Werbung, Kontakte und die Interaktionen mit den Kontakten, versendete und empfangene Nachrichten…
- Informationen über verwendete Geräte (Hardware, Software, IP-Adressen, individuelle Geräte IDs wie IMEI/UDID oder MAC-Adressen, gerätespezifische Werbe-IDs wie AAID von Google oder IDFA von Apple, Informationen zur Mobilfunkverbindung wie Dienstanbieter und Signalstärke sowie Information der Gerätesensoren wie Beschleunigungssensor, Kompass oder Gyroskope)
- Daten zu Geolocation werden via GPS, Bluetooth, oder WiFi-Verbindungen ermittelt, die Ermittlung der Geolocation kann auch im Hintergrund erfolgen, wenn man die Dienste von Tinder nicht nutzt.
- Falls man *Do Not Track* (DNT) im Browser aktiviert hat, wird es ignoriert.

Wir teilen Ihre Daten mit anderen Unternehmen der Match Group. […] Die Unterstützung kann technische Verarbeitungsvorgänge wie Datenhosting und -wartung, Kundenbetreuung, Marketing und gezielte Werbung […] umfassen.

Wir dürfen Ihre Daten auch an Partner weitergeben, die uns bei der Verbreitung und Vermarktung unserer Dienste unterstützen.

\(^4\)https://www.gotinder.com/privacy
Das ist ein Freibrief, um sehr private Details an beliebige Dritte zu verkaufen.

**Big Data Scoring** aus Estland bewertet die Kreditwürdigkeit von Personen im Auftrag von Banken und anderen Kreditgebern sowie für Kunden aus der Immobilienbranche anhand der Facebook Profile und der Aktivitäten bei anderen Social Media Sites. Das Ergebnis der Bewertung ist eine Zahl von 0...10.

**Towerdata** sammelt die Informationen anhand von E-Mail Adressen. Jeder kann auf der Website eine Liste von E-Mail Adressen hochladen, bezahlen und nach Zahlungseingang die Daten abrufen. Ein kleiner Auszug aus der Preisliste soll den Wert persönlicher Informationen zeigen:

- Alter, Geschlecht und Ort: 1 Cent pro E-Mail-Adresse
- Haushaltseinkommen: 1 Cent pro E-Mail-Adresse
- Ehestand: 1 Cent pro E-Mail-Adresse
- vorhandene Kinder: 1 Cent pro E-Mail-Adresse
- Wert des bewohnten Hauses: 1 Cent pro E-Mail-Adresse
- Relation von Krediten zum Vermögen: 1 Cent pro E-Mail-Adresse
- vorhandene Kreditkarten: 1 Cent pro E-Mail-Adresse
- Fahrzeuge im Haushalt: 1 Cent pro E-Mail-Adresse
- Smartphone Nutzung: 1 Cent pro E-Mail-Adresse
- Beruf und Ausbildung: 2 Cent pro E-Mail-Adresse
- Tätigkeit als Blogger: 1 Cent pro E-Mail-Adresse
- wohltätige Spenden: 1 Cent pro E-Mail-Adresse
- Präferenzen für hochwertige Marken: 1 Cent pro E-Mail-Adresse
- Präferenzen für Bücher, Zeitschriften: 1 Cent pro E-Mail-Adresse
- …

**Present-Service Ullrich GmbH** hat sich auf die Erkennung von Schwangerschaften und Geburten spezialisiert. Von den jährlich 650.000 Geburten in Deutschland kann die Present-Service Ullrich GmbH nach eigenen Angaben 50% erkennen und ist der Marktführer in Deutschland (Stand: 2014). Die Daten werden zusammen mit Informationen über die finanzielle Situation der Eltern für das Direktmarketing genutzt und verkauft.

Für das Direktmarketing nutzt die Firma 10.000 aktive Partner im Gesundheitswesen (Frauenärzte, Hebammen, Krankenschwestern) und verspricht den Kunden:


### 2.2 Techniken der Datensammler


---

5[https://www.towerdata.com/email-intelligence/pricing](https://www.towerdata.com/email-intelligence/pricing)

Techniken zum Tracking des Surfverhaltens

Das Surfverhalten liefert die meisten Informationen über unsere Vorlieben. Dabei werden folgende Techniken eingesetzt:

**Cookies** sind noch immer das am häufigsten eingesetzte Mittel, um Browser zu markieren und das Surfverhalten zu verfolgen.

Blockieren der Cookies von Drittseiten schützt nur teilweise vor dem Tracking mit Cookies. Die Datensammler haben Methoden entwickelt, um Tracking Cookies als First-Party Content zu platzieren\footnote{https://www.heise.de/-1626368}. Empirische Studien zeigen, dass es 160 Trackingdienste gibt, die mehr als 40% des Surfverhaltens verfolgen können, wenn das Setzen von Cookies für Drittseiten möglich ist. Wenn man Cookies von Drittseiten verbietet, dann können immer noch 44 Trackingdienste mehr als 40% des Surfverhaltens verfolgen. Dazu zählen:

- Google Analytics, Chartbeat.com oder AudienceScience.com schreiben die Tracking Cookies mit Javascript als First-Party Content.
- WebTrekk nutzt DNS-Aliases, um eigene Server als Subdomain der aufgerufenen Webseite zu deklarieren und sich First-Party Status zu erschließen.
- Yahoo! Web Analytics protzt damit, dass sie ebenfalls ihre Tracking Cookies als First-Party Content einsetzen können.

Mit diesen First-Party Cookies wird das Surfverhalten innerhalb einer Website beobachtet. Zusätzlich werden weitere Methoden eingesetzt, die eine Verknüpfung der gesammelten Daten über mehrere Webseiten hinweg ermöglichen. WebTrekk nutzt dafür Browser Fingerprinting.


Für das Fingerprinting des Browsers werden verschiedene Techniken eingesetzt:

1. HTTP-Header: Es werden die Informationen ausgewertet, die der Browser bei jedem Aufruf sendet (Sprache, Browsername und -version, Betriebssystem und -version, unterstützte Zeichensätze, Dateitypen, Kodierungen).

Mittels Canvas Font Fingerprinting können die installierten Schriftarten ermittelt werden. Das Verfahren wurde 2016 in dem OpenWPM Paper beschrieben.

• *Bluecava* nutzt ausschließlich Browser Fingerprinting und protzt mit 30% besseren Ergebnissen als Cookie-basierte Techniken.\(^{18}\)

• *Zanox.com* nutzt den Fingerprint des Browsers, wenn Cookies gelöscht oder per Browser-Einstellung blockiert werden.\(^{19}\)

• *WebTrekk* berechnet einen Fingerprint auf Grundlage von Geolocation anhand der IP-Adresse, Bildschirmgröße und Farbtiefe des Monitors, innere Größe des Browserfensters, bevorzugte Sprache, User-Agent des Browsers, Version des Betriebssystems sowie Einstellungen für Java, JavaScript und Cookies.\(^{20}\)

• **Multicounter** nutzt den Fingerprint zusätzlich zu Cookies oder EverCookies zur Verbesserung der Erkennungsraten.\(^{21}\)

• *Anonymizer Inc.* verwendet Browser Fingerprinting auf sämtlichen Webseiten, verschweigt es aber im Privacy Statement. (Eine seltsame Auffassung für jemanden, der Anonymität verkaufen will.)

• *Yahoo! Web Analytics* nutzt Fingerprinting, wenn Cookies blockiert werden.


• *AudioContext Fingerprinting* wurde bei drei Trackingdiensten nachgewiesen, die jedoch nur einen sehr geringe Reichweite haben und nur auf wenigen Webseiten eingebunden sind.

Da Browser Fingerprinting keine Markierungen einsetzt, die man löschen könnte, ist eine Verteidigung besonders schwer realisierbar. Wichtigste Verteidigungsmassnahmen sind das Blockieren von JavaScript (vor allem für Drittseiten), blockieren von Flash und die Nutzung von AdBlock, um Tracking-Scripte zu blockieren.

**Keystroke Biometrics** verwendet das Schreibverhalten der Nutzer auf der Tastatur als Identifizierungsmerkmal. Der HTML5 Standard definiert eine API, um auf Tastaturereignisse reagieren zu können. In Firefox 38.0 wurden erste Teile der API standardmäßig aktiviert. In Kombination mit hochgenauen Timern können Webapplikationen das Schreibverhalten der Surfer in Webformularen analysieren und als biometrischen Login verwenden (z.B. von der Firma KeyTrac angeboten) oder als Trackingfeature.

Mit Windows 10 hat Microsoft begonnen, das Schreibverhalten der Anwender im Hintergrund durch das Betriebssystem analysieren zu lassen und die erstellten biometrischen Profile an die Firma BehavioSec zu senden, die mit der DARPA und Microsoft kooperiert. Laut Eigenwerbung kann BehavioSec 99% der Nutzer korrekt erkennen. Die dabei entstehenden umfangreiche Sammlung der biometrischen Profile kann zukünftig zum Tracking und zur Deanonymisierung genutzt werden.

**Wischen, Tippen, Zoomen** sind die üblichen Gesten für die Bedienung der Touchscreens auf Smartphones. Ein australisches Forschungsteam präsentiert auf der PETS 2018 das Paper *Quantifying the Uniqueness of Touch Gestures for Tracking*,\(^{22}\) in dem gezeigt wird, dass diese Touchgesten individuell unterschiedlich sind und für die Wiedererkennung von Smartphone Nutzern geeignet sind.

\(^{18}\)http://www.bluecava.com/visitor-insight-campaign-measurement
\(^{19}\)http://blog.zanox.com/de/zanox/2013/09/11/zanox-stellt-tpv-fingerprint-tracking-vor/
\(^{20}\)http://www.webtrekk.com/de/index/datenschutzerklaerung.html
\(^{21}\)http://www.multicounter.de/features.html
Die Touch-Daten können über APIs von allen Smartphone Apps ausgelesen werden.

**Tracking von E-Mail Newslettern**


- Wie beim Tracking des Surfverhaltens werden kleine 1x1 Pixel große Bildchen in die E-Mail eingebettet, die beim Lesen im HTML-Format von einem externen Server geladen werden. Durch eine individuelle, nutzerspezifische URL kann die Wanze eindeutig einer E-Mail Adresse zugeordnet werden. Ein Beispiel aus dem E-Mail Newsletter von Paysafecard, das einen externen Trackingservice nutzt:

  `<IMG src="http://links.mkt3907.com/open/log/43.../1/0">`

Easyjet.com (ein Billigflieger) kann offenbar die Aufrufe seiner Newsletter selbst zählen und auswerten. In den E-Mails mit Informationen zu gebuchten Flügen findet man folgende kleine Wanze am Ende der Mail:

  `<IMG src="http://mail.easyjet.com/log/bEAS001/mH9..." height=0 width=0 border=0>`


- Die Links in den E-Mails führen oft nicht direkt zum Ziel. Sie werden über einen Trackingservice geleitet, der jeden Klick individuell für jede Empfängeradresse protokolliert und danach zur richtigen Seite weiterleitet. Als Beispiel soll ein Link aus dem Paysafecard Newsletter dienen, der zu einem Gewinnspiel auf der Paysafecard Webseite führen soll:


Als Schutzmaßnahme gegen dieses Tracking sollte man Mails als Text lesen.

**Tracking von Dokumenten (PDF, Word usw.)**

Die Firma ReadNotify bietet beispielsweise einen Service, der Word-Dokumente und PDF-Dateien mit speziellen unsichtbaren Elementen versieht. Diese werden beim Öffnen des Dokumentes vom Server der Firma nachgeladen und erlauben somit eine Kontrolle, wer wann welches Dokument öffnet. Via Geo-Location ermittelt ReadNotify auch den ungefähren Standort des Lesers. Aus der Werbung von ReadNotify:

  _We not only let you know when your document or PDF was opened, but we will also endeavor to let you know:_

[23]https://emailprivacytester.com/
2.3 Tendenzen auf dem Gebiet des Tracking

Obwohl 80% der Internetnutzer das Tracking des Surfverhaltens ablehnen, wird es stetig weiter ausgebaut. Dabei wird es sowohl technisch durch die großen Datensammler immer weiter ausgebaut und durch politische Entscheidungen werden Datensammlungen erleichtert.

1. Mehr Trackingelemente werden auf den Webseiten eingesetzt. Das Projekt Web Privacy Census der University of California verfolgt seit mehreren Jahren die Entwicklung und dokumentiert einen stetigen Anstieg von Trackingelementen bei den meistbesuchten Webseiten (Top-100, Top-1000 und Top-25.000). Als Beispiel soll die Anzahl der Cookies dienen, die beim Besuch der 100 populärsten Webseiten gesetzt werden (ohne Login, nur beim Betrachten der Webseiten):

<table>
<thead>
<tr>
<th>Jahr</th>
<th>Anzahl der Cookies</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009</td>
<td>3.602</td>
</tr>
<tr>
<td>2011</td>
<td>5.675</td>
</tr>
<tr>
<td>2012</td>
<td>6.485</td>
</tr>
<tr>
<td>2015</td>
<td>12.857</td>
</tr>
</tbody>
</table>

2. Das Projekt registriert eine überproportionale Zunahme schwer blockierbarer Trackingfeatures (EverCookies). Immer mehr Webseiten verwenden HTML5 DOM-Storage, IE_userdata oder ETags aus dem Cache für die Verfolgung des Surfverhaltens. Für die meistbesuchten Webseiten wurden folgende Zahlen zur Nutzung von EverCookies ermittelt:

<table>
<thead>
<tr>
<th>Jahr</th>
<th>Nutzung von EverCookies</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>19% der Webseiten</td>
</tr>
<tr>
<td>2012</td>
<td>34% der Webseiten</td>
</tr>
<tr>
<td>2015</td>
<td>76% der Webseiten</td>
</tr>
</tbody>
</table>

3. Durch den Aufkauf kleinerer Anbieter durch die Großen der Branche erfolgt eine Marktbereinigung. Es bilden sich sogenannte Tracking-Familien, die die Daten untereinander austauschen und somit eine große Reichweite bei der Beobachtung des Surfverhaltens haben. Die größten Tracking-Familien sind:

KAPITEL 2. ANGRiffe Auf die Privatsphäre

Trackingelemente der Google-Familie

<table>
<thead>
<tr>
<th>Jahr</th>
<th>auf % der Webseiten</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>auf 7% der Webseiten</td>
</tr>
<tr>
<td>2006</td>
<td>auf 16% der Webseiten</td>
</tr>
<tr>
<td>2008</td>
<td>auf 55% der Webseiten</td>
</tr>
<tr>
<td>2012</td>
<td>auf 74% der Webseiten</td>
</tr>
<tr>
<td>2015</td>
<td>auf 92% der Webseiten</td>
</tr>
</tbody>
</table>

(b) Auf den Plätzen 2 und 3 folgen Facebook und Twitter, die vor allem mit Like-Buttons und ähnlichem Social Media Kram tracken und 2016 eine Abdeckung von mehr 10% der 1-Million-Top-Sites erreichten. Die Kooperation von Facebook mit den eigenständigen Trackingdiensten BlueKai und Epsilon ist dabei noch nicht enthalten.

(c) Auf den folgenden Plätzen liegen etwas abgeschlagen die Tracking-Familien von Microsoft (u.a. mit den Trackingdiensten atdmt.com, adbureau.com, aquantive.com), die Yahoo! Familie (mit den Trackingdiensten adrevolver, yieldmanager, overture), die AOL-Familie (mit adsonar.com, tacoda.net, advertising.com) und die Oracle Data Cloud (mit BlueKai, Datalogix, AddThis) mit einem Marktanteil von jeweils 3-8%.


- Im Februar 2013 hat Facebook eine Kooperation mit den Datenhändlern Axiom und Datalogix bekannt gegeben. Diese Firmen werten umfangreiche Daten aus der realen Welt aus (Kreditkartenzahlungen, Rabattkarten usw.). Damit sollen die Werbeeinblendungen bei Facebook individueller und zielgerichteter auf die Interessen der Mitglieder zugeschnitten werden.


  Dank Nestis eingebauter Sensoren weiß Google jetzt, wann Sie zuhause sind, in welchem Raum Sie sich aufhalten und dank der Feuchtigkeitssensoren im Schlafzimmer auch, wie oft, wie lange und wie leidenschaftlich Sie Sex haben. (M. Morgenroth)

- Außerdem interessiert sich Google für die Offline Einkäufe mit Kreditkarten. Über Partnerschaften kennt Google 70% der Zahlungen mit Kreditkarten in den USA (Stand: Mai 2017). Ähnliche Partnerschaften in Europa sind in Vorbereitung.²⁵


ist.

Die EFF.org kommentierte:

\textit{In yesterday’s Senate hearing, we heard the advertising industry admit that their near-ubiquitous online tracking program is being used for issues that are the purview of law enforcement.}

Durch die Snowden-Dokumente wurden konkrete Beispiele bekannt.\footnote{https://www.eff.org/deeplinks/2013/12/nsa-turns-cookies-and-more-surveillance-beacons}

- Außerdem nutzt die NSA die Standortinformationen, die von Smartphone Apps an Datensammler (Service Provider, Entwickler) gesendet werden, um Personen zu lokalisieren (HAPPYFOOT).


Auf dem IT-Gipfel 2016 in Saarbrücken hat Bundeskanzlerin Merkel diese Linie der Bundesregierung noch mal betont und sich vom Grundprinzip der Datensparsamkeit als Leitlinie verabschiedet. Sie sagte wörtlich:

\textit{Denn das Prinzip der Datensparsamkeit, wie wir es vor vielen Jahren hatten, kann heute nicht die generelle Leitschnur sein für die Entwicklung neuer Produkte.}

Wir werden also zukünftig mehr auf Selbstschutz angewiesen sein. Dieser Selbstschutz könnte zukünftig aber schwieriger werden. In der Auseinandersetzung zwischen Werbewirtschaft und AdBlockern stellen sich Bundestag und Bundesrat auf die Seite der Werbewirtschaft. In dem \textit{Abschlussbericht der Bund-Länder-Kommission zur Medienkonvergenz} vom Juni 2016 befasst sich ein eigenes Kapitel damit, wie sich Medien gegen den zunehmenden Einsatz von Werbeblockern schützen können. Ein gesetzliches Verbot von Werbeblockern wird diskutiert:

\ldots eine zeitnahe Prüfung durch Bund und Länder klären, ob im Hinblick auf die wirtschaftlichen Auswirkungen und damit verbundenen medienpolitischen Risiken gegebenenfalls eine gesetzliche Flankierung geboten ist.


Google und Facebook haben daraufhin erklärt, dass sie auch ohne Safe Habour Abkommen so weitermachen wie bisher und die Daten europäischer Nutzer in die USA transferieren und dort verarbeiten werden. Sie sehen die EU-Standardvertragsklauseln nach Artikel 26, Absatz 2 der EU-Datenschutzrichtlinie von 1995 (EC95/46) als ausreichende Grundlage an. In dieser Ansicht werden sie von der EU-Kommision unterstützt.


Dass das neue Privacy Shield Abkommen (der Nachfolger von Safe Harbour) eine Kapitulation der EU beim Thema Datenschutz gleichkommt, konnte man erwarten und ist keine Überraschung.

8. Die zukünftige Entwicklung könnte durch folgende Eckpunkte gekennzeichnet sein:

- Weitere Ausweitung des Marktes auf die zwischenmenschliche Kommunikation
- Vereinzelung der Individuen durch Pseudogemeinschaften in der virtuellen Welt
- Kontrolle aller digitalen Aktivitäten durch die smarte Diktatur

2.4 Crypto War 3.0


Ein generelles Verbot starker Kryptografie wird nicht ernsthaft diskutiert. Es wäre nicht durchsetzbar und eine kommerzielle Nutzung des Internets wäre praktisch tot.

28 https://www.heise.de/tp/artikel/46/46186/1.html
2.4. CRYPTO WAR 3.0

Damit sind nicht Googles Werbeeinnahmen gemeint sondern industrielle Anwendungen, mit den denen richtig viel Geld umgesetzt wird (z. B. im Bereich Banken, Börsen usw.).

Ein Schwerpunkt der aktuellen Angriffe auf Verschlüsselung richtet sich gegen Krypto Messenger Apps. Dabei sind zwei Angriffs-Muster erkennbar:

Forderung nach Backdoors in der Verschlüsselung: Diese Strategie ist nicht neu und wurde schon mehrfach gegen Kommunikationsdienste erfolgreich eingesetzt, sobald diese Dienste eine nennenswerte Popularität erreichten.

- Blackberry wurde in Kanada, in Indien und in anderen Ländern gezwungen, den Behörden die Schlüssel für die Entschlüsselung zur Verfügung zu stellen.

Mit Gesetzen wird versucht, diese Praxis auf alle Krypto Messenger auszudehnen:

- In Deutschland hat Bundesinnenminister Seehofer im Mai 2019 ähnliche Vorstellungen geäußert. Nach seinen Vorstellungen sollten alle Messaging Dienste gezwungen werden, die gewünschten Kommunikationsdaten selbst zu entschlüsseln und in entschlüsselter Form den Strafverfolgungsbehörden zur Verfügung zu stellen. Die vehemente Kritik des Bundesverbandes für IT-Sicherheit, eco-Verband der Internetwirtschaft, CCC, Digitale Gesellschaft... u.a.m. verhinderte die Umsetzung dieser Pläne.


Seit Mitte 2018 ist daher ein Umdenken bei den Befürwortern der Überwachung erkennbar. Es wird keine Entschlüsselung der Kommunikation gefordert, aber die Betreiber von Messaging Diensten sollen Behörden dabei unterstützen, sich als Œtile

Teilnehmerin eine verschlüsselte Kommunikation einzuklinken und so Chats bzw. Gruppenchats live und unbemerkt belauschen zu können:

It’s relatively easy for a service provider to silently add a law enforcement participant to a group chat or call...

We’re not talking about weakening encryption or defeating the end-to-end nature of the service. In a solution like this, we’re normally talking about suppressing a notification on a target’s device, and only on the device of the target and possibly those they communicate with. That’s a very different proposition to discuss and you don’t even have to touch the encryption.

Salopp gesagt: Die Dienste möchten also den Multi-Device-Support moderner Krypto-Protokolle exploitieren und dabei nicht erwischt werden. Sie möchten die Möglichkeit haben, ein neues Gerät im Namen eines Benutzers zu registrieren ohne das Benutzer eine Warnmeldung bekommt, und mit diesem Gerät alles mithören. (Vereinzelt waren Polizeibehörden mit der Methode bereits erfolgreich, weil Kriminelle mögliche Schutzfunktionen dagegen nicht aktivierten oder Warnungen ignorierten.)

Die Befürworter dieses Ansatzes argumentieren, dass diese Überwachung nicht anders wäre, als der Einsatz von Krokodilklemmen bei der alten Telefonie und das damit die Sicherheit der Verschlüsselung nicht generell geschwächt werden muss.


**Aufhebung der Haftungsprivilegierung:** Mit dem Earn IT Act wurde im März 2020 von einigen Senatoren in den USA der Vorschlag eingebracht, dass sich Krypto Messenger nicht mehr auf die Haftungsprivilegierung für den Transport verschlüsselten Inhalte berufen können, wenn sie keine Möglichkeit haben, die verschlüsselten Inhalte im Auftrag der Behörden zu scannen.


Im August 2020 hat der für digitale Dienste zuständige EU-Binnenmarktkommissar T. Breton hat bestätigt, dass auch die EU Maßnahmen ergreifen will, um Anbieter von Messengerdiensten in der Pflicht zu nehmen. Diese Dienste müssten sich das Privileg der Haftungsfreistellung für transportierte Inhalte erst verdienen, indem sie ihrerseits das technisch Mögliche tun, um illegale Inhalte zu erkennen und zu blockieren.

Im Vorfeld hatte Kommissarin Ylva Johansson (Inneres) angekündigt, dass Anbieter von Krypto-Messaging ihren Plattformen routinemäßig nach pädokriminellen Inhalten durchsuchen müssten. Als Begründung nannte sie den explosionsartigen Anstieg der gemeldeten pädokriminellen Videos von 300.00 zwischen 2015 und 2017 auf über 3,5 Millionen aktuell in den USA. (Für Europa nannte sie keine Zahlen.)


---

32 [https://heise.de/-4595181](https://heise.de/-4595181)
den von Facebook oder Microsoft erkannten Videos handelt sich in der Regel nur um Lockangebote. Die echt harte Ware wird nicht auf Social Media Plattformen angeboten sondern auf Marktplätzen im Darknet.

Der Verlust der Haftungsprivilegierung würde für die Betrieb von Messengern mit Ende-zu-Ende Verschlüsselung ohne eine Backdoor, mit der Betreiber verschlüsselte Inhalte scannen könnten, in der EU ein erhebliches Risiko bedeuten. Sollte bei Ermittlungen nachgewiesen werden, dass der Messengerdienst für die Verteilung illegaler Inhalte genutzt wurde, könnte der Betreiber als Störer in Haftung genommen werden.

Das betrifft nicht nur kommerzielle, zentralisierte Dienste. Der Betrieb eines [matrix] Homeservers mit offener Registrierung für unbekannte Dritte könnte damit zum ähnlichen unakulierbarem Risiko werden, wie der Betrieb eines Tor Exit Nodes.

**Staatsliches Hacking und Einsatz von Trojanern:** Da Hintertüren in der Verschlüsselung von Kommunikation zur Zeit in der EU und den USA nicht populär sind, versucht man es mehr mit staatlichen Hackerangriffen, die gesetzlich legitimiert und personell besser ausgestattet werden sollen.

- In Deutschland nimmt die im Nov. 2015 angekündigte Bundes-Hacker-Behörde zur Unterstützung von Geheimdiensten und Strafverfolgung beim Brechen von Verschlüsselung langsam Gestalt an. Die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (Zitis) soll seit 2017 mit 60 Mitarbeitern einsatzbereit sein und dann schrittweise auf 400 Mitarbeiter ausgebaut werden.\(^{33}\)


- In den USA soll Rule 41 of the US Federal Rules of Criminal Procedure ab Dez. 2016 das staatliche Hacken von Tor- und VPN-Nutzern für das FBI massiv erleichtern, unabhängig davon, in welchem Land die Tor-Nutzer sich befinden.\(^{34}\)

  Dass das FBI den TorBrowser knacken und installieren kann, haben sie 2013 und 2015 bewiesen. Der 2015 verwendete Exploit scheint auch 2016 noch zu funktionieren. TorProject.org und die Mozilla Foundation haben sich um eine Veröffentlichung des Exploit bemüht, aber das Wissen um diese Schwachstelle wurde unter Hinweis auf die Nationale Sicherheit als geheim klassifiziert.

  Die Kompetenzen der NSA im Rahmen des Programms BULLRUN wurden durch die Dokumente von Snowden/Greenwald bekannt. Egotisticalgi-raffe heißt das Programm, welches Methoden zum offensiven Angriff auf Tor entwickelt.

- In Schweden darf die Polizei ab März 2020 Bundestrojaner einsetzen. In der Be- gründung für das Gesetz wird darauf verwiesen, das 90% der Kommunikation, für die die Polizei eine Lizenz zur Überwachung hat, verschlüsselt über Messenger wie Signal App erfolgt.

### 2.5 Fake News Debatte

Manche nennen es Fake News, andere sprechen von alternativen Fakten, umgangssprachlich nennt man es Lügen und in den wundersamen Geschichten des Baron von Münchhausen

\(^{33}\)https://netzpolitik.org/2016/bundesregierung-will-entschluesselungsbehoerde-schaffen

\(^{34}\)https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government
erlangte das Phänomen literarischen Weltruhm.


2.5.1 Der Kampf gegen Fake News

Alternative Medien und Diskussionen in abgeschotteten Facebook Gruppen sollen eine Gefahr für die Demokratie sein, die die Informationshoheit der etablierten Mainstream Medien in Frage stellen und mit Falschmeldungen untergraben. Um uns vor Fake News zu schützen wurden hektisch Maßnahmen diskutiert:

1. Es wurden Faktenchecker eingerichtet wie Correctiv oder die ARD/ZDF Faktenchecker, die das Vertrauen genießen und Fake News entlarven sollten. Da diese Faktenchecker aber selbst eine politische Agenda verfolgen, hat sich schnell gezeigt, dass sie für eine neutrale Bewertung von News und Wahrheitsfindung ungeeignet sind.


3. Um die Deutungshoheit westlicher Mainstream Medien zu sichern und die Reichweite von Alternativen einzuschränken, überarbeitet Google seinen Suchalgorithmus:


- Im Nov. 2017 hat Google CEO Erich Schmidt bekannt gegeben, dass die russische Nachrichtenseite RT.com und das Portal Sputnik News im Google News Service benachteiligt werden sollen, um die Reichweite zu reduzieren. We are working on detecting and de-ranking those kinds of sites - it's basically RT and Sputnik. [...] But we don’t want to ban the sites - that’s not how we operate.

(Die Verschwörungstheorien von heute sind oft die Wahrheiten von morgen. In allen unten genannten Beispielen würde die neue Bewertung von Google die Fake News gegenüber der Wahrheit mehr und mehr bevorzugen.)

37 https://www.wsws.org/de/articles/2017/08/05/goog-a05.html
2.5.2 Fake News Beispiele

Mir fallen spontan folgende Fake News aus den letzten 20 Jahren ein, die teilweise schwerwiegendere Folgen hatten als ein Wahlergebnis in Deutschland:

- **FAKE:** Im Januar 1999 haben serbische Soldaten beim Massaker von Racak Zivilisten aus dem Kosovo massakriert.
  WAHR: Nach dem Vormarsch der UCK im Kosovo ging die serbische Armee zum Gegenangriff über und es kam bei der Ortschaft Racak zu Gefechten zwischen der UCK Brigade 161 und der serbischen Armee.
  Das Massaker von Racak war die Begründung für die NATO, um an der Seite der UCK in den Bürgerkrieg einzugreifen und Belgrad zu bombardieren. Auch Deutschland hat sich an diesem völkerrechtswidrigen Angriff beteiligt.

- **FAKE:** Irakische Soldaten haben beim Überfall auf Kuweit frühgeborene Säuglinge aus den Brutkästen gerissen und auf dem Boden des Krankenhauses liegen gelassen, wo die Säuglinge starben. (Brutkastenlüge, vom damaligen US-Präsidenten George H. W. Bush und von Menschenrechtsorganisationen vielfach zitiert.)
  WAHR: Die Brutkastenlüge wurde völlig faktenfrei von der PR-Agentur Hill & Knowlton im Auftrag der kuwaitischen Exil-Regierung erfunden. Die Krankenschwester, die als Zeugin aussagte, war die Tochter des des kuwaitischen Botschafters in den USA.

- **FAKE:** Der Irak hat Massenvernichtungswaffen! Insbesondere verfügt Dikator Saddam Hussein über mobile Biowaffen Labore, die auf Tiefladern montiert sind und hochbeweglich. (US-Verteidigungsminister Rumsfeld und US-Außenminister C. Powell)

- **FAKE:** Whistleblower Edward Snowden könnte ein russischer Spion sein. (G. Maaßen, Chef des BfV) oder Snowden ist ein Russen-Agent. (J. R. Schindler)

- **FAKE:** Es wird ein No-Spy-Abkommen mit den USA geben. (Bundeskanzlerin A. Merkel, Innenminister H.-P. Friedrich, Kanzleramtsminister R. Pofalla, S. Seibert)

- **FAKE:** Die AfD ist eine rechts-populistische Partei der Geringverdiener und ein Sammelbecken für die sozial Abgehängten der Gesellschaft.
  WAHR: Die Mitglieder der AfD gehören überwiegend zur Mittelschicht. Der Anteil der Geringverdiener (unter 2.000 Euro Netto) unter den AfD-Anhängern entspricht mit 27% der Anhängerschaft der CDU (28% Geringverdiener) und ist geringer als bei SPD (32%) und Linke (37%).


WAHR: Es gab keinen Angriff auf die Telekom, der Ausfall der Router war nur ein Kolateralschaden. Die kriminellen Betreiber des Mirai Botnetzes wollten Zyxel-Router angreifen, die der irische Provider Eir an seine Kunden verteilt und die einen Security Bug im TR-069 Interface haben. Die Telekom Router hatten sich bei den automatisierten Tests des Mirai Botnetzes auf Verwundbarkeit selbst abgeschaltet.41

Der für den schrecklichen Angriff auf die Telekom Router verantwortliche Hacker wurde vom LG Köln zu eine Bewährungsstrafe(!) von 20 Monaten verurteilt.42

FAKE: Russische Hacker wollen die Wahlen in Deutschland manipulieren und haben auch aktive in die Wahlen in Frankreich und den USA eingegriffen. (Dieses Mantra wird ständig wiederholt, nicht nur in den Medien sondern auch im Verfassungsschutzbericht oder im Wikipedia Artikel über die Wahl in Frankreich.)

WAHR (nach Ländern sortiert):

– Eine kurze, klare Begründung, warum russische Hacker wahrscheinlich nicht in den deutschen Wahlkampf eingreifen werden, hat der Postillon in seiner typisch treffenden Art begründet.43

Der russische Hacker Anatoli Fadejew ist verzweifelt: Schon bald ist Bundestagswahl und der 27-jährige aus Sankt Petersburg hat sich immer noch nicht entschieden, ob er Angela Merkel (CDU) oder Martin Schulz (SPD) attackieren soll, um den jeweils anderen zu begünstigen. Offenbar findet der von Putin beauftragte Hacker beide diesjährigen Kanzlerkandidaten nicht überzeugend.

– Bezüglich der Präsidentschaftswahlen in Frankreich teilte der Chef der französischen Nationalen Agentur für Sicherheit der Informationssysteme (ANSSI), Guillaume Poupard, laut der Agentur AP mit, das es keine Spur von russischen Hackerangriffen bei den Wahlen gab.44


Forensic studies of Russian hacking into Democratic National Committee computers last year reveal that on July 5, 2016, data was leaked (not hacked) by a person with physical access to DNC computer. […] Key among the findings of the independent forensic investigations is the conclusion that the DNC data was copied onto a storage device at a speed that far exceeds an Internet capability for a remote hack. (Die Daten wurden mit einer mittleren Geschwindigkeit von 22,1 MB/s kopiert, Spitzenwert 49 MB/s. Das spricht für ein lokal angeschlossenes USB Device.)

41 https://www.heise.de/-3520212
45 https://de.sputniknews.com/politik/20170517315781593-usa-russland-leaks-hillary-mord
46 https://twitter.com/wikileaks/status/763041804652539904


! Achtung Fake News !

Es wird behauptet und rasch verbreitet, das Bundesministerium für Gesundheit / die Bundesregierung würde bald massive weitere Einschränkungen des öffentlichen Lebens ankündigen. Das stimmt NICHT! Bitte helfen Sie mit, ihre Verbreitung zu stoppen.

WAHR: Drei Tage später wurden die Lockdown Maßnahmen verkündet, die ab 23. März in Deutschland in Kraft traten: Kontaktverbot, Schließung der Geschäfte außer Baumärkte und Lebensmittelversorgung, Schließung der Restaurants, Bars, Spielplätze und des gesamten öffentlichen Lebens, Verbot von Reisen und Demonstrationen...

- Zu personenbezogenen Fake News könnte man noch erwähnen, dass der GCHQ Räumungen im Internet gezielt plant und umsetzt (wahrscheinlich nicht nur der GCHQ). Zu den konkreten Methoden der JTRIG (Joint Threat Research Intelligence Group) gehört es, Personen mit Sexangeboten in kompromittierende Situationen zu locken, Falschinformationen unter ihrem Namen im Netz zu publizieren oder Mails an Freunde und Kollegen unter ihrer Identität zu verschicken. Eine weitere Taktik besteht darin, sich in Foren als Opfer einer Person auszugeben, die man schädigen möchte.


Die Integrity Initiative ist eine britische Beeinflussungskampagne gegen Russland, deren Budget 2 Mio. Pfund jährlich beträgt (250.000 Pfund vom US-Außenministerium, 215.000 von der NATO...) Durch eine Leak von internen Dokumenten der Integrity Initiative wurden weitere Kampagnen in Großbritannien, Italien und Norwegen bekannt:
KAPITEL 2. ANGRiffe AUf diE PRIVATSPhÄRE


– In Italien folgte die Berichterstattung in den Medien über den Fall Skripal nicht dem vorgegebenen Narrativ aus GB. Der italienische Cluster der Integrity Initiative wurde aktiv, um die Berichterstattung im Mainstream auf Linie zu bringen.


• Ein weiteres Phänomen im Zeitalter von Twitter und Facebook sind sogenannte Influencer, die sich in ihren emotional aufputschenden Berichten nur den Likes ihrer Follower verpflichtet sehen. Auf der Jagd nach mehr Likes und zur Bestätigung der vorherrschenden Meinung in der Echokammer der Follower werden oft Geschichten erfunden, die man klar in die Gruppe der Fake News einordnen kann.

Ein typisches Beispiel dafür ist der 24-jährige Henryk Stöckl aus dem Umfeld der AfD. Auf seinem Youtube und Facebook Account veröffentlicht er emotional, menschlich und scheinbar authentische aber oft falsche Berichte. In Social Media ist er zu einem der auffälligsten rechten Meinungsmacher in Deutschland geworden. Er selbst nennt sich Privat-Journalist, Kommentator, Aktivist oder Berichterstatter.

In einem Interview mit BuzzFeed wurde er mit einigen seiner eigenen Aussagen konfrontiert und nach den Quellen gefragt. Seine Reaktion:

...ähm... also - ähm...ähmm... Diese Frage lassen wir mal besser aus.

An anderer Stelle nennt er Erzählungen von Dritten als Quelle seiner Fake News.

Das sich viele seiner Berichte immer wieder als Lügen entlarvt werden, scheint seine Follower wenig zu interessieren. In den Antworten auf seine Beiträge steigern sie sich bis hin zu Mordaufrufen gegen Personen aus einem vermeintlich linken Spektrum.

Auch auf der linken Seite gibt es Spinner, die mit der massenweise Abschlachtung von Untermenschen eine neue Nazidiktatur verhindern wollen. Denken verboten?

54 https://consortiumnews.com/2019/01/14/the-twitter-smearing-of-corbyn-and-assange/
55 https://www.heise.de/tp/features/Integrity-Initiative-Britische-Beeinflussungskampagne-gegen-Russland-4232365.html
58 https://www.heise.de/tp/features/Integrity-Initiative-taucht-ab-4286004.html
60 https://www.heise.de/4265180
61 https://twitter.com/BuzzFeedNewsDE/status/1064538241880203264
62 https://www.privacy-handbuch.de/diskussion.htm#08_01_19
2.5. FAKE NEWS DEBATTE

Andere Beispiele sind falsche Politiker Zitate, mit denen man hohe Klickraten und Likes erzielt, die aber leicht als Fake erkennbar sind, wie zum Beispiel das Zitat in Abb. 2.5 aus dem Blog von Sven Liebich. In einem Spiegel Interview sagte M. Schulz, dass man die Typen von der AfD bekämpfen muss, aber er sagte nichts von Lagern.63

Abbildung 2.5: Fake News: Falsches Zitat von M. Schulz mit hohen Klickraten


2.5.3 Medienkompetenztraining

Der beste Schutz gegen Fake News und Propagandalügen ist Medienkompetenz. Übererelte gesetzliche Regelungen oder Privatisierung der Wahrheitsfindung durch Unternehmen wie Facebook sind im Spannungsfeld von freier Meinungsäußerung keine Lösung.

Ein bisschen Medienkompetenztraining an Fake News Beispielen:

Quellen prüfen: Im Dez. 2016 kursierte das Gerücht, dass die syrische Armee bei der Befreiung Allepos mehrere hochrangige NATO-Offiziere gefangen genommen haben soll, die dort die Rebellen bzw. Terroristen unterstützt haben sollen.

Als Quelle für diese Fake News wurde immer wieder der Nachrichtenkanal Russia-Today genannt und auf das Video Syrischer UN-Botschafter nennt die Namen der gefangenen NATO-Offiziere im UN-Sicherheitsrat verwiesen, das angeblich vom russischen Nachrichtensender RT.com stammen soll.64

ABER: Man findet dieses Video nicht im Youtube Channel von RT.com, das RT-Logo ist amateurhaft in das Video hinein montiert und hat durch die Kompression die grafische Struktur verloren, der Hintergrund ist echt unprofessionell ausgeleuchtet... Zum Vergleich kann man sich ein echtes Video aus dem Youtube Channel von RT.com anschauen, Die Unterschiede zur professioneller Technik sind offensichtlich.


63 http://www.spiegel.de/politik/ausland/martin-schulz-ueber-afd-diese-typen-muss-man-bekaempfe-a-1078912.html
64 https://www.youtube.com/watch?v=VwrYuAvMPE
Assoziation falscher Zusammenhänge: PI-News berichtet im September 2017 über die bayrische Kriminalstatistik.65


Eine genauere Analyse66 der Zahlen zeigt, dass die Zahl der Vergewaltigungen im Vergleich zum Vorjahr nur gering gestiegen ist, um 5% von 68 auf 71 und damit innerhalb der normalen Schwankungen. Die Zahl der tatverdächtigen Deutschen ist etwas gesunken und die Zahl der tatverdächtigen Zuwanderer ist von 8 auf 17 gestiegen. Ein explosionsartiger Anstieg durch 1,5 Mio Zuwanderer sieht anders aus.

2.5.4 Fake News oder Propaganda - was ist der Unterschied?


The recent history of Ukraine in general and Crimea in particular over the past several years may be among the most egregious examples of fake news in recent memory.

Nein, das war eine Propaganda Kampagne, die u. a. auch Fake News als Elemente verwendete. Ich erinnere mich z. B. an eine Meldung, dass die Aufständischen in der Ostukraine OSZE Beobachter gefangen genommen hätten. Das war nur eine Falschmeldung. (Die OSZE dementierte kurz Zeit später und es stellte sich heraus, dass die gefangenen deutschen Offiziere in Spionagemission unterwegs waren.)

Es wurden neben Fake News auch alle anderen propagandistischen Methoden verwendet. Die Berichterstattung des ÖRR wurde vom Programmbeirat der ARD als fragmentarisch, tendenziös, mangelhaft und einseitig gerügt68. Und das nennt man Propaganda.

2.6 Geotagging


68https://www.heise.de/tp/features/Ukraine-Konflikt-ARD-Programmbeirat-bestaetigt-Publikumskritik-3367400.html
2. Die Analyse des Sozialen Umfeldes ist mit den Standortdaten ebenfalls möglich. Die Summe aller Standortdaten ist mehr, als die Anhäufung der Standorte von Person A, B und C. Wie die Studie "Inferring social ties from geographic coincidences" zeigt, ermöglicht diese Sammlung detaillierte Informationen über das soziale Umfeld, auch wenn man bei Facebook nicht befreundet ist. Die Standortdaten der Smartphones verraten, mit wem man regelmäßig ein Bier trinkt, mit wem man ins Bett steigt, ob man an Pegida Demonstrationen teilnimmt oder sich in Antifa Zirkeln trifft und vieles mehr.


Sehr geehrter Kunde, sie sind als Teilnehmer eines Aufstands registriert.

Die Firma Dataminr bietet Kunden via API Zugriff auf die Twitter Postings und wirbt in einem Flyer am Beispiel eines Studentenprotestes in Südafrika damit, wie man das neue Geospatial Analyse Tool Bild 2.6 zum Monitoring von politischen Demonstrationen nutzen kann.

Abbildung 2.6: Auswertung der Twitter Postings eines Studentenprotests in Südafrika aufgrund der Geolocaction der Postings


Es entsteht ein fast vollständiges Modell. Mit der Beobachtung dieser Signale kann man ganze Firmen, ganze Städte, eine ganze Gesellschaft röntgen.

Das Magazin Wired berichtete im Danger Room (Oktober 2011), dass das FBI Smartphones bereits seit Jahren mit der Zielstellung der “Durchleuchtung der Gesellschaft”

69 http://www.pnas.org/content/107/52/22436.short
70 https://www.heise.de/tr/artikel/Immer-im-Visier-276659.html
KAPITEL 2. ANGRiffe auf die Privatphäre


...the pushpins on the new FBI geo-maps indicate where people live, work, pray, eat and shop, not necessarily where they commit or plan crimes.

Im September 2012 hat in den USA der Sixth Circuit Court of Appeals entschie- den, das bezügliche Standortdaten keine Ansprüche auf Privatsphäre bestehen. Diese Entscheidung ermöglicht es US-Firmen, diese Daten hemmungslos zu sammeln. Die Dienste der USA dürfen ohne richterliche Prüfung Standortdaten von GPS-Geräten verfolgen.

Die Daten werden mit verschiedenen Methoden gesammelt:

- Hauptlieferanten für Geodaten sind Smartphones und Handys. Vor allem Apps kön- nen genutzt werden, um Geodaten zu sammeln. Über die Hälfte der in verschiede- nen Stores downloadbaren Apps versenden Standortdaten unabhängig davon, ob sie für die Funktion der App nötig sind. Der Bundesdatenschutzbeauftragte erwähnt beispielsweise eine App, die das Smartphone zur Taschenlampe macht und dabei den Standort an den Entwickler der App sendet.


Für die Datensammlungen rund um das iPhone wurde Apple mit dem BigBrother Award 2011 geehrt. Auszug aus der Laudation von F. Rosengart und A. Bogk:


Das chinesische Staatsfernsehen bezeichnete die Möglichkeit des Auslesens häufig besuchter Orte im iPhone als Risiko für die nationale Sicherheit, da die Daten bei US-Firmen gespeichert werden, die im Rahmen von PRISM mit der NSA kooperieren.

- Millionen von Fotos werden über verschiedene Dienste im Internet veröffentlicht (Flickr, Twitter, Facebook...). Häufig enthalten diese Fotos in den EXIF-Attributen die GPS-Koordinaten der Aufnahme. Die Auswertung dieses Datenstromes steht erst am Anfang der Entwicklung. Ein Beispiel ist die mit Risikokapital ausgestattete Fir- ma Heypic, die Fotos von Twitter durchsucht und auf einer Karte darstellt.


---

73 https://www.heise.de/-2257924
Die Deaktivierung von Places scheint bei Facebook wirklich umständlich zu sein. Damit wird aber nicht die Erfassung der Daten deaktiviert, sondern nur die Sichtbarkeit für andere Nutzer!

- Lokalisierungsdienste wie Gowalla oder Foursquare bieten öffentlich einsehbare Standortdaten und versuchen, durch spielfarbenen Charakter neue Nutzer zu gewinnen. Im Gegensatz zu den oben genannten Datensammlungen kann man bei Gowalla oder Foursquare aber gut kontrollieren, welche Daten man veröffentlicht oder die Dienste nicht nutzen.

Nichts zu verbergen?

Wer ein praktisches Beispiel braucht: Krankengeld gestrichen und Job verloren, weil er auf Facebook Urlaubsfotos veröffentlichte. Andreas H. litt an Depressionen. Er ging zum Arzt und wurde krank geschrieben. Seine Ärzte rieten ihm zu einem Urlaub. Facebook-Fotos mit Surfbrett am Strand kosteten ihn erst das Krankengeld - und dann den Job.²⁴

2.7 Kommunikationsanalyse

Geheimdienste verwenden seit Jahren die Kommunikationsanalyse (wer mit wem kommuniziert), um die Struktur von Organisationen aufzudecken. Damit gelingt es, automatisiert umfangreiche Informationen zu beschaffen, ohne die Verschlüsselung von Inhalten der Kommunikation knacken zu müssen.

Auch ohne Kenntnis der Gesprächs- oder Nachrichteninhalte - die nur durch Hineinhören zu erlangen wäre - lässt sich allein aus dem zeitlichen Kontext und der Reihenfolge des Kommunikationsflusses eine hohe Informationsgüte extrahieren, nahezu vollautomatisch. (Frank Rieger)


²⁴https://www.apotheke-adhoc.de/nachrichten/detail/pta-live/uraub-trotz-krankengeld/
Zivile Kommunikations-Analyse


Wie man die Freundschaftsbeziehungen in sozialen Netzen wie Facebook oder ...VZ werden analysieren kann, um omosexualle Orientierung zu erkennen, haben ehemalige Studenten des MIT mit Gaydar - die Schwulenfalle demonstriert. Die TU Berlin hat zusammen mit der Wirtschaftsuniversität Wien erfolgversprechende Ergebnisse zur Rasterfahndung nach Meinungsmachern veröffentlicht.

Ein Beispiel


Als Beispiel nehmen wir eine Gruppe mit dem Namen ”Muppet Group”, abgekürzt ”mg”. Als Ausgangslage ist bekannt, dass Anton und Beatrice zur ”mg“ gehören.

Durch Auswertung aller zur Verfügung stehenden Kommunikationsdaten von Anton und Beatrice erhält man ein umfangreiches Netz ihrer sozialen Kontakte (Bild 2.8). Dabei wird nicht nur die Anzahl der Kommunikationsprozesse ausgewertet, es wird auch die zeitliche Korrelation einbezogen.

![Abbildung 2.8: Soziales Netz von Anton und Beatrice](image)

Ideal wäre es, an dieser Stelle die Kommunikation von Clementine und Detlef näher zu untersuchen. Beide sind aber vorsichtig und es besteht kein umfassender Zugriff auf die Kommunikationsdaten. Dann nimmt man als Ersatz vielleicht Frida, um das Modell zu präzisieren.

Frida unterhält vor allem einen engen Kontakt zu Detlef, was zu einer Umbewertung der Positionen von Detlef und Clementine führt (Bild 2.9). Bei Emil handelt es sich evtl. um einen zufällig gemeinsamen Bekannten von Anton und Beatrice, der nicht in die "mg" eingebunden ist.

Abbildung 2.9: Präzisierte Struktur der "mg"

Reale Datenmengen

Reale Kommunikationsnetzwerke sind wesentlich komplexer. Auf Grundlage der Daten, die von T-Mobile über den Politiker Malte Spitz gespeichert wurden, hat Michael Kreil von OpenDataCity die Grafik in Bild 2.10 mit den Rohdaten erstellt.

Etwas besser aufbereitete Daten visualisiert Bild 2.11 mit den Kommunikationsdaten einer Woche von Ton Siedsmas.

Wenn man auch die Standortdaten des Smartphone mit auswerten kann, werden die Informationen deutlich detaillierter. Bild 2.12 zeigt einen Tag von Ton Siedsmas.

Analysetools wie i2 Analyst’s Notebook von IBM oder rola rsCASE können diese Daten hübsch aufbereiten und die Schlapphüte bei der Analyse effektiv unterstützen (Bild 2.13).

2.8 Überwachungen im Internet

Eine umfassendere Übersicht zu verschiedenen Sicherheits-Gesetzen der Jahre bis 2017 bietet www.daten-speicherung.de. Sehr schön erkennbar ist das Muster der Zustimmung durch die jeweiligen Regierungsparteien und meist Ablehnung durch die Opposition, von Böswilligen als Demokratie-Simulation bezeichnet. Unabhängig vom Wahlergebnis wird durch die jeweiligen Regierungsparteien die Überwachung ausgebaut.75

Identifizierungspflicht für nummernunabhängige Dienste Für Messenger, E-Mail Provider und ähnliche Dienste, die unabhängig von der Telefonnummer nutzbar sind, soll eine Identifizierungspflicht der Nutzer eingeführt werden. Die Provider sollen

75https://www.daten-speicherung.de/index.php/ueberwachungsgesetze
KAPITEL 2. ANGRiffe AUF Die PRIVatsphären

Abbildung 2.10: Kommunikationsnetzwerk von Malte Spitz

Namen, Geburtsdatum und Adressen der Nutzer erfassen, verifizieren und den Behörden auf Abruf im Rahmen der Bestandsdatenauskunft zur Verfügung stellen.

Im Unterschied zum Klarnamen-Zwang können die Dienste weiterhin mit einem Pseudonym genutzt werden, aber die realen Identitäten hinter den Pseudonymen müssen der Strafverfolgung und Geheimdiensten zur Verfügung gestellt werden.

- Auf der Innenministerkonferenz im Juni 2020 wurde diese Forderung mit der Notwendigkeit der Verfolgung von Kinderpornografie begründet.
- Die SPD hat die Identifizierungspflicht für nummemunabhängige Dienste in den Entwurf des Wahlprogramms für die Bundestagswahl 2021 aufgenommen, um als möglicher Juniorpartner Bereitschaft zur Umsetzung weiterer Überwachungen zu signalisieren.
- Das Bundesinnenministerium unter H. Seehofer versucht, die Identifizierungspflicht für E-Mail und Messenger Provider in der aktualisierten TKG-Novelle zu platzieren. Mit dem Vorschlag zur Novellierung des TKG vom Dez. 2020 sollen auch Over-the-Top Dienste wie Messenger und E-Mail als TK-Dienste klassifiziert werden, was diese Dienste zur TKÜ bei schweren Straftaten verpflichten würde und außerdem zur Unterstützung beim Rollout von Trojanern zur Quellen-TKÜ und Online-Durchsuchung.

Vorratsdatenspeicherung: (Neusprech: Daten-Mindestspeicherfrist oder ganz neu: private Vorsorgespeicherung)


- 1997 wurde die Vorratsdatenspeicherung aufgrund verfassungsrechtlicher Bedenken abgelehnt.
2.8.ÜBERWACHUNGEN IM INTERNET

2002 wurde ein ähnlicher Gesetzentwurf vom Deutschen Bundestag abgelehnt und die Bundesregierung beauftragt, gegen einen entsprechenden Rahmenbeschluss auf EU-Ebene zu stimmen (Bundestag-Drucksache 14/9801).

2005 hat das EU-Parlament mit Mehrheit der christ- und sozialdemokratischen Fraktionen die Richtlinie zur 6-monatigen Datenspeicherung der Verbindungs- und Standortdaten (VDS) beschlossen (Directive 2006/24/EG). Um die Richtlinie mit einfacher Mehrheit in der EU-Kommission ohne Mitsprache des Parlamentes verabschieden zu können, wurde sie nicht als Sicherheits- und Polizeimaßnahme behandelt sondern als Maßnahme zur Regulierung des Binnenmarktes definiert, was außerdem die EU-Länder zu einer Umsetzung zwingt.

2006 hat der Wissenschaftliche Dienst des Bundestages ein Rechtsgutachten mit schweren Bedenken gegen die VDS vorgelegt.


<table>
<thead>
<tr>
<th>Straftaten im Internet</th>
<th>2008 (o. VDS)</th>
<th>2009 (mit VDS)</th>
<th>2010 (o. VDS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Straftaten im Internet</td>
<td>167.451</td>
<td>206.909</td>
<td>223.642</td>
</tr>
<tr>
<td>Aufklärungsrate (Internet)</td>
<td>79.8%</td>
<td>75.7%</td>
<td>72.3%</td>
</tr>
</tbody>
</table>

2010 erklärt das Bundesverfassungsgericht in einem Grundsatzurteil das Gesetz zur VDS als nicht vereinbar mit dem Grundgesetz. (Az: 1 BvR 256/08)

2012 zeigte das Max-Planck-Instituts (MPI) für ausländisches und internationales Strafrecht in einer umfangreichen wissenschaftlichen Analyse, dass KEINE Schutzlücke ohne Vorratsdatenspeicherung besteht und widerspricht damit der Darstellung von mehreren Bundesinnenministern und BKA-Chef Ziercke, wonach die VDS für die Kriminalitätsbekämpfung unbedingt nötig wäre. Die in

http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html
KAPITEL 2. ANGRiffe AUF Die PRIVATSphÄRE

Abbildung 2.12: Standortdaten eines Tages von T. Siedsmas

Abbildung 2.13: Screenshot von i2 Analyst’s Notebook (IBM)

der Presse immer wieder herangezogenen Einzelbeispiele halten einer wissen-
schaftlichen Analyse nicht stand.\footnote{https://www.ccc.de/de/updates/2012/mythos-schutzluecke}

- 2012 gibt es einen nicht erfolgreichen Anlauf, die VDS international im Rahmen
der UNODC als verpflichtende Richtlinie zu etablieren. Der Verfassungsschutz

- 2014 wird die Richlinie 2006/24/EG vom EuGH als nicht vereinbar mit der
Charta der Grundrechte der Europäischen Union gekippt. (Urteil C-293/12 und
C-594/12)

- 2015 wird im Eilverfahren ein neues Gesetz zur Speicherpflicht für Verkehrsdaten
verabschiedet. Bundesjustizminister H. Maas konnte auf der Pressekonferenz
zur Verabschiedung des Gesetzentwurfes im Bundeskabinett auf Nachfrage kei-
nen Grund nennen, warum die Vorratsdatenspeicherung notwendig sein soll:
2.8. ÜBERWACHUNGEN IM INTERNET

Frage: Kann der Minister die Notwendigkeit der Vorratsdatenspeicherung beweisen (was eine Voraussetzung für Grundrechtseingriffe wäre)?


Für die Bundesdatenschutzbeauftragte A. Voßhoff ist die VDS verfassungswidrig und widerspricht Urteilen von BVerfG und EuGH. Der ehemalige Bundesdatenschutzbeauftragte P. Schaar kommentierte:

_Brauchen wir das überhaupt? Die Bundesregierung bleibt den Nachweis schuldig, dass dieser erhebliche Grundrechtseingriff unerlässlich ist._

- 2017 legt der Wissenschaftliche Dienst zum wiederholten Mal ein Gutachten zur Vorratsdatenspeicherung vor, dass zu dem Schluss kommt, dass die aktuelle Gesetz nicht nicht mit geltendem EU-Recht vereinbar ist. In mehreren Punkten verstößt das neue Gesetz gegen die Vorgaben des Europäischen Gerichtshofes.²⁹

Warum bemüht man sich seit Jahren, eine Überwachungsmaßnahme einzuführen, die uns einige hundert Millionen Euro kosten wird, die so gut wie keine Beitrag zur Verbesserung der Strafverfolgung bietet und in erster Linie den Geheimdiensten (Neusprech: Gefahrenabwehrdiensten) neue Kompetenzen verschafft wird?


- Passworte für den Zugriff auf E-Mail Konten und Cloud-Speicher.
- PINs zum Ent sperren von Smartphones.
- Zugriff auf die Endgeräte (Router), die den Kunden vom DLS-Provider kosten-los bereitgestellt werden (TR-069 Schnittstelle).

Die Piratenpartei kommentierte den Gesetzentwurf kurz und bündig:

_Der Entwurf der Bundesregierung ist schlicht verfassungswidrig._


1. In der ersten Stufe unterzeichneten im Frühjahr 2009 die fünf großen Provider freiwillig einen geheimen Vertrag mit dem BKA. Sie verpflichteten sich, eine Liste von Webseiten zu sperren, die vom BKA ohne nennenswerte Kontrolle erstellt werden sollte.

³¹ http://blog.odem.org/2009/05/quellenanalyse.html


4. Im Rahmen der Evaluierung des Gesetzes geht das BKA nur halbherzig gegen dokumentierten Missbrauch vor, wie eine Veröffentlichung des AK-Zensur zeigt. Gleichzeitig wird weiter Lobbyarbeit für das Zensurge setz betrieben.  


BKA Gesetz: Mit dem BKA Gesetz wurde eine Polizei mit den Kompetenzen eines Geheimdienstes geschaffen. Zu diesen Kompetenzen gehören neben der heimlichen Online-Durchsuchung von Computern der Lauschangriff außerhalb und innerhalb der Wohnung (incl. Video), Raster- und Schleierfahndung, weitgehende Abhörbefugnisse, Einsatz von V-Leuten, verdeckten Ermittlern und informellen Mitarbeitern...

Im Rahmen präventiver Ermittlungen (d.h. ohne konkreten Tatverdacht) soll das BKA die Berechtigung erhalten, in eigener Regie zu handeln und Abhörmaßnahmen auch auf Geistliche, Abgeordnete, Journalisten und Strafverteidiger auszudehnen. Im Rahmen dieser Vorfeldermittlungen unterliegt das BKA nicht der Leitungs befugnis der Staatsanwaltschaft.

Damit wird sich das BKA bis zu einem gewissen Grad jeglicher Kontrolle, der justiziellen und erst recht der parlamentarischen, entziehen können.

Telekommunikationsüberwachungsverordnung Auf richterliche Anordnung wird eine Kopie der gesamten Kommunikation an Strafverfolgungsbehörden weitergeleitet. Dieser Eingriff in das verfassungsmäßig garantierte Recht auf unbeobachtete Kommunikation ist nicht nur bei Verdacht schwerer Verbrechen möglich, sondern auch bei einigen mit Geldstrafe bewehrten Vergehen und sogar bei Fahrlässigkeitsdelikten (siehe §100a StPO).

82 http://ak-zensur.de/2010/08/kapitulation.html
83 http://www.eco.de/verband/202_8727.htm
85 http://www.berlinonline.de/berliner-zeitung/print/politik/725127.html
2.9 Terrorismus und der Ausbau der Überwachung


Jemand hat die Toten durch Terroranschläge in Europa in den letzten Jahrzehnten aufgeschlüsselt. Die Grafik 2.14 auf Basis der Daten der Global Terrorism Database zeigt, ...

Laut Gesetz kann die Überwachung auch ohne richterliche Genehmigung begonnen werden. Sie ist jedoch spätestens nach 3 Tagen einzustellen, wenn bis dahin keine richterliche Genehmigung vorliegt.


Die Anzahl der von dieser Maßnahme Betroffenen verdoppelt sich Jahr für Jahr. Gleichzeitig führen nur 17% der Überwachungen zu Ergebnissen im Rahmen der Ermittlungen.

§129a StGB Auf Basis des §129a StGB (Bildung einer terroristischen Vereinigung) wurden in den letzten Jahren so gut wie keine Verurteilungen ausgesprochen. Die sehr weit gehenden Befugnisse für Ermittlungen nach diesem Paragraphen wurden jedoch mehrfach genutzt, um politische Aktivisten auszuforschen. Mehrfach haben verschiedene Gerichte die Anwendung des §129a StGB durch Ermittlungsbehörden für illegal erklärt.

• Doppeleinstellung in Sachen §129
• Razzien im Vorfeld des G8-Gipfels waren rechtswidrig
• Konstruieren und Schnüffeln mit §129a
• Durchsuchungen beim LabourNet waren rechtswidrig

Dieser Missbrauch der Anti-Terror Befugnisse sollte gestoppt und evaluiert werden.


Jemand hat die Toten durch Terroranschläge in Europa in den letzten Jahrzehnten aufgeschlüsselt. Die Grafik 2.14 auf Basis der Daten der Global Terrorism Database zeigt, ...
KAPITEL 2. ANGRiffe auf die privilegSpäHre

dass Europa hinsichtlich Terrorgefahr noch nie so sicher war, wie heute.

Abbildung 2.14: Opfer von Terroranschlägen in Westeuropa


Bis 2010 konnte durch politische Maßnahmen die Zahl der Terroranschläge im Vergleich zu 2006 halbiert werden, es gab nur noch 246 Anschläge93. Der Europol-Bericht TE-SAT 2014 listet noch 152 Terroranschläge mit 7 Toten auf, der niedrigste Stand.94

2015 wurde wieder ein Anstieg bei Terroranschlägen verzeichnet (insgesamt 211 Anschläge). Während sich linke und separatistische Anschläge weiter verringerten (nur noch 65), kam es zu einer Zunahme von jihadististischen Anschlägen vor allem in Frankreich. Dabei starben 148 Personen, da jihadististische Selbstmordattentäter eine möglichst hohe Zahl von Todesopfern erzielen wollen. 687 potentielle islamistische Attentäter wurden verhaftet, davon wurden 98% verurteilt.95


In Deutschland gab es einen Anschlag in diesem Kontext, der Terrorist Anis Amri fuhr mit einem LKW im Dez. 2016 in den Berliner Weihnachtsmarkt. Auch dieser Terrorist war den Sicherheitsbehörden bekannt, er war in den Wochen vor dem Anschlag das Top-1-Thema der deutschen Terrorabwehr, BKA und Verfassungsschutz waren über die Gefahr informiert, der marokkanische Geheimdienst hatte gewarnt und trotzdem…96

Als Konsequent aus dem Anschlag forderten Bundesinnenminister Thomas de Maizière (CDU) und andere Politiker reflexartig einen Ausbau der Überwachung. Insbesondere die

93 https://www.counterextremism.org/resources/details/id/229
96 https://www.heise.de/tp/features/Amri-TOP-1-der-Terrorabwehr-3914967.html
2.9. TERRORISMUS UND DER AUSBAU DER ÜBERWACHUNG

Wir können doch nicht dieselben Leute weitermachen lassen, die so versagt haben.

Abbildung 2.15: Alle 24 Terroristen mit islamistischen Hintergrund waren vor den Anschlägen als gewaltbereite Gefährder bekannt


97 https://deutsch.rt.com/inland/61697-neue-vorwurfe-im-fall-amri-us-interessen/
KAPITEL 2. ANGRiffe AUF die PriVATSPHÄRE

Schweinegrippe oder Ebola. Das 700.000 Kinder in der Sahel-Zone verhungern, interessierte dagegen kaum jemanden.


Die neuen Terroristen haben gelernt, die Panik-Medien für ihre Interessen immer besser zu nutzen. Auch die Apologeten der Überwachung nutzen die resultierende Angst für ihre eigenen Interessen und nicht für die Bekämpfung des Terrorismus. Der Schock durch die Anschläge wurde von der deutschen Regierung genutzt, um den bereits geplanten Ausbau der Geheimdienste um 475 Mitarbeiter anzukündigen. Noch nie war die Manipulation der Emotionen so stark und großflächig wie heute. *Der moderne Krieg ist kein Krieg um Territorien sondern ein Krieg um die Köpfe.* Dieser Satz stammt aus der aktuellen Überarbeitung der NATO Doktrin, er trifft aber auch beim Kampf gegen Terror zu.


![Abbildung 2.16: Staaten, die Terroristen finanzieren](image)

Ein konsequenter, politischer Druck auf Saudi Arabien (der größte Finanzier des ISIS), die USA und die Türkei könnte im Kampf gegen Terrorismus mehr erreichen, als alle Bomben zusammen. Das wird aber nicht diskutiert. Statt dessen werden die wirtschaftlichen Sanktionen gegen Syrien, Russland und den Iran aufrecht erhalten.
Auch Frankreich ist seit Jahrzehnten als Förderer von staatlich Terrorismus bekannt und hat in afrikanischen Ländern mehrere blutige Putsche organisiert, weil die gewählten Regierungen nicht den neo-kolonialen Wirtschaftsinteressen von Frankreich folgten.\footnote{https://www.heise.de/tp/artikel/46/46592/1.html}

### 2.10 Ich habe doch nichts zu verbergen

Dies Argument hört man oft. Haben wir wirklich nichts zu verbergen? Einige Beispiele für spezielle Detektoren und Einzelbeispiele sollen exemplarisch zeigen, wie tief Big Data in unser Leben eingreift und wie willkürlich gesammelte Daten unser Leben gravierend beeinflussen können:

#### Erkennung einer neuen Liebesbeziehung


- Marketingexperten haben herausgefunden, dass man sich in dieser Situation leichter zum Wechsel von Marken bewegen lässt und mehr Geld ausgibt.

- Headhunter wissen, dass man Menschen in dieser Situation leichter zu beruflichen Veränderungen bewegen kann.

- Personalmanager großer Firmen interessieren sich für die Auswirkungen auf die Produktivität bei Affären innerhalb der Firma.

- Geheimdienste interessieren sich für die Erpressbarkeit von Ziel-Personen.

#### Arbeitslos?

Unser Smartphone liefert die aktuelle Position des Nutzers an viele Trackingdienste. Außerdem verraten Postings bei Twitter oder Facebook unseren Aufenthaltsort.

In der Regel sind wir Nachts zuhause und an Werktagen tagsüber an unserem Arbeitsplatz. Was kann man schlussfolgern, wenn sich dieses Verhalten ändert und man auch tagsüber über einen längeren Zeitraum zuhause bleibt in Kombination mit einem sparsameren Konsumverhalten bei Online Einkäufen oder Offline Einkäufen mit Rabattkarten bzw. Kreditkarten? Welchen Einfluss hat das auf unsere Kreditwürdigkeit?

#### Unzufrieden mit dem Job?


L. Reppesgaard hat im Rahmen eines Selbstversuches mehrere E-Mails von seinem Gmail Account versendet mit kritischen Bemerkungen zu seinem Arbeitsverhältnis. Unmittelbar darauf konnte er Veränderungen in der personalisierten Werbung registrieren, die plötzlich auf Headhunter und kommerzielle Jobbörsen hinwies.
Kein Studienplatz?

In Großbritannien werden Studienbewerber für bestimmte Fachrichtung geheimdienstlich überprüft. 739 Bewerber wurde bereits abgelehnt, weil aufgrund dubioser Datensammlungen der Geheimdienste befürchtet wurde, dass die Bewerber zu Terroristen werden und die im Studium erworbenen Kenntnisse zur Herstellung von Massenvernichtungswaffen nutzen könnten. Die geheimdienstlichen Gesinnungs-Prüfungen sollen zukünftig ausgeweitet werden.\(^{99}\)

Einzelbeispiele

- Emma L. hatte sich auf dem Dating-Portal OkCupid zu einem Treffen verabredet. Das Date war ein Reinfall (kommt manchmal vor). Wenig später wurde ihr der Dating-Partner von Facebook als Freund empfohlen, in der People You May Know Section. Maria L. wurden ihre Tinder-Dates von Facebook als Freunde empfohlen. Es gibt auf Twitter noch viele weitere Beispiele für diese seltsamen Facebook Empfehlungen.\(^{100}\)

Weder OkCupid noch Tinder geben Daten an Facebook weiter. Die Empfehlungen für Freunde werden anhand der Geolocation (zur gleichen Zeit am gleichen Ort) und aufgrund ähnlicher Interessen (Dating-Webseite besucht) ermittelt. Daraus könnten sich auch unangenehme Folgen ergeben, wie Netzpolitik.org an Beispielen zeigt.\(^{101}\)

- Target ist einer der größte Discountere in den USA. Eines Tages stürmte ein wütender Vater in eine Filiale und beschwert sich, dass seine minderjährige Tochter Rabattmarken für Babysachen erhalten hat. Später musste der Vater kleinlaut zugeben, dass seine Tochter wirklich schwanger war, er selbst aber nichts davon wusste. Target hatte die Schwangerschaft der minderjährigen Tochter an den kleinen Änderungen im Kaufverhalten erkannt.\(^{102}\)

- Im Rahmen der Zulassigkeitsprüfung für Piloten wurde Herr J. Schreiber mit den vom Verfassungsschutz gesammelten Fakten konfrontiert:\(^{103}\)

  2. Offensichtlich wurde daraufhin sein Bekanntenkreis durchleuchtet.
  3. Als Geschäftsführer einer GmbH für Softwareentwicklung habe er eine vorbestrafste Person beschäftigt. Er sollte erklären, welche Beziehung er zu dieser Person habe.

Für Herrn S. ging die Sache gut aus. In einer Stellungnahme konnte er die in der Akte gesammelten Punkte erklären. In der Regel wird uns die Gelegenheit zu einer Stellungnahme jedoch nicht eingeräumt. Es werden Entscheidungen getroffen und wir haben keine Ahnung, welche Daten dabei eine Rolle spielten.

- Ein junger Mann meldet sich freiwillig zur Bundeswehr. Mit sechs Jahren war er kurzzeitig in therapheutischer Behandlung, mit vierzehn hatte er etwas gekiff. Seine besorgte Mutter ging mit ihm zur Drogenberatung. In den folgenden Jahren gab es keine Drogenprobleme. Von der Bundeswehr erhält er eine Ablehnung, da er ja mit

\(^{99}\) https://www.heise.de/tp/artikel/44/44538/1.html
\(^{100}\) https://twitter.com/search?q=facebook%2Bsuggest%20tinder
\(^{101}\) https://netzpolitik.org/2016/facebook-nutzt-standort-fuer-freundesvorschlage/
\(^{102}\) http://www.tagebau.com/?p=197
\(^{103}\) http://www.pilotundflugzeug.de/artikel/2006-02-10/Spitzelstaat
sechs Jahren eine Psychotherapie durchführen musste und Drogenprobleme gehabt hätte.\footnote{https://blog.kairaven.de/archives/998-Datenstigmaanekdote.html}


- "Leimspur des BKA": Wie schnell man in das Visier der Fahnder des BKA geraten kann, zeigt ein Artikel bei Zeit-Online. Die Webseite des BKA zur Gruppe "mg" ist ein Honeypot, der dazu diente, weitere Sympathisanten zu identifizieren. Die Bundesanwaltschaft verteidigt die Maßnahme als legale Fahndungsmethode.


Nicht immer treten die (repressiven) Folgen staatlicher Sammelwut für die Betroffenen so deutlich hervor. In der Regel werden Entscheidungen über uns getroffen, ohne uns zu benachrichtigen. Wir bezeichnen die (repressiven) Folgen dann als Schicksal.

\section*{Politische Aktivisten}

Wer sich politisch engagiert und auf gerne vertuschte Mißstände hinweist, hat besonders unter der Sammelwut staatlicher Stellen zu leiden. Einige deutsche Beispiele:

1. Erich Schmidt-Eenboom veröffentlichte 1994 als Publizist und Friedensforscher ein Buch über den BND. In den folgenden Monaten wurden er und seine Mitarbeiter vom BND ohne rechtliche Grundlage intensiv überwacht, um die Kontaktpersonen zu ermitteln. Ein Interview unter dem Titel \textit{"Sie beschatteten mich sogar in der Sauna"}\footnote{http://www.spiegel.de/politik/deutschland/0,1518,384374,00.html} gibt es bei SPON.


3. Dr. Rolf Gössner ist Rechtsanwalt, Vizepräsident der Internationalen Liga für Menschenrechte, Mitherausgeber des Grundrechte-Reports, Vizepräsident und Jury-Mitglied bei den Big Brother Awards. Er wurde vom Verfassungsschutz 38 Jahre lang
überwacht. Obwohl das Verwaltungsgericht Köln bereits urteilte, dass der Verfassungsschutz für den gesamten Bespitzelungszeitraum Einblick in die Akten gewähren muss, wird dieses Urteil mit Hilfe der Regierung ignoriert. Es werden Sicherheitsinteressen vorgeschoben!

Mit dem Aufbau der “neuen Sicherheitsarchitektur” bedeutet eine Überwachung nicht nur, dass der direkt Betroffene überwacht wird. Es werden Bekannte und Freunde aus dem persönlichen Umfeld einbezogen. Sie werden in der AntiTerrorDatei gespeichert, auch ihre Kommunikation kann überwacht werden, es ist sogar möglich, Wanzen in den Wohnungen der Freunde zu installieren.
Kapitel 3
Digitales Aikido

Die folgende grobe Übersicht soll die Orientierung im Dschungel der nachfolgend beschriebenen Möglichkeiten etwas erleichtern.

- **Einstieger (Trackingschutz):** Datensammler nutzen verschiedenste Möglichkeiten, Informationen über Menschen, über ihre Interessen und Vorlieben usw. zu aggregieren und diese Daten zur Manipulation des Einkaufsverhaltens oder politischer Ansichten zu nutzen. Um sich dem zu entziehen, kann man das allgegenwärtige Tracking mit verschiedenen Mitteln erschweren.
  - Spurenarm Surfen: Datensammler meiden und Alternativen nutzen, Cookies und Javascript kontrollieren, Werbung filtern
  - E-Mail: Auswahl des Providers, E-Mail Client sicher konfigurieren, unterschiedliche Alias E-Mail Adressen für unterschiedliche Aufgaben verwenden
  - Messenger: Nachdenken über einen oder mehrere geeigneter Dienste für Instant Messaging, boykottieren von Datensammlern
  - Social Media: Dienste meiden, die in erster Linie Daten sammeln, um ihre Nutzer an die Werbeindustrie zu verkaufen
  - ...

Man kann in kleinen Schritten anfangen und darüber nachdenken, welche Spuren man beim Surfen, Einkaufen usw. im Netz hinterlässt und Alternativen bewusst wählen.

- **Level 2 (Verschlüsselung):** Das Verschlüsseln persönlicher Daten und der privaten Kommunikation verwehrt es Dritten, Kenntnis über diesen privaten Bereich des Lebens zu erlangen. (E-Mails, Daten und Backups, Telefonie und Chats verschlüsseln)

- **Level 3 (Anonymisierung):** Wie ein Geist durch das Internet streifen, nicht greifbar sein wie ein Hauch von Nebel oder als sWhistleblower wirklich anonym bleiben…
  Anonymisierungsdiensle wie Tor bilden die technische Basis dafür. Tor Onion Router bietet eine dem realen Leben vergleichbare Anonymität beim Surfen usw. Man kann anonym an Diskussionsforen teilnehmen oder Artikel kommentieren, indem man sich mit Wegwerfadressen registriert und Pseudonyme häufig wechselt…
  Neben der technischen Basis kommt es dabei aber vor allem auf das eigene Verhalten an. Man muss den inneren Drang nach Selbstdarstellung überwinden und auf die Reputation oder Anerkennung als Person verzichten. Das ist manchmal nicht leicht und häufig sind es die kleinen Eitelkeiten, die zur Deanonymisierung führen können.
  In der Regel wird man sowohl als reale Person im Internet unterwegs sein (bei Einkäufen mit Lieferung, als IT-Nerd, als Wissenschaftler, als Fotograf oder als Blogger… - es gibt viele Gründe) und bei anderen Themen versuchen, anonym zu bleiben.
  Wichtig ist, diese unterschiedlichen Identitäten vollständig zu trennen.
Level 4 (Dan, Guru): Wenn man nicht nur beim passiven Konsumieren anonym bleibt sondern es schafft, Reputation für eine virtuelle Identität aufzubauen (beispiw. als Blogger, Autor oder Händler), die nicht mit einer realen Person verknüpft werden kann, dann hat man einen Dan Level erreicht.

(Das ist auch der Traum krimineller Drogen- und Waffenhändler u.ä. im Internet.)

Die technische Basis bieten Tor Onion Services oder anonyme Peer-2-Peer Netze wie das Invisible Internet Projekt (I2P) oder das GNUnet Projekt. Eine dezentrale und verschlüsselte Infrastruktur verbirgt die Inhalte der Kommunikation und wer welchen Dienst nutzt. Auch Anbieter von Informationen sind in diesen Netzen anonym.

Die einzelnen Level bauen aufeinander auf! Es macht wenig Sinn, die IP-Adresse zu verschleiern, wenn man anhand von Cookies eindeutig identifizierbar ist. Auch die Versendung einer anonymen E-Mail ist in der Regel verschlüsselt sinnvoller.

3.1 Nachdenken

Eine Graduierung in den Kampfsportarten ist keine Garantie, dass man sich im realen Leben erfolgreich gegen einen Angreifer zur Wehr setzen wird. Ähnlich verhält es sich mit dem Digitalen Aikido. Es ist weniger wichtig, ob man gelegentlich eine E-Mail verschlüsselt oder einmal pro Woche Anonymisierungsdienste nutzt. Entscheidend ist ein konsequentes, datensparsames Verhalten.

Ein kleines Beispiel soll zum Nachdenken anregen. Es ist keinesfalls umfassend oder vollständig. Ausgangspunkt ist eine reale Person P mit Namen, Geburtsdatum, Wohnanschrift, Fahrerlaubnis, Kontoverbindung…).

Im Internet verwendet diese Person verschiedene Online-Identitäten:

1. Facebook Account (es könnte auch Xing oder ein …VZ sein).
2. Eine E-Mail Adresse mit dem realen Namen.
3. Eine anonyme/pseudonyme E-Mail Adresse bei einem ausländischen Provider.
4. Pseudonyme in verschiedenen Foren, die unter Verwendung der anonymen E-Mail Adresse angelegt wurden.
5. Für Kommentare in Blogs verwendet die Person meist ein einheitliches Pseudonym, um sich Anerkennung und Reputation zu erarbeiten. (Ohne Reputation könnte das soziale Gefüge des Web 2.0 nicht funktionieren.)

Mit diesen Online-Identitäten sind verschiedene Datenpakete verknüpft, die irgendwo gespeichert und vielleicht nicht immer öffentlich zugänglich sind. Um übersichtlich zu bleiben nur eine minimale Auswahl:

- Das Facebook Profil enthält umfangreiche Daten: Fotos, Freundeskreis…
- Von den anonymen E-Mail Postfach findet man Daten bei den Empfängern der E-Mails. (Google has most of my emails because it has all of yours.) Auch diese Datenpakete enthalten einen Zeitstempel sowie oft die IP-Adresse des Absenders. Durch zeitliche Korrelation kann das anonymen E-Mail Postfach mit dem Real-Name Postfach und dem Surf-Profil verknüpft werden.
Abbildung 3.1: Datenverkettung

- In Foren und Blogs findet man Postings und Kommentare, häufig mit den gleichen Pseudonymen, die auch für die E-Mail Adressen verwendet werden.

- Online-Einkäufe erfordern die Angaben zur Kontoverbindung und einer Lieferadresse, die der Person zugeordnet werden können.

**Verkettung der Informationen und Datenpäckchen**

Viele Datenpakete können auf vielfältige Art verknüpft werden. Diese Datenverkettung ist eine neue Qualität für Angriffe auf die Privatsphäre, die unterschätzt wird.

1. Online Communities wie Facebook bieten viele Möglichkeiten. Neben der Auswertung von Freundschaftsbeziehungen gibt es auch viele Fotos. Dieser Datenpool ist schon sehr umfangreich:
   - Wirtschaftswissenschaftler haben eine Methode vorgestellt, um Meinungsmacher und kreative Köpfe in Online-Communities zu identifizieren.
   - MIT-Studenten erkennen homosexuelle Neigungen ihrer Kommilitonen anhand der Informationen über Freundschaften in den Facebook-Profilen.
   - Der Grünen-Vorsitzende Özdemir pflegte eine Freundschaft mit dem Intensivstraftäter Muhlis Ari, ist in seinem Facebook Profil erkennbar.


3. Durch Analyse der im Rahmen der VDS gespeicherten IP-Adressen können bei zeitlicher Übereinstimmung beide E-Mail Adressen der gleichen Person zugeordnet werden. Ein einzelner passender Datensatz reicht aus. (Wenn nicht konsequent Anonymisierungsdienste für das anonyme Postfach verwendet werden.)


---

1. [https://www.heise.de/tp/r4/artikel/31/31691/1.html](https://www.heise.de/tp/r4/artikel/31/31691/1.html)
2. [https://www.heise.de/tp/r4/artikel/31/31181/1.html](https://www.heise.de/tp/r4/artikel/31/31181/1.html)
3. [https://www.heise.de/tp/r4/artikel/32/32138/1.html](https://www.heise.de/tp/r4/artikel/32/32138/1.html)

6. Durch Datenschutzpannen können Informationen über Online-Einkäufe mit anderen Daten verknüpft werden. Dabei schützt es auch nicht, wenn man sich auf das Gütesiegel des TÜV Süd verlässt und bei einem Händler einkauft, der bisher nicht negativ aufgefallen ist. Eine kleine Zusammenfassung vom 29.10.09 bis 04.11.09:

- Die Bücher der Anderen (500.000 Rechnungen online einsehbar 4)
- Die Libris Shops (Zugang zu Bestellungen von 1000 Buchshops 5)
- Sparkassen-Shops (350.000 Rechnung online einsehbar 6)
- Acht Mio. Adressen von Quelle-Kunden sollen verkauft werden 7

Eine reichhaltige Quelle für Datensammler, die Profile ihrer Zielpersonen vervollständigen wollen oder nach potentiellen Zielpersonen rastern.


- Die Datensammlungen werden mit kommerziellen Zielen ausgewertet, um uns zu manipulieren und Kaufentscheidungen zu beeinflussen.
- Personalabteilungen rastern routinemäßig das Internet nach Informationen über Bewerber. Dabei ist Google nur ein erster Ansatzpunkt. Bessere Ergebnisse liefern Personensuchmaschinen und soziale Netzwerke. Ein kurzer Auszug aus einem realen Bewerbungsgespräch:
  - Personalchef: Es stört Sie sicher nicht, dass hier geraucht wird. Sie rauchen ja ebenfalls.
  - Bewerber: Woher wissen Sie das?
  - Personalchef: Die Fotos in Ihrem Facebook-Profil . . .

Qualifizierten Personalchefs ist dabei klar, dass eine kurze Recherche in Sozialen Netzen kein umfassendes Persönlichkeitsbild liefert. Die gefundenen Indizien können aber den Ausschlag für eine Ablehnung geben, wenn man als Frau gebrauchte Unterwäsche anbietet oder der Bewerber eine Nähe zur Gothic-Szene erkennen lässt.


- Firmen verschaffen sich unrechtmäßig Zugang zu Verbindungs- und Bankdaten, um ihre Mitarbeiter auszuforschen (z. B. Telekom- und Bahn-Skandal).

• Identitätsdiebstahl ist ein stark wachsendes Delikt. Kriminelle durchforsten das Web nach Informationen über reale Personen und nutzen diese Identitäten für Straftaten. Wie sich Datenmissbrauch anfühlt: Man wird plötzlich mit Mahnungen für nicht bezahlte Dienstleistungen überschüttet, die man nie in Anspruch genommen hat.1

• Mit dem Projekt INDECT hat die EU ein Forschungsprojekt gestartet und mit 14,8 Mio Euro ausgestattet, um unsere Daten-Spuren für Geheimdienste zu erschließen.2

Ich habe doch nichts zu verbergen…

…oder habe ich nur zu wenig Fantasie, um mir die Möglichkeiten der Datensammler vorzustellen, mein Leben zu beeinflussen?

3.2 Ein Beispiel

Das Seminar für angewandte Unsicherheit (SAU) hat ein sehr schönes Lehrbeispiel im Internet vorbereitet. Jeder kann nach Informationen dieser fiktiven Person selbst suchen und das Profil verifizieren. Es geht um folgende Person:

Name: Fiona Flauderer
geboren: 17.06.1995
E-Mail: fiona.flauderer@gmail.com
Status: Studentin
Anschrift: Dorthenstr. 17, 10995 Berlin

Diese Informationen könnte ein Personalchef einer Bewerbung entnehmen oder sie sind der Krankenkasse bekannt oder sie ist bei einer Demo aufgefallen… Eine kurze Suche bei Google und verschiedenen Personensuchmaschinen liefert nur sehr wenige Treffer, im Moment sind es 3 Treffer. Gleich wieder aufgeben?

Die moderne Studentin ist sozial vernetzt. Naheliegend ist es, die verschiedenen Netzwerke wie StudiVZ usw. nach F. abzusuchen. Bei Facebook wird man erstmals fündig. Es gibt ein Profil zu dieser Person mit Fotos, Interessen und (wichtig!) eine neue E-Mail Adresse:

goegr17@gmail.com

Bezieht man diese Adresse in die Suche bei anderen Sozialen Netzwerken mit ein, wird man bei MySpace.com erneut fündig. Hier gibt es ein Profil mit dieser E-Mail Adresse und man findet den Twitter-Account von F. sowie ein weiteres Pseudonym:

flaudi85

Mit den beiden gefundenen Pseudonymen g.....17 und f.....85 kann man erneut bei Google suchen und die Ergebnisse mit den Informationen aus den Profilen zusammenfassen.

• g.....17 ist offenbar depressiv. Das verordnete Medikament deutet auf Angstzustände hin, wurde von der Patientin nicht genommen sondern ins Klo geworfen.

• Sie hat Probleme im Studium und will sich krankschreiben lassen, um an Prüfungen nicht teilnehmen zu müssen.

• Außerdem hat sie ein massives Alkoholproblem und beteiligt sich am Syncron-Saufen im Internet. Scheinbar ist sie auch vereinsamt.

• F. ist offenbar lesbisch, sie sucht nach einer Frau bei abgefuckt.de.

8http://www.zeit.de/digital/datenschutz/2010-01/identitaetsdiebstahl-selbsterfahrung
9https://www.zeit.de/digital/datenschutz/2009-09/indect-ueberwachung
• F. ist im linksradikalen Spektrum aktiv. Sie hat an mehreren Demonstrationen teilgenommen und berichtet über Erfahrungen mit Hausdurchsuchungen. Möglicherweise ist das die Ursache für ihre Angstzustände.

• Öffentlich prangert sie in einem Diskussionsforum die Firma ihres Vaters an (wegen Ausspionierens von Mitarbeitern).

• Ihre linksgerichtete Grundhaltung wird durch öffentliche Unterstützung der Kampagne *Laut ficken gegen Rechts* unterstrichen.

• Von regelmäßiger Arbeit hält sie nicht viel.

• Die angebene Adresse ist falsch. F. wohnt in einer 11-Personen-WG in einem besetzten Haus in Alt-Moabit. Die WG sucht nach einem neuem Mitglied.

• Die Wunschliste bei Amazon und Fotos bei Flickr…

Würden sie als Personalchef diese fiktive Person einstellen?

Welche Ansatzpunkte ergäben sich für den Verfassungsschutz?

Was könnte zukünftig für die Krankenkasse interessant sein?

Was hätte F. tun können, um die Profilbildung zu vermeiden?

### 3.3 Schattenseiten der Anonymität

Auf den ersten Blick scheint Anonymität eine Lösung für fast alle beschriebenen Probleme zu sein. Anonymität verhindert das Tracking durch kommerzielle Datensammler, schützt die Privatsphäre vor neugierigen Blicken der Spanner, schränkt die Überwachungsmöglichkeiten der Geheimdienste ein, bietet Whistleblower Schutz....


Ein anonymer Schwarm vereinzelter Individuen kann sich zu einem Shitstorm zusammenfinden. Der Schwarm kann kurzzeitig viel Lärm produzieren ohne gesellschaftlichen
Diskurs und wird dann wieder zerfallen. Er wird kein Wir! entwickeln und kann keine gemeinsamen Ziele verfolgen, die über einen kurzzeitigen Hype in den Medien hinausgehen. Außerdem lassen sich Empörungswellen durch eine kritische Masse anonymer Sockenpuppen leicht manipulieren.

Ein Beispiel für den Konflikt zwischen Anonymität und Vertrauen:

1. Ich kann mir ganz anonym in meiner Einsiedlerzelle mit einem Anonymisierungsdienst bei YouPorn, RedTube, XHamster....

2. Oder ich kann eine Frau im Arm halten, die sich sehnsuchtsvoll an mich drängt, ihre Haut spüren, das gegenseitige Begehren fühlen und eintauchen in einen Strudel der ....

Bei Variante 1) bleibt meine Anonymität gewahrt aber sie hinterlässt gähnende Leere und Einsamkeit. Variante 2) funktioniert nur mit gegenseitigem Vertrauen und Respekt. Um die Liebesbriefe in 2. gegen mitlesende, sabbernde Schlapphüte zu schützen, ist jedes Mittel zulässig, aber Kryptografie, TorBrowser, JonDonym usw. sind nur Werkzeuge und kein Selbstzweck.

Für ein soziales Zusammenleben und gemeinsame Ziele brauchen wir Vertrauen. Vertrauen kann missbraucht werden, man muss es nicht leichtfertig verschenken. Es ist aber wichtig, bei aller gebotenen Vorsicht, auch einen Weg zu finden, um gegenseitiges Vertrauen aufzubauen.


3.4 Wirkungsvoller Einsatz von Kryptografie

Nach einer anerkannten Faustregel ist der wirkungsvolle Einsatz von Kryptografie von folgenden allgemeinen Faktoren abhängig:

- zu 10% hängt der Schutz von der eingesetzten Technik ab
- zu 60% beeinflusst das Wissen der Anwender über Möglichkeiten und Grenzen den wirkungsvollen Einsatz kryptografischer Verfahren
- zu 30% hängt die Wirksamkeit von der Disziplin der Anwender ab


Beispiel: wenn man einem Bekannten eine verschlüsselte E-Mail mit einem Link zu der Sammlung von Urlaubsfotos bei Facebook schickt, dann gibt es keine Privatsphäre, die durch die Verschlüsselung der E-Mail geschützt werden könnte.
2. Wenn man einen Bereich gefunden oder festgelegt hat, den man gegen Datensammler und Überwachung schützen möchte, dann sollte die technische Umsetzung des Schutzes vollständig und umfassend sein. Es ist nur wenig nachhaltig, wenn man gelegentlich eine verschlüsselte E-Mail schreibt und gleichzeitig zwei unverschlüsselte E-Mails mit dem gleichen Inhalt an anderer Empfänger (mit Google Accounts?) schickt.

- Studien haben nachgewiesen, dass es ausreichend ist, in einer organisierten Gruppe nur 10-20% der Mitglieder zu überwachen, um über die Struktur der Gruppe und ihre wesentlichen Aktivitäten informiert zu sein.
- Wenn man Anonymisierungsdienste zur Verwaltung von E-Mail Konten, für ein anonymes Blog, für digitale Identitäten oder zur Recherche zu sensiblen Themen nutzt, dann muss man sie in diesem Kontext immer nutzen. Anderenfalls könnten die Aktivitäten aus der Vergangenheit nachträglich deanonymisiert werden und für die Zukunft ist die Anonymität in diesem Kontext nicht mehr gegeben.
- Schützenswerte, private Daten (was das ist, muss man selbst definieren) sollten immer verschlüsselt gespeichert und transportiert werden. Das betrifft nicht nur die Speicherung auf dem eigenen Rechner sondern auch alle Backups und jede Kopie bei Dritten. Wer private Dateien ohne zusätzliche Verschlüsselung via Skype verschickt, sollte sich darüber klar sein, dass Microsoft immer mitliest.


3. Die meisten Protokolle zur verschlüsselften Kommunikation verwenden Public Key Verfahren (SSL/TLS, OpenPGP, OTR, SSH). Wenn man für hohe Anforderungen wirklich sicher sein will, dass nur der Kommunikationspartner (oder der Server bei SSL) die gesendeten Daten entschlüsseln kann, dann muss man den öffentliche Schlüssel der Gegenseite über einen sicheren, unabhängigen Kanal verifizieren.


Krypto-Messenger wie Signal App, Matrix/Riot oder Threema bieten die Möglichkeit, die Schlüssel des Gegenübers anhand der Fingerprints zu verifizieren und unterstützen diese Verifikation bei persönlichen Treffen durch QR-Codes, die man gegenseitig scannen kann ohne lange Zahlenkolonnen vergleichen zu müssen.

Alternativ könnte man sich den öffentlichen Schlüssel von vertrauenswürdigen Dritten beglaubigen lassen. Wenn man einen vertrauenswürdigen(!) Dritten findet, der die Identität der Inhaber der kryptografischen Schlüssel wirklich geprüft hat.)

- OpenPGP bietet dafür das Web of Trust, dass die meisten Nutzer nicht ganz verstanden haben und das in der Praxis kaum eine Rolle spielt.
Mit DANE/TLSA gibt es einen Ansatz, die SSL-Zertifikate auf einem kryptografisch gesicherten, unabhängigen Weg zu verifizieren. Leider verbreitet es sich nur langsam und wird von den meisten Programmen (noch?) nicht unterstützt.
Kapitel 4

Spurenarm Surfen

Es gibt noch immer einige Zeitgenossen, für die Privatsphäre ein wichtiges Thema ist und die sich nicht ständig über die Schulter schauen lassen wollen beim Lesen von News, beim Kaufen von Theaterkarten oder beim Entspannen auf irgendwelchen You-Dingends Seiten.

In diesem Kapitel soll das Thema **spurenarmes Surfen** behandelt werden. Zur Abgrenzung und zur Vermeidung von Missverständnissen ist es nötig, die Zielstellung zu klären:

**Spurenarmes Surfen** ist in erster Linie ein Schutzkonzept gegen das allgegenwärtige Tracking und Beobachten zur Erstellung von umfassenden Persönlichkeitsprofilen, die dann zur gezielten Manipulation der betroffenen Person missbraucht werden können. Anonymität (z. B. für Risikogruppen wie Whistleblower) steht dabei nicht im Fokus.

Schutz gegen Tracking erreicht man durch mehrere Maßnahmen:

- Datensammelnden Dienste kann man meiden und Trackingelemente wie Werbeanzeigen, anti-soziale Like-Buttons, JavaScript Trackingcode oder HTML-Wanzen werden blockiert.
- Langfristige Markierungen für das Tracking (Cookies, EverCookies) werden gelöscht oder eingesperrt.
- Features deaktivieren, die sich für Browserfingerprinting eignen.
- …


Durch starke Anonymisierung ist ein Tracking von einzelnen Individuen zur Erstellung von Persönlichkeitsprofilen natürlich auch unmöglich, ein positiver Nebenefekt.

**Sicher Surfen** stellt den Schutz des eigenen Rechners und der lokalen Daten gegenüber Angriffen aus dem Internet in den Mittelpunkt.

- Wichtigste Punkt sind regelmäßige Updates von Browser und OS.
- Überflüssige Features deaktivieren, um die Angriffsfläche gering zu halten.
4.1 Auswahl des Webbrowsers

Firefox ist der Webbrowser der Mozilla Foundation. Er ist kostenfrei nutzbar und steht auf der Website des Projektes ² für Windows, MacOS und Linux zum Download bereit.

Die Extented Support Releases ³ (ESR-Versionen) von Firefox werden im Gegensatz zu den 4-wöchigen Updates des Firefox für ca. ein Jahr gepflegt. Es werden keine neuen Features eingebaut, was sich positiv auf die Stabilität auswirkt. Allerdings fehlen damit aktuelle Verbesserungen und neue Features.

Linux-Distributionen enthalten den Browser in der Regel. Man kann den Browser mit der Paketverwaltung installieren:

**Debian GNU/Linux, RedHat** enthalten den Firefox-ESR. Der Browser wird aus den Repositories mit folgenden Kommandos installiert:

Debian: `> sudo apt install firefox-esr firefox-esr-l10n-de`
RedHat: `> sudo yum install firefox`

**Fedora, Ubuntu** und Derivate bringen den aktuellen Firefox mit, den man mit folgenden Kommandos installiert, wenn er nicht bei der Installtion des OS installiert wurde:

Ubuntu: `> sudo apt install firefox firefox-locale-de`
Fedora: `> sudo dnf install firefox`

Für Ubuntu LTS (16.04 und 18.04) gibt es zwei PPA-Repositories mit Firefox ESR:

1. Das Mozilla Team stellt einen Firefox ESR in folgendem PPA bereit: ⁴
   `> sudo add-apt-repository ppa:mozillateam/firefox-esr`
   `> sudo apt update`
   `> sudo apt install firefox-esr`

2. Außerdem gibt es eine Portierung des Firefox ESR von Debian: ⁵

---

¹ https://heise.de/-3734142
⁴ https://launchpad.net/mozillateam/+archive/ubuntu/ppa
⁵ https://launchpad.net/jonathon/+archive/ubuntu/firefox-esr

Einige Distributionen wie Ubuntu und davon abgeleitete Derivate bringen ein Apparmor Profil für Firefox mit. Das Paket apparmor-profiles muss installiert und die Regeln für Firefox sind zu enforcen:

```bash
> sudo apt install apparmor-profiles apparmor-utils
> sudo aa-enforce usr.bin.firefox
```

Mit `sudo aa-status` kann man prüfen, ob Firefox im enforced mode unter Kontrolle von apparmor läuft, nachdem der Browser neu gestartet wurde.

Freunde von *BSD finden Firefox und Firefox ESR in pkgsrc und können die jeweils aktuelle Version mit dem üblichen Dreisatz selbst compilieren.

**Schnellkonfiguration für einen privacy-freundlichen Firefox**

Wer sich nicht mit den Details beschäftigen möchte, kann diese Anleitung zur Schnellkonfiguration nutzen, um Firefox privacy-freundlich zu konfigurieren. Das Kapitel Spurenarm Surfen mit den ausführlichen Erläuterungen könnte man überspringen und im nächsten Kapitel weiterlesen.

Empfehlung für Firefox 78+:


- Das Add-on CanvasBlocker kann Zugriffe auf Canvas-API, Screen-API und Audio-API faken (geringfügig modifizieren) um ein Fingerprinting des Browsers zu verhindern. Als Einstellungen sind die vorbereiteten Stealth Settings empfehlenswert.

- Das Add-on Skip Redirect entfernt Umleitungen in der URL. Diese Umleitungen werden häufig genutzt, um die Klicks auf Links zu externen Domains zu tracken. Hinweis: Für WiFi Hotspot Logins muss man das Add-on deaktivieren.

- Das Add-on Neat URL entfernt bekannte Tracking Parameter von Google Analytics, Facebook, Youtube und anderen Trackern aus der URL.

- Außerdem sind weiteren Einstellungen in der Konfiguration privacy-freundlich zu setzen. Um die Werte nicht alle einzeln setzen zu müssen, kann man die minimale user.js, die moderate user.js oder strenge user.js Konfiguration von der Webseite herunterladen und im Browserprofil speichern. Beim Start überschreiben die Werte der user.js die Preferenzen.6

- Das Add-on NoScript ist für höhere Sicherheitsanforderungen in Kombination mit der strenge user.js empfehlenswert. Das Add-on kann Freigaben für Javascript und anderen Content detailliert verwalten. Außerdem enthält es eine XSS-Protection.

6https://www.privacy-handbuch.de/handbuch_21u.htm
Optional: Außerdem gibt es noch Add-ons, die für die Privatsphäre nicht relevant aber trotzdem sinnvoll sein könnten und die gefahrlos installiert werden können:

Das Add-on **Binnen-I be gone** ersetzt ideologisch motivierte Sprachverhunzungen in Texten durch das generische Maskulin. Wer beim Lesen von Konstrukten wie **InfluencerInnen** oder **Verbrecher:innen** oder **Politiker*innen** immer genervt ins Stolpern kommt und sich fragt, wie man das jetzt aussprechen müsste, wird es mögen.

(Ein Tipp für alle, die sich politisch korrekt ausdrücken wollen: Der Duden gibt Hinweise zum sprachlich korrekten Gendern und diese Verballhornungen gehören amtlich nicht dazu. Sprache muss man sprechen können. Die Verwendung von Binnen-Is ist kein amtlich korrektes Deutsch und demonstriert ideologische Verblendung.)

Um die Installation von privacy-freundlichen **Suchmaschinen** zu vereinfachen, sind einige Such-Plugins vorbereitet. Wenn man auf die Webseite https://www.privacy-handbuch.de/handbuch_21browser.htm aufruft, kann man mit einem Klick auf die drei Punkte in der URL Zeile klicken und in dem ausklappenden Menü die gewünschten Suchmaschinen hinzufügen. Das funktioniert auch auf den Webseiten der Suchmaschinen.

Abbildung 4.1: Suchmaschinen hinzufügen

### 4.2 Datensparsame Suchmaschinen

Suchmaschinen werden am häufigsten genutzt, um sich im Web zu orientieren. Neben den bekannten Datensammlern wie Google, Bing oder Yahoo! gibt es auch Alternativen.

Für alle alternativen Suchmaschinen gilt, dass sie eine andere Sicht auf das Web bieten und die Ergebnisse sich von Google unterscheiden. Man sollte bei der Beurteilung der Ergebnisse beachten, dass auch Google nicht die reine Wahrheit bieten kann, sondern nur eine bestimmte Sicht auf das Web.

Es ist nicht einfach, eine Suchmaschine aufzubauen, die die Privatsphäre der Nutzer respektiert, einen umfangreichen Index zur Verfügung stellt und gute Ergebnisse liefert. Zwei Alternativen zur Google Suche:

**Qwant** ([https://www.qwant.com](https://www.qwant.com))


**DuckDuckGo.com** ([https://duckduckgo.com](https://duckduckgo.com))

DuckDuckGo ist eine privacyfreundliche Suchmaschine. Es gibt eine JavaScript-freie Version (HTML), aber die Ergebnisse der JavaScript Version sind irgendwie besser. Neben der eigentlichen Suche bietet DuckDuckGo viele nette Erweiterungen. Das
Suchfeld kann als Taschenrechner genutzt werden oder zum Umrechnen von Einheiten, Fragen nach dem Wetter können beantwortet werden (in englisch: *weather* oder *is it raining*).

Meta-Suchmaschinen leiten die Suchanfrage an eine oder mehrere Suchmaschinen weiter. Sie sammeln die Ergebnisse ein und sortieren sie neu. Außerdem schützen sie die Privatsphäre der Nutzer, indem sie die Identität der Nutzer gegenüber den angefragten Suchmaschinen verbergen, da sie als Proxy agieren.

**Startpage** ([https://startpage.com](https://startpage.com)) bietet privacy-freundlichen Zugriff auf die Google-Suche. Dabei werden eindeutig identifizierende Informationen über den Surfer entfernt. Um Missbrauch zu verhindern und Werbung von Google Adwords einzublenden, werden aber einige Informationen über den Browser an Google weitergegeben, siehe Privacy Policy:


Bei Startpage ist standardmäßig ein Family-Filter aktiv. Wer etwas Anstößiges sucht, erhält keinen Hinweis auf den Filter sondern nur:

> Es wurden keine mit Ihrer Suchanfrage übereinstimmende Dokumente gefunden.

Das Mycroft Project bietet ein Such-Plugin mit ungefilterten Suchergebnissen, das auch Ergebnisse für die Suche nach *Dildos* anzeigt. In den Einstellungen kann man den Filter auch deaktivieren.


Metager finanziert sich ebenfalls aus Werbung. Um die Relevanz der Werbeanzeigen etwas zu verbessern, werden Informationen aus der User-Agent-Kennung des Browsers und die ersten beiden Blöcke der IP-Adresse des Surfers zusammen mit der Suchanfrage an die Werbepartner weitergegeben.

Metager bietet wie Startpage einen Proxy, um Ergebnisse aus der Suchliste anonym aufzurufen. Die Server stehen in Deutschland.

Spezielle Anwendungsfälle

- Wikipedia kann man auch ohne Umweg über Google direkt fragen, wenn man Informationen sucht, die in einer Enzyklopädie zu finden sind.
- Statt Google übersetzen zu lassen, kann man LEO\textsuperscript{7} oder DeepL\textsuperscript{8} nutzen. Die Translator kennen neben Englisch und Deutsch weitere Sprachen.

Peer-2-Peer Suchmaschine

Yacy\textsuperscript{9} ist eine zensurresistente Peer-2-Peer Suchmaschine. Jeder kann sich am Aufbau des Index beteiligen und die Software auf seinem Rechner installieren. Der Crawler ist in Java geschrieben, benötigt also eine Java- Runtime (JRE), die es für WINDOWS bei Oracle\textsuperscript{10} zum kostenlosen Download gibt. Linuxer können das Paket default-jre mit der Softwareverwaltung installieren. Danach holt man sich die Yacy-Software von der Website des Projektes und startet den Installer - fertig. Für Debian, Ubuntu und Linux Mint bietet das Projekt ein Repository\textsuperscript{11} mit fertigen Paketen.


Die Beantwortung der Suchanfragen dauert mit 5-10sec ungewohnt lange. Außerdem muss JavaScript für \url{http://localhost} freigegeben werden, damit die Ergebnisse sauber dargestellt wird. Mit den Topwords unter den Ergebnissen bietet Yacy ein Konzept, um die Suchanfrage zu präzisieren.

Google ???


\textbf{Tracking der Klicks auf Suchergebnisse:} Bei Klick auf einen Link in den Suchergebnissen wird die Ziel-URL umgeschrieben. Aus der für den Surfer sichtbaren Zieladresse

\url{https://www.privacy-handbuch.de/index.htm}

wird im Moment des Klick eine Google-URL:

\url{https://www.google.de/url?q=https://www.privacy-handbuch.de/......}

Die zwischengeschaltete Seite enthält eine 302-Weiterleitung auf die ursprüngliche Ziel-URL. Der Surfer wird also fast unbemerkt über einen Google-Server geleitet, wo der Klick registriert wird. Bei deaktiviertem JavaScript ist stets die Google-URL sichtbar, nicht die Zieladresse.

\textsuperscript{7}\url{https://dict.leo.org}
\textsuperscript{8}\url{https://www.deepl.com/translator}
\textsuperscript{9}\url{http://yacy.net}
\textsuperscript{10}\url{https://java.com/de}
\textsuperscript{11}\url{https://wiki.yacy.net/index.php/De:DebianInstall}
Diese Umschreibung der Links gibt es auch bei Bing, Facebook, Youtube und anderen Datensammlern. Das Firefox Add-on **Skip Redirect** entfernt diese Umleitungen. Es ist natürlich besser, eine privacyfreundliche Suchmaschine zu nutzen statt Google.

**Browser Fingerprinting:** Mittels JavaScript wird die innere Größe des Browserfensters ermittelt. Folgenden Code findet man in den Scripten:

```javascript
I[ch].oc= function() {
  var a=0, b=0;
  self.innerHeight?(a=self.innerWidth, b=self.innerHeight):....;
  return {width:a, height:b}
};
```

Die ermittelten Werte werden als Parameter `biw` und `bih` in der Google-URL übergeben. Sie haben aber keinen Einfluss auf die Bildschirmdarstellung. Auch wenn das Browserfenster zu klein ist und die Darstellung nicht passt, bleibt die Größe der HTML-Elemente erhalten.


Auf der Webseite der Google-Suche kann man dem Tracking kaum entgehen. Wer unbedingt die Ergebnisse von Google braucht, kann die Suchmaschine **Startpage.com** als anonymisierenden Proxy nutzen. Andere Suchmaschinen bieten eine andere Sicht auf das Netz - auch nicht schlecht, erfordern aber etwas Umgewöhnung.

**Firefox konfigurieren**

Die Suchmaschinen kann man in den **Einstellungen** in der Sektion **Suche** konfigurieren.

Die standardmäßig im Firefox installierten Suchmaschinen verraten überflüssige Informationen über die Installation. Wenn man z. B. unter Ubuntu den Firefox aus dem Repository nutzt, wird bei jeder Suchanfrage irgendwie ein Hinweis auf Ubuntu angehängt:

- `https://www.google.de/search?...&client=ubuntu`
- `https://duckduckgo.com/?...&t=canonical`
- `http://www.amazon.com/s?...&tag=wwwcanonicom-20`

Nimmt man den offiziellen Firefox für Windows von der Mozilla Downloadseite, dann werden folgende Informationen angehängt:

- `https://www.google.de/search?...&rls=org.mozilla:de:official`
- `http://www.amazon.com/s?...&tag=firefox-de-21`


---

12 [https://mycroft.mozdev.org/]
4.2. DATENSPARSAME SUCHMASCHINEN

Abbildung 4.2: Suchmaschinen verwalten


Die Standardsuchmaschine wird an mehreren Stellen von Firefox ohne weitere Nachfrage genutzt. Es sollte eine privacy-freundliche Suche ausgewählt werden.


URL-Leiste mit extra Suchfeld


Um die Anzeige von Vorschlägen bei Eingabe einer URL etwas zu reduzieren, kann man die Suchfunktion bei URL Eingabe abschalten (wenn man suchen will, dann verwend- det man das Suchfeld). Wenn die Anzeige von Suchvorschlägen aktiv ist, wird jede Tasteneingabe bei Eingabe einer URL an die gewählte Standardsuchmaschine gesendet. Das
möchte man nicht unbedingt, daher ist dieser Parameter relevant für die Privatspäre.

```javascript
browser.urlbar.suggest.searches = false
```

Wer nicht mit Vorschlägen belästigt werden möchte, kann weitere Werte deaktivieren, beispielsweise die Vorschläge aus den geöffneten Seiten deaktivieren oder Lesezeichen, da man auf diese Quelle direkt zugreifen kann, wenn man möchte.

```javascript
browser.urlbar.suggest.openpage = false
browser.urlbar.suggest.bookmark = false
browser.urlbar.suggest.history = false
```

Außerdem kann man die Anzeige der Suchmaschinen bei URL Eingabe abschalten:

```javascript
browser.urlbar.oneOffSearches = false
```

GeoIP-spezifische Standardsuche deaktivieren (FF78)


Um festzustellen, ob es sich um einen US-amerikanischen Nutzer handelt, kontaktiert den Firefox beim Start den Server `location.services.mozilla.com`, um anhand der IP-Adresse entscheiden zu können, welche Suchmaschine genutzt werden soll. Dabei werden neben der Firefox Version auch die Lokalisierung, der Update Kanal und die Distribution übertragen. Um diese überflüssige Verbindungsaufnahme zu unterbinden, kann man unter der Adresse `about:config` folgende Variablen setzen:

```javascript
browser.search.geoSpecificDefaults = false
browser.search.geoip.url = "" (leerer String)
```

### 4.3 Cookies und EverCookies

Cookies werden für die Identifizierung des Surfers genutzt. Neben der erwünschten Identifizierung um personalisierte Inhalte zu nutzen, beispielsweise einen Web-Mail-Account oder um Einkäufe abzuwickeln, werden sie für das Tracking von Surfern verwendet.


Immer mehr Trackingdienste gehen dazu über, die Cookies im First-Party Context zu setzen, da Cookies von Drittseiten einfach blockierbar sind.

- Eine empirische Studie der Universität Leuven von 2014 zeigte, dass damals bereits 44 Tracking Dienste mehr als 40% des Surferverhaltens auch dann verfolgen konnten, wenn man Cookies für Drittseiten blockierte und nur First-Party Cookies erlaubt.

Ein Beispiel ist der Trackingdienst WebTrekk, der sich auf Webseiten wie `heise.de`, `zeit.de` oder `zalando.de` mit DNS-Aliases als Subdomain der überwachten Webseite First-Party Status erschließt, um seine Tracking Cookies zu setzen.

---

13. [http://heise.de/-1288914](http://heise.de/-1288914)
4.3. COOKIES UND EVERCOOKIEs

Abbildung 4.3: Liste der Cookies beim Besuch von Spiegel-Online
• Google kombiniert seit 2017 den Dienst Analytics mit dem AdWords Tracking, um den Trackingschutz von Apples Browser Safari zu umgehen. Für Google Analytics bindet der Webmaster Trackingcode direkt auf der Webseite ein, der damit First-Party Status erhält und die Cookies für das AdWords Tracking setzt.\textsuperscript{16}

• Microsofts folgte im Januar 2018 und hat eine Lösung umgesetzt, die das Cookie mit der Microsoft Click ID für das Conversation Tracking im First-Party Context setzt. Die Microsoft Tracking ID wird als URL-Parameter übertragen und dann von einem JavaScriptchen in ein Cookie geschrieben.\textsuperscript{17}

• Facebook folgte den Beispiel von Google und Microsoft im Herbst 2018, nachdem Mozilla angekündigt hat, nach dem Vorbild von Safari das Tracking via Third-Party Cookies in Firefox zu erschweren. Wie bei Microsoft wird die Tracking ID in URL-Parametern übertragen und dann mit Javascript in First-Party Cookies geschrieben.\textsuperscript{18}


EverCookies - never forget

Als EverCookies bezeichnet man den Missbrauch unterschiedlicher Webtechniken zur Markierung von Surfern für Trackingzwecke. Es werden eindeutige Markierungen im HTML5 Storage oder in die IndexedDB geschrieben, ETags für das Cache Management können Tracking-IDs enthalten, TLS Session und HSTS können für das Tracking missbraucht werden u.a.m.

• Nach empirischen Untersuchungen der University of California nutzten 2012 bereits 38% der TOP100 Webseiten verschiedene EverCookies zur Markierung der Surfer.

• Laut Web Privacy Census 2015 wurden drei Jahre später EverCookie Techniken von 76% der TOP100 Webseiten zum Tracking eingesetzt.

1: Schutz gegen Website-übergreifendes Tracking

Gegen Tracking mit Cookies und EverCookies über mehrere Websites bzw. Domains schützen Surf-Container. Es wird für jede Domain in der URL-Leiste gemäß Same-Origin-Policy automatisch ein neuer Surf-Container erstellt und alle Daten werden abgeschottet in diesem individuellen Context gespeichert. Für unterschiedliche Website ergeben sich damit unterschiedliche Tracking-IDs in Cookies, HTML5 Storage, unterschiedliche ETags im Cache und TLS Sessions...

• Für Firefox 78.x ESR kann man FirstParty.Isolate verwenden:

```
privacy.firstparty.isolate = true
privacy.firstparty.isolate.block_post_message = true
network.cookie.cookieBehavior = 4
```

• Für Firefox 85+ kann man das neu überarbeitete Konzept aus den beiden Komponenten Netzwerk Partitionierung und Total Cookie Protection verwenden.

\textsuperscript{16}https://www.heise.de/-3859526
\textsuperscript{18}https://marketingland.com/facebook-to-release-first-party-pixel-for-ads-web-analytics-from-browsers-like-safari-249478
1. **Die Netzwerk Partitionierung** isoliert alle Cache Speicher (HTTP, Bilder, Fonts…), SSL Session IDs, HSTS, OCSP, DNS… in getrennten Containern für jede First-Party Domain und ist seit Firefox 85.0 standardmäßig aktiv, wenn man FirstParty.Isolate deaktiviert:

   ```
   privacy.firstparty.isolate = false
   privacy.partition.network_state = true
   ```

2. **Total Cookie Protection** ist das Konzept zur Isolation von Cookies, Third-Party Cookies, DOMStorage und IndexDB in getrennten Containern für jede First-Party Domain. Dieses Feature kann man unter `about:config` mit folgender Einstellung aktivieren:

   ```
   network.cookie.cookieBehavior = 5
   ```

2. **Schutz gegen langfristiges Tracking**

   Langfristiges Tracking verhindert man mit dem Löschen der Daten beim Schließen.

   ```
   network.cookie.lifetimePolicy = 2
   privacy.history.custom = true
   privacy.sanitize.sanitizeOnShutdown = true
   privacy.clearOnShutdown.cache = true
   privacy.clearOnShutdown.cookies = true
   privacy.clearOnShutdown.downloads = true
   privacy.clearOnShutdown.formdata = true
   privacy.clearOnShutdown.history = true
   privacy.clearOnShutdown.offlineApps = true
   privacy.clearOnShutdown.sessions = true
   privacy.clearOnShutdown.siteSettings = true
   ```


3. **Schutz gegen Redirect Tracking**

   Beim Redirect Tracking wird der Surfer bei Klick auf einen Link nicht direkt von der Webseite A zur Webseite geleitet (A -> B) sondern von der Webseite A zur Zwischenstation T geschickt, die den Besucher mit Trackingelementen im First-Party Context markiert und dann automatisch zur gewünschten Webseite B weiterleitet (A -> T -> B). Der Redirect wird vom Surfer in der Regel kaum bemerkt.

   Das Add-on **Skip Redirect** kann diese Tracking Umleitungen in URLs entfernen, wenn sie nicht kodiert wurden. (Für WiFi Hotspot Logins muss man das Add-on deaktivieren.)

KAPITEL 4. SPURENARM SURFEN

Cookie-Management mit zusätzlichen Add-ons

Zusätzliche Add-ons wie CookieAutoDelete oder CookieController tun in der Regel das, was der Name vermuten lässt. Sie löschen oder verwalten Cookies automatisch, die nicht mehr gebraucht werden oder nach vorgegeben Regeln (und machen um jedes gelöschten Cookies viel Getöse).

Das einfache Löschen von Cookies schützt nur wenig gegen Tracking. Trackingdienste verwenden EverCookies, um gelöschte Tracking Cookies wiederherzustellen. Diese Add-ons erfüllen ihre Aufgabe, bieten aber hinsichtlich Trackingschutz kaum Verbesserungen.

4.4 Surf-Container

Surf-Container sind ein Konzept von TorProject.org und Mozilla, um Website-übergreifendes Tracking mit Cookies und EverCookie Techniken zu verhindern.

- Ein Surf-Container enthält alle Daten, die von Webseiten gespeichert wurden, in einer abgeschotteten Umgebung (Cookies, HTML5-Storage, IndexedDB, Cache, TLS Sessions, Shared Workers, HTTP Authentication... usw.) Diese Daten bilden dann den sogenannten Context für das Surfen in diesem abgeschotteten Container.


Aber: Surf-Container schützen nicht gegen Tracking anhand des Browser Fingerprint! Da das gleiche Browser Profil mit identischer Konfiguration und Add-ons genutzt wird und außerdem die IP-Adresse identisch ist, können viele Trackingdienste eine Verknüpfung des Surfverhaltens in unterschiedlichen Containern herstellen!

Konzepte für Surf-Container in Firefox

Mozilla hat mehrere Konzepte für Surf-Container in Firefox implementiert:

1. FirstParty.Isolate wurde für den TorBrowser unter dem Titel Cross-Origin Identifier Unlinkability entwickelt und ist mit Firefox 58+ auch von Mozilla implementiert worden. Das Feature kann man unter about:config mit folgendem Wert aktivieren:

   privacy.firstparty.isolate = true

Damit wird für jede Domain in der URL-Leiste gemäß Same-Origin-Policy automatisch ein neuer Surf-Container erstellt und alle Daten werden in einem individuellen Context gespeichert. Tracking über Webseiten mit (Ever-)Cookies ist nicht möglich. Webseiten können die Javascript API windows.postMessage verwenden, um Daten zwischen unterschiedlichen Domains auszutauschen, die in verschiedenen Containern gekapselt sind. Um diese Lücke zu schließen, muss man unter about:config folgenden Wert setzen:

   privacy.firstparty.isolate.block_post_message = true

FirstParty.Isolate kann zu Login Problemen bei einigen Websites führen, die Single Sign-on (SSO) Techniken nutzen. Betroffen sind beispielsweise fast alle Google Dienste, SoundCloud u.a.m. die einen Google Account für die Anmeldung verwenden. Bei diesen Login Problemen kann man mit folgender Option den Schutz aufweichen:

   privacy.firstparty.isolate.restrict_opener_access = false

2. Basierend auf den Erfahrungen mit FirstParty.Isolate hat Mozilla das Konzept überarbeitet und komplett neu implementiert. Dabei wurde der Schutz in zwei Komponenten aufgeteilt:

- **Netzwerk Partitionierung** isoliert alle Cache Speicher (HTTP, Bilder, Fonts), SSL Sessions, HSTS, OCSP, DNS… in getrennten Containern für jede First-Party Domain. Damit wird verhindert, das Trackingdienste diese Techniken, die nicht zur Speicherung von Daten vorgesehen sind, für die Markierung mit EverCookies missbrauchen können. Seit Firefox 85.0 ist die Netzwerk Partitionierung standardmäßig aktiviert:

  ```plaintext
  privacy.partition.network_state = true
  ```

- **Total Cookie Protection** ist das Konzept zur Isolation von Cookies, Third-Party Cookies, DOMStorage und IndexDB in getrennten Containern für jede First-Party Domain. Dieses Feature kann man mit folgender Einstellung aktivieren:

  ```plaintext
  network.cookie.cookieBehavior = 5
  ```


3. **userContext** steht seit Firefox 50+ zur Verfügung. Es werden mehrere Surf-Container bereitgestellt, die man selbst aktiv auswählen muss. Um das Feature zu aktivieren, muss man zuerst unter der Adresse about:config folgende Werte setzen:

  ```plaintext
  privacy.userContext.enabled = true
  privacy.userContext.ui.enabled = true
  ```

  Die Freigaben für den Zugriff auf Mikrofon, Kamera, Geolocation oder Webnotification können ebenfalls im userContext gekapselt werden und gelten dann nur, wenn die Webseite in einem spezifischen Context aufgerufen wird. Dafür ist folgende Variable unter der Adresse about:config zu aktivieren:

  ```plaintext
  permissions.isolateBy.userContext = true
  ```


## 4.5 JavaScript

JavaScript ist eine der Kerntechniken des modernen Internet, birgt aber auch einige Sicherheitsrisiken.

2. EverCookie Techniken nutzen JavaScript, um Markierungen im Browser zu hinterlegen und gelöschte Tracking Cookies wiederherzustellen.


**Prinzip Whitelisting**


**4.5.1 NoScript für Mozilla Firefox**

Mit dem Add-on NoScript kann man nicht nur Einstellungen für JavaScript verwalten sondern auch für Flash- und Silverlight Objekte, Frames, Fonts, WebGL u.a.


Vertrauenswürdige Webseiten (Trusted) dürfen JavaScript ausführen (Option script), das reicht in der Regel. iFrames kann man mit NoScript oder uBlock Origin blockieren (s.u.), ich habe mich für NoScript entschieden. Wenn eine Webseite unbedingt Frames oder WebGL benötigt, dann kann man individuelle Konfigurationen für diese Webseiten

---

4.5. JAVASCRIPT

definieren. Als *Untrusted* definierte Webseiten dürfen nichts.

Wer es lieber ein bisschen komfortabler und weniger restrikiv mag, der kann die Option *Temporary set top-level sites to TRUSTED* aktivieren. Dann darf die aufgerufene Webseite immer ihre Scripte ausführen. Es werden nur Drittseite blockiert, die oft Trackingscripte enthalten. Viele Webseiten funktionieren damit problemlos.

Auf dem Reiter *Per-site Permissions* kann man die Freigaben für einzelne Webseiten verwalten. NoScript bringt eine Menge Freigaben standardmäßig mit, die man erstmal ausmisten kann. Google braucht man nicht, wenn man keine Google Dienste verwendet und Microsofts Live und Passport auch nicht.

Abbildung 4.4: Per-site Permissions in der NoScript Konfiguration

Ein grünes Schloss bedeutet in den *Per-site Permissions*, dass die Freigabe nur für HTTPS gilt (sicherer). Wenn die Freigabe auch für unverschlüsseltes HTTP gilt, dann wird ein rotes Schloss angezeigt. Mit einem Klick auf das Schloss kann man die Berechtigung umschalten.

**Skripte von Drittseiten**

Skripte von Drittanbietern (googletagmanager, ioam...) werden üblicherweise nur zum Spionieren verwendet und sind für die Funktionalität selten notwendig. Ausnahmen von dieser Regel sind:

**Captcha:** Einige Webseiten verwenden Captchas von Drittanbietern als Spamschutz. Die Captchas funktionieren nur, wenn JavaScript für den Captcha-Provider freigegeben wird. Wenn das Captcha auf einer Webseite nicht funktioniert, kann man in der Liste nachschauen, ob evtl. ein Captcha-Provider dabei ist und diese temporär freigeben.

- Für das häufig verwendete Google Captcha muss man JavaScript temporär für google.com und gstatic.com freigeben.

**Videos:** Firefox braucht keinen Flash Player, um Videos abspielen zu können, aber man muss JavaScript für einige Drittseiten freigegeben. Dabei handelt es sich in der Regel um Content Delivery Networks (CDN) des Dienstes. Diese CDN-Server sind für die Auslieferung von statischem Content und großen Dateien optimiert.

- Um auf der Youtube Webseite Videos zu sehen, muss man JavaScript für youtube.com, youtube-nocookie.com, ytimg.com und googlevideo.com freigeben. Da viele Webseiten Youtube Videos einbinden, kann man diese Freigaben dauerhaft speichern.

- Um Vimeo-Videos von abzuspielen, muss man JavaScript für vimeo.com und vimeocdn.com freigeben.
88

KAPITEL 4. SPURENARM SURFEN
• Um Videos von Bild.de abzuspielen, muss man JavaScript für bild.de und bildstatic.de temporär freigeben.
• Für Youporn Videos muss man JavaScript für die Domainnamen youporn.com
und phncdn.com temporär freigeben.
• ...

Schutz gegen XSS-Angriffe
Im Gegensatz zum Internet Explorer und den auf Webkit basierenden Browsern wie Google
Chrome hat Firefox keinen eingebauten Schutz gegen XSS-Angriffe. NoScript rüstet diese
fehlende Sicherheitsfunktion nach und zeigt eine Warnung bei einem XSS-Angriff:

Die XSS-Protection von NoScript ist standardmäßig aktiv und muss nicht wie beim Internet
Explorer oder Google Chrome durch den Webserver mit dem HTTP Response Header XXSS-Protection: 1; mode=block aktiviert werden.
JIT-Compiler
Just-In-Time Compiler sollen die Ausführung von JavaScript beschleunigen. Der JavaScript Code wird nicht Anweisung für Anweisung interpretiert sondern vor der Ausführung
durch einen Compiler gejagt, der verschiedene Optimierungen vornimmt. Diese zusätzliche Komplexität schafft auch zusätzliche Fehlerquellen. Es gab bereits mehrere sicherheitskritische Bugs in den JIT-Compilern von von Firefox, beispw. Bug #1607443 in Firefox 72.21
iSEC Partners empfiehlt deshalb in einem Sicherheitsaudit für den TorBrowser, die JITCompiler für hohe Sicherheitsanforderungen (strenge Einstellungen) zu deaktivieren:
javascript.options.ion
javascript.options.baselinejit

= false
= false

Diese Einstellungen können die Performance einiger Webseiten deutlich verringern.

4.6

iFrames

Einige Trackingdienste verwenden iFrames, um HTML-Wanzen zu laden, wenn JavaScript
blockiert ist und keine Trackingscripte ausgeführt werden können. Auf vielen Webseiten
findet man den Code von GoogleTagManager (Google Universal Analytics tracking code):
<noscript>
<iframe src="//www.googletagmanager.com/ns.html?id=blabala..."
height="0" width="0" style="display:none;visibility:hidden">
</iframe>
</noscript>
Die Tracking Technik des DoubleClick Bid Manager wurde von Invite Media entwickelt
und in DoubleClick integriert, nachdem Google die Firma Invite Media aufgekauft hatte.
Auch dieses Tracking nutzt einen unsichtbaren iFrame, um Tracking Wanzen mit oder ohne
JavaScript zu platzieren:
<script type="text/javascript">
...
<document.write(’
<iframe src="http://nnnn.fls.doubleclick.net/activityi;src=xxxx;...."
width="1" height="1" frameborder="0" style="display:none"></iframe>’);
</script>


4.6. IFRAMES

Embedded Youtube Videos
Viele Webseiten integrieren Youtube Videos. Die Integration erfolgt als iFrame:

\[
\text{\textlt{iframe src=\"https://www.youtube.com/embed/xyz........\}}
\]

Mit dem Aufruf der Webseite, welche das eingebettete Video enthält, wird auch der iFrame von Youtube geladen und der Surfer mit einem Cookie von Youtube markiert. Um mit europäischem Datenschutzrecht konform zu sein, bietet Youtube eine Adresse für die Einbettung von Videos in Webseiten an, die auf das Setzen von Tracking Cookies verzichtet:

\[
\text{\textlt{iframe src=\"https://www.youtube-nocookie.com/embed/xyz........\}}
\]

Leider wählen nicht alle Webseitenbetreiber die privacy-freundlichere Youtube Variante. Man kann das Add-on Privacy Enhanced Mode for Embedded Youtube installieren. Es schreibt die Adressen für embedded Youtube Videos auf die No-Cookie Adresse um.

iFrames blockieren
Mit dem Add-on uBlock Origin kann man iFrames von Drittseiten blockieren, indem man auf dem Reiter Eigene Filter einige Filterregeln einfügt (Abb: 4.5).

Abbildung 4.5: Blockieren der Frames von Drittseiten mit uBlock Origin

Frames von Drittseiten werden mit der folgenden Filterregel blockiert und können mit einem Klick bei Bedarf geladen werden (z. B. eingebettete Videos):

\[
*\$3p,frame,redirect=click2load.html
\]

Die blockierten iFrames werden beim Laden der Seite so dargestellt, wenn sie sichtbar sind:

\[
\text{https://www.youtube-nocookie.com/embed/\&7lc10f \&VE?autoplay=1 \text{\textlt{iframe}}}
\]

Diese drastische Regel für zu deutlichen Einschränkungen, da viele deutsche News Webseiten mit dieser Einstellung nicht mehr lesbar sind. Deshalb ist es in unserer uBlock Config nicht enthalten und man muss es selbst aktivieren, wenn man die Einschränkungen

22https://addons.mozilla.org/de/firefox/addon/youtube-nocookie/
Die reduzierte Version in unserer uBlock Konfiguration blockiert nicht generell alle iFrames sondern nur die eingebetteten Videos von großen Anbietern:

||youtube-nocookie.com/embed/$3p,frame,redirect=click2load.html
||youtube.com/embed/$3p,frame,redirect=click2load.html
||scribd.com/embeds/$3p,frame,redirect=click2load.html
||player.vimeo.com/video/$3p,frame,redirect=click2load.html
||dailymotion.com/embed/$3p,frame,redirect=click2load.html

(iFrames von Trackingdiensten werden i.d.R. auch durch die Filterlisten blockiert.)

Probleme mit einige News Webseiten

Einige News Webseiten wie spiegel.de, zeit.de oder Golem.de sind nicht kostenfrei lesbar, wenn man alle iFrames generell blockiert, weil sie die Zustimmungsseite mit iFrames von Dritten realisieren und kostenfreies Lesen nur zulassen, wenn sich der Surfer beobachten lässt. Es gibt folgende Optionen:

1. Man könnte diese Seiten ignorieren, wenn man sie als weniger wichtig und austauschbar ansieht, und sich auf anderen Webseiten über aktuelle News informieren.

2. Wenn man der Meinung ist, dass diese Seiten wesentliche Informationen liefern, auf die man nicht verzichten will, sollte man fair sein und ein Abonnement bezahlen.

3. Alternativ könnte man den Werbe- und Trackingblocker uBlock Origin auf diesen Webseiten deaktivieren und den Deal *kostenlosen Lesen gegen Daten akzeptieren.*

4. Als letzte Option könnte man das TorBrowserBundle nehmen, das aufgrund des Anonymitätskonzeptes auch ohne diese Ticks gegen Trackingversuche schützt.

4.7 Werbung, HTML-Wanzen und Social Media


- Der Blutspendendienst des Bayrischen Roten Kreuzes stellt auf seiner Webseite einen Vorcheck bereit. Durch ein eingebundenes Tracking-Skript von Facebook wurden die Antworten auf sensible Fragen zu Schwangerschaft, Drogenkonsum, Diabetes oder HIV an Facebook gesendet, wie eine Analyse der Süddeutschen Zeitung ergab.


23 https://www.sueddeutsche.de/dgital/blutspende-brk-facebook-patientendaten-1.4576563
24 https://heise.de/-4513282
25 http://heise.de/-2429990

- Im Januar 2013 lieferten die Server des Werbenetzwerkes OpenX bösartige Scripte aus, die den Rechner über Sicherheitslücken im Java Plug-in und im Internet Explorer kompromittierten.26

- Zum Jahreswechsel 2014 wurden innerhalb von 4 Tagen 27.000 Surfer durch Werbung von Yahoo mit Malware infiziert.27

- Eine erfolgreiche, mehrwöchige Malvertising Kampagne konnte im Aug. 2015 mit Hilfe von Doubleclick einige Millionen Surfer infizieren.28

- Im Nov. 2015 wurden die Server des Werbenetzwerkes Pagefair gehackt, um bösartigen JavaScript Code in der Werbung auszuliefern.29


Die Like Buttons werden von Facebook und anderen Soziale Netzen verwendet, um Daten zu sammeln. Mit dem Aufruf einer Webseite mit Facebook Like Button werden Daten an Facebook übertragen und dort ausgewertet, auch wenn der Surfer selbst kein Mitglied bei Facebook ist. Die Verwendung der Like Buttons ist nach Ansicht von Thilo Weichert (ULD) nicht mit deutschen Datenschutzrecht vereinbar. Deutsche Webseitenbetreiber sind aufgefordert, die Facebook Buttons von ihren Seiten zu entfernen30.

Forscher der Universität Cambridge (Großbritannien) konnten im Rahmen einer Untersuchung durch Auswertung der Klicks auf Facebook Like Buttons die sexuelle Orientierung und politische Einstellung der Teilnehmer vorhersagen31. Man verrät mit einem Klick auf einen Like Button möglicherweise Informationen, die man nicht im Netz veröffentlichen möchte.

### 4.7.1 Tracking-Filter für Firefox


---

26 [http://heise.de/-1787511](http://heise.de/-1787511)
30 [https://www.datenschutzzentrum.de/facebook](https://www.datenschutzzentrum.de/facebook)
31 [http://heise.de/-1820638](http://heise.de/-1820638)
32 [https://cyberlaw.stanford.edu/node/6730](https://cyberlaw.stanford.edu/node/6730)
KAPITEL 4. SPURENARM SURFEN

Abbildung 4.6: Effektivität verschiedener Tracking-Filter

zusammen, daher die gleichfalls guten Ergebnisse.


4.7.2 Tracking Protection in Firefox

Firefox enthält einen eingebauten Trackingschutz, den man in den Einstellungen in der Sektion Datenschutz und Sicherheit aktiviert. Es wird eine Blockliste von Disconnect genutzt, die von einem Mozilla-Server heruntergeladen wird. Diese Blockliste ist nicht dafür ausgelegt, möglichst viel Werbung auf allen Webseiten zu blockieren. Sie blockiert Trackingdienste und damit als Nebeneffekt Werbebanner, die für Tracking genutzt werden. Folgende Schutzlevel stehen dabei zur Auswahl:

Standard: In Firefox 69.0 ist der Schutz gegen Trackingscripte standardmäßig nur in privaten Fenstern aktiv, der Schutz gegen Trackingcookies und Krypto-Miner ist immer aktiv.

Streng: Im strengen Modus sollen Scripte zum Tracking in allen Fenstern blockiert werden, außerdem Trackingcookies, Krypto-Miner sowie Scripte zum Fingerprinting des Browsers.

Benutzerdefiniert: Außerdem gibt es die benutzerdefinierte Konfiguration, in der man selbst entscheiden kann, welche Schutzmechanismen aktiviert werden sollen. An die-

33 http://drawbrid.ge
34 http://www.tapad.com
35 https://www.ghostery.com
4.7. HERBUNG, HTML-WANZEN UND SOCIAL MEDIA

ser Stelle könnte man auch die allgm. Richtlinien zur Behandlung von Cookies konfigurieren.

Der Trackingschutz ist nur bedingt brauchbar, wie ein oberflächlicher Test zeigt. Für den kleinen Test wurde die strenge Tracking Protection von Firefox 69.0 aktiviert und dann wurden ein paar Webseiten aufgerufen. Dabei wurde vor allem beobachtet, welche Third-Party Cookies jetzt als Trackingcookies erkannt und blockiert wurden.

- Auf den Webseiten Heise.de und Zeit.de ist die Werbung verschwunden aber die Trackingcookies von Webtrekk werden nicht blockiert. Das ist evtl. nicht verwunderlich, da sich Webtrekk mit DNS-Aliases auf beiden Webseiten einen First-Party Status erschleicht und der in Firefox 69.0 implementierte Schutz gegen Trackingcookies nur Third-Party Cookies analysiert und in gute und böse Cookies einteilt.

Trackingscripte von Google und OpenX werden auf Heise.de und Zeit.de blockiert, aber man wird auf beiden Webseiten mit Third-Party Cookies von EASYmedia beobachtet, die nicht von der Tracking Protection blockiert werden. In der Datenschutzpolicy von EASYmedia findet man folgenden Satz zum Austausch von Daten mit Dritten:

- EASYmedia ist mit einer großen Anzahl von Partnern wie z.B. Google, OpenX, SmartAds und vielen anderen verbunden. Um die Bereitstellung unseres Dienstes im Cookie-basierten Advertising Ökosystem zu ermöglichen, tauscht EASYmedia automatisiert pseudonyme IDs mit solchen Partnern aus…

- EASYmedia kann auch Informationen von Dritten erhalten, um gezielte und maßgeschneiderte Werbung auf Webseiten und mobilen Anwendungen zu ermöglichen.

(Es gibt Tracking-Familien, die die Daten untereinander austauschen und damit eine große Reichweite bei der Beobachtung des Surfverhaltens erreichen... und das Google-Imperium ist die größte Familie.)

- Auf YouTube.com wird man trotz strengem Trackingschutz mit einem Cookie von DoubleClick.net markiert, das zur Auswahl von individuell optimierter Werbung verwendet wird, siehe IDE Cookie bei Googles Cookie-Arten:

Wir verwenden Cookies auch für Werbung, die wir an verschiedenen Stellen im Web zeigen. Unser wichtigstes Cookie für Anzeigenvorgaben für Websites, die nicht zu Google gehören, heißt IDE. Es wird in Browsern unter der Domain doubleclick.net gespeichert. [...] Andere Google-Produkte wie YouTube nutzen dieses Cookie möglicherweise ebenfalls zur Auswahl relevanter Werbung.

(Also wenn das kein bekanntes Trackingcookie ist...)


Das sind nur Beispiele und ist keine wiss. Analyse. Es zeigt aber, dass der Trackingschutz von Firefox oft nur oberflächlich arbeitet und andere Lösungen mit optimierten Filterlisten für deutsche Surfer bessere Ergebnisse erreichen un dauch mehr Features bieten.

Bei Aktivierung der Tracking Protection werden aber nicht nur die Filter aktiviert sondern auch Do-Not-Track (DNT). Mit jedem HTTP Request wird ein DNT Header gesendet, der allen Webservern den Wunsch des Nutzers anzeigen soll, dass man nicht beschüffelt werden möchte. Do-Not-Track ist politisch gescheitert, es wird von Trackingdiensten ignoriert. Die Aktivierung des DNT Headers schafft aber ein Differenzierungsmerkmal für das Browser Fingerprinting, wie auch die DNT Working Group des W3C in ihrer Spezifikation
anmerkt. Deshalb ist es empfehlenswert, die Firefox Tracking Protection abschalten und statt dessen einen anderen AdBlocker verwenden:

\[
\text{privacy.trackingprotection.enabled} = \text{false}
\]

Das gleiche gilt für den Private Browsing Mode (PBM). Im PBM wird die Tracking Protection standardmäßig aktiviert und es wird damit ein DNT Header gesendet, womit das Fingerprinting des Browsers erleichtert wird. Mit folgender Option deaktiviert man die Tracking Protection im Private Browsing Mode:

\[
\text{privacy.trackingprotection.pbmode.enabled} = \text{false}
\]

### 4.7.3 uBlock Origin für Firefox

uBlock Origin\(^{36}\) ist ein effizienter und einfach installierbarer Werbeblocker für Firefox. Zur Installation muss man nur auf den Downloadbutton auf der Webseite klicken.

Nach der Installation findet man oben rechts in der Toolbar des Browsers das uBlock Symbol. Mit einem Klick auf des Symbol kann man die Filterung für die aktuelle Webseite anpassen oder ganz deaktivieren. Mit einem Klick auf das kleine Symbol für Einstellungen rechts unter dem dicken Schalter kann man die Konfiguration anpassen.

Um die Anpassungen zu vereinfachen, stellen wir die Config Datei `ublock-config-2.txt`\(^{37}\) zum Download bereit, die man auf dem Reiter Einstellungen importieren kann. Diese Konfiguration aktiviert mehr Filterlisten (siehe unten), enthält die Filter für den Schutz gegen Zugriffe auf lokale URLs sowie eine kleine Whitelist und verhindert das Senden von CSP Reports, wobei für NoScript die notwendigen Ausnahmen definiert werden.


#### Laden externer Schriftarten mit uBlock blockieren?


Statt dessen wird der Google CSS Font Server `fonts.googleapis.com` mit einem eigenen uBlock Filter blockiert:

\[
||\text{fonts.googleapis.com}$important,third-party
\]

Um Schutz gegen Tracking via Schriftarten zu gewährleisten, ist folgende Einstellungen unter about:config besser geeignet:

\[
\begin{align*}
\text{browser.display.use_document_fonts } &= \text{0} \\
\text{layout.css.font-loading-api.enabled} &= \text{false} \\
\text{gfx.downloadable_fonts.enabled} &= \text{false}
\end{align*}
\]

#### uBlock Origin zusammen mit NoScript verwenden

Wenn man uBlock Origin zusammen mit NoScript benutzt und aus Privacygründen das Senden von CSP-Reports blockiert, dann muss man auf dem Reiter Meine Regeln eine Regel hinzufügen, damit NoScript arbeitsfähig bleibt:

\(^{36}\)https://addons.mozilla.org/de/firefox/addon/ublock-origin

\(^{37}\)https://www.privacy-handbuch.de/download/ublock-config-2.txt
4.8. FIREFOX ACTIVITY-STREAM

Abbildung 4.7: Dashboard von uBlock Origin

no-csp-reports: * true
no-csp-reports: noscript-csp.invalid false

4.8 Firefox activity-stream


- Das Suchfeld könnte man als praktisch aber überflüssig bezeichnen, da man in der Adressleiste bereits ein Suchfeld hat.
- Häufig besuchte Webseiten und zufällige Vorschläge aus der History sind überflüssig, wenn man diese Daten nicht speichert.
KAPITEL 4. SPURENARM SURFEN

Abbildung 4.8: Gesponserte Empfehlungen auf der NewTab Seite und Startseite

Außerdem sammelt Pocket Telemetriedaten über den Aufruf des activity-stream und Informationen darüber, ob der activity-stream vom User abgeschaltet wurde. (Also wieder jemand, der sich für unsere Interessen interessiert, um tolle Vorschläge zu machen, und mit individuellen Vorschlägen ein bisschen Werbung verteilt.)


Wie konnte die Webseite Bild.de die Trackingcookies setzen? Um die NewTab Page darzustellen (seit Firefox 61 auch die Startseite), holt Firefox eine JSON Datei von Mozilla, die eine Liste mit den URLs für die darzustellenden Icons aller 900+ Top Webseiten enthält. Für Bild.de findet man folgenden Eintrag:

```
{
  "domains": ["bild.de"]
  "image_url": "https://bilder.bild.de/fotos/bild-de-....../3.bild.png"
}
```

Das Icon für Bild.de wird also von dem Webserver bilder.bild.de geholt und dieser nutzt die Möglichkeit, um einige Trackingcookies zu setzen. Das ist bei anderen Empfehlungen auch möglich.
4.8. FIREFOX ACTIVITY-STREAM

Abbildung 4.9: Cookies von Bild.de nach Aufruf eines neuen Tab

activity-stream deaktivieren


Unter der Adresse about:config kann man Einstellungen ebenfalls vornehmen und den activity-stream für die Startseite und für neue Tabs abschalten:

```
browser.startup.page = 0
browser.newtabpage.enabled = false
```

Wenn man eine eigene Startseite verwenden möchte, die nicht privacy-invasiv ist, dann kann man folgende Parameter unter about:config setzen:

```
browser.startup.page = 1
browser.startup.homepage = <URL>
```

Außerdem kann man die Highlights im Menü der Bibliothek abschalten:

```
browser.library.activity-stream.enabled = false
```

Firefox zeigt die handverlesenden Topsites außerdem in der Liste der Vorschlägen bei Eingabe einer Adresse in der URL Leiste an. Das deaktiviert man mit:

```
browser.urlbar.suggest.topsites = false
```
KAPITEL 4. SPURENARM SURFEN

Abbildung 4.10: Leere Seite für Startseite und neue Tabs konfigurieren

Bezahlte Werbeeinblendungen deaktiviert mit folgenden Einstellungen:

```python
browser.newtabpage.activity-stream.showSponsored = false
browser.newtabpage.activity-stream.showSponsoredTopSites = false
```

Oberflächlich sieht damit alles ok aus, man hat eine Startseite sowie NewTab Page ohne überflüssigen Schnickschnack und wird nicht mit handverlesenen Empfehlungen belästigt. Beim Starten kontaktiert Firefox aber weiterhin die Server mit dem Empfehlungen und holt die aktuellen Dateien. Das kann man Firefox mit folgenden Optionen abgewöhnen:

```python
browser.newtabpage.activity-stream.feeds.topsites = false
browser.newtabpage.activity-stream.feeds.snippets = false
browser.newtabpage.activity-stream.section.highlights.includePocket = false
browser.newtabpage.activity-stream.feeds.system.topsites = false
```

Im Hintergrund werden außerdem Telemetrie Pings an den Pocket Server gesendet und Firefox teilt damit dem Pocket Server laufend mit, dass man activity-stream feeds deaktiviert hat. Um diese Telemetrie Pings ebenfalls zu deaktivieren, muss man noch einige weitere Werte unter about:config setzen:

```python
browser.newtabpage.activity-stream.telemetry = false
browser.newtabpage.activity-stream.feeds.telemetry = false
```

Außerdem ist die Ping-Centre Funktion für Datenversand zu deaktivieren:

```python
browser.ping-centre.telemetry = false
```

Firefox speichert Screenshots von jeder besuchten Webseite auf der Festplatte, um sie später als Thumbnails activity-stream einzublenden. Diese Speicherung gefällt mir nicht, da ich mein Surfverhalten nicht protokollieren möchte, auch nicht auf dem eigene Rechner. Da man diese Thumbnails nicht mehr benötigt, wenn eine leere Seite statt des activity-stream angezeigt wird, kann man eine neue Variable vom Typ Boolean unter about:config erstellen um die Erstellung der Thumbnails zu deaktivieren:

```python
browser.pagethumbnails.capturing_disabled = true
```

4.9 Contextual Feature Recommender (CFR)

Mit Firefox 64.0 hat Mozilla den Contextual Feature Recommender (CFR) eingeführt, was einfach gesagt nur ein Werbesystem für Add-ons und Features ist.

Mir ist unklar, nach welchen Richtlinien Mozilla die Empfehlungen für Add-ons auswählt. Mit der Empfehlung für das Web-Security Add-on hatte Mozilla schon gründlich daneben gegriffen und ein Tracking Add-on als Trackingschutz empfohlen (Bugzilla #1483995). Das Add-on Web-of-Trust konnte sich ebenfalls lange als angebliches Security Add-on verkaufen bevor man entdeckte, dass mit diesem Add-on massenweise Daten
4.10 Browsercache und Surf-Chronik


Eine Studie der University of California von 2010 zeigte, dass ca. 1% der Websites versuchten, die Chronik über zuvor besuchte Websites anhand der unterschiedlichen Formatierung der Links von besuchten und nicht besuchten Webseiten auszulesen.40

---

38 https://www.tagesschau.de/inland/tracker-online-103.html
39 https://blog.mozilla.org/firefox/make-your-firefox-browser-a-privacy-superpower-with-these-extensions/
40 https://www.heise.de/newsticker/meldung/Plaudertasche-Web-Browser-erleichtert-Deanonymisierung-919076.html
Trackingdienste wie Tealium oder Beancounter versuchten ebenfalls, die Formatierung von Links auszuwerten. (Gegen diese Angriffe sind aktuelle Firefox Versionen imunisiert.)


Schutz gegen Tracking über mehrere Webseiten


Schutz gegen langfristiges Tracking

Gegen längerfristige Wiedererkennung auf häufiger besuchten Webseiten schützt das Deaktivieren der Surf-History und das Löschen des Cache usw. beim Beenden des Browsers.

Abbildung 4.12: Deaktivieren der Surf-History und Löschen des Cache


Wenn man auf den Button Einstellungen hinter Die Chronik löschen, wenn Firefox geschlossen wird, kann man festlegen, welche Daten beim Schließen des Browsers gelöscht werden.

Alternativ kann man unter about:config folgende Werte setzen:

```
network.cookie.lifetimePolicy = 2
places.history.enabled = false
privacy.history.custom = true
privacysanitize.sanitizeOnShutdown = true
```

41 https://heise.de/-1288914
4.10. BROWSERCACHE UND SURF-CHRONIK

Abbildung 4.13: Konfiguration der zu löschenden Daten beim Beenden

```
privacy.clearOnShutdown.cache = true
privacy.clearOnShutdown.cookies = true
privacy.clearOnShutdown.downloads = true
privacy.clearOnShutdown.formdata = true
privacy.clearOnShutdown.history = true
privacy.clearOnShutdown.offlineApps = true
privacy.clearOnShutdown.sessions = true
privacy.clearOnShutdown.siteSettings = true oder false
privacy.clearOnShutdown.openWindows = false
```


Abbildung 4.14: Chronik während des Surfens löschen

Disk-Cache deaktivieren

Firefox verwendet einen Cache im Hauptspeicher und einen Disk-Cache auf der Festplatte. Der Cache im Hauptspeicher ist mit 64 MB groß genug für eine Surf-Session. Den Disk-Cache kann man deaktivieren und damit auch überflüssige Spuren auf dem Rechner ver-
meiden, die forensisch sichtbar gemacht werden könnten. Unter about:config sind dafür folgende Variablen zu setzen:

```plaintext
browser.cache.disk.enable false
browser.cache.disk_cache_ssl false
browser.cache.offline.enable false
```

### 4.11 Referer

Mit jedem Klick auf einen Link sendet Browser einen Referer im HTML Header an die aufgerufenen Webseite und teilt mit, von welcher Webseite der Surfer gekommen ist.


Die Studie *Privacy leakage vs. Protection measures*\(^{42}\) zeigt, dass außerdem viele Webseiten private Informationen via Referer an Trackingdienste übertragen. Das folgende Beispiel zeigt den Aufruf eines Werbebanners nach dem Login auf der Webseite http://sports.com

```
GET http://ad.doubleclick.net/adj/....
Referer: http://submit.sports.com/...?email=name@email.com
Cookie: id=123456789.......
```

Mit einer eindeutigen UserID (im Beispiel ein Tracking-Cookie) kann das Surverhalten über viele Webseiten verfolgt werden. Durch zusätzliche Informationen (im Beispiel eine E-Mail Adresse) werden die gesammelten Datensätze personalisiert. Im Rahmen der Studie wurde 120 populäre Webseiten untersucht. 56% der Webseiten sendeten nach dem Login private Informationen wie E-Mail Adresse, Name oder Wohnort an Trackingdienste.

Mit Firefox 87 (März 2021) hat Mozilla auf dieses Risiko für die Privatsphäre reagiert und kürzt den Referer beim Aufruf von Elementen von Drittseiten auf die Domain. Das Beispiel für den Aufruf eines Werbebanners von DoubleClick sieht dann so aus:

```
GET http://ad.doubleclick.net/adj/....
Referer: http://submit.sports.com/
Cookie: id=123456789.......
```

Firefox bietet auch die Möglichkeit, das Senden des Referers an Drittseiten zu blockieren. Dafür setzt man unter der Adresse about:config folgende Option:

```plaintext
network.http.referer.XOriginPolicy = 2
```

Mit dieser Einstellung werden Subdomains als Drittseiten behandelt und es wird auch an Subdomains kein Referer gesendet. Das schützt somit auch gegen Trackingdienste, die sich mit DNS-Aliases als Subdomains auf populären Webseiten einschleichen (z. B. WebTrekk bei Heise.de und Zeit.de). Allerdings bringt es möglicherweise vereinzelt Probleme bei einigen Websites mit sich. Folgende Einstellung minimiert die Probleme:

```plaintext
network.http.referer.XOriginPolicy = 1
```

Damit werden Subdomains wie die Hauptdomain behandelt und es wird ein Referer gesendet. Lediglich an echte Drittseiten wird kein Referer übergeben.

Einige Webseiten zum Thema Privacy empfehlen, das Senden des Referers mit folgender Option komplett zu deaktivieren:

```plaintext
network.http.sendRefererHeader = 0
```


## 4.12 URL-Parameter

URL-Parameter werden häufig für mit folgenden Intentionen für das Tracking verwendet:


3. Außerdem können Tracking-IDs in Parametern kodiert werden, die die Container von Firefox austricksen und Webseiten-übergreifendes Tracking ermöglichen.


Ein Beispiel von der Webseite heise.de (Mobilversion) zeigt beide Anwendungen für das Tracking mit URL-Parametern durch WebTrekk mit dem Referer (wt_ref) und einer numerischen ID (wt_t):

https://m.heise.de/foto/?wt_ref=https%3A%2F%2Fwww.heise.de&wt_t=1618985578


Das Add-on ClearURLs kann viele Trackingparameter aus URLs entfernen. Es kennt die häufig verwendeten Trackingparameter der Großen der Branche aber es ist nicht in der Lage, alle Parameter zu erkennen, da das Konzept enumerating the badness nie 100% erreichen kann. Das Add-on hat noch mehr Funktionen. Im Rahmen des hier vorgestellten Gesamtkonzeptes soll es sich aber nur um die URL-Parameter kümmern. Alle anderen Funktionen kann man abschalten.

Auch mit dem Add-on uBlock Origin kann man Parameter aus URLs entfernen. Dafür muss man eine Liste von Filterregeln definieren, beispielsweise für das Google Kampagnen Tracking:

```css
$removeparam=utm_campaign
$removeparam=utm_channel
$removeparam=utm_cid
$removeparam=utm_content
$removeparam=utm_medium
$removeparam=utm_name
$removeparam=utm_place
```
KAPITEL 4. SPURENARM SURFEN

... oder die unterschiedlichen Facebook Parameter:

$removeparam=fb_action_ids
$removeparam=fb_action_types
$removeparam=fb_comment_id
$removeparam=fb_ref
$removeparam=fb_source
$removeparam=fbclid

Es gibt aber noch keine Liste, die so umfangreich ist wie die Liste vom Add-on ClearURLs und außerdem die notwendigen Ausnahmen für einige Webseiten definiert.

4.13 Risiko Plugins

Für die Darstellung von Inhalten, die nicht im HTML-Standard definiert sind, kann Firefox Plug-ins nutzen. Sie werden in der Add-on Verwaltung in der Sektion PPluginsaktiviert. Um zu verhindern, dass bei der Installation von irgendwelchen Softwarepaketen ungewollt Browser Plug-ins automatisch aktiviert werden, kann man folgende Variable unter about:config setzen:

plugin.default.state = 0

Um unter Windows das automatische Scannen der Registry nach neuen Plug-ins zu deaktivieren, ist unter about:config folgende Variable zu setzen:

plugin.scan.plid.all = false

4.13.1 Media Plug-ins für Video und Audio

Die Einstellungen zum Deaktivieren des automatischen Abspielens von Audio und Video hat Mozilla immer wieder geändert. Mit folgenden Einstellungen unter about:config deaktivierte man das automatische Abspielen von Videos und Audio:

media.autoplay.default = 5
media.autoplay.blocking_policy = 2

Das Deaktivieren des automatischen Abspielens von Videos ist auch ein Sicherheitsfeature, das den Start eines böswilligen Videos im Hintergrund verhindert und die Angriffsfläche für Drive-by-Download Angriffe verringert.

Für einige Video- und Audioformate verwendet Firefox externe Plug-ins zum abspielen. Standardmäßig werden von Firefox zwei Media Plug-ins verwaltet:

OpenH264 Videocodewird von Cisco für WebRTC benötigt. Wenn man WebRTC abschaltet, kann man auch den Videocodec und das Update deaktivieren (bei einige Linux Distributionen wie Fedora ist es standardmäßig so konfiguriert)

media.gmp-gmpopenh264.autoupdate = false
media.gmp-gmpopenh264.enabled = false
4.13. RISIKO PLUGINS

Außerdem kann das OpenH264 Plugin in der Add-on Verwaltung ausblenden:

```text
media.gmp-gmpopenh264.visible = false
```

**Widevine Content Decryption Module** von Google zur Wiedergabe von DRM geschützten Videos ist unter Windows standardmäßig aktiviert, bei den meisten Linux Distributionen aber standardmäßig deaktiviert. Man braucht es nicht notwendigerweise. Mit folgendem Wert unter `about:config` kann man es komplett deinstallieren:

```text
media.eme.enabled = false
```

Damit es auch nicht in den Einstellungen als aktivierbare Option erscheint, kann man die Konfigurationsoption verstecken:

```text
browser.eme.ui.enabled = false
```

# 4.13.2 Anzeige von PDF Dokumenten


```text
pdfjs.disabled = true
```

Statt funktionsüberladener Monster-Applikationen kann man einfache PDF-Reader nutzen, die sich auf die wesentliche Funktion des Anzeigens von PDF-Dokumenten beschränken. Die FSFE stellt auf PDFreaders.org [Open Source Alternativen](http://www.pdfreaders.org/index.de.html) vor.

- Für Windows werden *Sumatra PDF* oder *MuPDF* empfohlen.
- Für Linux gibt es *Okular* (KDE) und *Evince* (GNOME, XFCE, Unity).
- Für MacOS wird *Vindaloo* empfohlen.

Die Linux Distribution **QubesOS** bietet für potentielle **Landesverräter** und andere Risikogruppen, die als Target für den Einsatz der neuen Bundestrojaner in Frage kommen, einige besondere Sicherheitsfeatures. Dazu gehört die Anzeige von PDFs in einer Wegwerf-VM oder die Umwandlung von PDF Dokumenten aus unbekannten Quellen in Trusted PDFs, die man risikolos weitergeben kann. Die Funktionen kann man nach dem Download mit einem Rechtsklick auf ein PDF Dokument im Dateimanager aufrufen.

Für die Umwandlung in Trusted PDFs wird **qubes-app-linx-pdf-converter** gestartet, das Rendering des (möglicherweise bösartigen) PDF Dokumentes erfolgt in einer Wegwerf-VM, die danach gelöscht wird. Die gerenderten Bitmaps werden zu einem neuen, ganz harmlosen PDF zusammengesetzt. Wie bei QubesOS üblich, dauert der Vorgang insbesondere bei großen PDF Dokumenten einige Zeit. (Eile ist ein Feind der Sicherheit!)

---

4.14 HTTPS-Verschlüsselung erzwingen und härten


Abbildung 4.16: Nur-HTTPS-Mode in Firefox 83+ aktivieren
Firefox bietet den Nur-HTTPS-Modus, bei dem Webseiten immer via HTTPS aufgerufen werden. Firefox Release und ESR Version unterscheiden sich in der Konfiguration:

- Im Firefox 78.x ESR muss man unter about:config folgenden Wert setzen:

  ```
  dom.security.https_only_mode = true
  ```

- Wenn keine HTTPS Verbindung möglich ist, dann wird eine Warnung angezeigt und man kann mit einem Klick die unverschlüsselte HTTP Seite aufrufen (Abb: 4.17).

Die Konfiguration des Routers ist somit problemlos möglich, nur ein Klick mehr.

Abbildung 4.17: Warnung bei Aufruf einer unverschlüsselten HTTP Seite

- Für lokale Verbindungen zum eigenen Rechner wird kein HTTPS erzwungen. Man kann z. B. den Druckserver CUPS (Linux) wie gewohnt im Browser administrieren. Wenn man auch für http://localhost oder http://127.0.0.1 ein Upgrade auf HTTPS erzwingen möchte, könnte man folgenden Wert setzen (aber warum?):

  ```
  dom.security.https_only_mode.upgrade_local = true
  ```

- Neben HTTP unterstützt Firefox 78 ESR auch noch das FTP-Protokoll aus ... Gründen. Für FTP erfolgt kein(!) Upgrade auf TLS im Nur-HTTPS-Modus. Um unsichere FTP Verbindungen auszuschließen, muss man es komplett deaktivieren:

  ```
  network.ftp.enabled = false (nur für Firefox 78 ESR)
  ```

- Downloads über unsichere Verbindungen kann Firefox 80+ blockieren. Webseiten können via HTTP aufgerufen werden (im Nur-HTTPS-Modus nach Bestätigen der Warnung). Aber Downloads, die man auf der Festplatte speichert, sollten immer via HTTPS geladen werden. Unsichere Downloads blockiert man mit der Option:

  ```
  dom.block_download_insecure = true
  ```

  (Da seriöse Downloads in der Regel über HTTPS angeboten werden, ist diese Option immer empfehlenswert in allen user.js Konfigurationen aktiviert.)
• *Mixed Content* nennt man die Elemente in HTTPS-Webseiten, welche über einen unverschlüsselten HTTP-Link geladen werden. Mit folgender Option erzwingt das Upgrade auf HTTPS auch für alle Inhalte der Webseite wie Bilder, Fonts, usw.

```
security.mixed_content.upgrade_display_content = true
```

Das Laden von aktiven Inhalten wie Javascript via unverschlüsseltem HTTP ist beim Aufruf von Webseiten über HTTPS standardmäßig verboten.

• *Insecure Renegotiation* wird seit 2009 als schwerwiegender Bug des SSL-Protokolls eingestuft. Tools zum Ausnutzen der Insecure Renegotiation gibt es auch als OpenSource (z. B. dsniff). Deshalb sollte man es verbieten:

```
security.ssl.require_safe_negotiation = true
security.ssl.treat_unsafe_negotiation_as_broken = true
```

• *Certifikate Pinning* schützt gegen Man-in-the-Middle Angriffe. Mit folgender Option wird für eine populäre Webseite wie Google, Youtube, Twitter, TorProject, Dropbox u. a. eine verschlüsselte Verbindung nur dann akzeptiert, wenn das Zertifikat des Servers von einer CA signiert wurde, die im Code von Firefox festgeschrieben ist:

```
security.cert_pinning.enforcement_level = 2
```

Wenn einige Webseiten mit dieser Einstellung nicht aufrufbar sind, dann sitzt ein Man-in-the-Middle in der TLS-Verschlüsselung (das kann z. B. ein Virenscanner sein).


Es gibt einige Gründe, die dagegen sprechen, diese Zertifikate zu nutzen und nur dem Zertifikatspeicher von Firefox zu vertrauen. Man steuert das Verhalten mit:

```
security.enterprise_roots.enabled = false (Default)
```

Wenn bei einer HTTPS-Verbindung der Zertifikatsfehler `CertError: Man-in-the-Middle` auftritt, aktiviert Firefox automatisch die Enterprise Root Certificates und versucht erneut, das fehlerhafte Zertifikat zu validieren. Diese automatische Aktivierung verhindert man mit folgender Einstellung unter `about:config`:

```
security.certerrors.mitm.auto_enable_enterprise_roots = false
```

Bei Bedarf kann man Verwendung von Enterprise Root Certificates, die im Betriebssystem installiert wurden, selbst aktivieren (z. B. in Firmenumgebungen).

• Weitere Add-ons wie HTTPSEverywhere oder HTTPZ sind damit überflüssig.

### 4.14.1 Anzeige der HTTPS Verschlüsselung

Standardmäßig zeigt Firefox 70+ einen HTTPS-verschlüsselten Transport der Daten nur mit einem kleinen, unscheinbar grauen Icon neben der Adresse an:
4.14. HTTPS-VERSCHLÜSSELUNG ERZWINGEN UND HÄRTEN

Etwas auffälliger war das beruhigende Grün für das Symbol bei älteren Firefox Versionen, welches man mit folgender Option unter about:config wieder aktivieren kann:

```
security.secure_connection_icon_color_gray = false
```

Neben einfachen SSL-Zertifikaten gibt Extended Validation Certificates, bei denen die Certification Authority (CA) die Identität des Inhabers aufwendiger prüft, bevor ein Zertifikat ausgestellt wird. Firefox 70+ zeigt keinen Hinweis mehr bei EV-Zertifikaten an. Wenn man die Sicherheitsinformation zum verifizierten Inhaber des SSL-Zertifikates wieder sehen möchte, muss man folgende Optionen unter about:config aktivieren:

```
security.identityblock.show_extended_validation = true
security.OCSP.enabled = 1
```


```
security.insecure_connection_icon.enabled = true
security.insecure_connection_icon.pbmode.enabled = true
security.insecure_connection_text.enabled = true
security.insecure_connection_text.pbmode.enabled = true
```

Beide Optionen können auch kombiniert werden, das sieht dann so aus:

```
security.insecure_connection_icon.enabled = true
security.insecure_connection_icon.pbmode.enabled = true
security.insecure_connection_text.enabled = true
security.insecure_connection_text.pbmode.enabled = true
```

4.14.2 Vertrauenswürdigkeit von HTTPS


Certificate-based attacks are a concern all over the world, including in the U.S., since governments everywhere are eagerly adopting spying technology to eavesdrop on the public. Vendors of this technology seem to suggest the attacks can be done routinely.

Anbieter von fertige Appliances für diesen auch als Lawful SSL Interception bezeichneten Angriff findet man beim Stöbern in den SpyFiles von Wikileaks. Für staatliche Schnüffler gibt es mehrere Möglichkeiten, um diese Technik mit gültigen SSL-Zertifikate für schwer erkennbare man-in-the-middle Angriffe zu kombinieren:

45https://eff.org/deeplinks/2010/03/researchers-reveal-likelihood-governments-fake-ssl

2. Certification Authorities könnten unter Druck gesetzt werden, um staatlichen Stellen SubCA-Zertifikate auszustellen, mit denen die Zertifikate für man-in-the-middle Angriffe signiert werden könnten. Ein Kommentar zum TürkTRUST Desaster:

   I think you will see more and more events like this, where a CA under pressure from a government will behave in strange ways. (A. Shamir)

Im Juni 2014 signierte die staatliche indische Certification Authority (NIC) gefälschte SSL-Zertifikate für Google Dienste und Yahoo!. 45 gefakte Zertifikate wurden nachgewiesen. Ob es um eine staatliche Überwachung, einen Hackerangriff oder einen Konfigurationsfehler (?) handelt, ist unklar.


Kriminelle Subjekte haben ebenfalls nachgewiesen, dass sie für man-in-the-middle Angriffe auf die SSL-Verschlüsselung gültige Zertifikate verwenden können (bspw. bei einem Angriff auf das Bitcoin Forum). Man kann sich sehr einfach als Unberechtigter ein gültiges SSL-Zertifikat für einen Server ausstellen zu lassen, wenn man den richtigen Mail-Account kontrolliert. Für die Ausstellung Domain-validierte SSL-Zertifikate werden die E-Mail Adressen webmaster@domain.tld, postmaster@domain.tld, ssladministrator@domain.tld u.a.m. akzeptiert. Eine unverschlüsselte E-Mail mit einem Verification Link an eine der genannten E-Mail Adressen ist die einzige Prüfung auf Rechtmäßigkeit durch die CAs.


4.14.3 SSL-Zertifikate via OCSP validieren

Das Online Certificate Status Protocol (OCSP) sollte eine Überprüfung der SSL-Zertifikate ermöglichen. Bevor der Browser eine SSL-Verbindung akzeptiert, fragt er bei der Certification Authority nach, ob das verwendete Zertifikat für diesen Server noch gültig ist. Um SSL-Zertifikate via OCSP zu verifizieren, wurden zwei Verfahren definiert:


Einige CAs nutzen die OCSP-Anfragen zum Tracking des Surfers mit Cookies, wie der folgende Mitschnitt eines OCSP-Request zeigt:

46 https://www.heise.de/-2255992
47 http://crypto.stanford.edu/ssl-mitm/
48 http://www.monkey.org/dugsong/dsniff/
49 https://moxie.org/software/sslniff
4.14. HTTPS-VERSCHLÜSSELUNG ERZWINGEN UND HÄRTEN

POST http://ocsp2.globalsign.com/gsorganizationvalg2 HTTP/1.1
Host: ocsp2.globalsign.com
User-Agent: Mozilla/5.0 (...) Gecko/20130626 Firefox/17.0 Iceweasel/17.0.7
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Proxy-Connection: keep-alive
Content-Length: 117
Content-Type: application/ocsp-request
Cookie: __cfduid=57a288498324f76b1d1373918358

Auch wenn aktuelle Firefox Versionen keine Cookies von OCSP.Get Antworten mehr akzeptieren, erhält die Certification Authority (CA) laufend Informationen, von welcher IP-Adresse die SSL-geschützten Webseiten bzw. Mailserver o.ä. kontaktiert wurden. Da die OCSP-Anfrage und Antworten unverschlüsselt übertragen werden, kann auch ein Lauscher am Draht diese Informationen abgreifen. Aus Privacy Gründen kann man die Validierung via OCSP Server deaktivieren

security.OCSP.enabled = 0

Wenn man die Validierung von SSL-Zertifikaten via OCSP-Server als Sicherheitsfeature nutzen möchte (damit beispielsweise Extended Validation Informationen der Zertifikate angezeigt werden), dann muss man auch darauf bestehen, dass das Ergebnis geliefert und ausgewertet wird. Anderenfalls ist es als Sicherheitsfeature unbrauchbar. Diese verschärfte OCSP Validierung aktiviert man unter about:config mit:

security.OCSP.enabled = 1
security.OCSP.require = true


OCSP.Stapling ist ein modernes Verfahren, dass die oben genannten Probleme vermeidet. Der Browser ruft ein Token vom Webserver ab, das die Gültigkeit des Zertifikates für einen kurzen Zeitraum bestätigt und von der CA signiert wurde.


Firefox ist sinnvoll vorkonfiguriert. Es wird standardmäßig OCSP.Stapling genutzt, wie man unter about:config überprüfen kann:

security.ssl.enable_ocsp_stapling = true
security.ssl.enable_ocsp_must_staple = true

4.14.4 Tracking via TLS Session

Beim Aufbau einer verschlüsselten HTTPS-Verbindung zwischen Browser und Webserver wird eine sogenannte Session initialisiert. Diese Session kann für 48h genutzt werden. Das beschleunigt das Laden der Webseite bei erneutem Zugriff, da die Details der Verschlüsselung nicht jedes mal neu zwischen Browser und Webserver ausgehandelt werden müssen. Da die TLS Session eindeutig ist, kann sie für das Tracking genutzt werden (RFC 507751).

Die SSL-Session-ID kann von nahezu allen Webserven für das Tracking der Zugriffe genutzt werden. IBM WebSphere, Apache und andere bieten eine API für den Zugriff auf die SSL Session-ID. Einige Webshops sind für das Tracking via SSL Session-ID vorbereitet (z. B. die *xtcModified eCommerce Shopsoftware*). Dieses Tracking-Verfahren ist so gut wie nicht nachweisbar, da es vollständig durch den Webserver realisiert wird und keine Spuren im Browser hinterlässt.

In Firefox ist der SSL Session Cache in den Surf-Containern gekapselt. Unser Konzept aktiviert folgende Schutzmaßnahmen gegen das Tracking:

- **FirstParty.Isolation** verhindert das weBSITE-übergreifende Tracking.
- Löschen von Cache und SiteSettings beim Schließen des Browsers verhindert das langfristige Tracking über einen längeren Zeitraum.

Dieser Schutzlevel entspricht dem Schutz gegen Tracking mit Cookies und EverCookie ohne das Surfen durch ständiges Neuaufladen der TLS Sessions zu verlangsamen.

### 4.14.5 Tracking via HTTP Strict Transport Security (HSTS)


Als Schutz gegen *ssl-stripe* Angriffe sendet der Webserver beim Aufruf einer Webseite einen zusätzlichen HSTS-Header, um dem Browser mitzuteilen, dass diese Website für eine bestimmte Zeit immer via HTTPS aufgerufen werden soll. Außerdem enthält Firefox die *HSTS Preload List* mit mehr als 1.000 Webseiten, die nur via HTTPS aufgerufen werden dürfen. Das verhindert einen Downgrade auf unverschlüsselte HTTP-Verbindungen.


Ob man HSTS im Browser deaktiviert und sich nur auf die *HSTS Preload List* verlässt, um sich gegen ein Trackingverfahren zu schützen, oder ob man HSTS aktiviert, um sich gegen *ssl-stripe* Angriffe zu schützen (Standard im Firefox), ist also eine Wahl zwischen Skylla und Charybdis. Überlegungen dazu:

- In der Regel nutzt man nur eine begrenzte Anzahl von Websites regelmäßig, bei denen sensitive Informationen durch SSL-Verschlüsselung wirklich geschützt werden müssen (E-Mail Provider, Website der Bank, Diskussionsforen, bevorzugte Suchmaschine...). Mit der HSTS Preload List oder HTTSEverywhere kann man SSL-Verschlüsslung für diese Websites erzwingen und ist damit auch ohne HSTS gegen *ssl-stripe* Angriffe geschützt.
- Unter der Adresse *about:config* kann man folgende Variable setzen:

  ```
  privacy.clearOnShutdown.siteSettings = true
  ```


---

53 [http://heise.de/-2511258](http://heise.de/-2511258)
54 [https://heise.de/-3998754](https://heise.de/-3998754)
4.14. HTTPS-VERSCHLÜSSELUNG ERZWINGEN UND HÄRTEN

4.14.6 SSL/TLS Konfiguration

Die SSL-Verschlüsselung ist ein komplexer Standard, der über Jahre gewachsen ist. Neben aktuell starken Algorithmen sind auch schwache kryptografische Verfahren enthalten, die aus Kompatibilitätsgründen unterstützt werden:

1. Das Protokoll SSLv3 ist geknackt. Mozilla hat SSLv3 in Firefox 34 standardmäßig abgeschaltet. TLS 1.0 und TLS 1.1 sollen seit 2017 nicht mehr verwendet werden.

2. Die RC4-Cipher sind schwach und genügen aktuellen Anforderungen nicht mehr. Laut Empfehlung der IETF (RFC 7465) darf RC4 nicht mehr für die Verschlüsselung genutzt werden und ist in Firefox seit Version 44 deaktiviert.


5. SHA sollte laut Empfehlung der IETF nicht mehr als Signaturalgorithmus für die Beuglaubigung von Zertifikaten verwendet werden. Die Certification Authorities haben inzwischen alle Zertifikate umgestellt auf SHA256.

6. FIPS-kompatible Cipher sind per Design schwach ausgelegt und in Firefox standardmäßig deaktiviert.

Tracking Risiko durch seltsame Auswahl der SSL/TLS Cipher

Wenn der Browser eine SSL-verschlüsselte Verbindung zu einem Webserver aufbauen will, dann sendet er Liste der unterstützten TLS-Features, Cipher und der nutzbaren elliptischen Kurven für EC-Crypto. Die Reihenfolge und der Inhalt der Listen ist unterschiedlich für verschiedene Browser und Browser Versionen.

- Firefox 53 sendet beispielsweise:

  ```xml
  <e name='Firefox/53.0' protocol='771' extTypes='21 23 65281 10 11 16 5 18 40 43 13' suites='4865 4867 4866 49195 49199 52393 52392 49196 49200 49171 49172 51 53' curves='29 23 24 25 256 257' points='AA==' compress='AA=='/>
  ```

- Google Chrome sendet:

  ```xml
  <e name='Chrome/57.0.2951.0' protocol='771' greateExt='1' extTypes='65281 0 23 35 13 5 18 16 30032 11 40 45 43 10 21' greaseSuite='1' suites='4865 4866 4867 49195 49199 49196 49200 52393 52392 52244 52243 49171 49172' 156 157 47 53 10' greaseCurves='1' curves='29 23 24' points='AA==' compress='AA=='/>
  ```

Das sieht etwas kryptisch aus, man kann sich auf verschiedenen Webseite aber auch anzeigen lassen, was es bedeutet.

4.15 Installierte Schriftarten verstecken

Informationen über installierte Schriftarten können mit JavaScript, Flash oder Java ausgelesen und zur Berechnung eines individuellen Fingerprint des Browsers genutzt werden. Viele Trackingdienste nutzen inzwischen diese Technik. Die Studie *Dusting the web for fingerprinters* der KU Leuven (2013) kommt zu den Schluss, dass mindestens 0,5 - 1,0% der Webseiten die installierten Schriftarten für Trackingzwecke auslesen.

Der Download von (exotischen) Schriftarten wird auch von Google zum Tracking genutzt. Viele Webdesigner nutzen Schriften vom Google Font Service statt 5min Arbeit zu investieren und die Schriftarten auf dem eigenen Webserver bereitzustellen.

Für den Webdesigner ist die Einbindung der Google Fonts sehr einfach;

1. Der Webdesigner muss nur ein kleines CSS-Stylesheet importieren. Um die Schriftart OpenSans zu nutzen, reicht folgende Zeile:

   ```html
   <link href='https://fonts.googleapis.com/css?family=Open+Sans' rel='stylesheet' type='text/css'>
   ```


3. Der Browser holt sich dann die Dateien mit Schriftarten vom Server fonts.gstatic.com und zeigt die Webseite an. Die Font Dateien werden für 24h im Cache gespeichert.


Potente (staatliche) Hacker kombinieren Bugs im Font Rendering gern mit 0-Days Bugs im Browser, um nach der Kompromittierung des Browsers den Rechner zu übernehmen:

- Der Bug *ms15-078* wurde von der Firma Hacking Team zur Installation eines Überwachungstrojaners genutzt.


Bruce Schneier vermutet einen staatlichen Angreifer wie die NSA dahinter. Allerdings ist das Spekulation und es gibt keine echten Beweise, die auf die NSA zeigen.

---

57 https://www.google.com/intl/de/policies/privacy
58 https://www.heise.de/-4155012
4.15. INSTALLIERTE SCHRIFTARTEN VERSTECKEN

Blockieren externer Schriftarten mit Add-ons?

Einige Firefox Add-ons wie uBlock Origin oder uMatrix können mit einer Option den Download von zusätzlichen Schriftarten blockieren. Dabei gibt es folgende Nachteile:


2. Die Add-ons können nicht zwischen Fonts für eine hübsche Schrift (entbehrlich) und notwendigen Fonts für die Darstellung von Icons für die Navigation unterscheiden. Viele Webseiten werden dadurch unbrauchbar.

3. Das Blockieren des Downloads externer Schriftarten schützt nicht gegen das Auslesen lokal installierter Fonts für das Fingerprinting des Browsers.

Deshalb ist die Nutzung des Features externe Schriftarten blockieren in uBlock Origin oder uMatrix suboptimal und wird hier nicht empfohlen.

Konfiguration der Schriftarten in Firefox

Um das Laden von externen Schriftarten zu blockieren, deaktiviert man in den Einstellungen die Optionen Webseiten das verwenden von eigenen Schriften erlauben und die CSS Font Loading API. Damit sehen einige Webseiten nicht mehr ganz so hübsch aus, die Einschränkungen sind aber gering:

```
browser.display.use_document_fonts = false
layout.css.font-loading-api.enabled = false
```

Das Underline Handling sollte man deaktivieren, da es zum Fingerprinting der installierten Schriftarten und zur Erkennung des Betriebssystems verwendet werden kann:

```
font.blacklist.underline_offset = "" (leerer String)
```


```
Verfassen
```

Um diese Probleme zu vermeiden, ist die Freigabe von downloadbaren Schriften für die Darstellung von Symbolen empfehlenswert für weniger strenge Sicherheitsanforderungen. Damit werden Icons wieder korrekt dargestellt:

```
gfx.downloadable_fonts.enabled = true
```

Für hohe Sicherheitsanforderungen kann man das Rendering von OpenType SVG Fonts und die Graphite Engine deaktivieren, um die Angriffsfläche zu reduzieren. Die Graphite Engine wird nur für die verbesserte Darstellung komplexer asiatischer Schriften benötigt:

```
gfx.font_rendering.opentype-svg.enabled = false
gfx.font_rendering.graphite.enabled = false
```

KAPITEL 4. SPURENARM SURFEN

Abbildung 4.18: Schriftarten auswählen

4.16 HTML5 Canvas Elemente

Das HTML5 Canvas Element ist ein Grafikbereich auf der Webseite, in den der Browser mit JavaScript zeichnen kann. Ähnlich wie bei einem Zeichenprogramm kann man auch Text schreiben. Die Trackingbranche hat Methoden entwickelt, um diese Technologie für die Berechnung eines individuellen Fingerprinting des Browser zu nutzen.


Schutz gegen Fingerprinting mit HTML5 Canvas

Das Add-on CanvasBlocker kann Zugriffe auf Canvas-API faken (geringfügig modifizieren) oder faken. Daneben werden noch weitere Javascript-APIs modifiziert wie die

60 https://www.browserleaks.com/canvas
61 https://www.browserleaks.com/rects
62 https://addons.mozilla.org/de/firefox/addon/canvasblocker/
4.16. HTML5 CANVAS ELEMENTE

Audio-API oder die Screen-API zum Auslesen der Fenster- und Bildschirmgröße, die als Informationen für Browserfingerprinting genutzt werden.

Der Name des Add-ons CanvasBlocker kommt daher, dass die Entwicklung mit dem Faken bzw. Blockieren der Canvas-API begann, um Tracking mit der Canvas-API zu stören. Inzwischen hat sich das Add-on zu einem umfangreicheren Tool entwickelt.

CanvasBlocker bietet viele Einstellungsmöglichkeiten. Um die Konfiguration zu vereinfachen, bietet es drei Presets von Einstellungen, die bei der Installation angeboten werden:

1. Convenient Settings (nur leichte Modifikationen der APIs)

2. Stealth Settings (meiner Meinung nach die besten Einstellungen, da sie einen umfangreichen Schutz bieten aber schwer als Fakes erkennbar sind)
   
   Wenn man den Expert Mode aktiviert, kann man zusätzlich die persistente Speicherung von Daten abschalten oder nach X Tagen löschen lassen, damit man langfristig nicht anhand der immer gleichen Fakes auf einer Domain identifiziert wird.

3. Maximum Protection (maximaler Schutz aber mit kleinen Störungen auf einigen Websites, außerdem sind die Fakes teilweise durch Trackingscripte erkennbar)


Abbildung 4.19: CanvasBlocker: Presets für die Konfigurationsparameter auswählen
Whitelisting vertrauenswürdiger Webseiten


Wenn der Zugriff auf eine geschützte Javascript API festgestellt wird, erscheint in der URL-Leiste ein kleiner Fingerabdruck als Symbol. Wenn man auf den Fingerabdruck klickt, erscheint eine Fenster mit den Informationen, auf welche APIs die Webseite zugreift.

Mit einem Klick auf das grüne Häckchen kann man einen dauerhaften Eintrag für die Whitelist erstellen oder mit einem Klick auf das grüne Häckchen mit der Uhr einen temporären Eintrag, der bis zum Schließen des Browsers gültig ist. Im zweiten Schritt legt man fest, ob der Eintrag für die gesamte Domain gültig sein soll oder nur für die aktuelle Seite.

4.17 Zugriff auf lokale URLs blockieren

Neugierige oder bösertige Webseiten könnten z.B. mit JavaScript über Adressen wie http://localhost... oder http://192.168.1.1... auf lokale Dienste auf dem eigenen Rechner, auf den Router oder auf andere Dienste im lokalen Netzwerk (LAN) zugreifen:


- Bösertiger JavaScript Code könnte lokale Dienste wie CUPS oder andere Rechner im LAN angreifen. Im Mai 2015 wurde ein Exploit-Kit entdeckt, der als böses JavaScript auf Webseiten platziert wird und bei Aufruf der Webseite den Router angreift, um DNS Einstellungen zu ändern und den Internetzugriff beliebig zu manipulieren.64

- Die Firma ThreadMetrix hat 2015 für die Webseiten von Banken einen Sicherheitsmechanismus entwickelt, der unter anderem via Javascript bestimmte Ports auf dem lokalen Rechner scannt, die für einige Viren, Fernwartungssoftware und Remote Desktops wie VNC typisch sind. Seit Mai 2020 ist ein ähnliches Feature auch bei eBay aktiv, wenn eBay vermutet, dass der Anwender Windows nutzt. Dabei handelt sich um ein Sicherheitsfeature und keinen Angriff oder Tracking, aber trotzdem...

---

63 https://mailman.boum.org/pipermail/tails-dev/2015-April/008607.html
64 https://heise.de/-2665387
4.18 DER UNSINN VOM SPOOFEN DER USER-AGENT KENNUNG

Nachdem eBay im Mai 2020 begonnen hatte, die lokalen Ports zu scannen, hat das uBlock Team reagiert und eine Filterliste erstellt. Diese Filterliste blockiert für Webseiten aus dem Internet den Zugriff auf lokale URLs, Adressen im LAN sowie häufige Router Adressen.

Zukünftig wird die LAN-Block-Filterliste (wahrscheinlich) in die Standardlisten von uBlock Origin aufgenommen werden aber bei Installation standardmäßig deaktiviert sein. Aktuell muss man die LAN-Block-Filterliste von gwarsers noch selbst auf dem Reiter Filterlisten hinzufügen, indem man die Liste von folgender Adresse lädt:


Abbildung 4.20: uBlock Origin: Filterliste hinzufügen

4.18 Der Unsinn vom Spoofen der User-Agent Kennung

Bei jedem Aufruf einer Webseite oder dem Laden von Bildern o.ä. sendet der Browser in den HTTP Request Header Informationen wie die bevorzugten Dateitypen, die bevorzugte Sprache oder die User-Agent Kennung mit Informationen über den verwendeten Browser, die Version des Browsers und das Betriebssystem. Firefox 72 für Linux sendet zum Beispiel:

Mozilla/5.0 (X11; Linux x86_64; rv:72.0) Gecko/20100101 Firefox/72.0

Aus unterschiedlichen Gründen wird immer wieder empfohlen, die User-Agent Kennung zu modifizieren (faken). Linuxer und MacOS Nutzer sollen als Fake die Kennung von Google Chrome für Windows verwenden, weil dieser Browser häufiger verwendet wird und man damit angeblich besser in der Masse untertaucht. Windows Nutzer sollen ein Linux spoofen, um sich gegen Drive-by-Downloads von Malware zu schützen… u. a. m.

Es ist nahezu unmöglich, die User-Agent Kennung eines Browsers plausibel zu faken. Eine unsachgemäße Änderung kann zu einem einzigartigen Gesamtbild führen, welches das Tracking enorm erleichtert und man erreicht das Gegenteil des Beabsichtigten. Der Anonymitätstest von JonDonym entlarvt viele Fehler:


http://ip-check.info
Das Add-on *User-Agent-Overrider* (Version 0.2.5.1) sollte im Test einen Internet Explorer 9.0 für Win64 faken. Die Header Signatur entlarvt den Browser jedoch als einen Firefox, der sich als IE tarnen will.

**Signatur**
```
8eb3a216c55e8986e30e65c306466 (Firefox)
```

**User-Agent**
```
Mozilla/5.0 & compatible, MSIE 9.0, Windows NT 6.4, WCWS64, Trident9.0
```

Das Add-on *Random-Agent-Spoof* (Version 0.9.5.2) sollte im Test einen Google Chrome Browser 41.0 für Win64 faken. Die User-Agent Header entlarvt den Browser ebenfalls als Firefox, der sich tarnen will.

**Signatur**
```
8eb3a24cc56864e30e65e9b04eb94c6 (Firefox)
```

**User-Agent**
```
Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36
```

Firefox Release Versionen und Firefox ESR Versionen unterscheiden sich nicht nur in der Version in der User-Agent Kennung sondern auch in anderen Eigenschaften. Firefox 68.x ESR und Firefox 72+ unterscheiden sich im HTTP-Accept Header:

Firefox 68: ...application/xml;q=0.9,*/*;q=0.8
Firefox 72: ...application/xml;q=0.9, image/webp,*/*;q=0.8


**Javascript:** Das Add-on User Agent Platform Spoof macht aus einem Firefox für Windows einen Firefox für Linux und umgekehrt, um die automatische Installation von Malware im Drive by Download zu erschweren. Auch hier ist der Fake nicht vollständig, wie ein kurzer Test unter Linux zeigt. Mit Javascript kann der genutzte Browsertyp und Betriebssystem ermittelt werden:

```
User-Agent via HTTP Header: Mozilla/5.0 (Windows NT 10.0; Win64; x64;... 
Browsertyp via JavaScript: Mozilla/5.0 (X11) 20100101/...
```

Das gleiche gilt auch für TorBrowser unter Linux, wenn man bei einem Firefox für Linux die Option *privacy.resistFingerprinting* aktiviert oder *general.useragent.override* verwendet, um ein anderes Betriebssystem vorzutäuschen. Via Javascript kann man diese Fakes recht einfach entlarven.


**Seltsamkeiten:** Der Browser hängt in viele Dinge von Bibliotheken des Betriebssystems ab. Durch Auswertung einige Seltsamkeiten lässt sich das real verwendete Betriebssystem teilweise identifizieren oder zumindest ein User-Agent Fake entlarven. Ein Beispiel OS-spezifische Seltsamkeiten ist das Ergebnis der folgenden Berechnung:

```
Math.tan(-1e300) = -4.987183803371025 (Windows)  
Math.tan(-1e300) = -1.4214488238747245 (Linux, iOS) 
```

**Plug-ins:** verraten in der Regel das verwendete Betriebssystem und können dafür keinen Fake konfigurieren. Wenn man auf Flash u.a. nicht verzichten kann, dann sollte man keinen User-Agent Fake verwenden.
4.19. HARDWARE FINGERPRINTING

Schlussfolgerung

Es ist nahezu unmöglich, die User-Agent Kennung von Firefox plausibel in allen Punkten zu faken. Selbst die Entwickler des TorBrowserBundles, die jahrelange Erfahrungen dabei haben und für alle für Nutzer des Anonymisierungsdienstes den einheitlichen Fingerprint eines englischen Firefox ESR für Windows anstreben, können nicht vollständig verhindern, dass Linux oder MacOS Nutzer erkannt werden können.

Ein unvollständiger Fake-Versuch ist aber ein gutes Identifizierungsmerkmal für Trackingdienste, da man sich von der großen Masse der Surfer stärker unterscheidet.

Eine kleine Ausnahme für Linuxer

Viele Linux Distributionen bauen einen Firefox, der in der User-Agent Kennung des Browser den Namen der Linux Distribution mit einfügt. Hier könnte man einen generischen Firefox für Linux vortäuschen, um die überflüssige Information der genutzten Linux Distribution aus der Kennung zu entfernen indem amn folgenden Wert für die Variable general.useragent.override einträgt:

```
Mozilla/5.0 (X11; Linux x86_64; rv:73.0) Gecko/20100101 Firefox/73.0
```

Bei jedem Update des Browsers ist die Kennung an die aktuelle Version anzupassen.

4.19 Hardware Fingerprinting

Über verschiedenen API-Schnittstellen können Trackingscripte Informationen über die Hardware des Rechners sammeln. Durch Messung der Performance aufwendiger Grafik Rendering Operationen oder beim Abspielen von Videos können Trackingscripte ebenfalls Informationen über die Hardware sammeln.

**Bildschirm:** Informationen über die Größe des Monitors und des Browserfensters werden am häufigsten für das Hardwarefingerprinting genutzt. Es liegen keine wissenschaftlichen Analysen zur Verbreitung dieser Trackingmethode vor, aber grob geschätzt werden diese Informationen von 30-50% der Webseiten ausgewertet. Insbesondere auf größeren Portalen wie heise.de, spiegel.de, zeit.de oder google.com findet man fast immer Trackingscripte, die Bildschirmgröße und Größe des Browserfensters für das Fingerprinting des Browsers nutzen.

Das Add-on CanvasBlocker kann Zugriffe auf die Screen-API faken und verwendet die am besten passende Bildschirmgröße aus folgenden häufigen Werten: 1366x768, 1440x900, 1600x900, 1920x1080, 4096x2160 und 8192x4320.

Die Verwendung von CanvasBlocker ist empfehlenswert, da es für den Fake Bildschirmgrößen verwendet, die in-the-wild häufig vorkommen. Daneben gibt es noch die von TorProject.org entwickelte Option zum Faken der Bildschirmgröße, die mit den folgenden Variablen unter about:config aktiviert wird:

```
privacy.resistFingerprinting = true
privacy.resistFingerprinting.letterboxing = true
```


Außerdem werden noch folgende Features mit dieser Option aktiviert:
• Als User-Agent wird die Kennung eines Firefox ESR für Windows verwendet. Der unvollständiger Fake des User-Agent ist eher kontraproduktiv und erleichtert Fingerprinting, wenn man keinen Firefox ESR für Windows verwendet!
• Zeitzone des Browsers wird auf UTC gesetzt (anhand der IP-Adresse ist trotzdem erkennbar, in welcher Zeitzone der Nutzer sich befindet).
• Die Option Öffnen mit... wird im Download Dialog deaktiviert. Downloads müssen gespeichert werden und können nicht aus dem Browser heraus mit anderen Anwendungen geöffnet werden.
• navigator.plugins and navigator.mimeTypes sind nicht auslesbar.
• Auslesen der Screen Rotation liefert immer Querformat.
• Die Genauigkeit von Timming Events wird auf min. 100ms reduziert.


AudioContext: Mit der Audio-API kann Javascript unhörbare Soundschnipsel im Audio-Buffer generieren, manipulieren und die Ergebnisse wieder auslesen. Dabei unterscheiden sich die Ergebnisse in Abhängigkeit von der Audiohardware und -software. Die Daten können für das Fingerprinting genutzt werden, wie die AudioContext Fingerprint Test Page zeigt. Das Add-on CanvasBlocker kann Zugriffe auf die Audio-API faken (geringfügig modifizieren) und damit ein Fingerprinting des Browsers verhindern. Das Ergebnis ist zwar unique aber immer wieder anders. Alternativ kann die Audio-API mit folgender Option deaktiviert werden:

```javascript
dom.webaudio.enabled = false
```

Das Faken der Audio-API mit dem Add-on CanvasBlocker ist unauffälliger und schwerer erkennbar als das Blockieren der API und deshalb empfohlen.


```javascript
gfx.direct2d.disabled = true
layers.acceleration.disabled = true
media.hardware-video-decoding.enabled = false
```

Statistiken für Videos: Die Übermittlung von Statistiken beim Abspielen von Videos (Framerate usw.) kann unter about:config deaktiviert werden:

```javascript
media.video_stats.enabled = false
```


```javascript
dom.gamepad.enabled = true (Default in Firefox)
```

AudioContext: Mit der Audio-API kann Javascript unhörbare Soundschnipsel im Audio-Buffer generieren, manipulieren und die Ergebnisse wieder auslesen. Dabei unterscheiden sich die Ergebnisse in Abhängigkeit von der Audiohardware und -software. Die Daten können für das Fingerprinting genutzt werden, wie die AudioContext Fingerprint Test Page zeigt. Das Add-on CanvasBlocker kann Zugriffe auf die Audio-API faken (geringfügig modifizieren) und damit ein Fingerprinting des Browsers verhindern. Das Ergebnis ist zwar unique aber immer wieder anders. Alternativ kann die Audio-API mit folgender Option deaktiviert werden:

```javascript
dom.webaudio.enabled = false
```

Das Faken der Audio-API mit dem Add-on CanvasBlocker ist unauffälliger und schwerer erkennbar als das Blockieren der API und deshalb empfohlen.


```javascript
gfx.direct2d.disabled = true
layers.acceleration.disabled = true
media.hardware-video-decoding.enabled = false
```

Statistiken für Videos: Die Übermittlung von Statistiken beim Abspielen von Videos (Framerate usw.) kann unter about:config deaktiviert werden:

```javascript
media.video_stats.enabled = false
```


```javascript
dom.gamepad.enabled = true (Default in Firefox)
```

66) https://audiofingerprint.openwpm.com
4.20 WEBRTC MIT FIREFOX

**Vibrator-API:** kann eine Vibration des Gerätes auslösen. Die Funktion liefert keine Informationen zur realen Ausführung. Das Ergebnis ist FALSE, wenn die Parameter nicht korrekt waren und TRUE in allen anderen Fällen. Wenn eine ausgelöste Vibration länger als die maximal zulässige Dauer ist, wird sie ohne Rückmeldung gekürzt.

Die Vibrator-API kann in Kombinationen mit anderen Mechanismen die Privatsphäre gefährden, wie das W3C in den *Security and Privacy Considerations* schreibt:

> Vibration API provides an indirect privacy risk, in conjunction with other mechanisms. This can create possibly unexpected privacy risks, including cross-device tracking and communication. Additionally, a device that is vibrating might be visible to external observers and enable physical identification, and possibly tracking of the user.

Die komplette Deaktivierung der Vibrator-API könnte als Fingerprinting Merkmal ausgewertet werden, da die API im Navigator Objekt nicht mehr sichtbar wäre. Unauffälliger ist es, die max. Vibrationsdauer auf 0 zu setzen.

```javascript
dom.vibrator.max_vibrate_ms = 0
```

**Sensoren:** Die Sensor-API von Firefox liefert folgende Daten aus der Umgebung:

1. Ambient Light Sensor: kann die die Helligkeit der Umgebung abfragen.
4. Device Motion Sensor: liefert Informationen über die Bewegung des Gerätes.


Sensoren für die Lage eines Gerätes und Gyroskope zur Beobachtung von Bewegungen sind in Smartphones vorhanden aber in der Regel nicht in PCs oder Laptops. Daher liefern die beiden letztgenannten APIs auf diesen Geräten in keine Daten und können daher aktiviert bleiben. Webseiten könnten eine Deaktivierung erkennen und als Merkmal für das Fingerprinting verwenden, wie Browsersleaks demonstriert.\(^\text{67}\)

Aus den gleichen Gründen wird die Deaktivierung der gesamten Sensor-API nicht empfohlen. Für Smartphones ist das Risiko anders zu bewerten..

**4.20 WebRTC mit Firefox**

WebRTC wurde von Google und Mozilla initiiert und später vom W3C standardisiert, um der Konkurrenz von Microsoft Skype etwas entgegen zu setzen. Google und Mozilla entschieden sich dafür, die Funktionalität in die Browser zu integrieren, um den Browser als universele Anwendung für jegliche Internetkommunikation auszubauen.


\(^{67}\)https://browserleaks.com/features
OpenH264 Videocodecs

Um WebRTC mit Firefox zu verwenden, wird das OpenH264 Plugin von Cisco benötigt, das die Videocodecs bereitstellt. Das Plugin ist Closed Source und wird beim ersten Start von Firefox automatisch herunter geladen und im Profilverzeichnis gespeichert.

Mit folgende Einstellungen unter about:config wird das OpenH264 Plugin aktiviert:

```
media.gmp-gmpopenh264.enabled = true
media.gmp-gmpopenh264.autoupdate = true
media.gmp-gmpopenh264.provider.enabled = true
```

Bei einigen sicherheitsoptimierten Linux Distributionen wie RHEL oder Fedora ist das Plugin standardmäßig deaktiviert. Oft sind Probleme mit browserbasierten Videokonferenzen darauf zurück zu führen, dass das Plugin nicht aktiviert wurde.

Internet Connectivity Establishment (ICE)

Der Datenstrom soll bei WebRTC möglichst direkt zwischen den Teilnehmern ausgetauscht werden. Es wird der ICE Standard (Internet Connectivity Establishment) verwendet, um eine direkte Verbindung zwischen den Clients aufzubauen. ICE versucht im Hintergrund sehr aggressiv, die direkte Verbindung irgendwie herzustellen. Es werden Proxy Einstellungen umgangen, via UPnP wird versucht, ein Loch in Router und Firewalls zu bohren, VPNs werden teilweise ausgetrickst... Dabei kommt ein STUN Server zum Einsatz, der die verschiedenen Möglichkeiten ausprobiert. Wenn wirklich keine direkte Verbindung möglich ist, wird ein TURN Server als Proxy für den Datenstrom verwendet.

Aufgrund dieser aggressiven Strategie zum Verbindungsaufbau können der Gegenseite folgende Informationen bekannt werden, wie der WebRTC Test von Browserleaks zeigt:

- Alle IP-Adressen und Interfaces des Rechners oder der VM im lokalen LAN. (Ein Angreifer oder Trackingservice könnte das verwenden, um mehrere Rechner innerhalb eines Firmennetzwerkes oder in einem Haushalt zu unterscheiden.)
- Externe Adresse des Routers/Gateways zum Internet. (Diese Adresse sollte eigentlich geheim bleiben, wenn man einen Proxy wie Tor Onion Router oder ein VPN verwendet. Aber alle Proxys und einige VPN Techniken können von ICE ausgetrickst werden und damit den Nutzer deanonymisieren.)
- Externe Adresse des Proxy oder VPN Endpunktes. (Diese Information lässt sich natürlich nicht geheim halten.)

Firefox bietet einige Möglichkeiten, die Privacy Probleme von ICE zu reduzieren:

1. Bei privater Nutzung kann man davon ausgehen, dass man innerhalb der Wohnung mündlich kommuniziert und nicht via WebRTC. Die internen Adressen aus dem LAN müssen nicht publiziert werden. Mit folgenden Optionen man es abschalten:

```
media.peerconnection.ice.default_address_only = true
media.peerconnection.ice.no_host = true
```

2. Wenn man verhindern möchte, dass die Gegenseite die externe IP-Adresse des Routers erfährt und damit Schlussfolgerungen über den Standort via Geolocation ziehen könnte, kann man direkte Verbindungen generell ausschließen und immer eine Verbindung über einen TURN Proxy Server erzwingen:

   *https://browserleaks.com/webrtc*
3. Wenn man den STUN/TURN Servern des Videokonferenzanbieters nicht vertraut, kann man eigene Server verwenden:

```javascript
media.peerconnection.use_document_iceservers = false
```

Die eigenen Server muss man in der folgenden Variable definieren:

```javascript
media.peerconnection.default_iceservers = <Serverliste>
```

4. Wenn man WebRTC nur via VPN verwenden möchte aber nicht, wenn man ohne VPN surft, dann kann man die zulässigen Netzwerkinterfaces definieren:

```javascript
media.peerconnection.ice.force_interface = tun1
media.peerconnection.ice.no_host = true
```

Wenn das VPN nicht aktiviert wurde und damit das virtuelle VPN Interface `tun1` nicht vorhanden ist, kann man ganz normal surfen aber eine WebRTC Verbindung wird nicht akzeptiert. Nur wenn das VPN aktiv ist, ist eine WebRTC Verbindung möglich, deren Daten immer durch das VPN geschickt werden.

5. Ähnlich wie bei der VPNs kann man auch die Verwendung eines Proxy erzwingen und WebRTC nur via Proxy zulassen:

```javascript
media.peerconnection.ice.proxy_only = true
```

In den meisten Fällen wird WebRTC mit dieser Einstellung nicht funktionieren, da HTTP- oder SOCKS-Proxy wie Tor Onion Router nicht UDP-fähig sind.

Mit dem WebRTC Test⁶⁹ kann man prüfen, ob die Einstellungen korrekt funktionieren.

### Media Device Enumeration

Um WebRTC nutzen zu können, muss Firefox wissen, welche Media Input Devices vorhanden sind und nach Zustimmung durch den Nutzer Zugriff darauf erlangen können:

```javascript
media.navigator.enabled = true
media.navigator.video.enabled = true
```

Trackingdienste können die Media Device Enumeration von WebRTC ausnutzen, um Daten über Kamera und Mikrofon zu sammeln und für das Hardware Fingerprinting zu verwenden. Der Surfer wird dabei nicht um Zustimmung für einen Zugriff auf Kamera oder Mikrofon gebeten. Der WebRTC Test von Browserleaks demonstriert es.

Firefox verwendet als Device-IDs einen gesalzenen Hash. Der Salt für die Berechnung des Hashes wird beim ersten Start festgelegt und immer erneuert, wenn Cookies und Cache Daten gelöscht werden. Außerdem ist der Salt in Surfcontainern unterschiedlich. Damit ist die Device-ID in gleicher Weise wie langlebige Cookies für das Tracking geeignet oder nicht geeignet wie Cookies und als Schutz gegen Tracking anhand der Device-IDs kann man die Empfehlungen für Cookies umsetzen.

⁶⁹[https://test.webrtc.org/](https://test.webrtc.org/)
KAPITEL 4. SPURENARM SURFEN

Abbildung 4.21: Media Device Enumeration via WebRTC

WebRTC und OpenH264 Plugin deaktivieren

Wenn man den Browser nur zum Surfen verwendet und nicht für Videokonferenzen mit Jitsi Meet oder ähnlichen Systemen, kann man WebRTC, Media Device Enumeration und das OpenH264 Plugin deaktivieren, um Trackingfeatures und Angriffsfläche zu minimieren:

```
media.peerconnection.enabled = false
media.navigator.enabled = false
media.navigator.video.enabled = false
media.gmp-gmpopenh264.enabled = false
media.gmp-gmpopenh264.autoupdate = false
media.gmp-gmpopenh264.provider.enabled = false
media.gmp-gmpopenh264.visible = false
```

4.21 DNS-over-HTTPS mit Firefox

DNS (Domain Name Service) ist das Telefonbuch des Internet. Es übersetzt lesbare URLs wie www.privacy-handbuch.de in die IP-Adresse des Servers, der diese Webseite zur Verfügung stellt. Eine ausführliche Anleitung zu diesem zentralen Internetdienst findet man im Kapitel DNS und DNSSEC.

Firefox kann DNS-over-HTTPS nutzen, um die DNS Daten beim Surfen zu verschlüsseln und eine Zensur durch DNS-Server der Provider zu umgehen. Das Feature heißt TRR (Trusted Recursive Resolver). Die Konfiguration ist einfacher, als als einen DNS Daemon mit DNS-over-TLS Support oder DNSCrypt zu installieren. Es schützt allerdings nur den DNS Datenverkehr beim Surfen mit Firefox und alle andere Anwendungen nicht.

Da DNS ein zentraler Dienst für alle Internet Anwendungen ist, ist eine zentrale Konfiguration der DNS-Server sinnvoller als die Konfiguration einzelner Webbrowser.

Browserfingerprinting mittels DNS Server

Eine Trackingdienst könnte ermitteln, welcher DNS-Server vom Browser verwendet wird, und diese Information als Parameter für das Fingerprinting des Browser verwenden:

4.21. DNS-OVER-HTTPS MIT FIREFOX

2. Der Browser versucht die IP-Adresse für diese Subdomain zu ermitteln. Der konfigurierte Upstream DNS-Server hat die Information nicht im Cache und muss deshalb den authoritativen Server des Trackingdienstes anfragen.

3. Der authorative DNS-Server des Trackingdienstes registriert die DNS Anfrage und die IP-Adresse des anfragenden DNS-Servers und sendet beides an den Trackingservice, wo die Information mit dem Aufruf der Webseite korreliert werden kann.

Es gibt bisher noch keine Studien, die untersucht haben, ob dieses Verfahren genutzt wird. Aber es ist prinzipiell möglich. Deshalb sollte man kurz nachdenken, ob es Gründe gibt, einen selbst ausgewählten DNS-Server zu nutzen, ob der Vorteil an Sicherheit und Schutz gegen Zensur evtl. unerwünschte Nebeneffekte kompensiert. (Trackigdienste, die via uBlock Origin o.ä. blockiert werden, können auch den DNS Server nicht auswerten.)

**Konfiguration in den Netzwerk Einstellungen**

In den Einstellungen für die Netzwerkverbindung kann man DNS-over-HTTPS aktivieren und die URL für den DNS-Server eintragen, wenn man die Option *Custom* wählt. Eine Liste von Servern findet man unten in der Konfiguration für Experten.

Wenn man eine der user.js Konfiguration installiert hat, dann kann man einen privacyfreundlichen Provider direkt auswählen, der HTTPS-over-DNS anbietet (Abb 4.22).

![Abbildung 4.22: Konfiguration der DNS-over-HTTPS](image)

**Konfiguration für Experten**

Mit folgenden Werten könnte man TRR in Firefox unter *about:config* konfigurieren:

- Mit dem TRR-Mode kann man auswählen, wie DNS-over-HTTPS verwendet wird:

  ```
  network.trr.mode = 0 (Abgeschaltet aufgrund der Default Einstellung.)
  network.trr.mode = 1 (Fragte System DNS und TRR und verwendet erstes Ergebnis.)
  network.trr.mode = 2 (Verwende TRR und System DNS nur als Fallback.)
  network.trr.mode = 3 (Verwende ausschließlich TRR nach dem Start.)
  network.trr.mode = 4 (TRR parallel zum System DNS aber nicht verwenden.)
  network.trr.mode = 5 (Abgeschaltet aufgrund der Entscheidung des Nutzers. FF61+)
  ```
Firefox für Windows deaktiviert DNS-over-HTTPS unabhängig von den Einstellungen für network.trr.mode, wenn ein VPN genutzt wird, wenn ein Proxy in den Windows Systemeinstellungen konfiguriert wurde oder wenn mittels NRPT spezielle DNS Server für einzelne Domains festgelegt wurden. Wenn man mit Firefox für Windows trotz VPN, Proxy oder NRPT einen DNS-over-HTTPS Server verwenden möchte, muss man folgende Einstellungen aktivieren:

```plaintext
network.trr.enable_when_vpn_detected = true
network.trr.enable_when_proxy_detected = true
network.trr.enable_when_nrpt_detected = true
```

- Wenn man TRR-Mode 1-3 verwenden möchte, dann muss man die zwingend notwendige Validierung von SSL-Zertifikaten via OCSP-Server abschalten. Ansonsten beißt sich die Katze in den Schwanz. Firefox will das SSL-Zertifikat des DNS-over-HTTPS Server prüfen und braucht dafür die IP-Adresse des OCSP Servers vom DNS-over-HTTPS Server... Also entweder OCSP komplett deaktivieren:

```plaintext
security.OCSP.enabled = 0
```

Oder nicht zwanghaft auf eine OCSP Antwort bestehen:

```plaintext
security.OCSP.required = false
```

- Konfiguration für den DNS-over-HTTPS Server von Freifunk München:

```plaintext
network.trr.uri = https://doh.ffmuc.net
network.trr.bootstrapAddress = 5.1.66.255
```

- Konfiguration für den DNS-over-HTTPS Server der Digitalen Gesellschaft (CH):

```plaintext
network.trr.uri = https://dns.digitale-gesellschaft.ch/dns-query
network.trr.bootstrapAddress = 185.95.218.42
```

- Konfiguration für den DNS-over-HTTPS Server von dnsforge.de (mit Ad-Filter):

```plaintext
network.trr.uri = https://dnsforge.de/dns-query
network.trr.bootstrapAddress = 176.9.1.117
```

- Konfiguration für den DNS-over-HTTPS Server von BlahDNS DE (mit Ad-Filter):

```plaintext
network.trr.uri = https://doh-de.blahdns.com/dns-query
network.trr.bootstrapAddress = 159.69.198.101
```

- Konfiguration für den DNS-over-HTTPS Server von BlahDNS FI (mit Ad-Filter):

```plaintext
network.trr.uri = https://doh-fi.blahdns.com/dns-query
network.trr.bootstrapAddress = 95.216.212.177
```

- Konfiguration für Quad9 DNS-over-HTTPS Server:

```plaintext
network.trr.uri = https://dns.quad9.net/dns-query
network.trr.bootstrapAddress = 9.9.9.9
```

- Konfiguration für Standard Cloudflare DNS-over-HTTPS Server:

```plaintext
network.trr.uri = https://cloudflare-dns.com/dns-query
network.trr.bootstrapAddress = 1.1.1.1
```
4.22 Sonstige Maßnahmen

Am Schluss der Konfiguration gibt es noch ein paar kleine Maßnahmen, die überflüssige Features im Browser deaktivieren, die Informationen preisgeben.

Überflüssige Cloud-Dienste deaktivieren

Firefox bietet mehrere Dienste, die die User Experience verbessern sollen und dafür irgendwelche Daten auf irgendwelche Cloud Server hochladen:

Pocket-API ist eine Erweiterung, mit der man Webseiten komplett in einem sogenannten Pocket speichern und später lesen kann. In der Praxis kann man natürlich auch Lesemarken dafür nutzen oder die Download Funktion, wenn man eine Webseite später in genau diesem Zustand lesen möchte. Die Pocket-API ist überflüssig, kann man unter about:config deaktivieren:

```plaintext
extensions.pocket.enabled = false
```

Screenshots ist eine Erweiterung, mit der man Bildschirmfotos erstellen kann, die automatisch auf den Cloud-Server screenshots.mozilla.com hochgeladen werden und von dort ganz einfach mit einem Klick auf Social Media Webseiten verbreitet werden könnten. In den Datenschutzhinweisen weist Mozilla darauf hin, dass nicht nur der Upload der Screenshots protokolliert wird, sondern auch jeder Abruf durch Dritte, die die Screenshot auf irgendwelchen Social Media Webseiten betrachten, wo sie veröffentlicht wurden. Den Upload von Screenshots kann man unter about:config mit folgendem Parameter deaktivieren:

```plaintext
extensions.screenshots.upload-disabled = true
```

Wenn ich einen Screenshot haben möchte, dann gibt es dafür genügend Tools, die Screenshots erstellen können und ich entscheide dann, wie ich sie publiziere. Die Screenshot Extension kann man auch unter about:config komplett deaktivieren:

```plaintext
extensions.screenshots.disabled = true
```

---

70 https://www.mozilla.org/de/privacy/firefox
Keine Daten beim Ausfüllen von Formularen speichern


Firefox bietet einige Schutzfunktionen gegen Phishing Angriffe auf automatisch ausgefüllte Formularedaten. Trotzdem ist es nicht auszuschließen, dass raffinierte Angreifer Wege finden werden, um unsichtbare Formulare automatisch ausfüllen zu lassen und die Daten auslesen. Unter about:config kann man das Speichern von Formulardaten abschalten:

```
browser.formfill.enable = false
```

Zusätzlich kann man folgende Features deaktivieren:

```
extensions.formautofill.addresses.enabled = false
extensions.formautofill.creditCards.enabled = false
extensions.formautofill.heuristics.enabled = false
```

WebGL konfigurieren oder deaktivieren

WebGL stellt eine JavaScript-API für das Rendering von 3D-Objekten bereit. Wenn die Debug Informationen via Javascript auslesbar sind, können Informationen über den Hersteller das Modell der Grafikkarte ausgelesen werden. Diese Informationen sind gut für das Fingerprinting geeignet. Deshalb sollten die WebGL Debug Informationen in jedem Fall abgeschaltet werden:

```
webgl.enable-debug-renderer-info = false
```

WebGL kann die Performance der Grafikhardware und OpenGL Software für das Fingerprinting verwenden, wie die Studie Perfect Pixel: Fingerprinting Canvas in HTML5\(^\text{71}\) zeigte. Das Fingerprinting via WebGL kann mit folgenden Einstellungen reduziert werden:

```
webgl.min_capability_mode = true
webgl.disable-fail-if-major-performance-caveat = true
```


```
webgl.disabled = true
webgl.enable-webgl2 = false
```

Timing APIs deaktivieren

Die hochgenauen Timing APIs können von Webanwendungen zur Analyse des Ladens von Ressourcen oder des Nutzerverhaltens missbraucht werde, siehe: Timing Attacks on Web Privacy\(^\text{72}\). Wenn man seinen Browser zum Lesen von Webseiten und nicht vorrangig für Games verwendet, sollte man die APIs deaktivieren:

```
dom.enable_resource_timing = false
dom.enable_performance = false
dom.enable_performance_navigation_timing = false
```

\(^{71}\)http://www.w2spconf.com/2012/papers/w2sp12-final4.pdf

\(^{72}\)http://sip.cs.princeton.edu/pub/webtiming.pdf
4.22. SONSTIGE MASSNAHMEN

Clipboard Events deaktivieren

Mit den Clipboard Events informiert Firefox eine Webseite, dass der Surfer einen Aus- schnitt in die Zwischenablage kopiert hat oder den Inhalt der Zwischenablage in ein Formularfeld eingefügt hat. Es werden die Events `oncopy`, `oncut` and `onpaste` ausgelöst, auf die die Webseite reagieren kann. Man kann diese Events unter `about:config` deaktivieren:

```
    dom.event.clipboardevents.enabled = false
```

Außer bei Google Docs und ähnliche JavaScript-lastigen GUIs zur Dokumentenbearbeitung in der Cloud ist mir keine sinnvolle Anwendung dieses Features bekannt.

Spekulatives Laden von Webseiten

Firefox beginnt in einigen Situationen bereits mit dem Laden von Webseiten, wenn sich der Mauszeiger über einem Link befindet, also bevor man wirklich klickt. Damit soll das Laden von Webseiten einige Millisekunden beschleunigt werden. Wenn man Verbindungen mit unerwünschten Webservern vermeiden möchte, kann man das Feature unter `about:config` abschalten:

```
    network.http.speculative-parallel-limit = 0
```

Kill Switch für Add-ons abschalten

Die Extension blocklist\(^\text{73}\) kann Mozilla nutzen, um einzelne Add-ons im Browser zu deaktivieren. Es ist praktisch ein kill switch für Firefox Add-ons und Plug-ins. Beim Aktualisieren der Blockliste werden detaillierte Informationen zum realen Browser und Betriebssystem an Mozilla übertragen.

```
https://addons.mozilla.org/blocklist/3/%7Bec8030f7-c20a-464f-9b0e-13a3a9e97384%7D/10.0.5/Firefox/20120608001639/
/Linux_x86-gcc3/en-US/default/Linux\%202.6.37.6-smp\%20(GTK\%202.24.4)/default/default/20/20/3/
```

Ich mag es nicht, wenn jemand remote irgendetwas auf meinem Rechner deaktiviert oder deaktivieren könnte. Unter `about:config` kann man dieses Feature abschalten:

```
    extensions.blocklist.enabled = false
```

Update der Metadaten für Add-ons deaktivieren

Seit Firefox 4.0 kontaktiert der Browser täglich den AMO-Server von Mozilla und sendet eine genaue Liste der installierten Add-ons und die Zeit, die Firefox zum Start braucht. Als Antwort sendet der Server Statusupdates für die installierten Add-ons. Diese Funktion ist unabhängig vom Update Check für Add-ons, es ist nur eine zusätzliche Datensammlung von Mozilla. Unter `about:config` kann man diese Funktion abschalten:

```
    extensions.getAddons.cache.enabled = false
```

HTML5 Beacons deaktivieren

Mit Beacons kann ein Browser beim Verlassen/Schließen einer Webseite Daten zur Analyse an den Webserver senden, die via JavaScript gesammelte wurden. Unter `about:config` kann man dieses Feature abschalten:

```
    beacon.enabled = false
```

Wenn man HTML5 Beacons abschaltet, kann es vorkommen, dass eine Webseite nach einem Klick nicht aktualisiert wird. eBay.com ist ein Beispiel dafür. Man muss oft den Reload Button klicken, um eine wirklich aktuelle Seite zu sehen. Deshalb ist dieses Feature nur in der strengen user.js Konfiguration deaktiviert.

\(^\text{73}\)https://addons.mozilla.org/en-US/firefox/blocked
Safebrowsing deaktivieren


Unter about:config kann man Safebrowsing deaktivieren:

- browser.safebrowsing.phishing.enabled = false
- browser.safebrowsing.malware.enabled = false
- browser.safebrowsing.blockedURIs.enabled = false
- browser.safebrowsing.downloads.enabled = false
- browser.safebrowsing.downloads.remote.enabled = false
- browser.safebrowsing.downloads.remote.block_dangerous = false
- browser.safebrowsing.downloads.remote.block_dangerous_host = false
- browser.safebrowsing.downloads.remote.block_potentially_unwanted = false
- browser.safebrowsing.downloads.remote.block_uncommon = false
- browser.safebrowsing.downloads.remote.url = (leerer String)
- browser.safebrowsing.provider.*.gethashURL = (leerer String)
- browser.safebrowsing.provider.*.updateURL = (leerer String)


Healthreport und Übertragung von Telemetriedaten deaktivieren

Alle Übertragungen von Telemetriedaten, Healthreport usw. an Mozilla unterbindet man seit Firefox 41 mit folgendem globalen Kill-Switch:

datareporting.policy.dataSubmissionEnabled = false

daneben gibt es Parameter für einzelne Reports, die man zusätzlich deaktivieren kann, was aber eigentlich mit dem globalen Kill-Switch erledigt ist.

datareporting.healthreport.uploadEnabled = false

Zur Deaktivierung des Telemetrie Toolkit setzt man folgenden Wert:

toolkit.telemetry.unified = false

Einzelne Aktionen zur Telemetrie kann man mit folgenden Optionen deaktivieren:

toolkit.telemetry.archive.enabled = false

toolkit.telemetry.firstShutdownPing.enabled = false

toolkit.telemetry.hybridContent.enabled = false

toolkit.telemetry.bhrPing.enabled = false

toolkit.telemetry.newProfilePing.enabled = false

toolkit.telemetry.shutdownPingSender.enabled = false

toolkit.telemetry.updatePing.enabled = false

Außerdem kann man das Ping-Centre für Datenerhebung und -versand deaktivieren:

browser.ping-centre.telemetry = false
Im August 2018 hat Mozilla festgestellt, dass es keine Daten darüber gibt, wie viele Nutzer die Übertragung der Telemetriedaten abgeschaltet haben. Deshalb hat Mozilla im September 2018 das Add-on Telemetrie Coverage eingebaut und an 1% der Nutzer verteilt. Das Add-on ignoriert die Einstellungen zu Telemetrie und sendet folgende Daten an Mozilla: Firefox Version, Update Channel, Betriebssystem und -version sowie die Information, ob die Übertragung von Telemetriedaten deaktiviert wurde. Um diese Datenübertragung an Mozilla zu deaktivieren, muss man unter `about:config` folgende Variablen neu anlegen:

```
toolkit.coverage.endpoint.base = "" (leerer String)
toolkit.coverage.opt-out = true (laut Mozilla Doku)
toolkit.telemetry.coverage.opt-out = true (im Code verwendet)
```

### Firefox Location Tracking

Seit Firefox 80 trackt Firefox den Standort der Nutzer. Bei jedem Start wird der Server `location.services.mozilla.com` angepingt und anhand der IP-Adresse das Land ermittelt, in dem der Nutzer sich aufhält. Die Daten werden in zwei Variablen gespeichert:

- `Region.current` (das aktuelle Land, in dem der Nutzer sich aufhält)
- `Region.home` (das vermutete Heimatland des Nutzers)

Laut Dokumentation verwendet Mozilla diese Daten, um irgendwelchen relevanten Content auszuwählen und die Standardsuchmaschine zu definieren (in Abhängigkeit von den Verträgen, die Mozilla mit unterschiedlichen Suchdiensten abgeschlossen hat).

Das Aktualisieren des Standortes verhindert man mit folgendem Schalter:

```
browser.region.update.enabled = false
```

### Mozillas Werbung nach einem Update

Nach jedem Update von Firefox wird eine andere Startseite aufgerufen, die Mozilla für Werbung sowie statistische Auswertungen nutzt und die ein bisschen nervt. Unter der Adresse `about:config` kann man diese Einblendung abschalten:

```
browser.startup.homepage_override.mstone = ignore
```

### Mozillas Bewertungsfeature

Im Rahmen von Stichproben bittet Mozilla die Nutzer, ihre Erfahrungen mit Firefox zu bewerten. Die Bewertungsfunktion baut bei jedem Start von Firefox eine Verbindung zum Mozilla Server auf. Mit folgender Option unter `about:config` deaktiviert man die Bewertungsfunktion und die Verbindungsaufbau:

```
app.normandy.enabled = ignore
```

### Deaktivierung der Add-ons auf Mozillas Webseiten

Standardmäßig werden Add-ons auf folgenden Webseiten deaktiviert, um die Funktionalität sicherzustellen, da sie auch für interne Funktionen von Firefox genutzt werden:

- `accounts-static.cdn.mozilla.net`
- `accounts.firefox.com`
- `addons.cdn.mozilla.net`
- `addons.mozilla.org`
- `api.accounts.firefox.com`
- `content.cdn.mozilla.net`
- `discovery.addons.mozilla.org`
- `install.mozilla.org`
- `oauth.accounts.firefox.com`
profile.accounts.firefox.com
support.mozilla.org
sync.services.mozilla.com

Damit gibt es auf diese Webseiten zum Beispiel praktisch keinen Trackingschutz mehr, obwohl die Webseiten teilweise Trackingcode einbinden, den uBlock blockieren würde.

Man kann die Deaktivierung der Add-ons auf diesen Webseiten verhindern, wenn man folgende Variable unter about:config auf einen leeren String setzt:

extensions.webextensions.restrictedDomains =

Diese Einstellung kann aber in Abhängigkeit von den installierten Add-ons auch zu Problemen bei einigen internen Funktionen von Firefox führen, die diese Webdienste nutzen.

Systemfarben der Desktop Umgebung


Um das Auslesen der Desktop Einstellungen zu verhindern, kann man die eingebauten Standardwerte für die Systemfarben verwenden und den Darkmode deaktivieren:

ui.use_standins_for_native_colors = true
ui.systemUsesDarkTheme = 0

In der Empfehlung CSS Color Module Level 374 ist die Verwendung von Systemfarben als veraltet markiert.

Wi-Fi Hotspot Portalerkennung deaktivieren


- Wenn man einen Computer im eigenen LAN nutzt, ist die Wi-Fi Portal Erkennung überflüssig. Unter about:config kann man sie deaktiviert:

    network.captive-portal-service.enabled = false

    (Wenn man gelegentlich (selten) einen Wi-Fi Hotspot nutzt, kann man die Variable kurzzeitig per Hand auf true setzen, damit es funktioniert.)

- Wenn man häufig mit dem Laptop unterwegs ist, kann die Wi-Fi Portal Erkennung ganz nützlich sein. In diesem Fall könnte man die Adresse für den XMLHttpRequest anpassen und einen eigenen Server für den Test verwenden, um nicht ständig den Mozilla Server zu kontaktieren.

    Am einfachsten lädt man die Datei success.txt herunter und speichert sie auf dem eigenen Webserver. Unter about:config passt die URL an:

    network.captive-portal-service.enabled = true
    captivedetect.canonicalURL = http://www........../success.txt

    Hinweis: die Datei muss via HTTP abrufbar sein, also ohne SSL-Verschlüsselung. An- derenfalls ist kein Redirect möglich.

74 https://drafts.csswg.org/css-color-3
Microsoft Family Safety deaktivieren  
Microsoft Family Safety ist ein lokaler man-in-the-middle Proxy in Windows 10, der die Zugriffsrechte auf Webseiten steuern kann und damit per Definition ein Zensurtool ist. Ab Firefox 52 ist die Verwendung von Microsoft Family Safety standardmäßig aktiviert. Mit folgender Option kann man unter about:config die Nutzung abschalten:

```
security.family_safety.mode = 0
```

Browser Slow Startup Notifications abschalten  
Bei jedem Start prüft Firefox die Zeit, die der Browser zum Starten benötigt. Falls Firefox der Meinung ist, dass er zu langsam startet, wird die Deinstallation von Add-ons empfohlen. Da man sich überlegt, welche Add-ons man braucht und gern verwenden möchte und überflüssige Add-ons natürlich nicht installieren würde, ist dieses Feature überflüssig. Man kann es unter about:config deaktivieren:

```
browser.slowStartup.notificationDisabled = true
browser.slowStartup.maxSamples = 0
```

4.23 Zusammenfassung der Einstellungen  
Um die Werte nicht alle per Hand anpassen zu müssen, haben wir Beispielkonfigurationen für Firefox 60+ vorbereitet, die man herunter laden und im Firefox-Profil speichern kann. Man kann nicht alle Wünsche mit einer Konfiguration abdecken, deshalb gibt es mehrere Vorschläge, die man von der Webseite des Privacy-Handbuches herunterladen kann: https://www.privacy-handbuch.de/handbuch_21u.htm

Die Vorschläge sind Teil eines Gesamtkonzeptes und es wird davon ausgegangen, dass die Add-ons uBlock Origin und CanvasBlocker mit den empfohlenen Konfigurationen installiert wurden. Daraus ergeben sich einige Unterschiede zu vergleichbaren Projekten.

**Basis Einstellungen:** Die minimale user.js setzt folgende Einstellungen um:

- Deaktivierung von Spielereien, die Mozilla eingebaut hat (Activity Stream, Pocket, Telemetrie, Datareporting, Ping-Centre, Captive Portal Check, Safebrowsing, Family Safety, die bunte NewTabPage und Startseite...).
- Es wird kein Referrer an Drittsiten und beim Wechsel der Domain gesendet.
- Außerdem werden einige allgm. Sicherheitsfeatures aktiviert (AutoFill für Formulare deaktiviert, Anzeige von unsicheren Verbindungen als Text+Icon...)

**Moderate Einstellungen:** In der moderate user.js werden zusätzlich einige HTML5 Feature deaktiviert, die häufig zum Tracking genutzt werden. Die Funktion normaler Webseiten wird damit in der Regel nur wenig beeinflusst. Auf einigen featurereichen, interaktiven Webseiten kann es allerdings zu Problemen kommen.

- WebGL steht nur mit dem minimalen Featureset zur Verfügung.
- Deaktivierung einiger JavaScript APIs, die für das Fingerprinting des Browsers aber nur selten beim Surfen verwendet werden (Sensors, Gamepad, Media Navigator, WebRTC, Timing APIs...)
- Da installierte Schriftarten häufig für das Fingerprinting verwendet werden, ist die Verwendung von individuellen Schriften für HTML Dokumente deaktiviert. Man sollte deshalb gut lesbare Standardschriften konfigurieren. Einbindung externer Webicon Fonts für Navigationselemente ist zulässig.

**Strenge Einstellungen:** Die *strenge user.js* blockiert restriktiv vieles, was für Tracking sowie Sicherheit relevant sein könnte. Neben Trackingschutz sollen auch Möglichkeiten für Angriffe auf den Browser minimiert werden. Diese Einstellungen sind für Risikogruppen geeignet, die für höhere Sicherheit einige Einschränkungen in Kauf nehmen.

- Javascript Just-in-Time-Compiler sind aus Sicherheitsgründen deaktiviert, was die Ausführung von Javascript auf einige Webseiten verlangsamt.
- Anzeige von PDF Dokumenten im Browser ist deaktiviert.
- SVG, Flash, WebGL und WebGL2 sind komplett deaktiviert.
- Auto-Play und Hardware Video Decoding sind deaktiviert.
- Closed Source Video Codecs werden nicht verwendet.
- Favicons werden nicht geladen und nicht gespeichert.
- Es werden keine Login Credentials gespeichert.
- Push Services sind deaktiviert.
- Der Download von externen Schriftarten ist auch für Navigationssymbole deaktiviert. Um die resultierenden Einschränkungen etwas abzumildern, kann man häufig genutzte Webicon Fonts wie den Awesome Webicon Font installieren. Linux enthält passende Pakete, für Debian/Ubuntu funktioniert:
  
  > sudo apt install fonts-font-awesome

**Hotspot Login:** Die *Hotspot user.js* ist eine strenge user.js mit aktiviertem Captive Portal Service. Sie könnte in einem Profil eingesetzt werden, dass man nur für den Login bei Wi-Fi Hotspots nutzt. Die Startseite ist *about:profiles*, so dass man nach dem Hotspot Login schnell das gewünschte Profil zum Surfen starten kann.

Die gewählten Datei *user.js* ist im Firefox-Profil zu speichern und wird beim Start von Firefox eingelesen. Die Werte überschreiben die Einstellungen in *prefs.js*. Damit ist sichergestellt, dass man beim Start die gewünschten Einstellungen hat.

Das Firefox-Profil ist ein Unterverzeichnis mit seltsamen Buchstaben, das man in folgenden Verzeichnissen findet:

- Windows: `%APPDATA% -> Mozilla -> Firefox -> Profiles -> …
- MacOS: Library -> Application Support -> Firefox -> Profiles -> …
- Linux: `$HOME/.mozilla/firefox/…`

Hinweis: Wenn man feststellt, dass die gewählte Variante zu restriktiv ist und man auf eine weniger restriktive Variante wechseln möchte, dann muss man im Profilverzeichnis die Dateien *user.js* und *prefs.js* löschen. Wenn man etwas dazwischen will, kann man die weniger restriktive Variante wählen und die Einstellungen unter *about:config* ergänzen.

### 4.24 Snakeoil für Firefox (überflüssiges)

Auf der Website für Firefox Add-ons findet man tausende Erweiterungen. Man kann nicht alle vorstellen. Es kommen immer wieder Hinweise auf dieses oder jenes privacyfreundliche Add-on. Deshalb gibt es an dieser Stelle ein paar Dinge zusammengestellt, die nicht empfehlenswert sind.

Als Grundsicherung ist die Kombination von *FirstParty.Isolate* + *NoScript* + *uBlock Origin* empfehlenswert. Viele Add-ons bieten Funktionen, die von dieser Kombination bereits abgedeckt werden. Andere sind einfach nur überflüssig.
4.24. SNAKEOIL FÜR FIREFOX (ÜBERFLÜSSIGES)

Do-Not-Track ist am Lobbyismus gescheitert


Der eindeutige Wunsch der Nutzer, der mit Aktivierung von DNT im Browser zum Ausdruck gebracht wurde, wurde von der Trackingbranche ignoriert. Empirische Studien zeigten, dass sich das Tracking beim Surfen damit um weniger als 2% verringerte.

Es war ein genialer Schachzug von Microsoft, DNT im IE10 standardmäßig ohne Interaktion des Nutzers zu aktivieren. Das widersprach eindeutig den Intentionen des W3C Standard, der ausdrücklich definierte, dass ein DNT-Header nur vom Browser gesendet werden darf, wenn der Nutzer damit einen Wunsch aktiv zum Ausdruck bringen möchte:

> The basic principle is that a tracking preference expression is only transmitted when it reflects a deliberate choice by the user. In the absence of user choice, there is no tracking preference expressed.

> A user agent MUST have a default tracking preference of unset unless a specific tracking preference is implied by the user decision…


Laut Bloomberg haben nur 12% der Nutzer weltweit DNT aktiviert. Da DNT nicht nennenswert gegen Tracking schützt, schafft man mit der Aktivierung von DNT nur ein Differenzierungsmerkmal für das Fingerprinting des Browsers. Apple hat DNT deshalb aus dem Browser Safari entfernt. In Firefox deaktiviert man DNT unter about:config mit folgender Option:

```
privacy.donottrackheader.enabled  = false
privacy.trackingprotection.enabled = false
```

Statt der Trackingprotection von Firefox ist uBlock Origin empfehlenswert.

Web of Trust (WOT)

WOT war ein Add-on, das den Surfer über die Reputation der besuchten Webseite informierte und häufig empfohlen wurde. Während des Surfens sammelt WOT Daten über den Besuch jeder Webseite und überträgt die Daten an die Betreiber des Dienstes. Die Daten werden mit schwacher Anonymisierung zu Profilen verknüpft und auch an die
Werbeindustrie verkauft, wie Reporter des NDR zeigten. Die Daten konnten relativ einfach deanonymisiert werden und lieferten umfangreiche Informationen zu Krankheiten, sexuellen Vorlieben und Drogenkonsum einzelner identifizierbarer Personen.

Unschön, wenn über einen Richter bekannt wird, dass er eine Vorliebe für Sado-Maso-Praktiken hat oder wenn sich Valerie Wilms, Bundestagsabgeordnete der Grünen, aufgrund der Daten erpressbar fühlt.

Google Analytics Opt-Out

Die Add-ons NoScript zusammen mit einem AdBlocker wie uBlock Origin erledigen diese Aufgabe besser.

GoogleSharing


Statt GoogleSharing sollte man lieber datenschutzfreundliche Alternativen nutzen: die Suchmaschine Ixquick.com oder Startingpage.com, für E-Mails einen Provider nutzen, der den Inhalt der Nachrichten nicht indexiert, openstreetmap.org statt Google-Maps verwenden...

Zweite Verteidigungslinie?
Eine Reihe von Add-ons bieten Funktionen, welche durch die oben genannte Kombination bereits abgedeckt werden:

- **FlashBlock** blockiert Flash-Animationen. Das erledigt auch NoScript.
- **ForceHTTPS** kann für bestimmte Webseiten die Nutzung von HTTPS erzwingen, auch diese Funktion bietet NoScript.
- **Targeted Advertising Cookie Opt-Out** und **Ghostery** blockieren Surftracker. Es werden nur Tracker blockiert, die der oben genannten Kombination auch bekannt sind.
- **No FB Tracking** blockiert die Facebook Like Buttons, das können uBlock Origin oder AdBlock aber besser. Die SocialMediaBlock Listen für diese Werbeblocker blockieren nicht nur Facebook Like Buttons, sondern auch die Wanzen von anderen Social Networks.
- ....

Wer meint, es nutzen zu müssen - Ok.

---

75 https://www.tagesschau.de/inland/tracker-online-103.html
Kapitel 5
Passwörter und
2-Faktor-Authentifizierung

Wenn man sich bei einem Webdienst anmeldet, um personalisierte Angebote zu nutzen (z. B. bei einem E-Mail Dienst, bei Twitter, Facebook oder einem Webshop) muss man sich als berechtigter User authentifizieren.

Für diese Authentifizierung gibt es mehrere Methoden, die man grob in folgende Gruppen einteilen kann:


Unter den Bedingungen der zunehmenden Videüberwachung öffentlicher Plätze muss man auch damit rechnen, dass die Passworteingabe bei Nutzung von Smartphones durch Dritte beobachtet werden kann.

Risiko-basierte Authentifizierung (RBA) soll die Sicherheit von Accounts verbessern, die nur mit einem Passwort geschützt sind. Bei einem Loginversuch wird anhand von Merkmalen ein Risikolevel berechnet, ob möglicherweise ein missbräuchlicher Login erfolgt. Übersteigt der Risikolevel einen Grenzwert, wird eine zusätzliche Verifikation gefordert. In der Regel muss der Nutzer ein zusätzliches Token einzugeben, das per E-Mail, SMS o.ä. an eine vorher verifizierte Adresse gesendet wird.

Zur Berechnung des Risikolevels könnten die Zeit seit dem letzten Login, der Standort im Vergleich zum letzten Login, Uhrzeit, IP-Adresse, Browserversion, Tippverhalten bei der Eingabe des Passwortes oder andere Merkmale verwendet werden.

Die Akzeptanz von RBA ist bei den Nutzern wesentlich höher als eine 2-Faktor-Authentifizierung, da sie im Normalfall nur das Passwort eingeben müssen. 2-Faktor-Auth. wird in der Regel nur bei hohen Sicherheitsanforderungen akzeptiert.

RBA ist bei vielen großen Plattformen (Google, Amazon, PayPal, LinkedIn...) und auch bei Projekt wie Mastodon im Hintergrund aktiv, wenn man eine Adresse für die Verifikation angibt. Implikationen für die Privatsphäre muss man gegen den Sicherheitsgewinn abwägen. Wenn man 2-Faktor-Auth. verwendet, wird RBA meist deaktiviert.

RBA wird häufig ein Art 2-Faktor-Authentifizierung genannt, was aber nicht ganz korrekt ist. Man muss nicht den physischen Besitz eines Gerätes nachweisen, wie bei 2FA üblicherweise gefordert, sondern nur lesenden Zugriff auf eine Zieladresse, an die das Token gesendet wird. Die Sicherheit ist also geringer als bei 2FA.
KAPITEL 5. PASSWÖRTER UND 2-FAKTOR-AUTHENTIFIZIERUNG

Authentifizierung durch Besitz: Man muss nachweisen, dass man ein besonderes bzw. individuell konfiguriertes Token besitzt, das ein Angreifer nicht besitzen kann. Dabei unterscheidet man zwischen:

- **Harter Besitz** ist ein physisch vorhandenes, individuell konfiguriertes Token, welches nicht kopierbar ist (Yubikey, U2F-Stick, ePA, NitroKey…)
- **Weicher Besitz** ist eine Anhäufung speziell konfigurierter Bits und Bytes, die evtl. auf einem anderen Gerät gespeichert sind aber prinzipiell kopierbar sind (z. B. OTP-Apps oder X509 Zertifikate).

Im Consumer Bereich wird am häufigsten OTP (One-Time-Passwörter) mit Smartphone Apps oder Hardware Token angeboten. OTP schützt gegen Keylogger und gegen Mitlesen unter den Bedingungen der Videoüberwachung. Es schützt nicht(!) bei Einbrüchen auf dem Server. Da bei OTP-Server und Client den gleichen Algorithmus ausführen, könnte ein Angreifer bei erfolgreichem Einbruch auf dem Server die Parameter auslesen und clonen.


Die Verwendung von Zertifikaten gibt es eher bei Business Anwendungen, Serveradministration (SSH) oder für hoheitliche Aufgaben (ePA).

**Biometrische Merkmale**: (Fingerabdruck, Iris) sind für starke Authentifizierung eher ungeeignet, weil man sie bei einer Kompromittierung nicht ändern kann.

Im privaten Bereich bieten viele moderne Smartphones inzwischen die Freigabe des Sperrbildschirm via Fingerabdruck Scan. In diesem Fall würde ich die Verwendung des Fingerabdruck gegenüber der oft üblichen Wischgeste bevorzugen, da man die Wischgeste leicht beobachten und kann, während der Fingerabdruck sehr viel komplizierter zu faken ist.


5.1 Hinweise für Passwörter

Jeder kennt das Problem mit den Passwörtern. Es sollen starke Passwörter sein, sie sollen für jede Site unterschiedlich sein und außerdem soll man sich das alles auch noch merken und auf keinen Fall auf einen Zettel "speichern".

Was ist ein starkes Passwort

Ein 6-stelliges Passwort zu knacken, kostet 0,10 Euro. Eine 8-stellige Kombination hat man mit 300 Euro wahrscheinlich und mit weniger als 800 Euro sicher geknackt. Um eine 15-stellige Kombination aus zufälligen Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen oder eine Diceware Passphrase aus 6 Wörtern mit 50% Wahrscheinlichkeit zu knacken, würde man viele, viele Jahre benötigen.

Für eine gute Passphrase zum Schutz wichtiger Accounts wie E-Mail, Bank Account, Cloud Speicher oder VPN-Zugängen sollte man mindestens 12 zufällige Zeichen verwenden (Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen) oder eine Diceware Passphrase mit mindestens 5 Wörtern.

Wie findet man eine starke Passphrase?

Eine gute Passphrase muss eine wirklich zufällige Kombination von Zeichen oder Wörtern sein. Es gibt mathematisch begründete Verfahren, um starke Passwörter zu generieren:

- Passwortspeicher wie KeepasXC enthalten einen Generator für wirklich zufällige Zeichenkombinationen. Für eine gute Passphrase sind mind. 65 Bit Entropie nötig.

Abbildung 5.1: KeepassXC Passwortgenerator

Passwortspeicher sind die einzig brauchbare Methode für selten verwendete Passwörter, an die man sich nach einigen Wochen nicht mehr erinnern kann.


Die Akronym-Methode verwendet die Anfangsbuchstaben von einem leicht merkbaren Satz ableiten und den variablen Anteil aus der Verwendung:

- Merksatz: Die Sonne schien am ganzen Sonntag nur für uns.
- Passwort für die Webseite Heise.de: DSSagSn4u-HEIS
- Passwort für den Jabber Account: DSSgaSn4u-XMPP
- ...

Die Collage-Methode verwendet ein Wort in mehreren Übersetzungen und lässt die Vokale weg. Variable Anhängsel sind ebenfalls möglich:

- Ergebnis: Result=42 könnte folgendes Passwort ergeben: rgbns:Rslt=42
- Pferd?Horse!Cheval könnte folgendes Passwort ergeben: Pfrd?Hrs!Chvl
KAPITEL 5. PASSWÖRTER UND 2-FAKTOR-AUTHENTIFIZIERUNG

• Beim Diceware Verfahren werden zufällige Kombinationen aus Wörtern aus einer Liste verwendet statt zufälliger Zeichenkombinationen. Wortkombinationen kann man sich leichter merken als sinnlose Zeichenkombinationen.

Für den klassischen Weg zur Erstellung einer Diceware Passphrase benötigt man eine Wortliste (beispielsweise die DeReKo Liste mit den häufigsten deutschen Wörtern laut Leibnitz Institut) und einen Würfel. Für jedes Wort würfelt man 5x und erhält damit einen Zahlenkombination. Diese Zahlenkombination sucht man in der Wortliste und wiederholt den Vorgang für 5-7 Wörter.

26431 gebilde
53612 schmal
42221 macht
66123 zauber
34641 karwoche


Wenn man keine Würfel im Haushalt findet, könnte man auch Online würfeln.

Nicht ein Passwort mehrfach verwenden

• Der Hack von Anonymous gegen HBGary zeigte, dass es ein erhebliches Risiko ist, die gleichen Passwörter mehrfach zu verwenden. Den Aktivisten von Anonymous gelang es, Zugang zur User-Datenbank des Content Management Systems der Website zu erlangen. Die gleichen Passwörter wurden vom Führungspersonal für weitere Dienste genutzt: E-Mail, Twitter, Linked-In... Die veröffentlichten 60.000 E-Mails waren peinlich für HBGary.

• Im Sommer 2018 kursierten mehrere tausend Logindaten (Benutzername, Passwort) für den Dienst MEGA in den einschlägigen Darknet Foren. Die Login Credential stammten nicht aus einem Hack von MEGA sondern wurden durch automatisiertes Ausprobieren von Benutzername + Passwort Kombinationen aus anderen erfolgreichen Hacks ermittelt. Gegen dieses Credential Stuffing kann man sich nur schützen, indem man unterschiedliche Passwörter für verschiedene Dienste verwendet.

5.1.1 Firefox build-in Passwortspeicher

Wie alle anderen Browser hat auch Firefox einen Login Manager. Wenn man auf einer Webseite Login Credentials eingibt, fragt Firefox standardmäßig, ob er die Zugangsdaten für diese Webseite speichern soll. Zukünftig wird dann beim nächsten Aufruf der Webseite das Login Formular automatisch mit den passenden Daten ausgefüllt.

Wenn man in der Konfiguration ein Masterpasswort setzt, werden die Passwörter (nur die Passwörter, nicht die Webseiten und Usernamen) mit AES verschlüsselt.

Risiken bei der Nutzung des Passwortspeichers im Browser


1 https://www.privacy-handbuch.de/download/diceware-dereko.txt
2 https://online-wuerfel.de/5-wuerfel
3 https://www.heise.de/ct/artikel/Ausgelacht-1195082.html
5.1. HINWEISE FÜR PASSWÖRTER

Abbildung 5.2: Login Credentials für eine Webseite in Firefox speichern

Die Studie Web trackers exploit browser login managers hat 1.110 Webseiten gefunden, bei denen diese Trackingtechnik in-the-wild eingesetzt wird.4


Anpassungen Firefox Konfiguration

- Wer kompromisslos auf strenge Privatsphäre Wert legt, kann den Passwortspeicher von Firefox deaktivieren und memorisierbare Passwörter verwenden oder externe Passwortspeicher wie KeePassXC. Zur Deaktivierung des Passwortspeichers setzt man unter about:config folgenden Wert:

  signon.rememberSignons = false


  signon.rememberSignons = true
  signon.autofillForms = false

5.1.2 Passwortspeicher

Passwortspeicher sind kleine Tools, die Username/Passwort Kombinationen und weitere Informationen zu verschiedenen Accounts in einer verschlüsselten Datenbank verwalten. Es gibt mehrere Gründe, die für die Verwendung eines Passwortspeichers sprechen:

- Viele Programme (z. B. Pidgin) speichern Passwörter unverschlüsselt auf der Festplatte, wenn man die Option zur Speicherung der Passwörter nutzt (nicht empfohlen!). Andere Programme bieten keine Möglichkeit zur Speicherung von Passwörtern, fordern aber die Nutzung einer möglichst langen, sicheren Passphrase.

Bei vielen Accounts muss man sich neben Unsername und Passwort weitere Informationen merken wie z. B. die Antwort auf eine Security Frage oder PINs bei Bezahldiensten.

In der Regel enthalten Passwortspeicher eine Passwortgenerator, der wirklich zufällige und starke Passwörter generieren kann.

Das Backup wird deutlich vereinfacht. Man muss nur die verschlüsselte Datenbank auf ein externes Backupmedium kopieren.

Im Gegensatz zum Firefox Build-in Speicher werden alle Informationen verschlüsselt gespeichert, nicht nur die Passwörter.


Um kryptoanalytische Angriffe zu erschweren, wird die gesamte Passwortdatenbank mehrere 10.000x mit AES256 verschlüsselt.

Einige Passwortspeicher werben mit der Möglichkeit, die Datenbank zwischen verschiedenen Rechnern und Smartphones zu synchronisieren. Dabei wird die Datenbank in der Cloud gespeichert. Das ist für mich ein Graus, vor allem, weil der geheimdienstliche Zugriff auf Daten in der Cloud immer mehr vereinfacht wird.

Warnung: Zwischenablage für Linux Desktops

Die Linux Desktops wie KDE, Gnome oder XFCE enthalten Tools zur Verwaltung der Zwischenablage. Diese Tools speichern die letzten (n) Einträge, die in die Zwischenablage kopiert wurden und schreiben diese Einträge in der Standardkonfiguration meist unverschlüsselt auf die Festplatte.

- Klipper (KDE Desktop) speichert die Daten in
  
  $HOME/kde/share/apps/klipper/history2.lst

Abbildung 5.3: KeepassX Hauptfenster

Einige Passwortspeicher werben mit der Möglichkeit, die Datenbank zwischen verschiedenen Rechnern und Smartphones zu synchronisieren. Dabei wird die Datenbank in der Cloud gespeichert. Das ist für mich ein Graus, vor allem, weil der geheimdienstliche Zugriff auf Daten in der Cloud immer mehr vereinfacht wird.

Warnung: Zwischenablage für Linux Desktops

Die Linux Desktops wie KDE, Gnome oder XFCE enthalten Tools zur Verwaltung der Zwischenablage. Diese Tools speichern die letzten (n) Einträge, die in die Zwischenablage kopiert wurden und schreiben diese Einträge in der Standardkonfiguration meist unverschlüsselt auf die Festplatte.

- Klipper (KDE Desktop) speichert die Daten in
  
  $HOME/kde/share/apps/klipper/history2.lst

\(^5\) https://addons.mozilla.org/de/firefox/addon/keepassxc-browser

\(^6\) https://keepassxc.org/docs/keepassxc-browser-migration
5.2. ZWEI-FAKTOR-AUTHENTIFIZIERUNG

- Clipman (XFCE Desktop) speichert die Daten $HOME/.cache/xfce4/clipman/textsrc

Wenn man Passwortmanager wie KeepassX verwendet und die Passwörter wie vorgesehen via Zwischenablage kopiert, dann landen auch diese sensiblen Informationen unter Umständen unverschlüsselt auf der Festplatte und die verschlüsselte Speicherung in der Passwortdatenbank wird sinnlos. Um diese Lücke zu vermeiden, müssen die Tools zur Verwaltung der Zwischenablage vernünftig konfiguriert werden. Sie sollten nur wenige Einträge speichern und auf keinen Fall Daten unverschlüsselt auf die Festplatte schreiben oder nicht automatisch gestartet werden, wenn die Speicherung nicht deaktivierbar ist.

Abbildung 5.4: Konfiguration der KDE Zwischenablage Klipper

Als Beispiel zeigt Bild 5.4 die Konfiguration für die KDE Zwischenablage Klipper und Bild 5.5 zeigt, wie man den automatischen Start der Verwaltung der Zwischenablage Clipman in den XFCE Einstellungen für Sitzung und Startverhalten deaktiviert.

5.2 Zwei-Faktor-Authentifizierung


Bei der Zwei-Faktor-Authentifizierung muss man als ersten Faktor in der Regel ein Wissen nachweisen (Passwort, PIN) und als zweiten Faktor den Besitz eines kleinen Gerätes (OTP-Generator o.ä.) oder einer Chipkarte wie bei Bankaccounts. Das Verfahren ist durch Nutzung von EC- und Kreditkarten jedem bekannt. Internet verwendet man statt Chipkarte meist One-Time-Passwort Generatoren oder SecuritySticks (U2F, WebAuthn).

KAPITEL 5. PASSWÖRTER UND 2-FAKTOR-AUTHENTIFIZIERUNG

Abbildung 5.5: Starten von Clipman deaktivieren (XFCE Desktop)

2-Faktor-Authentifizierung für das Online Banking


chipTAN, Sm@rt-TAN verwenden Hardware TAN-Generatoren, welche die EC-Chipkarte der Bank für die Generierung einer TAN verwenden. Sie sind für hohe Sicherheitsanforderungen geeignet, da sie ein separates Gerät verwenden, das nicht mit dem Internet verbunden ist. Die Daten für die Generierung einer TAN können entweder optisch zwischen PC und TAN-Generator übertragen werden (durch Scannen eines Codes, der auf dem Bildschirm angezeigt wird) oder manuelle Eingabe.


2-Faktor-Authentifizierung für Webdienste

Für den Login bei Webdiensten werden für die 2-Faktor-Authentifizierung andere Verfahren genutzt, als beim Online Banking:
5.2. ZWEI-FAKTOR-AUTHENTIFIZIERUNG

**OTP:** Bei der Zwei-Faktor-Authentifizierung mit zusätzlichem One-Time-Passwort besteht das Passwort aus zwei Komponenten, die nacheinander oder manchmal auch zusammen in das gleiche Passwortfeld eingegeben werden. Der erste Teil ist üblicherweise ein n-stellige PIN, die man wissen muss. Der zweite Teil ist das One-Time-Passwort. Es wird von einem kleinen Spielzeug (Tokengenerator) geliefert und ist nur einmalig verwendbar.

Es gibt mehrere Verfahren für die Zwei-Faktor-Auth. mit OTP:

- **HOTP** (HMAC-based OTP) nutzt One-Time-Passwörter, die aus einem HMAC-SHA1-Hashwert abgeleitet werden, der aus einem Zähler und einem gemeinsam Secret berechnet wurde. Sie sind beliebig lange gültig aber die Verwendung eines Token mit größerem Zählerwert erklärt auch alle Token mit niedrigerem Counter für ungültig.
  

- **TOTP** (Time-based OTP) nutzt One-Time-Passwörter, die auf Basis der aktuellen Uhrzeit berechnet werden und nur innerhalb einer kurze Zeitspanne einmalig verwendet werden können.


**Angriffe auf 2-Faktor-Auth. mit OTP Token:**

- Die Sicherheitsfirma CERTFA berichtete Dez. 2018 in dem Blogartikel von einer Spear-Phishing Kampagne iranischer Hacker gegen Google und Yahoo! Accounts, welche die 2-Faktor Auth. austricksen konnte.\(^7\)

- Amnesty International berichtete ebenfalls von einer Phishing Angriffswelle aus Nahost gegen die Accounts von Aktivisten, welche die 2-Faktor-Auth von ProtonMail, Tutanota, Google und Yahoo! austricksen konnte.\(^8\)


- Wenn es einem Angreifer gelingt, zwei oder mehr TOTP Token abzugreifen und den Zeitpunkt der Verwendung zu protokollieren, kann er mit dem Tool *hashcat* versuchen, die Secret Keys ermitteln und dann selbst gültige TOTP Token erzeugen.

\(^7\)https://blog.certfa.com/posts/the-return-of-the-charming-kitten/


\(^9\)https://github.com/muraenateam
KAPITEL 5. PASSWÖRTER UND 2-FAKTOR-AUTHENTIFIZIERUNG

1. Die abgeschorcelten Token schreibt man zusammen mit den Zeitstempel im Format in eine Textdatei (in diesem Beispiel: inputs.txt):

   833060:1263384780
   549115:1528848780

2. Mit dieser Datei füttert man hashcat und protokolliert die Ergebnisse:

   ```
   > hashcat -m17300 -a3 -o totp.potfile inputs.txt
   ```

3. Nach einigen Stunden oder Tagen Rechenzeit (abhängig von Rechenleistung und Qualität der Keys) schaut man sich die Ergebnisse an:

   ```
   > cut -d: -f3 totp.potfile | sort | uniq -c | sort -nr | head
   ```

   Die Ergebnisliste kann man von oben beginnend ausprobieren. Nach weiteren 5min hat man einen TOTP Secret Key, der die Generierung gültiger Token ermöglicht, und man kann den Account übernehmen:

   ```
   > oauthtool --base32 --totp "Secret Key" -d 6
   ```

OTP schützt nicht bei Einbrüchen auf dem Server. Da bei OTP der Server und Client den gleichen Algorithmus zur Berechnung und Verifizierung des One-Time-Passworts ausführen, kann ein Angreifer bei einem erfolgreichem Einbruch auf dem Server die OTP Parameter auslesen und somit gültige OTP Token berechnen, insbesondere für TOTP ist es einfach, dabei unentdeckt zu bleiben:

   ```
   > oauthtool --base32 --totp <Secret Key> -d 6
   ```


Der Webdienst, bei dem man sich anmeldet, sendet das Einmalpasswort in der Regel über eine API an die YubiCloud und lässt es dort verifizieren. Nur wenige Webdienste bieten gebrandete Yubikeys und betreiben einen eigenen Server zur Validierung. Bezüglich Schutz gegen Phishing gilt das Gleiche wie für TOTP/HOTP.

- **FIDO-U2F:** ist ein kryptografisches Privat/Public Key Verfahren zur Authentifizierung mit einem kleinen SecurityStick (z. B. Nitrokey U2F oder verschiedene Yubikeys), das im Okt. 2014 standardisiert wurde.


Vorteile von FIDO-U2F gegenüber One-Time-Passwörtern:

---

11https://www.nitrokey.com/de
12https://www.yubico.com/products/yubikey-hardware/
5.2. ZWEI-FAKTOR-AUTHENTIFIZIERUNG

1. Da asymmetrische Kryptografie genutzt wird, kennt der Server nur einen public Key. Wenn ein Angreifer den Server kompromittiert, kann er die U2F Auth. nicht aushebeln.

2. Da die Login URL, die der Browser sieht, in die Berechnung der Signatur ein- fließt, schützt U2F auch gegen alle Angriffe mit Phishing Webseiten. Um Software wie Muraena + NecroBrowser gegen FIOD-U2F Auth. einzusetzen, müsste der Angreifer die TLS-Verschlüsselung knacken und sich als Man-in-the-Middle in die TLS-verschlüsselte Kommunikation zwischen Browser und Webdienst einklinken.

Auf der Testseite von Yubico\(^\text{13}\) kann man ein bisschen und prüfen, ob man mit U2F einen Account erstellen den U2F-Stick für einen Dummy Login nutzen kann.


WebAuthn/FIDO2 erweitert FIDO-U2F um folgende Punkte:


Auf der Webseite [https://WebAuthn.io](https://WebAuthn.io) kann man spielerisch mit seinem Token einen Account erstellen und sich mit dem Umgang beim Login vertraut machen.

Hinweis für Linuxer: Wenn FIDO2 oder U2F Sticks nicht out-of-the-box funktionieren, muss man die UDEV Regeln installieren. Meistens reicht es, folgende Pakete zu installieren:

```
Ubuntu: > sudo apt install libu2f-udev
Fedora: > sudo dnf install u2f-hidraw-policy
```

**SMS**: SMS-basierte Verfahren zur Authentifizierung gelten als nicht mehr sicher. Es gibt mehrere Publikationen zu dem Thema. Das NIST, BSI u.a. empfehlen, SMS nicht mehr für die Authentifizierung zu nutzen.\(^\text{14}\)

SMS-basierte Verfahren können mit SIM-Swap Angriffen oder SS7-Hijacking ausgehebelt werden. Das musste Twitter-CEO Jack Dorsey lernen, als sein Twitter Account trotz aktivierter 2-Faktor-Auth kompromittiert wurde. Ein Fehler beim Mobilfunkanbieter sei schuld gewesen, erklärte Twitter später, was auf einen erfolgreichen SIM-Swap hindeuten könnte.

**ePerso**: In Auswertung des US-Wahlkampfes 2016 und dem erheblichen Einfluss von gehackten E-Mail Accounts auf das Wahlverhalten der amerikanischen Bevölkerung hat die Bundesregierung die Cyber-Sicherheitsstrategien überarbeitet. Nach Ansicht der Bundesregierung ist die Sicherheit mit dem klassischen Benutzername/Passwort-Verfahren nicht mehr gegeben. Im Rahmen Cyber-Sicherheitsstrategien will die Regierung die Bürger stärker zur Nutzung der Onlineausweisfunktion des Personalausweises animieren.

\(^\text{13}\)[https://demo.yubico.com/u2f]
\(^\text{14}\)[https://pages.nist.gov/800-63-3/sp800-63b.html]
KAPITEL 5. PASSWÖRTER UND 2-FAKTOR-AUTHENTIFIZIERUNG

Bezüglich des klassischen Benutzername/Passwort-Verfahren stimmen wir mit der Bundesregierung überein. Wir empfehlen aber die Onlineausweisfunktion des ePerso nicht. Statt dessen sollte man Hardware Token nutzen, die nicht an eine ID-Karte gebunden und vollständig durch den Nutzer konfigurierbar sind.

5.3 Phishing Angriffe

Phishing ist eine der Plagen im Internet. Der Lagebericht des BSI zur IT-Sicherheit 2017 nennt diese Angriffe als zweitgrößte Gefahr nach den Erpressungstrojanern. Es gibt dabei ganz unterschiedliche Intentionen der Angreifer, um die Kontrolle über einen Account des anvisierten Opfers zu erlangen:

- Geheimdienste versuchen, die Accounts von politischen Oppositionellen zu hacken, um das Kontakt Netzwerk zu analysieren und die Kommunikation zu beobachten. Mit diesem Hintergrund wurden die Twitter Accounts von Erdogan-Kritikern von türkischen Hackern angegriffen.\(^{15}\)


  Criminals hack into an art dealer’s email account and monitor incoming and outgoing correspondence. When the gallery sends a PDF invoice to a client following a sale, the conversation is hijacked. Posing as the gallery, hackers send a duplicate, fraudulent invoice from the same gallery email address, with an accompanying message instructing the client to disregard the first invoice and instead wire payment to the account listed in the fraudulent document.

  Once money has been transferred to the criminals’ account, the hackers move the money to avoid detection and then disappear. The same technique is used to intercept payments made by galleries to their artists and others.

- Auch ganz normale, nicht exponierte Internetnutzer werden mit Phishing Angriffen konfrontiert. Für Kriminelle ist dabei alles interessant, was mit Geld zu tun hat (z. B. PayPal.com, Amazon Konten o.ä.) Spammer versuchen, verifizierte E-Mail Accounts zu kapern und das Adressbuch des Oplers zu nutzen, um dann bei Empfängern der Spam Nachrichten das Vertrauen in den bekannten Absender auszunutzen. Dabei kann es manchmal zu kuriosen Missverständnissen kommen:

  My religious aunt asked why I was trying to sell her viagra!

In der Regel werden normale Internetnutzer mit Bulk-Phishing attackiert. Die Angreifer versenden eine E-Mail mit alarmierendem Inhalt an tausende Empfänger in der Hoffnung, dass ein kleiner Teil der Empfänger so naiv ist und auf den Link-Button in der Mail klickt, um die Login Credentials auf der Phishing Webseite einzugeben.

Beispiele für den Inhalt von ganz normalen Phishing E-Mails:

- Das Passwort für Ihren Account wurde kompromittiert! Bitte loggen Sie sich sofort ein und ändern Sie Ihr Passwort.

- Ihr PayPal Account muss neu verifiziert werden, bitte loggen Sie sich hier ein und...

\(^{15}\)https://netzpolitik.org/2017/angriffe-gegen-twitter-accounts-von-erdogan-kritikern

5.3. PHISHING ANGRIFFE

Ihr Amazon Konto wurde deaktiviert, bitte loggen Sie sich ein und...
Ihre Lieferung wurde storniert, weitere Informationen finden Sie hier.

Professionelle Phishing Mails sind dem Design der originalen E-Mails sehr gut nachgemacht und für Laien schwer erkennbar. IT-Profis könnten sich die Header der Mails anschauen oder die Links genauer prüfen, aber das müchte man auch nicht für jede E-Mail ständig machen. Deshalb gibt es keine weitere Ratschläge für diesen Ansatz.

Abbildung 5.6: Beispiel für eine Phishing Mail

Schutz gegen Phishing Angriffe

Als Schutz gegen Phishing Angriffe empfehlen wir, Webseiten mit Formularen zur Eingabe von Login Credentials IMMER über Lesezeichen oder durch Eingabe der URL per Hand zu öffnen. Man sollte NIE auf die Link Buttons in irgendwelchen E-Mails klicken, um Login-Seiten für Accounts auszurufen. Dabei ist es egal, wie vertrauenswürdig eine Mail aussieht.

Es ist verführerisch einfach, schnell mal auf den Button oder Link zu klicken, wenn die Phishing Mail gut gemacht ist. Aber es ist auch nicht viel komplizierter, ein Lesezeichen oder die URL aus einem Passwortmanager wie KeePassXC aufzurufen.

Außerdem kann man 2-Faktor-Authentifizierung nutzen, wenn der Webdienst es unterstützt. Das erschwert einfache, primitive Phishing Angriffe. (Es gibt allerdings technisch ausgefeilteste Angriffe, die auch die 2-Faktor-Auth. mit OTP aushebeln können.)

Wenn man diese Regeln beherzigt, ist man gegen Phishing gut geschützt.
Kapitel 6

Bezahlen im Netz


PayPal.com nutzt seine Marktposition für die Durchsetzung politischer Interessen der USA. Gemäß der Embargo-Politik der USA werden Internetnutzer in über 60 Ländern ausgesperrt. Internationales Aufsehen erregte die Sperrung der Konten von Wikileaks. Daneben gibt es viele weitere Fälle. Mehr als 30 deutschen Online-Händlern wurden die Konten gesperrt 1, weil sie kubanische Produkte (Zigarren, Rum, Aschenbecher) in Deutschland anboten. Die Sperre wurde mit einem amerikanischen Handelsembargo gegen Kuba begründet, das für Europäer belanglos ist.

Aufgrund dieser politischen Instrumentalisierung hat Anonymous zum Boykott von PayPal.com aufgerufen und an Nutzer appelliert, ihre Accounts bei diesem Bezahldienst zu kündigen.

Zukünftig möchte PayPal.com auch in der realen Welt präsent sein. Das Bezahlsystem soll die Geldbörse in zwei Jahren ersetzen, wie Ebay-Chef John Donahoe sagte, natürlich mit den üblichen Schnüffeleien:

Beim Einsatz von PayPal in den Geschäften könnten die Einzelhändler mehr über Vorlieben ihrer Kunden erfahren und sie entsprechend besser bedienen.


Kreditkarten werden von einer Bank ausgegeben. Die Abwicklung des Bezahlvorgangs wird bei Visa und Mastercard aber von sogenannten Payment Processoren übernommen. Teilweise sammeln diese Payment Processoren Daten über online und offline Einkäufe und verkaufen die Daten an große Datensammler wie Acxiom oder BlueKai, wo sie mit anderen persönlichen Daten zusammengeführt werden.


1http://heise.de/-1320630

152
In dem Patent wird beschrieben, wie die Kreditkartenfirmen aus den Einkäufen anhand der Konfektions- und die Schuhgrößen die Größe und das Gewicht des Karteninhabers ermitteln können. Diese Daten könnten an Fluggesellschaften verkauft werden, die damit die Sitzverteilung für die Passagiere optimieren könnten.

Die Sicherheit von Kreditkarten als Zahlungsmittel wird öfters durch unsachgemäße Datenspeicherung beim Verkäufer oder einem Partner des Verkäufers kompromittiert. Eine dreistellige Prüfziffer soll den Missbrauch von Kreditkartennummern für unberechtigte Einkäufe zu Lasten des Karteninhabers verhindern. Wenn aber der Payment Processor oder sein Sub-Kontraktor die Prüfziffer zusammen mit der Kartennummer dauerhaft speichert und die Datenbank unzureichend gesichert ist… dann haben Kunden möglicherweise ein Problem, z. B. Millionen Hotelgäste, die via Booking.com oder Expedia gebucht hatten.\(^2\)


Die Kosten für virtuelle Kreditkarten sind meist geringer als vergleichbare echte Kreditkarten vom gleichen Anbieter aber sehr unterschiedlich. Bei KREDU kosten sie 149,- Euro pro Jahr + Zinsen für den Kredit, bei der Sparkasse 12,- Euro pro Jahr…


Die Schweizer Revolut bietet Disposable Virtual Cards für ihre Premiumkunden, ecoPayz bietet dieses Feature ab Silver Level, Eno von Capital One… u.a.m.

Disposable Virtual Cards sind sicherer und privacy-freundlicher aber nicht anonym.

**Google Pay** und **Amazon Pay** sind aus technischer Sicht ebenfalls Payment Processoren für Kreditkarten. In der Google Datenschutz Policy wird benannt, welche Daten dabei Nutzung dieser Bezahlmethode gesammelt werden:

\[\text{Bei jeder Transaktion über Google Pay können wir Informationen zur Transaktion erheben. Hierzu zählen: Datum, Uhrzeit und Betrag der Transaktion, Händlerstandort und -beschreibung, eine vom Verkäufer bereitgestellte Beschreibung der gekauften Waren oder Dienste, Fotos, die Sie der Transaktion beigefügt haben, der Name und die E-Mail-Adresse des Verkäufers und Käufers bzw. des Absenders und Empfängers, die verwendete Zahlungsmethode, […]}\]

Kein weiterer Kommentar nötig - ist ein ganz normaler Google Service.

**SOFORT Überweisung** ist ein Online-Zahlungssystem zur bargeldlosen Zahlung im Internet. Bei dem Bezahlvorgang stellt der Kunde dem Zahlungsdienstleister Sofort GmbH die notwendigen Credentials für den Online Zugriff (PIN usw.) auf sein Konto zur Verfügung. Die Sofort GmbH nutzt diese Informationen, um sich Daten über Kontostand u.ä. zu holen und danach die Transaktion auszuführen.

KAPITEL 6. BEZahlen IM NETZ

Würde man das Verfahren in die Offline-Welt übertragen, könnte man die Dienstleistung der SOFORT Überweisung wie folgt beschreiben: Weil man selbst zu faul ist, gibt man einem Fremden auf der Straße die EC-Karte und PIN, damit er zum Bankautomaten geht, sich über den Kontostand und die letzten Transaktionen informiert um danach die gewünschte Überweisung auszuführen.

In den AGBs verbieten es alle Banken und Sparkassen den Kunden, die Creditinals für den Online Zugriff Dritten zur Verfügung zu stellen. Mit der Nutzung von SOFORT Überweisung verstößt man also gegen die AGBs der Finanzinstitute.

Das Landgericht Frankfurt am Main hat es in einem Urteil klar formuliert, das die Nutzung des Dienstes unzumutbar ist, egal welche Sicherheitsgarantien von der Sofort GmbH versprochen werden:


Der Bundesgerichtshof hat in dem Urteil Az.: KZR 39/16 diese Rechtsauffassung letztinstanzlich bestätigt.


Bei der Bezahlung wird man von der Webseite des Händlers zur Webseite von Paysafecard weiter geleitet. Dort gibt man den gekauften Code ein und der Händler erhält die Information, dass die Bezahlung erfolgt ist.


Aufgrund des Gesetzes gegen Geldwäsche ist Paysafecard gezwungen, die Anonymität des Zahlungsmittels einzuschränken. Deutsche Nutzer sollen (aber müssen nicht) auf der Website unter “My PaySafeCard” einen Account erstellen und können diesen Account mit Gutscheincodes aufladen. Wer mehr als 100,- Euro pro Monat nutzen
möchte, muss sich mit Ausweisdocumenten identifizieren. Probleme mit gesperrten Gutscheinen soll es dann nicht geben.


6.1 Anonyme Online-Zahlungen vor dem Aus?

Die Bundesregierung bereitete unter dem Deckmantel des Kampfes gegen Geldwäsche ein Gesetz vor, das für anonyme Bezahlungen im Internet das Aus bedeutet hätte. Künftig sollen Verkaufsstellen von Paysafecards und UKash Vouchers die Käufer identifizieren und die Daten für eine mögliche Prüfung 5 Jahre bereithalten. Im Gegensatz zu Bareinzahlungen, die statt bisher ab 15.000 Euro zukünftig ab 1.000 Euro berichtspflichtig werden, sollten für E-Geld keine Mindestgrenzen gelten.

Nach Ansicht von Udo Müller (Paysafecard-Geschäftsführer) wären diese Anforderungen auch für die Vertriebsstruktur das AUS. 95% der Partner wie Tankstellen, Geschäfte usw. würden unter diesen Bedingungen den Verkauf von Paysafecard Gutscheinen und UKash Vouchers einstellen.


Ich appelliere an den Gesetzgeber, den überzogenen Ansatz der neuen Vorschläge entsprechend zu korrigieren.

Die 82. Konferenz der Datenschutzbeauftragten Ende September 2011 verfasste zu diesem Gesetzentwurf eine Stellungnahme:

Nach den vorgesehenen Regelungen würden noch mehr personenbezogene Daten unbeschollener Bürgerinnen und Bürger erfasst und ganz überwiegend anlasslos gespeichert. Dies steht in Widerspruch zur Rechtsprechung des Bundesverfassungsgerichts.


So begrüßenswert es ist, dass der anonyme Erwerb von E-Geld damit nicht generell abgeschafft wird, so kritisch sehe ich die nach wie vor bestehende Tendenz, individuelles Handeln in immer stärkerem Maße zu registrieren…

Die Diskussion über Identifikationspflichten - vor allem bei der Inanspruchnahme des Internets - ist damit aber sicherlich noch nicht beendet.

3http://heise.de/-1269409

6.2 Bargeld


In Italien, Spanien, Frankreich, Griechenland und Zypern wurden Bargeldzahlung über einen Höchstsatz von 1.000-3.000 Euro bereits verboten, in Frankreich wird ab August 2015 die Höchstgrenze für Bezahlung mit Bargeld auf 2.000 Euro abgesenkt (das Gesetz wurde nach dem Charlie-Hebdo-Attentat verabschiedet). In Dänemark wurde ein Gesetz aufgehoben, das Läden im Einzelhandel zwingt Bargeld akzeptieren müssen, außerdem wird die dänische Notenbank ab 2016 keine Geldscheine mehr drucken.

Der Wirtschaftsweise Bofinger und der US-Ökonom Rogoff haben im Mai 2015 nachdrücklich die Abschaffung des Bargelds gefordert. Sie appellierten an Bundeskanzlerin Merkel, dass Sie sich auf dem G7-Gipfel in Elmau für eine weltweite Abschaffung des Bargeld einsetzen soll. Dafür wurden folgende Gründe genannt: 5, die ich nur kurz kommentieren will:

Stärkung der Nationalbanken: Wollen wir wirklich irgendwelche Banken stärken? Wir sollten lieber über die Einführung von Vollgeld diskutieren (wie in Island oder in der Schweiz), um die Macht der Banken zu brechen und Banken auf ihren eigentlichen Funktion zurück zu führen.

Austrocknung des Schwarzmarktes: Schwarzmarkt == BÖSE (Drogen, Kipo werden genannt - klar)

Der Schwarzmarkt ist aber auch ein Regulativ zwischen der Gesetzgebung und den Bürgern. Wenn eine Regierung die Wünsche der Bürger konsequent missachtet, dann haben Bürger die Möglichkeit, auf den Schwarzmarkt auszuweichen (natürlich unter Androhung von Strafen). Je drakonischer und unbeliebter die Finanzgesetze werden, desto stärker wird der Schwarzmarkt wachsen.

Die Austrocknung des Schwarzmarktes wird also auch die Macht der Regierenden und Banken gegenüber der Bevölkerung stärken. Wollen wir diese Entwicklung?


Das würde bedeuten, dass sich die Sparer gegen diese Enteignung nicht mehr wehren könnten, indem sie das Geld einfach abheben. Einen sogenannten Bankenrun (wenn Kunden massenweise ihr Geld abheben) will keine Bank riskieren.

---

6.2. BARGELD

Kommentare zu den Vorschlägen von Bofinger/Rogoff

Um diese beiden Argumente ernsthaft als Vorteile durchgehen zu lassen, muss man ein Technokrat sein, der einen lückenlos organisierten Ameisenhaufen für die beste aller Gesellschaften hält. Wer Freiheit, Bürgerrechte und eine lebendige Demokratie bewahren will, den muss es schütteln, wenn jemand, der als Weiser gilt, solche Ansichten verbreitet.6

Noch etwas deutlicher:

Es geht dem ehemaligen Chefsökonom des Internationalen Währungsfonds (IWF) und dem IWF längst neben einer umfassenden Kontrolle der Bevölkerung auch darum, die Grundlage für die finanzielle Repression zu schaffen, um die ausufernde Verschuldung über die Enteignung der Sparer zu lösen.7

Forderungen deutscher Politiker

- Der NRW-Finanzminister Walter-Borjans (SPD) beteiligt sich an der Kampagne gegen Bargeld und forderte im Juli 2015 eine Obergrenze bei Barzahlung. Bezahlungen mit Bargeld sollten in Deutschland nur bis 2.000 - 3.000 Euro erlaubt sein. Ein höherer Betrag würde ihn skeptisch machen. (Warum eigentlich?)

- Der NRW Landeschef des Bundes Deutscher Kriminalbeamter (BDK), Sebastian Fiedler, unterstützt. Fiedler behauptet, wenn man 70.000 Euro für ein Auto oder 200.000 Euro für eine Immobilie bar bezahlt, dann handelt es sich um Geld aus Steuerhinterziehung oder Straftaten. (Kann man ein Auto anonym zulassen oder eine Immobilie anonym ins Grundbuch eintragen lassen und die Verwendung illegaler Einnahmen damit geheim halten? Wer findet den Denkfehler?)

- Im Januar 2016 wurde ein Plan der Bundesregierung bekannt, europaweit die Obergrenze für Barzahlungen auf max. 5.000 Euro festzulegen, um die Finanzierung von Terrorismus zu unterbinden. Da diese Forderung in Deutschland nur schwer durchsetzbar ist und auch von Finanz- und Datenschutzexperten abgelehnt wird, versucht die Bundesregierung wieder einmal den Weg über die EU.

- Außerdem fordert W. Schäuble zentrale Bankkontenregister in allen Mitgliedsstaaten der EU und die bessere Kontrolle von anonymen Prepaid-Zahlungsmittel und Kryptowährungen wie Bitcoin und Ripple zur Terrorbekämpfung.

Kommentare zu den Forderungen deutscher Politiker

- Wer etwas gegen die Finanzierung von Terrorismus tun will, der sollte die Beziehungen zu den Staaten wie Saudi Arabien, Katar oder USA überdenken, die als weltweit als die größten Finanzgeber von Terroristen bekannt sind. Man könnte auch Druck auf die Türkei ausüben, um die Verkaufswege von Erdöl aus den von der ISIS besetzten Gebieten zu unterbinden und damit eine wesentliche Geldquelle des ISIS treffen.


6 http://bitcoinblog.de/2015/05/18/bargeld-ist-macht
7 http://www.heise.de/tp/artikel/45/45089/1.html

6.3 Bitcoin

Bitcoin ist eine digitale Peer-to-Peer Währung ohne zentrale Verwaltung. Sie ist unabhängig von der Geldpolitik einer Zentralbank und entwickelt sich marktgetrieben durch die Aktivitäten der Teilnehmer, die Bitcoin als Zahlungsmittel akzeptieren oder verwenden.


Gegenwärtig ist Bitcoin der populärste Versuch zur Umsetzung einer Währung in Anlehnung an die Konzepte der Austrian school of economics. Die Software löst mit kryptografischen Methoden vor allem zwei Probleme:

1. Das Kopieren und mehrfache Verwendung der Bits und Bytes, die ein Coin repräsentieren, ist nicht möglich.


In der Praxis ist Bitcoin aber als Zahlungsmittel unbrauchbar geworden:

- In den letzten Jahren ist Bitcoin zu einem Spekulationsobjekt geworden. Durch gezielt verursachte Währungsschwankungen, die durch einzelne Spekulanten mit hohem finanziellen Einsatz verursacht werden, ist der Kurs sehr volatil. Wenn der Kurs in wenigen Wochen um 50% schwankt ist ein kalkulierter, kommerzieller Einsatz kaum möglich.


Auch wenn man die absoluten Zahlen zur Berechnung des Bitcoin Energy Consumption Index von Enthusiasten der Kryptowährung in Frage gestellt werden und man meint, es wären eher 10 TWh statt 30 TWh jährlich, kann man nicht leugnen, das Bitcoin Energie in gigantischem Ausmaß verbrennt für nichts.11

Schlussfolgerung: die real existierende Menschheit ist noch nicht in der Lage, mit einer Technologie wie Bitcoin umzugehen.

9https://www.heise.de/ct/ausgabe/2018-3-Bitcoin-3942380.html
10https://digiconomist.net/bitcoin-energy-consumption
Kapitel 7

E-Mail Kommunikation

E-Mail ist eines der meistgenutzten Kommunikationsmittel. Die folgenden Seiten sollen zum Nachdenken über die die Auswahl des E-Mail Providers anregen und Hinweise für die Konfiguration von Mozilla Thunderbird geben.

7.1 E-Mail Provider

Als erstes braucht man eine oder mehrere E-Mail Adressen. Es ist empfehlenswert, für unterschiedliche Anwendungen auch verschiedene E-Mail Adressen zu verwenden. Es erschwert die Profilbildung anhand der E-Mail Adresse und verringert die Spam-Belästigung. Wenn Amazon, Ebay oder andere kommerzielle Anbieter zu aufdringlich werden, wird die mit Spam überschwemmte E-Mail Adresse einfach gelöscht ohne die private Kommunikation zu stören.

Neben einer sehr privaten E-Mail Adresse für Freunde könnte man weitere E-Mail Adressen für Einkäufe im Internet nutzen oder für politische Aktivitäten. Um nicht ständig viele E-Mail Accounts abfragen zu müssen, kann man die für Einkäufe im Internet genutzten E-Mail Accounts auch an die private Hauptadresse weiterleiten lassen. Alle Mail-Provider bieten diese Option. Bei den großen deutschen Mail Providern GMX.de und WEB.de gibt es bis zu 100 Fun-Domains extra für diesen Zweck. Bereits mit der kostenlosen Version kann man bis zu 3 Fun-Adressen nutzen.

Wenn eine E-Mail Adresse nur für die Anmeldung in einem Forum oder das Veröffentlichen eines Kommentars in Blogs benötigt wird, kann man temporäre Mailadressen nutzen.

Eine kleine Liste von empfehlenswerten E-Mail Providern:

- **Mailbox.org** ¹ (deutscher Mailprovider, Server stehen in Deutschland, Accounts ab 1,- Euro pro Monat, PGP verschlüsselte Inbox, verschlüsselter Mailversand und -empfang nur über SSL/TLS aktivierbar, DANE, IP-Adressen der Nutzer und User-Agent werden aus dem Mail Header entfernt, anonyme Accounts möglich, Bezahlung per Brief oder Bitcoin, OTP-Login mit HW-Token und FreeOTP für Webinterface, Tor Hidden Service für POP3, IMAP, SMTP und XMPP)

- **Posteo.de** ² (deutscher Mailprovider, Server stehen in Deutschland, Accounts ab 1,- Euro pro Monat, S/MIME oder PGP verschlüsselte Inbox, verschlüsselter Mailversand aktivierbar aber nicht für Empfang, DANE, IP-Adressen der Nutzer werden aus dem E-Mail Header entfernt aber User-Agent Kennung nicht, anonyme Accounts möglich, anonyme Bezahlung per Brief, 2FA mit OTP suboptimal umgesetzt, außerdem unfreundliche Reaktion auf Kritik ³)

¹ [https://mailbox.org](https://mailbox.org)
² [https://posteo.de](https://posteo.de)
³ [https://www.privacy-handbuch.de/diskussion.htm#take-down-notiz-von-posteos-anwaelten](https://www.privacy-handbuch.de/diskussion.htm#take-down-notiz-von-posteos-anwaelten)
7.1. E-MAIL PROVIDER

- **Mailfence.com** ⁴ (belgischer Provider, kostenlose Accounts möglich, Premium ab 2,50 Euro pro Monat allerdings mit mehr Speicherplatz als die 1,- Euro Accounts der Mitbewerber, POP3, IMAP und SMTP nur für bezahlte Accounts, OpenPGP im Webinterface möglich mit eigener Implementierung, OTP-Login mit FreeOTP für Webinterface, anonyme Bezahlung via Bitcoin oder ohne Anonymität via Kreditkarte)

- **KolabNow** ⁵ (Groupware Hosting in der Schweiz mit Adressbuch, Kalender und E-Mail, Mailaccounts für 4.41 CHF pro Monat, Groupware für 10 CHF pro Monat, IP-Adressen der Nutzer und User-Agent werden aus dem E-Mail Header entfernt)

- **runbox.com** ⁶ (privacy-engagierter norwegischer E-Mail Provider, Server stehen ebenfalls in Norwegen, Accounts ab 1,66 Dollar pro Monat)

- **dismail.de** (DE) und **disroot.org** (NL) bieten neben Services wie XMPP auch kostenfreie E-Mail Accounts. Beide Provider bieten einen hochwertigen, privacyfreundlichen Service und werden durch Spenden finanziert. IP-Adressen der Nutzer werden aus dem E-Mail Header entfernt, disroot.org entfernt auch den User-Agent.

  (Nach den Erfahrungen der letzten Jahre muss man leider damit rechnen, das kostenfreie, spendenfinanzierte E-Mail Dienste (wie SecureMail.biz, Xalia u.a.) nur für ein paar Jahre verfügbar sind und dann eingestellt werden könnten.)

Hinweis: es kostet Geld, einen zuverlässigen Mailservice bereitzustellen. Es ist sinnvoll, die **alles kostenlos Mentalität** für einen vertrauenswürdigen Mailprovider fallen zu lassen.

**Nicht empfohlene E-Mail Provider**

Einige Gründe, warum verschiedene E-Mail Provider mit gutem Ruf nicht in die Liste der Empfehlungen aufgenommen wurden:

- **Web.de** und **GMX.de** sammeln bei der Registrierung zuviele Daten: Vor- und Nachname, Land, PLZ und Ort, Straße, Hausnummer und die Mobilfunknummer.

  Mit der Registrierung erklärt man sich damit einverstanden, dass die Daten für Marketing-Zwecke verwendet werden. Die Daten werden an den Mutterkonzern übermittelt und mit anderen verbundenen Unternehmen geteilt. Außerdem werden die Daten für postalische Werbung sowie für Markt- und Meinungsforschung genutzt und Non-Profit Organisationen für Werbung zur Verfügung gestellt. (Falls man sich schon öfters mal gefragt hat, woher Meinungsforschungsinstitute die Telefonnummern haben….)

  Der EmailPrivacyTest⁷ zeit, dass Web.de und GMX.de bei der Nutzung des WebGUI nicht gegen Tracking Elemente in E-Mails schützen und ermöglichen es damit vielen Diensten, die Nutzer beim Lesen der E-Mails zu beobachten. Web.de setzt selbst HTML-Wanzen in den eigenen Newslettern ein (3 Tracking Wanzen in jedem Newsletter) und verfolgt damit die Lesegewohnheiten der Nutzer.

- **Hushmail** speichert zuviel Daten. Neben den üblichen Daten beim Besuch der Webseite werden die E-Mails gescannt und folgende Daten unbegrenzt lange gespeichert:

  1. alle Sender- und Empfänger E-Mail Adressen (VDS-artig)
  2. alle Dateinamen der empfangenen und gesendeten Attachements
  3. Betreffzeilen aller E-Mails (nicht verschlüsselbar)
  4. URLs aus dem Text unverschlüsselter E-Mails
  5. ... and any other information that we deem necessary

---

⁴https://mailfence.com  
⁵https://kolabnow.com  
⁶https://secure.runbox.com  
⁷https://www.emailprivacytester.com
Diese Daten werden bei der Kündigung eines Account NICHT gelöscht.


  Außerdem hat US-Präsident Trump als eine seiner ersten Handlungen die Behörden in den USA per Dekret aufgefordert, den Datenschutz für Ausländer vollständig aufzuheben. Es ist unklar, welche Auswirkungen das Dekret und die damit angedeutete Richtung im Datenschutz zukünftig für EU-Bürger haben wird.9

  Aus diesem Grund ist ein Server-Standort USA für deutsche Nutzer eher ungeeignet. Das betrifft u.a. die E-Mail Provider SecureNym, S-Mail, Fastmail.fm, Rise-up.net...

- Weitere Beispiele werden auf der Webseite des Handbuches genannt.10

### 7.2 ProtonMail und Tutanota

Die E-Mail Dienste ProtonMail (Schweiz) und Tutanota (Deutschland) stellen einfache Nutzung von Verschlüsselung sowie Kompatibilität mit den gängigen E-Mail Protokollen in den Vordergrund und bemühen sich um Schutz gegen staatlichen Zugriff.


**Vorteile gegenüber Web.de, GMX.de, GMail.com u.a.**

ProtonMail und Tutanota bieten viele Vorteile für Normalanwender, die Ihre E-Mails bisher im Webinterface von GMail, Yahoo! oder Hotmail bearbeiten.

- Die Provider respektieren die Privatsphäre der Nutzer, schnüffeln nicht in den Mails, geben keine Daten weiter und beobachten euch nicht beim Lesen von Newslettern.

- Die Daten werden verschlüsselt auf den Servern gespeichert. Auch die Betreiber haben keinen Zugang zu den Daten. Das schützt gegen Beschlagnahme von Daten durch Behörden aber nicht gegen eine TKÜ nach §100 a/b StPO.


- Auch auf dem Smartphone ist verschlüsselte Kommunikation via E-Mail nutzbar. Tutanota und Protonmail bieten passende Apps im Google Playstore und für iPhones.

---


10 [https://www.privacy-handbuch.de/handbuch_31.htm](https://www.privacy-handbuch.de/handbuch_31.htm)
7.2. PROTONMAIL UND TUTANOTA


- Die SSL/TLS-Verschlüsselung für die Webseiten wird vom Qualsys SSL Server Test mit A+ bewertet und Features zur Verbesserung der Transportsicherheit für E-Mails werden zeitnah implementiert.

- Tutanota unterstützt U2F als zweiten Faktor zur Anmeldung im Webinterface.

Am besten kommen die Vorteile zur Geltung, wenn alle Kommunikationspartner einen Account bei ProtonMail bzw. Tutanota haben.

Nachteile der Verschlüsselung im Browser

Konzeptionell bedingt haben diese Mailprovider einige Schwächen. Die Verschlüsselung bietet hinreichende Sicherheit und ist für hohe Sicherheitsansprüche nicht geeignet. Das wird im Threat Model bei ProtonMail auch deutlich angesprochen:

*If you are Edward Snowden, or the next Edward Snowden, and have a life and death situation that requires privacy, we would not recommend using ProtonMail.*


Die alternative Nutzung starker Kryptografie mit OpenPGP Smartcards ist bei beiden Diensten nicht möglich, auch wenn man dazu in der Lage wäre.


- Server-basierte Kryptografie ist für hohe Sicherheitsansprüche politischer Aktivisten nicht geeignet wie P. Ball in einem Essay bei Wired.com\(^ {12}\) ausführlich dargelegt.

---


\(^{12}\) [http://www.wired.com/2012/08/wired_opinion_patrick_ball/all/](http://www.wired.com/2012/08/wired_opinion_patrick_ball/all/)
KAPITEL 7. E-MAIL KOMMUNIKATION

Tutanota und ProtonMail bieten inzwischen Apps für Android und iPhone an, die den Code für die Verschlüsselung enthalten und aus den Appstores installiert werden können. Damit entfällt diese Schwäche für Smartphone Nutzer.

Auf dem Desktop PC könnte man die ProtonMail Bridge als Mail-Gateway installieren oder die Software von Tutanota von Github auschecken und lokal installieren. Auch das schützt gegen diese Angriffe, ist allerdings komplizierter, als OpenPGP zu konfigurieren.

Key Recovery durch den Provider (aka Krypto-Key-Backdoor)

Die genannten Provider speichern alle Nachrichten und Kontakte verschlüsselt auf den Servern. Die Nutzer können auf die Daten zugreifen, wenn sie sich mit einem Passwort authentifizieren. Das Passwort schützt den Zugriff auf die Kryptoschlüssel.

Welche Möglichkeiten gibt es für ein Key Recovery, wenn man sein Passwort vergisst?

- ProtonMail bietet ein Key Recovery via externer Mailadresse, wenn man sein Passwort vergessen hat. Wenn man diese Möglichkeit nutzt, werden alle vorhandenen E-Mails und Daten gelöscht, da sie ohne das Passwort des Nutzers nicht mehr verschlüsselt werden können. Wer das Passwort vergisst, verliert zwar alle Daten aber nicht den Account.\(^{13}\)

- Tutanota bietet für normale Nutzer keine Möglichkeit des Key Recovery. Bei Tutanota Premium Accounts werden die Daten mit dem Key des Nutzers und dem Key der Account Administratoren verschlüsselt. Das heißt, der Administrator eines Premium Account könnte sich Zugriff auf die Daten verschaffen, aber die Administratoren von Tutanota haben keine konzeptionelle Backdoor für den Zugriff auf die Daten.\(^{14}\)

Somit gibt es bei beiden Services keine konzeptionelle Backdoor.

7.3 Mozilla Thunderbird

Alle E-Mail Provider bieten die Möglichkeit, die E-Mail Kommunikation im Webinterface mit einem Browser zu verwalten, aber trotzdem ist ein E-Mail Client empfehlenswert:

- Der Browser ist eine Sandbox zum Anzeigen von Webseiten. Aufgrund des Funktionsumfangs moderner Browser und der bösartigen Feindlichkeit des Internet muss man von viel mehr Angriffs möglichkeiten ausgehen, als bei einem Programm, dass speziell für die Bearbeitung von E-Mails optimiert wurde.


Informationen und Downloadmöglichkeiten für Mozilla Thunderbird stehen auf der deutschsprachigen Website des Projektes \(^{15}\) für Windows, Linux und MacOS zur Verfügung, Linux Distributionen enthalten Thunderbird. Mit der Paketverwaltung kann Thunderbird und die deutsche Lokalisierung installiert werden.

\(^{13}\)https://protonmail.com/support/knowledge-base/resetting-mailbox-password

\(^{14}\)https://tutanota.uservoice.com/knowledgebase/articles/470716-was-passiert-wenn-ich-mein-passwort-vergesse-k%C3%B6n

\(^{15}\)https://www.mozilla.org/de/thunderbird/
7.3. Mozilla Thunderbird

7.3.1 Account erstellen


Die Grafik im Bild 7.1 zeigt den Weg einer E-Mail vom Sender zum Empfänger. In der Regel ist man nicht direkt mit dem Internet verbunden. Der Zugang erfolgt über ein Gateway des Providers oder der Firma.

Abbildung 7.1: Der Weg einer E-Mail durch das Web


Abbildung 7.2: POP3-Account anlegen
Begriffserklärung: SMTP, POP3, IMAP

Diese Abkürzungen sind für den Laien etwas verwirrend.

**SMTP:** ist das Protokoll zum Versenden von E-Mails.

**POP3:** ist das Protokoll zum Herunterladen von empfangenen E-Mails auf den lokalen Rechner. Die E-Mails werden auf dem Server sofort (oder etwas später) gelöscht.


**IMAP:** ist ein Kommunikationsprotokoll, um die empfangenen E-Mails auf dem Server zu verwalten und nur zum Lesen temporär herunter zu laden. Auch die versendeten E-Mails und die E-Mail Entwürfe werden bei der Nutzung von IMAP auf dem Mailserver des Providers gespeichert.


**Kompromiss:** ist möglich, um mit mehreren Geräten (PC zuhause, Smartphone unterwegs...) auf einen E-Mail Account zuzugreifen:


Begriffserklärung: SSL/TLS oder STARTTLS

Wie einfach es ist, unverschlüsselte Verbindungen zu belauschen, die Passwörter zu extrahieren und das Mail-Konto zu kompromittieren, wurde von T. Pritlove auf der re:publica 2007 demonstriert 17.


---

16 [https://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-079.html](https://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-079.html)

7.3. MOZILLA THUNDERBIRD

SSL/TLS: Wenn man SSL/TLS verwendet, wird als erstes eine verschlüsselte Verbindung aufgebaut und danach beginnt die protokoll-spezifische Kommunikation. Es werden keine Daten unverschlüsselt übertragen.

Es werden keine Daten über eine unverschlüsselte Verbindung gesendet und der Server muss sich zuerst authentifizieren, bevor der Client irgendwelche Daten sendet.


Eine SMTP-Verbindung wird mit STARTTLS wie folgt aufgebaut:

Client: unverschlüsselter Connect
Server: 220 smtp.server.tld Simple Mail Transfer Service Ready
Client: EHLO 192.168.23.44
Server: 250-smtp.server.tld
Server: 250-SIZE 10000000
Server: 250-AUTH LOGIN PLAIN
Server: 250-STARTTLS
Client: STARTTLS
Server: 220 go ahead
SSL/TLS Handshake zwischen Client und Server
Client (TLS-verschlüsselt): EHLO 192.168.23.44


STARTTLS wurde als Erweiterung für bestehende Protokolle entwickelt, um TLS Verschlüsselung für unterschiedliche Domains mit unterschiedlichen Zertifikaten auf einem Server anbieten zu können. Es wurde nicht mit der Zielstellung entwickelt, die Sicherheit von SSL/TLS zu erhöhen. Man sollte sich nicht irritieren lassen und evtl. schlussfolgern, dass old-style SSL/TLS veraltet sein könnte.

Auch die IETF empfiehlt in RFC 8314 SSL/TLS gegenüber STARTTLS zu bevorzugen.

Hinweis für Nutzer der Telekom-Router


In der Router Konfiguration kann man im Menüpunkt „Internet - Liste der sicheren E-Mail-Server“ das Feature abschalten oder den SMTP-Server des Providers hinzufügen.

18https://heise.de/-206233
Dieses Feature wird auch bei einem Update der Firmware älterer Telekom-Router aktiviert. Wenn man trotz korrekter Konfiguration in Thunderbird keine E-Mails mehr versenden kann, sollte man einen Blick in die Konfiguration des Routers werfen.

### 7.3.2 Sichere Optionen für TLS-Verschlüsselung


1. In der aktuellen zivilen Kryptoanalyse gilt nur TLS 1.3 als uneingeschränkt sicher.

   Um den Handshake zur Aushandlung einer TLS-Verschlüsselung einige Millisekunden zu beschleunigen, wurde ein Zero-Round-Trip Handshake in TLS 1.3 eingeführt. Viele Sicherheitsexperten sehen dieses Feature kritisch und als zukünftigen Angriffspunkt. In Thunderbird wurde bereits eine Option implementiert, um es abzuschalten.

2. Bei TLS 1.2 gibt es Einschränkungen bezüglich Sicherheit, da nicht alle in diesem Standard definierten Cipher Suites als uneingeschränkt sicher eingestuft werden. Gemäß IETF RFC 7525 und BSI TR-03116-4 nur folgende Ciphersuiten als sicher:

   ```
   TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
   TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
   TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
   TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
   ```

   Die neueren Ciphersuiten mit CHACHA20-POLY1305 von D.J. Bernstein können ebenfalls als sicher eingestuft werden. Bei DHE-Ciphersuiten ist zu beachten, dass diese Cipher nur sicher sind, wenn hinreichend große Diffie-Hellman Parameter verwendet werden (was nicht immer gegeben ist). Es tritt immer wieder der Fehler auf, dass nur 1024 Bit DH-Parameter verwendet werden, was die NSA seit 2010 on-the-fly knacken kann. Deshalb ist die Deaktivierung der DHE-Cipher empfehlenswert.

3. TLS 1.0 und TLS 1.1 gelten als unsicher und sollten nicht mehr verwendet werden. Leider sind diese TLS Versionen nicht bei allen E-Mail Providern abgeschaltet, aber Thunderbird 78.x verwendet diese veralteten Protokolle nicht mehr.

### TLS 1.3-only Konfiguration für Thunderbird

Am einfachsten aktiviert man eine sichere TLS-Verschlüsselung, wenn man nur TLS 1.3 verwendet. Dafür aktiviert man in den erweiterten Einstellungen folgende Option:

```
security.tls.version.min = 4
```

Außerdem kann man den Zero-Round-Trip Handshake von TLS 1.3 deaktivieren:

```
security.tls.enable_0rtt_data = false
```


Außerdem kann es Probleme beim Abrufen von einigen RSS Feeds geben, wenn der Webserver, der den Feed bereit stellt, kein TLS 1.3 unterstützt.
TLS 1.2-secured Konfiguration für Thunderbird

Standardmäßig erlaubt Thunderbird 78.x die Nutzung von TLS 1.2 und TLS 1.3. Wenn man noch TLS 1.2 nutzen muss, weil der E-Mail Provider TLS 1.3 nicht flächendeckend auf allen Servern einsetzt, dann sollte man die schwachen Cipher Suiten des TLS 1.2 Standard deaktivieren. Folgende Einstellungen sind in diesem Fall empfehlenswert:

```
security.tls.version.min = 3 (default ab Thunderbird 78.x)
security.ssl3.dhe_rsa_aes_128_sha = false
security.ssl3.dhe_rsa_aes_256_sha = false
security.ssl3.ecdhe_ecdsa_aes_128_sha = false
security.ssl3.ecdhe_ecdsa_aes_256_sha = false
security.ssl3.ecdhe_rsa_aes_128_sha = false
security.ssl3.ecdhe_rsa_aes_256_sha = false
security.ssl3.rsa_aes_128_sha = false
security.ssl3.rsa_aes_256_sha = false
security.ssl3.rsa_des_ecb = false
```

Weiterer Einstellungen für die TLS Verschlüsselung

- Insecure Renegotiation verbieten wird seit 2009 als Sicherheitsproblem eingestuft. Ein Angreifer kann die Login Credentials (Username und Passwort) abschnorcheln ohne die Verschlüsselung knacken zu müssen. Tools zum Ausnutzen der Insecure Renegotiation für einen Angriff gibt es auch als OpenSource (z.B. dsniff). Deshalb:

```
security.ssl.require_safe_negotiation = true
security.ssl.treat_unsafe_negotiation_as_broken = true
```

- Strenges Certifikate Pinning erzwingen (z.B. für Add-on Updates):

```
security.cert_pinning.enforcement_level = 2
```

- Für RSS Feeds und die Webseiten Ansicht in Feeds kann man den HTTPS-only Mode aktivieren und das Laden von unverschlüsseltem Content verbietet:

```
security.mixed_content.upgrade_display_content = true
dom.security.https_only_mode = true
network.ftp.enabled = true
```

Verbindungsprobleme mit sicheren TLS-Einstellungen

Wenn man die im Bild 7.3 gezeigte, schwer verständliche Fehlermeldung beim Abrufen oder Senden von E-Mails erhält, gibt es Probleme beim Aufbau einer sicheren Verbindung und man wechselt am besten den Mail-Provider.

Abbildung 7.3: Fehlermeldung bei unsicherer Verbindung
7.3.3 Sichere Konfiguration des E-Mail Client

Einige Hinweise für die sichere Nutzung des Mediums E-Mail mit Mozilla Thunderbird:


Abbildung 7.4: E-Mails als reinen Text darstellen

- Die Option Anhänge eingebunden anzeigen im Menü Ansicht sollte man ebenfalls deakti-vieren, um gefährliche Anhänge nicht schon beim Lesen einer E-Mail automatisch zu öffnen. Der alte Trick mit einem Virus in der E-Mail wird noch immer genutzt, insbesondere wenn man ein Opfer gezielt angreifen will, um den Rechner mit einem Trojaner zu infizieren.

In der Konfiguration kann man dafür folgenden Parameter setzen:

\[
\text{mail.inline_attachments} = \text{false}
\]

- Es ist nicht immer möglich, E-Mails als Plain Text zu lesen. Viele Newsletter sind nur als HTML-Mail lesbar, eBay verwendet ausschließlich HTML-Mails für Benachrichti-gungen usw. In der Regel enthalten diese HTML Mails mehrere Trackingelemente. Um diese E-Mails trotzdem lesen zu können (wenn auch nicht in voller Schönheit), kann man die Darstellung Vereinfachtes HTML nutzen. Außerdem können folgende Features in den Ermöglichten Einstellungen deaktiviert werden, die jedoch nur für die Darstellung von HTML E-Mails in der Ansicht Original HTML relevant sind oder für andere Komponenten, die den HTML-Viewer nutzen:

\[
\begin{align*}
\text{javascript.enabled} &= \text{false} \\
\text{network.cookie.cookieBehavior} &= 2 \\
\text{beacon.enabled} &= \text{false} \\
\text{layout.css.visited_links_enabled} &= \text{false} \\
\text{media.hardware-video-decoding.enabled} &= \text{false} \\
\text{media.navigator.enabled} &= \text{false}
\end{align*}
\]

\(^{20}\text{https://emailprivacytester.com}\)
7.3. MOZILLA THUNDERBIRD

media.video_stats.enabled = false
gfx.downloadable_fonts.enabled = false
network.IDN_show_punycode = true
network.http.sendRefererHeader = 0
security.family_safety.mode = 0

Da JavaScript generell deaktiviert wird, muss man im Gegensatz zu Firefox die Geo-
location, DOMStorage, IndexedDB, AudioContext-API, Timing-APIs, Gamepad-API...
usw. nicht einzeln abschalten.
Thunderbird 60+ verwendet die Gecko Engine von Firefox Quantum zum Rendern
von HTML Content (z.B. in RSS Feeds) und kennt Surf-Container. Wie bei Firefox
kann man FirstParty.Isolate als Trackingschutz aktivieren:

privacy.firstparty.isolate = true

• Im Kopf einer E-Mail kann man zusätzliche Informationen anzeigen lassen:

1. Ein E-Mail Absender besteht aus einem Namen und der E-Mail Adresse. Stan-
dardmäßig zeigt Thunderbird nur den Namen an. Informativer und sicherer ist
die vollständige E-Mail Adresse mit anzuzeigen. Das aktiviert man in den
Erweiterten Einstellungen mit folgender Option:

e mail.showCondensedAddresses = false

2. Eine E-Mail kann den Absender im FROM Header und/oder im Header SEN-
der enthalten. Wenn beide angegeben sind, zeigt Thunderbird nur den FROM
Header an. Ein Angreifer könnte das nutzen, um eine E-Mail mit gefakten
S/MIME Zertifikaten als signiert erscheinen zu lassen. Um diesen Angriff zu
erkennen, kann man sich beide Absenderinformationen anzeigen lassen (wenn
vorhanden) und sollte stutzig werden, wenn sie unterschiedlich sind:

e mailnews.headers.showSender = true

3. Die Anzeige des E-Mail Programms, das der Absender verwendet, ist immer
mal wieder interessant. Diese Anzeige kann man mit folgender Option in den
Erweiterten Einstellungen aktivieren:

 mailnews.headers.showUserAgent = true

• Die Nutzung der Safebrowsing Funktion deaktiviert man in Thunderbird 60 genauso
wie in Firefox ESR. Gegen Phishing Angriffe schützen keine technische Maßnahmen
vollständig sondern in erster Linie das eigene Verhalten. Und gegen Malware schüt-
zen regelmäßige Updates des Systems besser als Virenscanner und URL-Listen.

 browser.safebrowsing.phishing.enabled = false
 browser.safebrowsing.malware.enabled = false
 browser.safebrowsing.blockedURIs.enabled = false
 browser.safebrowsing.downloads.enabled = false
 browser.safebrowsing.downloads.remote.enabled = false
 browser.safebrowsing.downloads.remote.block_dangerous = false
 browser.safebrowsing.downloads.remote.block_dangerous_host = false
 browser.safebrowsing.downloads.remote.block_potentially_unwanted = false
 browser.safebrowsing.downloads.remote.block_uncommon = false

• Alle Bilder in HTML-Mails, die von einem externen Server geladen werden, können
direkt mit der E-Mail Adresse des Empfängers verknüpft sein. Anhand der Logda-
ten kann der Absender erkennen, wann und wo die E-Mail gelesen wurde. Einige
Newsletter verwenden auch HTML-Wanzen. Im Newsletter von Paysafecard findet
man beispielsweise ganz unten eine kleine 1x1-Pixel Wanze, die offenbar mit einer
individuellen, nutzerspezifischen URL von einem Trackingservice geladen wird:
Easyjet.com (ein Billigflieger) kann offenbar die Aufrufe seiner Newsletter selbst zählen und auswerten. In den E-Mails mit Informationen zu gebuchten Flügen findet man folgende kleine Wanze am Ende der Mail:

Um Tracking mit Bildern und HTML-Wanzen zu verhindern, kann man in den Erweiterten Einstellungen das Laden externer Bilder blockieren:

```
permissions.default.image = 2
```


```
media.webm.enabled = false
media.wav.enabled = false
media.ogg.enabled = false
```

Die Links in HTML-Mails führen oft nicht direkt zum Ziel sondern werden ebenfalls über einen Tracking service geleitet, der jeden Aufruf des Link individuell für jede Empfängeradresse protokollieren kann. Als Beispiel soll ein Link aus dem Paysafe-card Newsletter dienen, der zu einem Gewinnspiel bei Paysafe-card führen soll:

```
Gewinne Preise im Wert von 10.000 Euro</a>
```


- Im SMTP-Dialog mit dem Mailserver beim Versenden einer E-Mail sendet Thunderbird im EHLO Kommando standardmäßig die lokale IP-Adresse:

```
SSL/TLS Handshake zwischen Client und Server
Client: EHLO 192.168.23.44
```

Viele Mailserver vermerken diese lokale IP-Adresse aus dem EHLO Kommando im ersten Received Header der E-Mail zusammen mit der externen IP-Adresse, die der Mailserver sieht, und teilen sie damit auch Dritten mit:

```
Received: from cefige3264.dynamic.kabel-deutschland.de
([188.192.92.109] helo=[192.168.23.44]) by smtp.server.tld
```

Um zu vermeiden, dass diese Information veröffentlicht wird, kann in den Erweiterten Einstellungen eine neue String Variable anlegen und einen Fake definieren:

```
mail.smtpserver.default.hello_argument = [127.0.0.1]
```

Privacy-freundliche E-Mail Provider entfernen den ersten Received Header vollständig, da er nicht nur die lokale IP-Adresse aus dem internen Netzwerk enthält, sondern auch die externe IP-Adresse, die Hinweise auf den Aufenthaltsort des Absenders liefert und von Datensammlern mit dem Surfprofil verknüpft werden kann.
7.3. MOZILLA THUNDERBIRD


Wenn man die E-Mail Adressen der Empfänger nicht automatisiert speichern möchte, dann kann man das kann man das Feature in den Einstellungen in der Sektion *Verfassen* abschalten.

Abbildung 7.5: Sammeln von E-Mail Adressen abschalten

In den *Erweiterten Einstellungen* kann man folgenden Wert setzen:

```plaintext
mail.collect_email_address_outgoing = false
```

Dann muss man sich aber selbst um die Pflege des Adressbuches kümmern.

- Die *extension blocklist* kann Mozilla nutzen, um einzelne Add-ons in Thunderbird zu deaktivieren. Es ist praktisch ein kill switch für Add-ons. Beim Aktualisieren der Blockliste werden außerdem detaillierte Informationen an Mozilla übertragen. Ich mag es nicht, wenn jemand irgendetwas remote auf meinem Rechner deaktiviert oder deaktivieren könnte. In den *Erweiterten Einstellungen* kann man es abschalten:

```plaintext
extensions.blocklist.enabled = false
```

- Thunderbird kontaktiert täglich den AMO-Server von Mozilla und sendet eine genaue Liste der installierten Add-ons. Als Antwort sendet der Server Status updates für die installierten Add-ons. Diese Funktion ist unabhängig vom Update Check für Add-ons, es ist nur eine zusätzliche Datensammlung von Mozilla. In den erweiterten einstellungen kann man dieses Feature abschalten:

```plaintext
extensions.getAddons.cache.enabled = false
```

- Alle Übertragungen von Telemetriedaten, Healthreport usw. an Mozilla unterbindet man ab Thunderbird 45 mit folgendem globalen Kill-Switch:

```plaintext
datareporting.policy.dataSubmissionEnabled = false
```

- Gespeicherte Passwörter für den Zugriff auf SMTP-, POP- oder IMAP-Server können mit einem Masterpasswort geschützt werden.
7.3.4 Datenverluste vermeiden

Die folgenden Hinweise wurden von den Mozilla-Entwicklern erarbeitet, um den Nutzer bestmöglich vor Datenverlusten zu schützen:

- Das Antiviren-Programm ist so einzustellen, dass es den Profilordner von Thunderbird NICHT(!) scannt. Die automatische Beseitigung von Viren kann zu Datenverlusten führen.

- Der Ordner *Posteingang* sollte so leer wie möglich gehalten werden. Gelesene E-Mails sollten auf themenspezifische Unterordner verteilt werden.

- Die Ordner sollten regelmäßig komprimiert werden, um gelöschte E-Mails engültig aus der MBOX zu entfernen und den Speicherplatz freizugeben.
  - In den Einstellungen in der Sektion *Erweitert* kann man eine automatische Komprimierung konfigurieren, sobald x MB Speicherplatz dadurch frei werden. Bei jedem Start prüft Thunderbird, ob die Ordner komprimiert werden können.


7.3.5 Wörterbücher installieren

Für die automatische Rechtschreibkontrolle beim Schreiben einer E-Mail muss man die nötigen Wörterbücher für die bevorzugten Sprachen installieren. Man kann neben dem immer vorhandenen Englisch die Wörterbücher für weitere Sprachen hinzufügen.

- Unter Linux nutzen Thunderbird und Firefox die Hunspell Wörterbücher für die Rechtschreibkontrolle. Mit dem bevorzugten Paketmanager kann man die Wörterbücher für verschiedene Sprachen installieren. Für Debian/Ubuntu könnte man `apt` verwenden. Neben `hunspell-de-de` für deutsches Deutsch gibt es auch Pakete für Österreichisches (`hunspell-de-at`) oder Schweizerisch (`hunspell-de-ch`):

  ```
  > sudo apt install hunspell-de-de
  ```

  Fedora und QubesOS fassen alle deutschen Sprachvariationen in einem Paket zusammen:

  ```
  > sudo dnf install hunspell-de
  ```


Danach kann man in den Einstellungen von Thunderbird die Rechtschreibprüfung aktivieren und die bevorzugte Sprache auswählen. Die Auswahl der Sprache kann man beim Schreiben einer Mail jederzeit ändern.

\(^2\) [https://addons.mozilla.org/de/thunderbird/language-tools/](https://addons.mozilla.org/de/thunderbird/language-tools/)
7.3. **MOZILLA THUNDERBIRD**

7.3.6 **Spam-Filter aktivieren**

Das Mozilla Team bezeichnet nicht erwünschte E-Mails (Spam) als Junk. Den integrierten lernfähigen Filter kann man in Account Einstellungen unter *Junk-Filter* aktivieren, wenn der E-Mail Provider keinen guten Spam-Filter einsetzt.

(Ich nutze lieber einen guten E-Mail Provider und brauche daher diesen Spam-Filter seit längerer Zeit nicht mehr.)

7.3.7 **Spam vermeiden**


**E-Mail Aliases nutzen**


Die Verwendung von E-Mail Aliases hat gegenüber temporären E-Mail Adressen und Wegwerf-Adressen einige Vorteile:

- E-Mail Aliases werden nicht gesperrt. In vielen Diskussionsforen (z.B. bei Zeit.de) sind E-Mail Adressen von Temp.-Mail Anbietern für die Registrierung von Accounts gesperrt.
- Gute E-Mail Provider haben ein sichere TLS Transportverschlüsselung für ihre Mailserver. Bei den Anbietern temporärer E-Mail Adressen werden die Mails in der Regel...
ohne oder mit schlechter TLS Verschlüsselung durch das Internet gesendet und könnes von Dritten (z.B. vom BND in Rahmen der Fernmeldeaufklärung) problemlos mitgelesen werden.

E-Mail Adresse-Erweiterungen

Bei vielen E-Mail Providern Mailbox.org, Runbox, Gmail, Yahoo! Mail Plus, Apple’s iCloud, Outlook.com oder FastMail kann man E-Mail Adresse-Erweiterungen nutzen. Wenn man die E-Mail Adresse name@provider.tld als Account oder E-Mail Alias registriert hat, kann man beliebig viele Adresse nach dem Muster name+extension@provider.tld zum Empfang verwenden. Es ist ein Standardfeature des MTA Postfix und kann auch auf eigenen Mailservern einfach aktiviert werden.

Einige E-Mail Provider bewerben dieses Feature als Spamschutz, aber der Wert als Spamschutz ist gering. Jeder, der sich ein bisschen mehr mit E-Mail Features beschäftigt hat (und davon kann man bei Datensammern ausgehen), kennt das Feature und kann die Erweiterungen leicht ausfiltern. Der Vorteil von E-Mail Adresse-Erweiterungen liegt eher in der einfach konfigurierbaren, automatischen Sortierung eingehender Nachrichten und nicht beim Spamschutz.

AnonBox des CCC

Bei der AnonBox.net des CCC kann ein E-Mail Account für den Empfang von einer Nachricht erstellt werden. Der Account ist bis 24:00 Uhr des folgenden Tages gültig (24-48h) und nicht verlängerbar. Die empfangene Nachricht kann man nur im Webinterface lesen und sie wird nach dem Abrufen gelöscht. Sie kann nur 1x gelesen werden! Zusammen mit der E-Mail wird auch der Account gelöscht. Man kann praktisch nur eine Mail empfangen.

Beim Erzeugen einer E-Mail Adresse erhält man einen Link, unter dem man die ankommende Mail lesen kann. Wenn noch nichts angekommen ist, dann bleibt die Seite leer. Der Link ist als Lesezeichen zu speichern, wenn man später nochmal nachschauen möchte.

Eine empfangene E-Mail wird im Quelltext dargestellt. Wer aus dem Konvolut nicht schlau wird, kann mit de rechten Maustaste in die Textwüste klicken und als Datei speichern, wie in Bild 7.7 gezeigt. Die Datei ist mit der Endung .eml zu speichern und kann dann in einem E-Mail Client wie z.B. Mozilla Thunderbird geöffnet werden (Bild 7.8).

Sicherheit unterliegt bei der AnonBox.net starken Schwankungen:

- Die SSL-Konfiguration des Webservers von AnonBox.net war früher mal auf dem aktuellen Stand der Technik mit Forward Secrecy und starken DH-Parametern und ist jetzt (Sept. 2018) katastrophal.

Wegwerf-Adressen

Einige Anbieter von Wegwerf-E-Mail-Adressen bieten einen sehr einfach nutzbaren Service, der keinerlei Anmeldung erfordert und auch kein Erstellen der Adresse vor der Nutzung. E-Mail Adressen der Form pittiplatsch@trash-mail.com oder pittiplatsch@weg-werf-email.de kann man überall und ohne Vorbereitung unbekümmert angeben. Das Postfach ist

---

22https://anonbox.net
Abbildung 7.7: E-Mail im Web-GUI der AnonBox.net als Datei speichern

unbegrenzt gültig.

In einem Webformular auf der Seite des Betreibers findet man später alle eingegangenen Spam- und sonstigen Nachrichten für das gewählte Pseudonym. Für das Webinterface des Postfachs gibt es in der Regel keinen Zugriffsschutz. Jeder, der das Pseudonym kennt, kann die Nachrichten lesen und löschen. Wenn eine Wegwerf-Adresse für die Registrierung eines Account genutzt wurde, könnte ein Angreifer problemlos die Passwort Recovery Funktion nutzen!

Nachrichten werden nach 6-12h automatisch gelöscht. Man muss also regelmäßig den Posteingang prüfen, wenn man eine Wegwerf-Adresse nutzt.

Liste einiger Anbieter (unvollständig):

- **https://discard.email** (SSL-Verschlüsselung für Webserver aber nicht für Mailserver, Passwortschutz, E-Mail schreiben möglich, Session-Cookies und JavaScript erforderlich)
- **https://www.trash-mail.com** (HTTPS, Cookies und JavaScript freigeben, Schreiben von E-Mails möglich)
- **https://www.guerrillamail.com** (HTTPS, Cookies und JavaScript freigeben, Schreiben von E-Mails möglich)
- **http://crapmail.dk** (Antwort schreiben möglich, Cookies freigeben)
- **http://vsimcard.com/trashmails.php** (bietet auch Wegwerf-SMS Nummern)
- **http://www.7mail7.com** (Cookies und JavaScript freigeben, RSS-Feed für Inbox)
- **http://www.mailcatch.com** (keine Cookies oder JavaScript nötig, E-Mails können gelöscht werden)
KAPITEL 7. E-MAIL KOMMUNIKATION

Abbildung 7.8: E-Mail aus AnonBox.net in Thunderbird geöffnet

- http://www.mailinator.com/ (JavaScript nötig freigeben, E-Mails können gelöscht werden)

In der Regel speichern diese Anbieter die Informationen über eingehende E-Mails sowie Aufrufe des Webinterface und stellen die Informationen bei Bedarf den Behörden zur Verfügung. Es handelt sich dabei nicht Anonymisierungsdienste.

Temporäre Adressen

Im Gegensatz zu Wegwerf-E-Mail-Adressen muss man eine temporäre E-Mail Adresse zuerst auf der Webseite des Anbieter erstellen, die dann für 10min bis zu mehreren Stunden gültig ist. Erst danach kann diese Mail-Adresse verwendet werden. Bei Bedarf kann die Verfügbarkeit der E-Mail Adresse im Browser mehrfach verlängert werden.


Die folgenden Anbieter erlauben nur zufällig erstellter E-Mail Adressen. Die Verwendung dieser Adressen für die Registrierung von Accounts ist sicherer, da ein Angreifer die Passwort Recovery Funktion des Webdienstes nicht nutzen kann, um sich ein neues Passwort zuschicken zu lassen und den Account zu übernehmen:

- https://temp-mail.ru (2h, HTTPS, Cookies und JavaScript freigeben, russisches GUI)
- www.10minutemail.com (10min gültig, verlängerbar)
- http://www.10minutemail.com/ (10min gültig, verlängerbar, Cookies und JavaScript freigeben)
- http://tmpeml.info (60min gültig, Cookies freigeben)
- http://disposable.pingfu.net (60min gültig, JavaScript freigeben)
- http://getairmail.com (24h gültig, Cookies und JavaScript freigeben)
Bei den folgenden Anbieter kann man neben zufällig generierten E-Mail Adressen auch selbst definierte E-Mail Adresse nutzen. Man kann damit einen bestimmten E-Mail Account mehrfach verwenden. Das ist für einige Anwendungsfälle ein Vorteil, manchmal eher ein Nachteil:

- [http://www.tempmailer.de](http://www.tempmailer.de) (60min gültig, Session-Cookies freigeben)
- [http://www.squizzy.de](http://www.squizzy.de) (60min gültig, Session-Cookies freigeben)
- [http://dontmail.net](http://dontmail.net) (24h, Cookies und JavaScript freigeben)
- [http://www.migmail.net](http://www.migmail.net) (24h, Cookies und JavaScript freigeben)

### 7.3.8 RSS-Feeds

RSS-Feeds bieten die Möglichkeiten, sich schnell über Neuigkeiten in häufig gelesenen Blogs zu informieren ohne die Webseiten einzeln abzuklappen zu müssen. Thunderbird enthält einen RSS-Reader, den man dafür nutzen kann.

Um mehrere interessante RSS-Feeds zu sammeln, erstellt man in der **Konten Verwaltung** ein neues Konto und wählt den Typ *Anderes Konto hinzufügen*....

![Konten Verwaltung](image)

Im zweiten Schritt wählt man den Typ **Blogs und RSS-Feeds** und danach eine beliebige Kontenbezeichnung.

In den Einstellungen für das RSS-Feed Konto kann man festlegen, in welchem Intervall die Feeds abgerufen werden sollen und ob die RSS-Feeds beim Start von Thunderbird aktualisiert werden sollen. Danach kann man die *Abonnements verwalten* und die Adressen der RSS-Feeds hinzufügen. Man kopiert die URL des RSS-Feeds von der Webseite des Blogs in das Feld für die Feed URL und klickt auf den Button *Hinzufügen* wie im Bild 7.9 dargestellt.


Aus Sicherheitsgründen ist es empfehlenswert, den RSS-Feed als Plain Text zu lesen und nicht als Webseite zu laden. Das sieht nicht so hübsch aus, verringert aber man die Angriffsmöglichkeiten durch bösgartigen Schadcode oder Media Elemente, wenn die Webbrowser-Komponente von Thunderbird kritische Lücken enthält (z.B. CVE-2016-9899 und CVE-2016-9893).

```
... 

rss.display.prefer_plaintext = true
rss.display.disallow_mime_handlers = 3
rss.display.html_as = 1
rss.show.content-base = 1

Bei jedem Start kontaktiert Thunderbird standardmäßig die Webserver, auf denen die RSS-Feeds liegen, und sucht nach den Favicons der Webseite für die Darstellung in der Liste der Feeds. Dieses Verhalten kann man Thunderbird abgewöhnen, indem man folgenden Parameter in den Einstellungen setzt:

browser.chrome.site_icons = false
```
7.3.9 Filelink


Ich kann dieses Feature nicht empfehlen.

1. Filelink ist nicht in die E-Mail Verschlüsselung integriert. Auch wenn man eine verschlüsselte E-Mail schreibt, werden die Uploads unverschlüsselt auf dem Server abgelegt. Man muss sich selbst um die Verschlüsselung der Dateien kümmern und könnte sie dann gleich zu einem 1-Click-Hoster hochladen.

2. Die bei einem Cloud-Service gespeicherten Dateianhänge unterliegen nicht dem besonderen Schutz des Post- und Fernmeldegeheimnisses.

3. Der standardmäßig unterstützte Dienst Box.com erfordert die Registrierung eines Accounts. Aufgrund der euphemistisch als Datenschutzerklärung bezeichneten Auflistung der Datensammeltechniken kann man von diesem Dienst nur abraten.

Es werden neben Cookies auch moderne Tracking Techniken wie HTML5 EverCookies eingesetzt. Do-Not-Track Header werden ausdrücklich ignoriert. Dabei wird nicht nur der Absender von Dateianhängen getrackt, sondern auch der Empfänger, der damit möglicherweise nicht einverstanden ist.

In Thunderbird 78.x kann man FileLink mit folgender Option komplett abschalten:

```plaintext
mail.cloud_files.enabled = false
```

---

23 https://www.box.com
24 https://support.mozilla.org/de/kb/filelink-fuer-grosse-dateianhaenge
25 https://www.box.com/de/de/legal/privacypolicy
7.4 Private Note


Gelegentlich möchte man aber nicht, dass eine vertrauliche Nachricht von Dritten gelesen wird. Verschlüsselung wäre eine naheliegende Lösung. Das ist aber nur möglich, wenn Absender und Empfänger über die nötige Kompetenz verfügen.

Als Alternative kann man PrivNote der Firma insophia nutzen. Man schreibt die Nachricht auf der Webseite des Anbieters und klickt auf den Button Create Note. JavaScript muss dafür freigegeben werden. In den Optionen kann man festlegen, wann die Nachricht gelöscht werden soll, man kann zusätzlich ein Passwort für das Lesen setzen und eine E-Mail bekommen, wenn die Nachricht gelöscht wird.

Das zusätzliche Passwort ist nur sinnvoll, wenn es über einen unabhängigen Kanal zum Empfänger übertragen wird. Man könnte z.B. bei einem Treffen ein Passwort vereinbaren und dieses Passwort dann nutzen, bis man ein neues Passwort austauscht. Das Passwort könnte man mit jeder Nachricht ändern, so dass die aktuelle Nachricht immer das Passwort für die nächste Nachricht enthält. Man kann es beliebig kompliziert gestalten, solange beide Seiten den Überblick behalten. Es ist aber nicht sinnvoll, ein Passwort zusammen mit dem Link zum Lesen der Nachricht in der gleichen E-Mail zu schicken, das ist Bullshit.

Wenn man auf den Button Create note klickt, wird ein Link generiert, unter dem man die Nachricht EINMALIG abrufen kann. Die Nachricht wird im Browser verschlüsselt auf dem Server gespeichert und nur der Link enthält den Key, um die Daten zu entschlüsseln.


Man kann den Link NICHT über irgendwelche Kanäle in Social Networks (z.B. Facebook) versenden. Wenn man auf den Link klickt, läuft im Hintergrund ein Crawls der Seite bevor man weitergeleitet wird. Facebook holt sich die Nachricht und der Empfänger kommt zu spät.

PrivNote ist nicht kryptografisch abhörsicher wie die E-Mail Verschlüsselung mit OpenPGP. Wenn ein Angreifer unbedingt den Inhalt der Nachricht lesen will, kann er die Nachricht vor dem Empfänger abrufen und über den Inhalt Kenntnis erlangen. Der eigentliche Empfänger kann nur den Angriff erkennen, da die Nachricht auf dem Server gelöscht wurde. Damit sind die Angebote für private Nachrichten geeignet, aber nicht geeignet für geheime oder streng vertrauliche Informationen.

\[26\text{https://privnote.com}\]
Abbildung 7.10: Eine Private Note schreiben
Kapitel 8

E-Mails verschlüsseln


**OpenPGP und S/MIME**

OpenPGP und S/MIME (*Secure MIME Protokoll*) sind fast 20 Jahre alte Standards für E-Mail Kryptografie. Sie können folgende Aufgaben erfüllen:


**OpenPGP und S/MIME nutzen Asymmetrische Kryptografie.** Das heißt, es wird ein Schlüsselpaar mit unterschiedliche Schlüssel zum Verschlüsseln und zum Entschlüsseln verwendet. Das Grundprinzip ist einfach erklärt:

- Jeder Anwender generiert ein Schlüsselpaar bestehend aus einem geheimen und einem öffentlichen Schlüssel. Während der geheime Schlüssel sorgfältig geschützt nur dem Anwender zur Verfügung stehen sollte, ist der öffentliche Schlüssel an alle Kommunikationspartner zu verteilen.
• Wenn Beatrice eine verschlüsselte Nachricht an Anton senden will, nutzt sie den öffentlichen Schlüssel von Anton, um die Nachricht zu chiffrieren. Nur Anton kann den Inhalt der E-Mail mit seinem geheimen Schlüssel dechiffrieren und lesen.

• Wenn der Anton eine signierte E-Mail an die Beatrice senden will, erstellt er eine Signatur (digitale Unterschrift) mit seinem geheimen Schlüssel. Beatrice kann mit dem öffentlichen Schlüssel von Anton die Unterschrift und damit die Echtheit der Nachricht verifizieren, da nur Anton Zugriff auf seinen geheimen Schlüssel haben sollte.

Verschlüsselung und Signatur können kombiniert werden. Dabei wird der Inhalt der Nachricht zuerst signiert und dann alles zusammen (Nachricht + Signatur) verschlüsselt.

PGP, GnuPG und S/MIME haben es in den letzten 20 Jahren nicht geschafft, eine massentaugliche Usability zu entwickeln. Wenn man erst einmal 20 Seiten Anleitung lesen muss, um die E-Mail Verschlüsselung zu verstehen, Software selbst konfigurieren muss, sich selbst die notwendigen Schlüssel erstellen muss oder beglaubigen lassen muss, sich um die Verteilung der Schlüssel selbst kümmern muss und es danach noch jedem Partner einzeln erklären muss, dann ist diese Krypto einfach nicht massentauglich.

Pretty Easy Privacy (PEP) und Autocrypt


Bei Pretty Easy Privacy (PEP) sind die Einschränkungen moderat:

• Bei der Einrichtung eines Accounts erstellt PEP im Hintergrund automatischen ein Schlüsselpaar (RSA, 2048 Bit). Der private Key wird standardmäßig nicht mit einem Passwort gesichert, da die PEP-Entwickler es als überflüssiges und störendes Feature ansehen. Es wird eine Verschlüsselung der Festplatte empfohlen.
  (Optional kann man einen Passwortschutz für private Schlüssel aktivieren und muss dann alle Schlüssel neu erstellen.)

  Hinweis: E-Mails mit BCC Adressen werden nicht(!) verschlüsselt.

• Der Betreff und weitere Header werden standardmäßig verschlüsselt (Memoryhole).

• Auf der Gegenseite akzeptiert PEP den ersten Key von einem Kommunikationspartner und verwendet ihn zukünftig automatisch (trust in first use). Alle weiteren Keys werden verworfen, um Sicherheitsprobleme wie bei Autocrypt zu vermeiden. (Dem erfahrene Anwender wird der Klick auf OpenPGP-Schlüssel importieren erspart.)

• Verifizierung von Schlüsseln ist anhand von Trustwords möglich, die über einen unabhängigen, sicheren Kanal oder bei einem Treffen verglichen werden müssen.

• PEP-Sync kann die Schlüssel zwischen mehreren Geräten synchronisieren.

• PEP verwendet statt GnuPG die eigene Implementierung Sequoia PGP als Backend.

Mit Autocrypt¹ wurden die Sicherheit von OpenPGP drastisch geschwächt, um den Austausch der Schlüssel zu vereinfachen. OpenPGP mit Autocrypt bietet keine sichere Verschlüsselung sondern nur noch some protection most of the time. Außerdem wurden

¹https://autocrypt.org
8.1. E-MAILS VERSCHLÜSSELN MIT THUNDERBIRD


Eine Ende-zu-Ende Verschlüsselung, die nicht mehr gegen die Provider schützt, ist einfach überflüssig. Bedauerlicherweise ist Autocrypt in vielen Tools zur E-Mail Verschlüsselung standardmäßig aktiviert, was die Nutzung von OpenPGP für sicherheitskritische Anwendungen (beispielsweise Whistleblower) kaputt gemacht hat.


Mit countermitm² gibt es eine Erweiterung für den Autocrypt Schlüsseltausch, die eine Verifizierung von Schlüsseln einführt und ein Network of Trust, um bei Autocrypt mögliche Man-in-the-Middle Angriffe für verifizierte Schlüsseln zu verhindern. countermitm gehört nicht zum Autocrypt Standard und wird unabhängig davon entwickelt.

8.1 E-Mails verschlüsseln mit Thunderbird

Thunderbird stellt alle Features für die Verschlüsselung mit OpenPGP und S/MIME bereit.

**Sichere Konfiguration:** Der Efail Angriff hat demonstriert, dass eine sichere Konfiguration des E-Mail Client eine notwendige Voraussetzung für sichere Verschlüsselung ist (E-Mails als Plain Text anzeigen, keine eingebundene Anzeige von Anhängen usw.)

**Masterpasswort aktivieren:** Thunderbird sichert die privaten Keys mit einer zufälligen Passphrase, die in der Passwortdatenbank gespeichert wird. Es ist daher wichtig, die Passwortdatenbank mit einem Masterpasswort zu sichern.

**Schlüssel erstellen:** Um die Verschlüsselung von E-Mails zu aktivieren, muss man in den Kontoeinstellungen in der Sektion Ende-zu-Ende Verschlüsselung einen PGP-Schlüsselpaar generieren oder importieren oder ein S/MIME Zertifikat importieren.

**Schlüssel verteilen:** Um verschlüsselt mit Kommunikationspartnern via E-Mail kommunizieren zu können, muss man die öffentlichen Schlüssel (public keys) austauschen. Bei modernen Krypto-Messengern wird das im Hintergrund automatisch erledigt. Bei der E-Mail Verschlüsselung muss man sich noch selbst darum kümmern.

1. Damit die Partner verschlüsselt schreiben oder Signaturen prüfen können, muss man ihnen den eigenen Schlüssel zusenden oder zum Download anbieten.
2. Damit man selbst verschlüsselt schreiben kann, muss man die Schlüssel der Kommunikationspartner in Thunderbird importieren.

**E-Mails schreiben:** Wenn man die Hürden beim Austausch der Schlüssel überwunden hat, kann man beim Schreiben die Verschlüsselung mit zwei Klicks aktivieren:

KAPITEL 8. E-MAILS VERSCHLÜSSELN

Leider bietet Thunderbird (noch) keine Möglichkeit, Präferenzen zur Verschlüsselung für bestimmte Empfänger zu definieren. Man muss vor dem Versenden einer E-Mail kurz innehalten und über die Verschlüsselungsoptionen nachdenken.

**E-Mails lesen:** Verschlüsselte E-Mails werden von Thunderbird automatisch entschlüsselt und angezeigt, wenn man sie öffnet. Man sieht oben rechts im Kopf der E-Mail ein oder zwei kleine Symbole bei verschlüsselten und/oder signierten E-Mails:

<table>
<thead>
<tr>
<th>Antworte</th>
<th>Weiterleiten</th>
<th>Archivieren</th>
<th>Junk</th>
<th>Löschen</th>
<th>Mehr</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Verschlüsselte E-Mails werden nicht in den globalen Index aufgenommen und können nicht bei einer Suche nach Begriffen aus dem Inhalt der Mail gefunden werden.

### 8.1.1 Eigenen OpenPGP Schlüssel erstellen oder importieren

Um OpenPGP zu aktivieren, muss man in der Verwaltung des E-Mail Account unter **Ende-zu-Ende Verschlüsselung** einen Schlüsselpaar für OpenPGP erzeugen oder importieren.

Wenn man ein neues Schlüsselpaares erstellt, gibt es nicht viele Fragen (Abb. 8.1).

Wenn man bereits OpenPGP verwendet, kann man seinen bereits in GnuPG vorhandenen privaten Schlüssel in eine Datei exportieren und diese in Thunderbird importieren. Auf der Kommandozeile erledigt man den Export aus GnuPG in die Datei mit:

```
> gpg --export-secret-keys --armor user@sever.tls > mein-key.asc
```

Die Datei mit dem Schlüssel kann man als eigenen Schlüssel importieren.

### 8.1.2 Eigenen OpenPGP Schlüssel mit GnuPG verwenden


Wer eine OpenPGP Smartcard verwendet oder den privaten Schlüssel nicht an Thunderbird übergeben sondern für hohe Sicherheitsanforderungen weiterhin die bereits vorhandene GnuPG Installation zur Verwaltung des privaten Schlüssel verwenden möchte, kann folgende Variable in den erweiterten Einstellungen von Thunderbird aktivieren:

```
mail.openpgp.allow_external_gnupg = true
```
8.1. E-MAILS VERSCHLÜSSELN MIT THUNDERBIRD

Abbildung 8.1: Neues OpenPGP-Schlüsselpaar in Thunderbird erstellen

Dann wird für die Einrichtung des eigenen Schlüssels eine dritte Option angeboten. Im folgenden Schritt kann man die ID des eigenen Schlüssels angeben, der im GnuPG Keyring liegt (Abb. 8.2). Der Zugriffsschutz für den privaten Key wird dann von GnuPG geregelt. Die Krypto-Operationen mit dem privaten Key werden dann ebenfalls von GnuPG ausgeführt statt mit OpenPGP.js in Thunderbird, was die kryptografische Sicherheit verbessert.


8.1.3 Den eigenen öffentlichen Schlüssel verteilen

Damit Kommunikationspartner mir verschlüsselt schreiben oder die Signatur meiner E-Mail verifizieren können, muss man ihnen den eigenen öffentlichen Schlüssel zusenden oder zum Download anbieten. Dafür gibt es mehrere Möglichkeiten:


³https://keys.openpgp.org
KAPITEL 8. E-MAILS VERSCHLÜSSELN

Abbildung 8.2: Privaten OpenPGP Schlüssel mit GnuPG verwalten


Abbildung 8.3: Öffentlichen OpenPGP Schlüssel per E-Mail verteilen

8.1.4 Fremde Schlüssel importieren

Für den Import der Schlüssel der Kommunikationspartner gibt es mehrere Möglichkeiten:

1. Wenn man einen OpenPGP Schlüssel als Anhang per E-Mail erhalten hat, kann man ihn mit zwei Mausklicks importieren.
2. Wenn eine E-Mail einen Autocrypt Header mit dem OpenPGP-Schlüssel des Absenders enthält, kann man ihn ebenfalls mit zwei Mausklicks importieren.

3. In der OpenPGP Schlüsselverwaltung, die man unter Extras - OpenPGP-Schlüssel verwalten findet, gibt es weitere Optionen zum Importieren von Schlüsseln:
   - Man kann einen oder mehrere Schlüssel aus einer Datei importieren.
   - Man kann einen Schlüssel aus der Zwischenablage importieren.
   - Man kann den Schlüssel von einer Download URL abrufen, wenn man die Download URL auf einer Webseite findet oder in der Signatur einer E-Mail.
   - Man kann den Schlüssel anhand der E-Mail Addr. via Web Key Discovery (WKD) und auf OpenPGP Keyservern suchen und importieren.

8.1.5 Fremde Schlüssel akzeptieren bzw. verifizieren.

Es reicht nicht aus, die Schlüssel der Kommunikationspartner in Thunderbird zu importieren, um sie anschließend verwenden zu können. Man die muss die importierten Schlüssel noch akzeptieren oder anhand des Fingerabdruck den Schlüssels verifizieren, um ausdrücklich zu bestätigen, dass man diese Schlüssel in Zukunft verwenden will.

Um Schlüssel zu akzeptieren bzw. zu verifizieren, öffnet man die Schlüsselverwaltung, wählt den frisch importierten Schlüssel aus und öffnet den Dialog Schlüsseleigenschaften.


8.2 Gedanken zum Mailvelope Browser Add-on

Mailvelope ist ein Add-on für die Browser Mozilla Firefox und Google Chrome, das OpenPGP Verschlüsselung im Webinterface ermöglicht.
KAPITEL 8. E-MAILS VERSCHLÜSSELN

Abbildung 8.4: Importierten OpenPGP Schlüssel akzeptieren oder verifizieren

Mailvelope kann die interne OpenPGP .js Implementierung nutzen oder eine externe GnuPG Installation. OpenPGP .js hat konzeptionell bedingt einige Schwächen und ist nicht für hohe Sicherheitsanforderungen geeignet. Konzeptionelle Schwächen von OpenPGP .js:


Mit JavaScript ist es nicht möglich, einen geheimen Schlüssel nach der Benutzung aus dem Hauptspeicher zu löschen (Overwriting memory - why?). Das normale Verhal-
ten von Mailvelope wurde bei Tor Onion Router als Security Bug eingestuft.\footnote{https://heise.de/-1746523}

Was in anderen Krypto-Implementierungen als schwerer Bug gilt, wird bei Mailvelope einfach als JavaScript Limitierung hingenommen.

In den FAQ von Mailvelope wird darauf hingewiesen, dass die geheimen Schlüssel durch das Senden eines Speicherabbildes in Absturzberichten an die Entwickler bei Mozilla oder Google kompromittiert werden könnten. Deshalb sollte man diese Funktion im Browser unbedingt deaktivieren.

### 8.2.1 Mailvelope mit GnuPG nutzen


Die Verwendung von GnuPG mit Mailvelope wird nicht funktionieren, wenn man unter Linux den Firefox Prozess unter Kontrolle von apparmor oder SELinux laufen lässt.

### 8.2.2 Mailvelope und Autocrypt

Standardmäßig verwendet Mailvelope den Autocrypt Schlüsseltausch. Da Autocrypt die Sicherheit von OpenPGP massiv schwächt, so dass die Verschlüsselung nur noch some protection most of the time bietet und keinen Schutz mehr gegen einen bösartigen E-Mail Provider, ist die Deaktivierung von Autocrypt im Dashboard dringend zu empfehlen.

```
General
Authorized Domains
Security
Security Background
Gmail API
Security Log
Key Server ➤
```

**Key Server**

**HKP key server**

```
https://keys.mailvelope.com
```

**Additional key sources**

- Use the Mailvelope key server. \url{Learn more} \footnote{https://heise.de/-1746523}
- Query keys from the recipients email provider (Web Key Directory). \url{Learn more}
- Use keys from Autocrypt headers of incoming email. \url{Learn more}

![Abbildung 8.5: Autocrypt in Mailvelope deaktivieren](image)

\footnote{https://heise.de/-1746523}

\footnote{https://www.mailvelope.com/de/faq#gnupg}
8.3 Einige Ergänzungen zum Thema GnuPG

GnuPG ist eine frei nutzbare Implementierung des OpenPGP Standards zur Verschlüsselung und Signierung von Daten. Es wird vom GNU Projekt ständig weiterentwickelt. Das Thunderbird Add-on Enigmail verwendet standardmäßig GnuPG 2.x.


Linux, BSD: installieren GnuPG 2.x nicht immer vollständig. Manchmal muss man etwas nachinstallieren. Für Debian/Ubuntu funtioniert:

```bash
> sudo apt install gnupg2 gpg-agent pinentry-gtk2 scdaemon
```

Bei einigen Linux Dsitibutionen ist gpg-agent im Paket gpgsm enthalten. Der gpg-agent wird für die Eingabe der Passphrase benötigt und sollte beim Login automatisch gestartet werden. Dafür fügt man in der Konfiguration $HOME/.gnupg/gpg.conf folgende Zeile am Ende ein:

```
use-agent
```

In der Datei $HOME/.gnupg/gpg-agent.conf kann man konfigurieren, wie lange der Agent die Passphrase für einen Key speichert. Standardmäßig wird eine Passphrase 10min (600s) gespeichert. GPA ändert den Wert aus Sicherheitsgründen auf 300s.

```
default-cache-ttl 300
max-cache-ttl 360
```

Verbesserte Konfiguration von GnuPG


Die Datei kann man mit einem Texteditor bearbeiten und folgende Optionen ergänzen bzw. durch Entfernen des Kommentarzeichens # aktivieren:

```
# keine Informationen über ersion und Betriebssystem einfügen
no-emit-version
no-comments

display-chars tf-8

# 16-stellige Key-IDs verwenden statt 8-stelliger (schwerer zu faken)
keyid-format 0xlong

# Keyserver-URLs in Keys ignorieren (Tracking möglich)
keyserver-options no-honor-keyserver-url, no-auto-key-retrieve, no-include-revoked

# Empfohlene Preferenzen für Krypto Algorithmen
personal-digest-preferences SHA512 SHA384 SHA256
personal-cipher-preferences AES256 AES192 AES TWOFISH
personal-compress-preferences Uncompressed ZIP ZLIB BZIP2
default-preference-list SHA512 SHA384 SHA256 AES256 AES192 AES Uncompressed
```

⁶http://www.gpg4win.org
# Signaturalgorithmus für Beglaubigungen
cert-digest-algo SHA512

# Einstellungen für symmetrische Verschlüsselung
s2k-cipher-algo AES256
s2k-digest-algo SHA384

# Cipher mit 64 Bit Blockgröße deaktivieren, weil sie
# schwach sind und ohne MDC verwendet werden (siehe: #Efail)
disable-cipher-algo 3DES
disable-cipher-algo IDEA

# SHA1 als schwachen Algorithmus markieren (wie MD5)
weak-digest SHA1

# sonstiges
fixed-list-mode
verify-options show-uid-validity
list-options show-uid-validity


Wenn man vor einigen Jahren seinen Schlüssel erstellt hat, dann wird in diesem Fall beispielsweise das angeknackste SHA-1 als Digest-Algorithmus bevorzugt verwendet. Man muss die persönlichen Preferenzen auch in die eigenen Schlüssel übernehmen und die Schlüssel danach neu verteilen. Das geht nur auf der Kommandozeile. Man muss das GnuPG Kommandozeilen Tool gpg2 mit der Option --edit-key und der Key-ID aufrufen. Danach kann man sich mit dem Kommando showpref die Preferenzen für diesen Schlüssel anzeigen und mit dem Kommando setpref die Defaults übernehmen:

```bash
> gpg2 --edit-key mustermann@server.tld
gpg (GnuPG) 2.1.x; Copyright (C) 2016 Free Software Foundation, Inc.
...
gpg> showpref
[ unbekannt ] (1). Max Mustermann <mustermann@server.tld>
  Verschl.: AES256, AES192, AES, CAST5, 3DES
  Digest: SHA1, SHA256, RIPEMD160
  Komprimierung: nicht komprimiert, ZLIB, BZIP2, ZIP
  Eigenschaften: MDC, Keyserver no-modify

gpg> setpref
Setze die Liste der Voreinstellungen auf:
  Verschl.: AES256, AES192, AES, 3DES
  Digest: SHA512 SHA384 SHA256, SHA1
  Komprimierung: nicht komprimiert
  Eigenschaften: MDC, Keyserver no-modify
Die Voreinstellungen wirklich ändern? (j/N) j
...
Sie benötigen die Passphrase, um den geheimen Schlüssel zu entsperren.
Benutzer: "Max Mustermann <mustermann@server.tld>"
...
gpg> quit
Änderungen speichern? (j/N) j
8.3.1 Gedanken zur Auswahl und Stärke von Schlüsseln

Aktuelle GnuPG Versionen unterstützen neben RSA und DSA Schlüsseln mit bis zu 4096 Bit Länge auch Schlüssel auf Basis elliptischer Kurven. Alle Optionen hat man zur Auswahl, wenn man ein Schlüsselpaar auf der Kommandozeile im Experten-Modus erstellt:

```
> gpg2 --expert --full-gen-key
```

Welche Schlüssel sollte man nutzen? Ein paar Gedanken zur Auswahl:

2. Das BSI ist derzeit der Meinung, dass RSA Schlüssel mit einer Länge von 2048 Bit bis 2022 eingesetzt werden können (BSI TR-02102-1). (Wenn man also jetzt einen neuen Schlüssel generiert, der für 5 Jahre gültig ist und dann möglicherweise verlängert werden soll, dann sollte man mindestens 3072 Bit Schlüssellänge wählen.)
3. Schlüssel auf Basis elliptischer Kurven werden nur in aktuellen PGP Implementierungen unterstützt, die sich aber noch nicht überall durchgesetzt haben.
4. Für den Einsatz elliptischer Kurven in PGP gibt es folgende Standards:
   • Der RFC 6637 der IETF empfiehlt nur die NIST-Kurven P-256, P-384 und P-512 für OpenPGP.
   • Die Java Bibliothek BountyCastle sowie PGP Implementierungen für C# und VB.net können außerdem mit den Brainpool Kurven nach RFC 5639 umgehen.
   • Das GnuPGP Team hat mit RFC 4880 bis Draft eine Erweiterung vorgeschlagen, auch die Unterstützung für die Kurven Ed25519 und Curve25519 zu integrieren. Dieser Draft ist bisher nur in GnuPG 2.1.x umgesetzt worden.

Wer jetzt schon Schlüssel auf Basis elliptischer Kurven verwendet, muss mit Problemen bei einigen Empfängern rechnen, insbesondere mit den elliptischen Kurven Ed25519 und Curve25519. Empfehlenswert für langfristige Nutzung sind RSA Schlüssel mit 4096 Bit Länge.

8.3.2 GnuPG Smartcards nutzen

Die Sicherheit asymmetrischer Verschlüsselung hängt von der sicheren Aufbewahrung des privaten Schlüssels ab. Es gibt mehrere Möglichkeiten, wie privaten Keys kompromittiert werden könnten:

- Wenn man GnuPG auf mehreren Computern nutzt, auf denen andere Nutzer Administrator- bzw. Root-Privilegien haben, könnten die privaten Keys von Administratoren eingesammelt werden.
- Böswillige Buben können mit einem Trojaner versuchen, den privaten Key zu kopieren und die Passphrase mit Keyloggern oder mit Tools wie Elcomsoft Distributed Password Recovery ermitteln.
- Die unbedachte Entsorgung einer Festplatte oder eines Computers ist ein weiteres Risiko, wenn die privaten Daten nicht sicher gelöscht wurden.


Ein paar Angebote für OpenPGP Smartcards:

7http://heise.de/-2817797
8.3. EINIGE ERGÄNZUNGEN ZUM THEMA GNUPG

- Die **GnuPG-Smartcard** gibt es von kernelconcepts.de\(^8\). Die Bestellung erfolgt per E-Mail und man braucht zusätzlich einen Smartcard Reader oder den ebenfalls dort erhältlichen Gemalto USB Adapter.

- Der **NitroKey**\(^9\) ist ein Open Source Hardware Projekt und der Nachfolger des Cryptostick. Der NitroKey Pro enthält zusätzliche einen OTP-Generator und Passwortspeicher. (Für diese Zusatzfunktion ist die NitroKey App\(^10\) zu installieren.)

- Der **Yubikey** ist ein One-Time-Passwordgenerator (OTP), den man für Logins bei Webdiensten nutzen kann. Er enthält zusätzlich eine OpenPGP Smartcard.\(^11\)

**Erster Test**

Die GnuPG Software Collection kann Smartcards *out-of-the-box* nutzen. Zuerst sollte man prüfen, ob alles funktioniert und die Smartcard erkannt wird. Smartcard anschließen und auf der Konsole bzw. in der DOS-Box folgendes Kommando eingeben:

```
> gpg2 --card-status
Application ID ....: D27600xxxxxxxxxxxxxxx
Version ...........: 2.0
Manufacturer ......: unknown
...                  
```


**Funktionen für Genießer**


```
> gpg2 --card-edit
...                  
gpg/card> admin
Admin-Befehle sind erlaubt

...                  
gpg/card> help
...                  
gpg/card> quit
```

Neue Schlüssel generiert man auf der Smartcard mit *generate*, die PIN und Admin-PIN kann man mit *passwd* ändern, mit *unblock* kann man den Zähler für Fehlversuche zurück setzen und *factory-reset* löscht alle Schlüssel auf der Smartcard.

**Neuer oder fremder Rechner - was nun?**

Ein nettes Feature von OpenPGP Smartcards ist es, an einem neuen oder fremden Rechner den Public Key von einer Download Adresse holen zu können. Der private Key ist auf der Card in einer sicheren Umgebung, somit kann man auch unterwegs auf einem halbwegs

\(^8\)https://www.floss-shop.de/de/search?Search=OpenPGP
\(^9\)https://www.nitrokey.com/de
\(^10\)https://www.nitrokey.com/de/download
\(^11\)https://www.yubico.com/products/yubikey-hardware/
vertrauenswürdigen, fremden Rechner eines Bekannten mit vollständiger GnuPG Installation die PGP-Verschlüsselung nutzen ohne den privaten Schlüssel zu kompromittieren.

Der Download des Public Key steht nur auf der Kommandozeile zur Verfügung. Nach dem Abrufen des Public Key von der Download URL muss man noch einmal den Card-Status aufrufen, damit der private Schlüssel an den Public Key gebunden wird:

```bash
gpg2 --card-edit
...  
gpg/card> fetch (Abrufen des Public Key von der Download URL)
gpg/card> quit
...  
gpg2 --card-status (Re-bind von private und public Key)
...
```

**Vorhandenen Schlüssel mit Smartcard weiter verwenden**

Wenn man bereits PGP für die Verschlüsselung nutzt und einen vorhandenen Schlüssel weiter verwenden möchte, dann kann man die Private Keys dieses Schlüssel auch auf eine OpenPGP Smartcard übertragen. Damit erspart man sich die Verteilung eines neuen Schlüssels und kann die Beglaubigungen des Web-of-Trust behalten.


Als erstes ruft man `gnupg2` mit der `edit-key` Funktion für den Schlüssel auf, den man auf die Smartcard verschieben will. Mit `toggle` schaltet man auf die Verwaltung der privaten Keys. Dann schiebt man mit `keytocard` zuerst den Hauptschlüssel als Signatur Key auf die Smartcard, wählt den Subkey mit `key 1` aus und schiebt den Encryption Subkey auf den passenden Platz auf der Smartcard.

```bash
> gpg2 --edit-key mustermann@server.tld
Geheimer Schlüssel ist vorhanden.
...
gpg> toggle

sec rsa2048/8A02F3F6
  erzeugt: 2016-06-18 verfällt: niemals Aufruf: SC
ssb rsa2048/08D68793
  erzeugt: 2016-06-18 verfällt: niemals Aufruf: E

gpg> keytocard
Den Hauptschlüssel wirklich verschieben? (j/N) j
Wählen Sie den Speicherort für den Schlüssel:
  (1) Signatur-Schlüssel
  (3) Authentisierungs-Schlüssel
Ihre Auswahl? 1

gpg> key 1

sec rsa2048/8A02F3F6
  erzeugt: 2016-06-18 verfällt: niemals Aufruf: SC
ssb* rsa2048/08D68793
```
8.3. EINIGE ERGÄNZUNGEN ZUM THEMA GNUPG

Ergänzung zu dem Thema GNUPG

erzeugt: 2016-06-18 verfällt: niemals Aufruf: E

gpg> keytocard

Wählen Sie den Speicherort für den Schlüssel:

(2) Verschlüsselungs-Schlüssel
Ihre Auswahl? 2

gpg> quit

Änderungen speichern? (j/N) j

Danach kann man den Status der Smartcard prüfen und sich davon überzeugen, dass die beiden Schlüssel jetzt als Signature key und Encryption key auf der Smartcard liegen:

> gpg2 --card-status

Reader ...........: 20A0:4108:000036C4000000000000000000:0
Application ID ...: D2760001240102010005000036C40000
Version ..........: 2.1
...
PIN retry counter : 3 0 3
Signature counter : 0
Signature key .....: C5DF 0BB0 11B7 3F49 3A37 AFC4 4472 A2E8 8A02 F3F6
created .......: 2016-06-18 15:32:07
Encryption key...: 94E1 D64A 51C0 8C78 CE60 6472 0059 00DC 08D6 8793
created .......: 2016-06-18 15:32:07
Authentication key: [none]
General key info..: pub rsa2048/8A02F3F6 <mustermann@server.tld>
sec rsa2048/8A02F3F6 erzeugt: 2016-06-18 verfällt: niemals
ssb rsa2048/08D68793 erzeugt: 2016-06-18 verfällt: niemals

8.3.3 Adele - der freundliche OpenPGP E-Mail-Roboter


1: Den eigenen Schlüssel an Adele senden: Als erstes schickt man den eigenen öffentlichen Schlüssel per E-Mail an adele@gnupp.de. Den Schlüssel hängt man als Anhang an die Mail an, indem man die Option OpenPGP - Meinen öffentlichen Schlüssel anhängen vor dem Versenden der Mail aktiviert (Bild ??)


Hallo,

hier ist die verschlüsselte Antwort auf Ihre E-Mail.

Ihr öffentlicher Schlüssel wurde von mir empfangen.

Anbei der öffentliche Schlüssel von adele@gnupp.de, dem freundlichen E-Mail-Roboter.

Viele Grüße,
adele@gnupp.de
KAPITEL 8. E-MAILS VERSCHLÜSSELN

-------BEGIN PGP PUBLIC KEY BLOCK-------
Version: GnuPG v1.4.9 (GNU/Linux)
mQGiBDyF1IkRBACfVHJvxv47r6rux7TwT4jHM7z/2VfyCrmcRegQEsbdLfqu3mEmK
RouuaDuquKNWh2V2Er0weFnJqdzpaeuPj10wp0uIEvU3FRHyltytw9dfwAHv4
MJ7639satXs9pfXbmZ0idPAoE451+VLhIG11Q1PGFppJ57S21E71/++/nkswCge8Mge
....
EQUIABgUCPIWUlQASCRDlczRpkg/9wd1R1BHAEEBv20AoJGheeZjMCSbXtmNSwW
QsL0d0+4AKCdxwt552yi9dBFxPo8pBI0nhtbQ==
=ERT8
-------END PGP PUBLIC KEY BLOCK-------


Alternativ holt man sich Adeles Schlüssel mit der ID 0x92AB3FF7 von einem Keyserver.


Hallo,

hier ist die verschlüsselte Antwort auf Ihre E-Mail.

Ich schicke Ihnen Ihre Botschaft im Wortlaut zurück, damit Sie sehen, dass ich sie erfolgreich entschlüsseln konnte.

> Hello Adele,
>
> hope you are feeling well.

Hinweis: PGP/Inline statt PGP/MIME verwenden: Adele ist schon eine etwas ältere Dame und versteht nur das alte Format PGP/Inline während Enigmail inzwischen das modernere PGP/MIME Format verwendet.

Beim Schreiben einer E-Mail an Adele muss man deshalb immer auf PGP/Inline umschalten, anderenfalls kann Adele die Mail nicht interpretieren. Menüpunkt Enigmail - Protokoll PGP/Inline aktivieren!

8.3.4 Memory Hole Project


To: Max Mustermann <mustermann@server.tld>
From: Maxi Muterfrau <musterfrau@server.tld>
Subject: Re: Plenum der K-Gruppe (KaG) am 32.02.2017 um 26:20 Uhr
References: <5cc396a27b873f3fa@mailbox.org>
in-Reply-To: <5cc396a27b873f3fa@mailbox.org>
Message-ID: <49e6a7bfbc433sfgcfe@secure.mailbox.org>
Date: Wed, 29 Mar 2017 21:55:37 +0200
MIME-Version: 1.0
8.3.3 EINIGE ERGÄNZUNGEN ZUM THEMMA GNUPG

Content-Type: multipart/encrypted;
  protocol="application/pgp-encrypted";

Das Memory Hole Projekt möchte einen Ansatz entwickelt, um die für den Transport unwichtigen Informationen ebenfalls zu verschlüsseln. Die Headerzeilen werden dabei in dem verschlüsselten PGP/MIME Part versteckt und können nur vom Empfänger bei der Entschlüsselung der Mail gelesen und sichtbar gemacht werden.

Enigmail unterstützt dieses Feature bereits. Wenn man die folgenden Parameter setzt, wird der Mail Header Betreff: in OpenPGP verschlüsselten E-Mails durch die konfigurierte Floskel Encrypted Message ersetzt und der originale Text in den verschlüsselten PGP/MIME Part verschoben. Wenn die Mail entschlüsselt wird, wird der Betreff wieder hergestellt.

```plaintext
extensions.enigmail.protectedHeaders = 2
extensions.enigmail.protectedSubjectText = Encrypted Message
```

Außerdem kann man die Header In-Reply-To: und References: im PGP/MIME Part verstecken, indem man zusätzlich folgenden Parameter setzt:

```plaintext
extensions.enigmail.protectReferencesHdr = true
```

Als Ergebnis würden dann die E-Mail Header aus dem oben gezeigten Beispiel wie folgt aussehen:

```plaintext
To: Max Mustermann <mustermann@server.tld>
From: Maxi Muterfrau <musterfrau@server.tld>
Subject: Encrypted Message
Message-ID: <49e6a7bfbc433sfgcfge@secure.mailbox.org>
Date: Wed, 29 Mar 2017 21:55:37 +0200
MIME-Version: 1.0
Content-Type: multipart/encrypted;
  protocol="application/pgp-encrypted";
```

8.3.5 Autocrypt

Das Verfahren Autocrypt will den Nutzern den manuellen PGP-Schlüsselaustausch abnehmen und ihn dadurch nutzerfreundlich machen. Der PGP-Schlüssel soll im Header jeder E-Mail mitgesendet werden, damit der Empfänger sofort automatisch verschlüsselt antworten kann, ohne sich um den Schlüsseltausch (und Validierung?) zu kümmern.

Für die theoretische Begründung der Sicherheit greift Autocrypt auf das Konzept Opportunistic Security (RFC 7435) zurück. Das bedeutet, das die Verschlüsselung nur noch gegen passive Angreifer schützt soll aber nicht mehr gegen aktive Angreifer, die sich als man-in-the-middle in die Kommunikation einschleichen können.


Wie könnte ein E-Mail Provider die Verschlüsselung kompromittieren?

1. Die E-Mail Header werden von den Mailprovidern ständig routiniert manipuliert. Es werden neue Header eingefügt, einige Header werden gelöscht... In gleicher Weise könnten die Autocrypt Header von den versendenden oder empfangenen E-Mail Providern manipuliert werden und ein falscher Schlüssel eingefügt werden.


Das ist kein Bug sondern ein Feature des zugrunde liegenden Konzeptes.


Der Autocrypt-Schlüsseltausch erfordert es, dass man dem E-Mail-Provider vertrauen muss und führt damit Ende-zu-Ende Verschlüsselung mit OpenPGP ad absurdum, es kompromittiert die Sicherheit zugunsten (zweifelhafter) Vereinfachungen der Usability.

8.3.6 Verschlüsselung in Webformularen

Auch bei der Nutzung eines Webmail Accounts oder Webforms für die Versendung anonymer E-Mails muss man auf Verschlüsselung nicht verzichten.

Einige grafische Tools für die Schlüsselverwaltung wie GPA\footnote{http://www.gnupg.org/related_software/gpa/index.de.html} (GNU Privacy Assistent) enthalten einen Editor. Man kann den Text in diesem Editor schreiben, mit einem Klick auf den entsprechenden Button signieren oder verschlüsseln und das Ergebnis über die Zwischenablage in die Textbox der Website einfügen. Das Entschlüsseln funktioniert in umgekehrter Reihenfolge.

Abbildung 8.6: Text mit GPA verschlüsseln
Andere grafische Tools wie *Kleopatra* von KDE Projekt bieten die Ver- und Entschlüs-
selung des Textes in der Zwischenablage an. Um eine verschlüsselte Nachricht zu versen-
den, schreibt man den Text mit einem beliebigen Editor (Notepad, gedit, mousepad, kwri-
te...), kopiert danach den gesamten Text in die Zwischenablage (mit den Tasten STRG-A
und STRG-C) und wählt dann die Option zum Verschlüsseln der Zwischenablage im Me-
nü (Abb: 14.2). Nach der Auswahl der Empfänger wird der Text aus der Zwischenablage
verschlüsselt und das verschlüsselte Ergebnis wieder in der Zwischenablage gespeichert.
Diesen unlesbaren Zeichensalat kann man im Textfeld im Webformular einfügen (Taste:
STRG-V). Entschlüsseln funktioniert wieder in umgekehrter Reihenfolge.

Abbildung 8.7: Kleopatra GnuPG GUI: Assistent zur Verschlüsselung von Dateien

Linuxer könnten auch das GnuPG Desktop Applet von den TAILS Entwicklern nutzen,
das ebenfalls den Text in der Zwischenablage ver- oder entschlüsseln kann. Das Applet
kann unter Debian/Ubuntu mit dem bevorzugten Paketmanager installiert werden:

> sudo apt install openpgp-applet

### 8.3.7 OpenPGP-Verschlüsselung für Kontaktformulare

Dass Metadaten (z.B. Absender und Empfänger einer E-Mail) für die Überwachung eine
große Rolle spielen, ist seit den Veröffentlichungen von Snowden/Greenwald allgm.
bekannt. Leser des Privacy-Handbuches haben es evtl. vorher gewusst (siehe: Kommuni-
kationsanalyse).

Kontaktformulare bieten eine Möglichkeit, diese Metadaten zu verschleiern. Wer ein
Blog oder eine Webseite betreibt, kann recht einfach ein Kontaktformular zur Verfügung
stellen. Es gibt Wordpress Plug-ins für Kontaktformulare, einfache PHP-Scripte oder
fertige Perl-CGI Scripte. Man kann eine individuell passende Lösung wählen.

Dabei sollte man auf folgendes achten:

1. Das Kontaktformular sollte den Absender nicht zur Eingabe seiner E-Mail Adresse
zwinger. Als work-around kann man im HTML-Code des Formulars das Feld für
die Absender E-Mail Adresse als *hidden* deklarieren und einen Standardwert setzen.
2. Das Script sollte die IP-Adresse des Absenders nicht in den Header der E-Mail einfüh-
Einfach ausprobieren.
3. Das Kontaktformular sollte immer via HTTPS (SSL-verschlüsselt) aufgerufen wer-
den. Wenn die Webseite auch via plain HTTP erreichbar ist, sollten alle Links auf der
Webseite zum Kontaktformular mit der vollständigen URL angegeben werden:

```html
<a href="https://www.server.tld/kontakt.html">Kontakt</a>
```
Jeder gute Webhoster bietet inzwischen SSL-Verschlüsselung für einen kleinen Aufpreis für alle Kunden, Wordpress.com hat es standardmäßig aktiviert.

Im folgenden möchte ich einige Möglichkeiten vorstellen, wie man ein Kontaktformular mit OpenPGP-Verschlüsselung aufmotzen könnte.

Hinweis: Bei allen Varianten handelt es sich um server based crypto, die nicht die gleiche Sicherheit wie richtige Ende-zu-Ende Verschlüsselung gewährleisten kann. Diese Verschlüsselung schützt gegen passive Lauscher am Draht, kann aber durch potente aktive Angreifer kompromittiert werden.

Ganz einfach ohne Programmierung

Man kann einen guten E-Mail Provider nutzen, der TLS-Verschlüsselung für eingehende E-Mails erzwingen kann und ein verschlüsseltes Postfach bietet, z.B. mailbox.org.

• Nachdem man einen E-Mail Account bei mailbox.org erstellt und bezahlt hat, ist der Alias für TLS-verschlüsselten Versand/Empfang zu aktivieren sowie das OpenPGP verschlüsselte Postfach zu aktivieren und der eigene public Key hochzuladen.

• Im Script des Kontaktformulars konfiguriert man als Empfänger die E-Mail Adresse <name>@secure.mailbox.org bzw. <name>@tls.mailbox.org.


Diese Variante schützt den Inhalt der Nachrichten gegen den allgemeinen Überwachungswahn und bei Beschlagnahmung von Daten. Sie schützt nicht gegen eine TKÜ nach §100 a/b StPO beim Hoster des Kontaktformulars oder beim E-Mail Provider, da der Inhalt als Plain-Text an diesen Stellen mitgelesen werden kann.

Mit JavaScript im Browser des Absenders

Diese Variante erfordert HTML-Kenntnisse, um einige Anpassungen im HTML-Code des Kontaktformulars vorzunehmen und die Bibliothek OpenPGPjs einzubinden.


1. Die Javascript Bibliothek openpgp.min.js aus dem Projekt OpenPGPjs ist bei Github auszuchecken und aus dem Verzeichnis dist auf den eigenen Webserver kopieren.

2. Das JavaScript Schnipselchen encrypt_message.js von der Webseite im Privacy Handbuch herunter laden und auf den Webserver kopieren. Dieses JavaScript Schnipselchen verschlüsselt das Textarea Feld mit der ID message mit dem OpenPGP-Schlüssel, der in dem DIV Container pubkey steht. Wenn das Textarea oder der DIV Container im Formular eine andere ID haben, sind die Zeilen 5 und 6 anzupassen:

   function encrypt_message() {
       if (!(window.crypto && window.crypto.getRandomValues)) {
           window.alert("Fehler: der Browser ist veraltet und wird nicht supported!");
       } else {
           var message = document.getElementById("message");
           var pgpkey = document.getElementById("pubkey");

13https://github.com/openpgpjs/openpgpjs
14https://www.privacy-handbuch.de/handbuch_32v.htm
if(message.value == "") {
    window.alert("Kein Text gefunden, das Textfeld ist leer!");
} else {
    // Verschlüsseln des Textes im Textarea
    var options = { data: message.value,
                    publicKeys: openpgp.key.readArmored(pgpkey.innerHTML).keys
                };
    openpgp.encrypt(options).then(function(ciphertext) {
        message.value = ciphertext.data;
    });
    // Button für Verschlüsseln deaktivieren
    document.getElementById("encrypt").disabled = true;
    document.getElementById("send").disabled = false;
}

3. Im HTML-Header der Webseite des Formulares sind die Scripte zu laden:

    ...<script src="openpgp.min.js" async></script>
    <script src="encrypt_message.js" async></script>
    ...


    <FORM name="contact" method="post" action="https://server.tld/....">
      <textarea id="message" ...></textarea>
      <input type="button" onclick="encrypt_message();" value="Verschlüsseln" id="encrypt" />
      <button type="submit" disabled="true" id="send">Senden</button>
    </FORM>

5. Außerdem ist der eigenen OpenPGP public Key als versteckter DIV-Container mit der ID pubkey irgendwo im HTML-Code einzubauen.

    <div id="pubkey" hidden="true">
    -----BEGIN PGP PUBLIC KEY BLOCK-----
    ...
    -----END PGP PUBLIC KEY BLOCK-----
    </div>

6. Für Surfer, die JavaScript standardmäßig deaktivieren kann man ein Hinweis einfügen, dass JavaScript für die Funktion des Formulares nötig ist:

    <NOSCRIPT>
    Bitte aktivieren Sie JavaScript für die Verschlüsselung der Nachricht!
    </NOSCRIPT>

8.3.8 OpenPGP Keyserver

Die OpenPGP Keyserver bilden eine Infrastruktur im Web, um öffentliche Schlüssel auch Unbekannten zum Download anzubieten. Die verschiedenen Server synchronisieren ihren Datenbestand. Man kann die Keyserver nach einem passenden Schlüssel durchsuchen.

- Auf der Kommandozeile bzw. DOS-Box kann man nach OpenPGP Schlüsseln anhand der E-Mail Adresse suchen und einen der gefundenen Schlüssel importieren:

  > gpg2 --search cane@privacy-handbuch.de

  Wenn man die Key-ID oder den Fingerprint des Schlüssels kennt und weiss, dass der Schlüssel auf einem Keyserver zu finden ist, kann man ihn auch direkt importieren:

  > gpg2 --recv 0x8F1E7F49912F0D9B73586C908CD51D2D7E36E399

- In Enigmail findet man die Suchfunktion in der Schlüsselverwaltung unter dem Menüpunkt Schlüssel-Server -> Schlüssel suchen.

Keyserver Pool von OpenPGP (mit E-Mail Verifikation)

Der Keyserver Pool https://keys.openpgp.org stellt einen modernen Keyserver für OpenPGP Schlüssel zur Verfügung, der einige Probleme der alten Keyserver wie die des SKS Keyserver Pools vermeidet. Insbesondere werden die E-Mail in den Schlüsseln verifiziert, um das Problem mit Fake Keys (siehe unten) zu lösen. Der Pool ist außerdem auch als Tor Onion Service v3 Adresse erreichbar.


Thunderbird verwendet standardmäßig nur diesen Keyserver, eine Anpassung der Konfiguration ist nicht nötig. Um den Keyserver auch mit dem Programm gpg2 auf der Kommandozeile zu nutzen, kann man den Keyserver in der Konfigurationsdatei $HOME/gnupg/dirmngr.conf (Linux) bzw. %APPDATA%/GnuPG/dirmngr.conf (Windows) konfigurieren und folgende Optionen einfügen:

  keyserver hkps://keys.openpgp.org
  keyserver hkp://zkaan2xfbuxia2xfp7ofnkz6r5dzbbvxunyp5g2iebopbf4iqmbad.onion

Wenn genau zwei Keyserver konfiguriert werden und einer davon ein Tor Onion Service ist, dann verwendet GnuPG automatisch den Onion Service, wenn Tor Onion Router läuft.

Nach der Änderung der Konfiguration muss Dirmngr beendet evtl. werden:

  > gpgconf --kill dirmngr

(Zukünftige Versionen von GnuPG werden diesen Keyserver standardmäßig nutzen.)

Hinweis: dieser Keyserver entfernt aus Sicherheitsgründen alle Signaturen von Dritten aus den hochgeladenen Schlüsseln. Die Verifikation von Schlüsseln anhand der Signaturen (Web of Trust) ist also nicht möglich.

Vorsicht bei der Nutzung von veralteten SKS-Keyservern

Man kann auf den Keyservern des SKS Pool u.ä. veralteten Servern nach Schlüsseln anhand E-Mail Adressen, 8-stellige oder 16-stellige Key IDs oder bekannten Fingerprints suchen.
8.3. EINIGE ERGÄNZUNGEN ZUM THEMA GNUPG

1. Wenn man nach der E-Mail Adresse sucht, dann werden unter Umständen mehrere Schlüssel zum Importieren angeboten. Es gibt immer wieder Witzbolde, die Schlüssel für fremde E-Mail Adressen auf den Keyservern hochladen (um zu stänkern?). Wenn man zum Beispiel den Schlüssel von Felix v. Leitner (Fefe) sucht, dann findet man fünf Schlüssel. Aber nur der Schlüssel von Okt. 2013 ist korrekt (nicht der neueste Schlüssel!), wie Fefe in seinem Blog schreibt.\(^\text{15}\)

Abbildung 8.8: Fünf OpenPGP-Schlüssel für eine E-Mail Adresse

J. Schmidt von Heise.de beklagt, dass ein Scherzkeks OpenPGP Schlüssel für seine E-Mail Adresse auf die Keyserver hochgeladen hat und dass er damit verschlüsselten E-Mails nicht lesen kann (Editorial c’t 6/2015).

Erinn Clark signierte die Downloads des TorBrowserBundle. Für ihre E-Mail Adresse wurden Fake Schlüssel auf den Keyserver publiziert.\(^\text{16}\)

Gavin Andresen signierte die Bitcoin Binaries, für seine E-Mail Adresse wurden ebenfalls Fake Schlüssel auf den Keyserver publiziert.\(^\text{17}\)

2. Statt E-Mail Adressen kann man auch nach der 8-stelligen Key-ID suchen (zB. 0xA534A9C6). Diese Methode liefert besser Ergebnisse, allerdings muss man die richtige Key-ID kennen. Auch diese Methode ist nicht sicher, da man diese Key-IDs ebenfalls faken kann, wie ein Forscherteam demonstrierte.\(^\text{18}\)

3. Die 16-stellige Key-ID (zB. 0xFC32CEECA534A9C6) ist schwieriger zu faken, aber auch nicht als kryptografisch sichere ID entworfen.

4. Am besten ist es, wenn man den gesuchten Schlüssel anhand des Fingerprint sucht (zB. 0x68995C53D2CEE11B0E4182F62146D0CD2B3CAA3E). Diese Suche liefert als einzige Variante vertrauenswürdige Ergebnisse.

8.3.9 Web des Vertrauens (WoT)

Im Prinzip kann jeder Anwender einen Schlüssel mit beliebigen E-Mail Adressen generieren. Um Vertrauen zu schaffen, gibt es das Web of Trust.


- Anton (A) vertraut dem Schlüssel von Conrad (C), weil er von Beatrice (B) unterschrieben wurde und Beatrice für Anton eine vertrauenswürdige Person ist.

\(^{15}\)https://blog.fefe.de/?ts=aa27d652
\(^{17}\)http://gavintech.blogspot.ch/2014/03/it-aint-me-ive-got-pgp-impostert.html
\(^{18}\)http://heise.de/-2473281
Abbildung 8.9: Beispiel für ein Web of Trust

- Anton (A) vertraut dem Schlüssel von Doris (D) nicht, obwohl er von Conrad unterzeichnet wurde und der Schlüssel Conrad durch die Signatur von Beatrice als vertrauenswürdig gilt.

Warum vertraut Anton (A) dem Schlüssel von Doris (D) nicht automatisch? Weil er Conrad (C) nicht kennt und ihn daher nicht als vertrauenswürdige Person definiert hat!

Es bildet sich also kein weltweites Vertrauensnetz automatisch, indem man irgendwelche Schlüssel irgendwie unterschreibt und dann verteilt! Das Web of Trust funktioniert nur in einer kleinen Umgebung, weil zwei(!) Bedingungen erfüllt sein müssen. Neben einer digitalen Signaturkette muss auch jeder unterschreibender Nutzer in der Kette als vertrauenswürdige Person gekennzeichnet sein. Das geht nur, wenn man die Personen kennt.


Das Web of Trust funktioniert nur in Ausnahmefällen, wenn man die Schlüssel direkt untereinander austauscht oder auf einer Webseite zum Download bereitstellt.

Certification Authorities

Diese Infrastruktur kann auch von vertrauenswürdigen Institutionen (Certification Authorities, CAs) genutzt werden. Die Nutzer wenden sich an die CA und lassen gegen Vorlage von Ausweisdokumenten den eigenen OpenPGP-Key signieren. Alle Partner benötigen lediglich den öffentlichen Schlüssel der CA, um die Echtheit der Schlüssel zu überprüfen.


Weitere Beispiele für Certification Authorities sind:
- CAcert.org signiert auch OpenPGP-Schlüssel
- Krypto-Kampagne der Zeitschrift c’t
• PCA des Deutschen Forschungsnetzes (DFN-PCA)
8.4 Verschlüsselte Dokumente per E-Mail senden


![Abbildung 8.10: Verschlüsselte Speicherung in LibreOffice aktivieren](image)

Wenn man keine OpenPGP Schlüssel verwendet sondern ein Kennwort, dann muss man dem Empfänger das Kennwort zu Öffnen der Datei über einen sicheren 2. Kanal mitteilen oder man schreibt im Text der E-Mail eine Andeutung, die nur der Empfänger interpretieren kann:

_Das Passwort ist der Name der Bar, in der wir neulich ein Bier getrunken haben._

Man muss nicht für jede Nachricht ein neues Passwort definieren, man kann ein einmal sicher ausgetauschte Passwort natürlich auch über einen längeren Zeitraum verwenden. Das ist sicherer, als immer wieder unsichere Methoden für den Passworttausch zu nutzen.
Kapitel 9

Instant Messaging und Telefonie


Die sogenannten Kanäle/Channels bieten eine Top-Down Kommunikation (der Boss spricht und Abonnenten dürfen lauschen). Außerdem unterscheiden sie sich von Gruppenchats darin, dass die Anzahl der Mitglieder unbegrenzt ist und dass ein Mitglied/Abonnent andere Mitglieder nicht sehen kann (Privatsphäre).


Messenger mit verschlüsselter Audio- und Videotelefonie


Telegram bietet viele Social Features und ist als zensurresistente Twitter Alternative mit Black Market Features populär geworden (z. B. bei Protesten in Hongkong und Belarus 2020) aber als Messenger für vertrauliche Kommunikation weniger geeignet.


Um die Synchronisation der Geräte zu gewährleisten, wird eine unverschlüsselte Datenbank mit den Metadaten auf den Servern geführt. Das ist praktisch eine Vorratsdatenspeicherung, die wir bei E-Mail seit 20 Jahren verhindern wollen. (Für Unternehmen mit Compliance Anforderungen und eigenen Servern ist das nicht relevant.) Wire Enterprise ist der bevorzugte Messenger der Bundesregierung und vom BSI für VS-NfD zugelassen. Wire ist eine gute Collaboration Plattform für Unternehmen.


Community-basierte Entwicklung und förderale Infrastruktur erschweren die Einführung und Umsetzung von Sicherheitsfeatures. M. Marlinspike hat diese Phänomene als systemimmanent für diese Open Source Projekte beschrieben. 1

Der bwmesseher ist ein Fork für den Einsatz von [matrix] in der Bundeswehr. Für die Nutzung des bwmesseher gelten in der Bundeswehr die gleichen Regeln, wie für unverschlüsselte E-Mail und Telefonie:

- Auf Standardgeräten (Smartphones, Laptops, PCs) darf der bwmesseher in der Bundeswehr nur für offenen eingestufte Kommunikation verwendet werden.

Briar (nur für Android) ist ein Messenger für hohe Sicherheitsanforderungen. Die Kommunikation und Speicherung ist vollständig verschlüsselt. Es werden keine zentralen Server genutzt sondern Peer-2-Peer Kommunikation via Tor Onion Router oder direkt via WLAN/Bluetooth, wenn kein Internet verfügbar ist.

Kontakte können nur bei einem persönlichen Treffen (Face-2-Face) hinzugefügt werden, indem man gegenseitig die QR-Codes scannet. Nur so ist nach Meinung der Entwickler sichergestellt, dass man wirklich mit der gewünschten Person kommuniziert.


Apps für verschlüsselte Audio- und Videotelefonie

Anwendungen für verschlüsselte Telefonie konnten sich in den letzten 10 Jahren im privaten Bereich nicht großflächig etablieren, obwohl die technischen Voraussetzungen seit

1https://www.signal.org/blog/the-ecosystem-is-moving
2https://www.presseportal.de/pm/76712/4764023


Wie andere Anwendungen, die Daten über eine DHT verteilen, sollten Jami aus dem Internet erreichbar sein. Anderenfalls kommt es zu zeitverzögerten, unregelmäßigen Zustellung von Nachrichten und verpassten Anrufen. Die Entwickler empfehlen, UPnP auf dem Router zu aktivieren und die Firewall abzuschalten, damit Jami das Port-forwarding auf dem Router automatisch konfigurieren kann und erreichbar ist.

Hinweis: Das BSI, das FBI oder die US Homeland Security empfehlen ausdrücklich die Deaktivierung von UPnP zur Vermeidung von Sicherheitsrisiken! Wenn man diese Empfehlungen folgt, wird man mit Jami im P2P Modus nicht glücklich.\(^3\)\(^4\)\(^5\)


Es gibt Apps für Android und iPhone. Im F-Droid Store gibt es eine Google-freie Version. Diese Version muss ständig laufen und sollte nicht beendet werden, wenn man Anrufe annehmen will, da die Google Push Services nicht verwendet werden werden.


Lösungen für Videokonferenzen

Kommerzielle Lösungen für Videokonferenzen wie Microsoft Teams, Zoom oder Slack sind nicht DSGVO-konform. Es gibt aber Alternativen, die man auch selbst betreiben kann:

**Jitsi Meet** ist eine Open Source Software für den eigenen Konferenzserver.

**Nextcloud Talk** ist eine weitere Open Source Lösung für Videokonferenzen.


\(^3\)https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/basisschutz_fuer_den_router.html
\(^4\)https://www.howtogeek.com/122487/htg-explains-is-upnp-a-security-risk/
Kommerzielle Angebote für Unternehmen

GSMK Cryptophones bieten einen ganzheitlichen Sicherheitskonzept und High End Security. Sie sind aber auch mit 2.000+ Euro entsprechend teuer.

Silent Circle bietet mobile, verschlüsselte Kommunikation für Unternehmen, NGOs und Regierungen mit Enterprise Features wie Verwaltung der Nutzer und Geräte.

SecuSUITE for Samsung Knox ist derzeit die bevorzugte Lösung für sichere, mobile Kommunikation in deutschen Bundesbehörden, vom BSI für VS-NfD zugelassen.

Mobile Encryption App der Telekom adressiert Unternehmen und Behörden, die sich etwas preiswerter gegen Spionage durch starke (ausländische) Angreifer schützen wollen. Die App verschlüsselt Telefonie nach dem GSMK-Protokoll.


9.1 Verschlüsselte Telefonie

Für verschlüsselte Telefonie gibt es mehrere Protokolle:


- Das GSMK-Protokoll verschlüsselt den Datenstrom doppelt mit AES256 und Twofish. Die niedrige, feste Datenrate von 4,8 kBit/s soll eine Kommunikation auch dann ermöglichen, wenn verschlüsselte VoIP Telefonie mittels DPI blockiert wird, wie es beispiw. in einigen Gebieten von Frankreich, in VAE oder Saudi Arabien üblich ist.

9.1. VERSCHLÜSSELTE TELEFONIE

9.1.1 SRTP/ZRTP Verschlüsselung

Das SRTP/ZRTP-Protokoll von Phil Zimmermann (Erfinder von PGP) spielt eine zentrale Rolle bei verschlüsselter Telefonie. Es gewährleistet eine sichere Ende-zu-Ende-Verschlüsselung der Sprachkommunikation. Wenn beide Kommunikationspartner eine Software verwenden, die das ZRPT-Protokoll beherrscht, wird die Verschlüsselung automatisch ausgehandelt. Kurze Erläuterung der Begriffe:


**SAS** dient dem Schutz gegen Man-in-the-Middle Angriffe auf ZRTP. Den beiden Kommunikationspartnern wird eine 4-stellige Zeichenfolge angezeigt, die über den Sprachkanal zu verifizieren ist. Üblicherweise nennt der Anrufer die ersten beiden Buchstaben und der Angerufenen die beiden letzten Buchstaben. Wenn die Zeichenfolge identisch ist, kann man davon ausgehen, dass kein Man-in-the-Middle das Gespräch belauschen kann.

9.1.2 Verschlüsselt chatten und telefonieren mit qTox

Tox ist ein Protokoll für verschlüsselte Telefonie und Chats. Die Kommunikation läuft direkt von Client zu Client. Die Teilnehmer finden sich gegenseitig über eine Distributed

---

KAPITEL 9. INSTANT MESSAGING UND TELEFONIE

Hash Table (DHT). Es gibt keinen Provider, der Kommunikationsprofile erstellen könnte oder zur Implementierung von Backdoors für Behörden gezwungen werden könnte.

Tox verwendet für die Krypto nicht die üblichen, vom NIST standartisierten Verfahren sondern Verfahren von D.J. Bernstein. Der ECDHE Schlüsseltausch nutzt curve25519, statt AES wird XSALSA20 verwendet und statt SHA256 kommt POLY1350 zum Einsatz.

Es gibt mehrere Clients, die das Protokoll beherrschen. Für PCs und Laptops eignet sich qTox am besten. Für Android gibt es Antox (im Google Playstore) und den TRIfA Tox Client im F-Doid-Store und Playstore. Für iPhones gibt es keinen Tox Client.

Bei Smartphones ist zu beachten, dass die Call History (Liste aller Anrufe) an Google übertragen wird, wenn die App die Anrufe auf dem Sperrbildschirm anzeigen kann. Dort werden die Daten für 4-6 Monate gespeichert (private Vorratsdatenspeicherung bei NSA PRISM Partnern). Geheimdienste haben Zugriff auf diese Daten und die Firma Elcomsoft liefert die nötigen Tools für die Auswertung. Die Datenspeicherung lässt sich deaktivieren, indem man die Nutzung der Google Cloud Services komplett deaktiviert.

Installation von qTox


Fedora, Debian 10+, Ubuntu 19.04+, SuSE usw. bieten qTox in den Repositories zur Installation an. Man kann den bevorzugten Paketmanager nutzen, um das Programm zu installieren und aktualisieren:

Fedora: > sudo dnf install qtox
Ubuntu: > sudo apt install qtox

Anwender von Fedora sollten das RPMFusion Repository vorher aktivieren, damit die notwendigen Codecs für Audio- und Videotelefonie mit installiert werden.

*BSD: Einen aktuellen Port findet man in PKGSRC unter net-im/qTox. Die Installation erfolgt wie üblich mit make und benötigt einige Zeit:

# cd /usr/ports/net-im/qTox
# make install clean

Account erstellen

qTox lässt sich mit Klick auf das Programmsymbol starten. Es öffnet sich sich das Profilmenü. Hier hat man die Wahl, ein bereits bestehendes Profil zu laden (LoadProfile) oder ein neues Profil anzulegen. Zunächst wählt man den Benutzernamen und das Passwort.
Es sollte ein starkes Passwort gewählt werden - je größer die Basis der möglichen Zeichen (Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen), je zufälliger diese Zeichen gewürfelt werden und je mehr Stellen das Passwort hat, desto stärker das Passwort.

Konfiguration von qTox

Im Hauptmenü wählt man in den Einstellungen, die man jederzeit durch Klick auf das Zahnrad erreicht, zunächst die Registerkarte General. Bei Language lässt sich die Sprache umstellen indem man auf English klickt und die Sprache Deutsch wählen.

Hier lässt sich nun auch einstellen, ob man qTox bei jedem Systemstart mitstarten lassen möchte, ob man regelmäßig nach Updates suchen möchte, ob in der Systemleiste ein Icon angezeigt werden soll, ob qTox bei Programmstart zunächst nur in diesem Icon oder mit einem Fenster starten soll, ob qTox beim Minimieren in die Systemleiste statt in die Taskleiste minimiert werden soll, ob bzw. nach welcher Zeit der Abwesenheit qTox den Status Abwesenheit anzeigen soll und ob geteilte Dateien automatisch angenommen werden sollen. Aus Sicherheitsgründen sollten Dateien nie automatisch angenommen werden!


Auf der Registerkarte Audio/Video kann man die Audio- und Videoeinstellungen konfigurieren und testen.

Auf der Registerkarte Erweitert kann man qTox in eine portable Programmversion umwandeln, die man auf dem USB-Stick mitnehmen kann.

Kontakt aufnehmen

Wenn Anton und Beatrice Tox für die Kommunikation nutzen wollen, müssen sie die Tox-ID austauschen. Das könnte in folgenden Schritten ablaufen:

1. Anton schickt seine Tox-ID irgendwie an Beatrice.
2. Beatrice sendet eine Freundschaftsanfrage an diese Tox-ID.
3. Anton akzeptiert die Freundschaftsanfrage von Beatrice.

Erhält man eine Freundschaftsanfrage eines anderen Benutzers, so wird oben links im Programmfenster ein grünes Feld mit der Aufschrift 1 neue Freundschaftsanfrage angezeigt. Durch Klick auf diese grüne Schaltfläche werden weitere Infos zur Freundschaftsanfrage angezeigt – etwa die ID, eventuell auch den Benutzernamen und/oder einen Begrüßungstext. Man hat nun die Wahl die Freundschaftsanfrage anzunehmen oder abzulehnen. Mit der Annahme der Freundschaftsanfrage werden die nötigen Krypto-Schlüssel ausgetauscht, die für die verschlüsselte Kommunikation benötigt werden.

Kontakte anrufen, Dateien schicken oder chatten

Wenn man auf das Profil eines Kontakts klickt, hat man viele Möglichkeiten. Man kann telefonieren und per Video schnattern (Buttons oben rechts)…
9.1. VERSchlÜSselte TeLeFonie

oder chatten und Dateien verschicken (Buttons untern rechts).

9.1.3 Skype???


Nach der Übernahme von Skype durch Microsoft wurde die zensur-robuste Infrastruktur von Skype umgebaut und die Ende-zu-Ende Verschlüsselung von Skype kompromittiert. Statt einer Peer-to-Peer Infrastruktur nutzt Skype jetzt sogenannte Super-Nodes, die alle in Microsoft Rechenzentren stehen. Die Keys für die Verschlüsselung werden in der Microsoft Cloud hinterlegt und Microsoft nutzt die sich daraus ergebenden Möglichkeiten zum Mitlesen7 (juristisch korrekt wird in den Datenschutzbestimmungen darauf hingewiesen).

Abhörerschnittstellen


7https://heise.de/-1857620
8https://secure.wikimedia.org/wikipedia/en/wiki/Calea
9http://www.online-recht.de/vorges.html?FUEV
10https://de.wikipedia.org/wiki/Telekommunikations-%C3%9Cberwachungsverordnung
bietet Skype Abhörschnittstellen in allen westeuropäischen Ländern und zunehmend auch in anderen Ländern wie Indien. In Deutschland sind Abhörprotokolle aus Skype Gesprächen alltägliches Beweismaterial.\footnote{11}

Skype ist seit 2011 PRISM Partner der NSA und damit direkt an das Spionagesystem der USA angeschlossen. Mit der Übernahme durch Microsoft 2012 und dem technischen Umbau konnte die von der NSA analysierte Datenmenge aus der Skype verdreifacht werden.\footnote{12}

### 9.2 Instant Messaging

Die Übernahme von WhatsApp durch Facebook zeigt, dass es einfach Sch.... ist, sich das gesamte Adressbuch mit allen Kontakten klauen zu lassen. Irgendwann landet es in den großen Datensammlungen von Google, Microsoft, Facebook oder Yahoo!, die alle als PRISM-Partner der NSA gelistet sind.\footnote{13}

In korrektem Juristen-Deutsch könnte man es DSGVO-konform z. B. so formulieren:\footnote{14}


Wer durch seine Nutzung von WhatsApp diese andauernde Datenweitergabe zulässt, ohne zuvor von seinen Kontaktpersonen aus dem eigenen Telefon-Adressbuch hierfür jeweils eine Erlaubnis eingeholt zu haben, begeht gegenüber diesen Personen eine deliktische Handlung und begibt sich in die Gefahr, von den betroffenen Personen kostenpflichtig abgemahnt zu werden.

Wenn man als WhatsApp Nutzer die Telefonnummern mit Bekannten austauscht, dann müsste man also eigentlich um die Zustimmung bitten, Name, Telefonnummer und Freundschaftsstatus an Facebook zu schicken. Das Gespräch könnte so ablaufen:

- Anton: *Du hast doch nichts dagegen, wenn ich Facebook Deinen Namen mit der Telefonnummer schicke und das wir Freunde sind - oder?*

- Beatrice: *Eyhh man, alles ok - mache ich doch auch?*

### Anforderungen an einen guten Messenger

Unter Berücksichtigung der massiven Überwachung von Instant Messaging, welche durch E. Snowden bekannt gemacht wurde, und des Crypto War 3.0 ergeben sich folgende Anforderungen an einen guten Messenger Dienst:


9.2. INSTANT MESSAGING

Abbildung 9.2: Auswertung von 160.000 Überwachungsberichten


4. Es sollte keine unerwünschten Uploads (Datenklau) ohne ausdrückliche Zustimmung durch den Nutzer geben. Der Dienst sollte auch komplett ohne Datenklau nutzbar sein und nur optional Daten wie das Adressbuch abgreifen.

5. Eine Google-freie Installation (beispielsweise via F-Droid) sollte möglich sein.


Im Gegensatz zu einigen Open Source Dogmatikern bin ich nicht der Meinung, dass die dezentrale Infrastruktur freier Messenger gegen die Installation von Backdoors auf den Servern schützt. Während bei Threema oder Signal App immer wieder angezweifelt wird, ob dort wirklich die audierte bzw. veröffentlichte Software auf den Servern läuft, werden die Open Source Admin von Jabber oder [matrix] Servern per Definition zu Heiligen erklärt, die niemals nie etwas anderes installieren würden als die offizielle Serversoftware und nie neugierig Metadaten beschnüffeln würden.


Die Gründe für Vertrauen sind sehr individuell. Manch einer sagt sich: Ich vertraue dem Admin, weil es ein Bekannter ist. und ein anderer denkt Ich vertraue dem Admin

\[16\] https://www.ejabberd.im/mod_otr
KAPITEL 9. INSTANT MESSAGING UND TELEFONIE

nicht, weil es ein Bekannter ist und die Neugier und Verführung zu einer kleinen Schnüffelei, die niemand bemerken würde, unter Bekannten größer ist. (Stichwort Love-INT o.ä.)

8. Es wäre schön, wenn die Bedienung so einfach wäre, dass auch meine Tante und ihre Kaffeekranz Freundinnen ohne lange Erklärungen damit umgehen können.

Einen idealen Messenger, der alle Bedingungen erfüllt, gibt es nicht. Man muss abwägen, was wichtig ist und welche Schwerpunkte man bei den Anforderungen setzt.

Multi-Device-Support und Ende-zu-Ende Verschlüsselung

Multi-Device-Support ist ein heutzutage ein häufig gewünschtes Feature für Messenger. Man möchte via PC und Laptop online sein, um eine vernüftige Tastatur und einen großen Bildschirm zu nutzen, und man möchte via Smartphone unterwegs erreichbar sein. Dieses Feature erschwert es aber, eine sichere Ende-zu-Ende Verschlüsselung zu realisieren.


- Das BKA hat diesen Angriff mehrmals erfolgreich gegen Telegram Nutzer eingesetzt. Das Team von Prof. Fedderath demonstrierte wie\textsuperscript{17} die Behörden gaben die Telefonnummer der Zielperson in der Telegram Web-App eingeben und die SMS zur Autorisierung des Zugriffs abfangen. Dann konnten die unverschlüsselten Gruppenchats unbeachtet mitgelesen werden. Die geheime Chats von Telegram konnten damit nicht geknackt werden, da die Verschlüsselung MTProto nicht Multi-Device fähig ist.


- Im Iran wurden seit 2014 wesentlich elegantere Angriffe staatlicher Hacker auf Telegram und WhatsApp eingesetzt. Mit der Zusendung eines böswilligen Dokumentes wurden die Smartphones der Opfer kompromittiert und dann die Account Credentials von WhatsApp oder Telegram ausgelesen. Damit konnten die Angreifer ein weiteres Gerät im Namen des Opfers registrieren und den Multi-Device Support exploiten.


- Ein kleiner Test von Riot ([matrix]) zeigte ebenfalls erhebliche Hürden in der Usability beim Schutz gegen das Einschleusen eines böswilligen Gerätes. (Wobei man noch hinzufügen muss, dass beide Teilnehmer in dem Chat als Krypto-Experten gelten und wirklich verstanden haben, wie sichere Krypto funktionieren könnte.)

  - Anton: Ok - habe Riot installiert und bin drin!
  - Beatrice: War doch ganz einfach - oder?

\textsuperscript{17}https://www.youtube.com/watch?v=wBaj0LxcnY8
9.2. INSTANT MESSAGING

Abbildung 9.3: Man-in-the-Middle Angriff auf OMEMO Verschlüsselung

– Anton: Aber der Chat ist unverschlüsselt. Sollte das nicht E-2-E sein?
– Beatrice: Du musst die E-2-E Verschlüsselung erst aktivieren.
– Anton: Habe ich in den Einstellungen aktiviert.
– Beatrice: Nee - DU musst es für JEDEN Chat einzeln aktivieren.
– Beatrice: Chat Settings, ganz runter scrollen, unten die letzte Option.
– Anton: Ok - hab's gefunden.
– Beatrice: Ist halt BETA, kann man noch verbessern.
– Anton: Hmmm - sehe gerade, dass Du hier mit 6 Geräten chattest!!! 2x Linux, 3x Ubuntu und ein seltsames Phone. Bist Du sicher, dass die alle von Dir sind - oder...???
– Beatrice: Kann schon sein, keine Ahnung - ich nutze Riot schon länger...
– Anton: Arrgghhh...

Es ist eine alte Weisheit, dass eine Kommunikation erst dann wirklich vertrauenswürdig ist, wenn man gegenseitig die Schlüssel verifiziert hat und sichergestellt, dass nur diese verifizierten Schlüssel verwendet werden. Die meisten Messenger bieten irgendwie eine Möglichkeit, bei einem Treffen die Schlüssel zu verifizieren, allerdings ist das nicht immer DAU-kompatibel.

Außerdem kann man bei vielen Multi-Device fähigen Messengern eine zweistufige Bestätigung für das Hinzufügen weiterer Geräte aktivieren. Damit ist eine zusätzliche Passphrase erforderlich, die sich vom Account Passwort unterscheiden sollte, wenn ein neues Gerät angemeldet wird.

Als Schutz gegen Angriffe bei (kurzzeitigem) physischem Zugriff auf ein entsperrtes Smartphone bieten hochwertige Messenger eine zusätzliche PIN-Sperre für die App, die man bei hohem Schutzbedarf aktivieren kann. Damit wird verhindert, dass ein Angreifer die App auf dem Smartphone starten kann und damit die Rechte erlangt, um heimlich ein zusätzliches Gerät anzumelden.

Anmerkung: Die Krypto-Protokolle OTR (Jabber/XMPP) und MTProto (Telegram) sind nicht Multi-Device fähig und daher von diesem Angriff nicht betroffen.

Harte und weiche Verifikation

Auch wenn die Krypto nicht gebrochen werden kann, sind verschiedene Angriffe möglich: Social Attacks greifen nicht die Krypto an. Stattdessen versucht ein Angreifer (Mallory) sich das Vertauen zu erschleichen, indem er sich als eine bekannte Person ausgibt:

• Mallory: Hi Anton, ich bin Beatrice und wollte über das geheime Ding...
• Anton: Hallo Beatrice - schön dass Du Dich meldest - also...

… und gleichzeitig in die andere Richtung:
• Mallory: Hi Beatrice, ich bin Anton. Also zu diesem geheimen Ding…
• Beatrice: Ohhh - Anton, schön dass Du Dich meldest. Tja also…

Und damit wäre Mallory ein MitM, solange Anton und Beatrice sich nicht gegenseitig verifizieren. Dieser Angriff ist bei Messengern einfacher, die anonyme Accounts ermöglichen, die nicht an eine Telefonnummer gebunden sind. Bei Signal App o.ä. wäre zus. noch ein SIM-Swap nötig.

**Angriffe auf die Schlüssel** attakieren den Schlüsseltausch. Um eine einfache Kontaktaufnahme zu ermöglichen wenn der Gegenüber offline ist, stellen viele einfach Messengern die public Keys der Nutzer auf den Servern zur Verfügung. Ein bösartiger Betreiber könnte prinzipiell die Keys austauschen und den Datenverkehr umleiten, so dass Mallory wieder in der Mitte sitzt und als Reflektor agieren kann, der die Nachrichten umschlüsselt und mitliest.

Ob man derartige Angriffe für möglich hält, hängt vor allem vom Vertrauen in den Provider ab. Da Ende-zu-Ende Verschlüsselung auch gegen bösartige Provider schützt, ist es aber legitim, diese Angriffe in Erwägung zu ziehen und zu diskutieren.

Gegen diese Angriffe schützt eine Verifikation der Kommunikationspartner:

**Weiche Verifikation** schützt gegen Social Attacks. Man könnte den Gegenüber via Audio- oder Videocall anrufen (Messenger unterstützen es) und wenn man den Gegenüber erkennt und die Verschlüsselung prüft, chattet man mit der richtigen Person.


- Bei Signal App ist das standardmäßig der Fall, so dass diese Social Attacks unter Bekannten, die die Telefonnummern ausgetauscht haben, schwer möglich sind.
- Bei Threema kann man einen Account optional mit einer Telefonnummer verknüpfen (und damit die Anonymität teilweise aufgeben). Threema speichert Hashwerte der verknüpften Telefonnummer oder E-Mail Adresse auf dem Server und zeigt eine schwache (weiche) Verifikation an, wenn der Client die verknüpfte Telefonnummer im Adressbuch findet.
- Bei Telegram wird die Telefonnummer aus dem Adressbuch unter dem Account angezeigt, die man vergleichen könnte. Aufgrund der Implikationen für die Privatsphäre ist es aber nicht empfehlenswert, Telegram den Zugriff auf das Adressbuch zu erlauben.

(Es ist also nicht grundsätzlich verwerflich, wenn Messenger Accounts mit Telefonnummern verknüpft werden. Es kommt darauf an, ob man den Messenger vor allem für vertrauliche, private Kommunikation mit Bekannten verwenden möchte oder ob man in erster Linie anonym irgendwo rumtrollen will.)

**Harte Verifikation** überprüft die verwendeten Schlüssel. Ein universelles Verfahren zur Überprüfung der Schlüssel ist ein Vergleich der Fingerabdrücke der Schlüssel bei einem Face-2-Face Treffen oder out-of-band über einen unabhängigen, sicheren Kanal.

Der Fingerabdruck muss nicht unbedingt anhand kryptischer Zeichenfolgen verglichen werden sondern könnte auch mit bunten Bildchen erfolgen, was intuitiver ist.

- Bei Face-2-Face Treffen scannt man gegenseitig einen angezeigten QR-Code.
- Bei einem unabhängigen Kanal muss man sicher sein, dass am anderen Ende des Kanal wirklich die gewünschte Person sitzt. Der Kanal muss verifiziert sein.


- Messenger für hohe Sicherheitsanforderungen wie Briar oder Tox haben einen sicheren Schlüsseltausch implementiert, der eine harte Verifikation einschließt.
9.2. INSTANT MESSAGING

• Signal App setzt nicht nur bei Verschlüsselung der Daten Maßstäbe sondern auch beim Schlüsseltausch. Beim X3DH Schlüsseltausch liegen nicht die public Keys auf dem Server sondern abgeleitete Schlüssel, die nur in Kombination mit den echten privaten Keys auf den primären Endgeräten der Nutzer sinnvoll genutzt werden können.\(^{18}\) Bei X3DH könnte ein bösertiger Provider die Verbindsaufnahme blockieren. Es ist aber (nach aktuellem Stand) nicht möglich, modifizierte Keys einzuschleusen.

• WhatsApp verwendet mit dem ECDH Schlüsseltausch ein ähnliches Verfahren, dass ebenfalls von den Signal Entwicklern entwickelt wurde.

• Die meisten anderen Messenger publizieren die public Keys auf den Servern und weisen mit Icons darauf hin, dass die Schlüssel verifiziert werden sollten.

**Link Previews in Messengern**

Einige Messenger bieten ein Link Preview, wenn man eine URL in das Eingabefeld tippt oder kopiert. Man kann den hübschen Preview versenden oder vor dem Versand löschen.

Abbildung 9.4: Link Preview in einem Chat in Signal App

Voraussetzung für einen Link Preview ist, dass die Webseite im HTML Header die Open Graph Metatags enthält. Anhand dieser Metatags wird der Preview generiert:

```
<HTML>
<HEAD>
...
<meta property="og:title" content="Ein Beispiel">
<meta property="og:description" content="Das ist nur ein sinnloses Beispiel">
<meta property="og:image" content="https://beispiel.tld/images/preview01.png">
...
```

Um einen Link Preview zu generieren, kontaktiert der Messaging Client den Webserver und versucht die Webseite zu laden, sobald eine URL im Eingabefeld erkannt wird. Wenn die Webseite im Header die Open Graph Tags enthält, wird ein Preview generiert und evtl. das Bild herunter geladen. Den Ablauf kann man sehr unterschiedlich implementieren:


• Signal App generiert Link Previews nur für Webseiten, die via HTTPS erreichbar sind. Signal App kontaktiert den Webserver ebenfalls direkt und tarnt sich als WhatsApp.

In den Datenschutz Einstellungen von Signal kann man die Previews abschalten.

\(^{18}\)https://signal.org/docs/specifications/x3dh/
• Telegram hat eine mittelmäßige Lösung implementiert. Die Link Previews werden auf dem Telegram Server generiert. Das verhindert Implikationen für die Privatsphäre wie bei WhatsApp, da nur der Telegram Server die Webseiten kontaktiert und das Abrufen der Informationen keinem Nutzer individuell zugeordnet werden kann.


9.2.1 Messenger Threema


Das Erstellen von Channels und Bots (die bei Telegram populär sind) ist nur mit dem kostenpflichtigen Zusatzfeature Threema/Broadcast möglich, was den Missbrauch reduziert. Die Channels und Bots können aber von allen Threema Nutzern abonniert werden.


Kommunikationspartner können dann Kontakte aus dem Adressbuch schnell finden und anhand der farbig dargestellten Vertrauensstufe verifizieren, dass sie mit dem Bekannten verbunden sind, mit dem sie die bereits die Telefonnummer ausgetauscht haben.

Threema kennt folgende Vertrauensstufen bei Kontakten:

• rot: ID und öffentlicher Schlüssel wurden vom Server geholt. Da kein passender Kontakt im Adressbuch gefunden wurde, kann man sich nicht sicher sein, ob die Person wirklich die ist, die sie in ihren Nachrichten vorgibt zu sein.

• orange: Der Kontakt wurde im Adressbuch gefunden. Da der Server Handynummern und E-Mail-Adressen prüft, kann man sich ohne zusätzliches Verifizieren relativ sicher sein, dass diese Person wirklich diejenige ist, die man meint.

19https://broadcast.threema.ch/de
20https://threema.ch/de/faq/code_audit
• **grün:** Der öffentliche Schlüssel der Person wurde persönlich durch Scannen des QR-Codes verifiziert. Solange das Gerät der Person nicht gestohlen/gehackt wurde, ist es unmöglich, dass ein Dritter die Nachrichten fälschen oder mitlesen kann.


Das Backup wird mit einem Passwort verschlüsselt und kann auf dem Threema Server gespeichert werden oder auf einem beliebigen WebDAV Server. Wenn man das Backup auf einem eigenen WebDAV Server speichern möchte, muss man dort ein Verzeichnis für Threema Safe anlegen (beispielsweise *threema-safe*) und ein Unterverzeichnis *backups*. In dem Threema Safe Verz. ist die Datei *config* mit folgendem Inhalt anzulegen:

```json
{
    "maxBackupBytes": 524288,
    "retentionDays": 180
}
```

Dann kann man auf dem Smartphone ein Threema Safe Backup erstellen und als Experte die eigene WebDAV Adresse des Threema Safe Verzeichnisses angeben inklusive Login Credentials für den WebDAV Server (Abb. 9.5).

![Abbildung 9.5: Eigenen WebDAV Server für Threema Backup auswählen](https://shop.threema.ch/)

Der Name der Backupdatei ist die mit dem Backup Passwort verschlüsselte Threema-ID. Auch wenn das Backup auf dem Threema Server rumliegt, ist nicht erkennbar, zu welchem Account das Backup gehört. Trotzdem kann die Datei beim Restore eindeutig gefunden werden. Dieses Konzept ist bisher unter Messengern einmalig.


\(^{21}\)https://shop.threema.ch/
KAPITEL 9. INSTANT MESSAGING UND TELEFONIE

Threema war in mehreren Jahren die populärste kostenpflichtige App im Apple App Store und hat mehrere Millionen Nutzer. Es ist einer der sichersten Messenger. Die Umsetzung der Designziele (Whitepaper) und aller Sicherheitsempfehlungen für Smartphone Apps gemäß Stand der Technik wurde durch zwei Audits bestätigt.

9.2.2 Messenger Signal App


*I’m not really into advertising for stuff here but the recent update of TextSecure made a gigantic impression on me. The application works well, is uber user friendly, and looks just great. (Collin R. Mulliner)*

*For the record – @moxie writes crypto software that blinds the #NSA & #GCHQ. He is their nightmare. Usable crypto developer with a backbone! (J. Appelbaum)*


Dass Signal App die Telefonnummer als Identifier verwendet, wird oft kritisiert (Datensparsamkeit usw.) Dabei wird unterschlagen, dass die Verifizierung des Gegenübers anhand der Telefonnummer ein Sicherheitsfeature ist. Man kann sich relativ sicher sein, dass man wirklich mit der gewünschten Person verbunden ist, mit der man die Telefonnummer ausgetauscht und im Adressbuch gespeichert hat, und nicht irgendein unbekannter Dritter sich durch Vorspielung einer falschen Identität Vertrauen erschleicht.

Außerdem erleichtert es das Finden von Kontakten und Etablieren einer sicheren Kommunikation mit Freunden und Bekannten, was das Hauptziel von Signal App ist.


Signal bietet verschlüsselte Audio- und Videotelefonie. Videokonferenzen (Group Calls) mit bis zu 8 Teilnehmern sind möglich. Für eine Konferenz erstellt man eine Gruppe mit den Teilnehmern und tippt auf das Group Call Symbol (Abb. 9.6)


\(^{22}\)https://github.com/WhisperSystems
9.2. INSTANT MESSAGING

Abbildung 9.6: Videokonferenz mit bis zu 5 Personen starten


Beim Zugriff auf das Adressbuch bemüht sich Signal um einen Kompromiss zwischen einfacher Benutzbarkeit und Privatsphäre. Wenn man nach neuen Kontakten sucht, werden die Hashwerte der Telefonnummern aus dem Adressbuch zu den Servern hochgeladen und dort niemals gespeichert. Ein Blogartikel erklärt das Verfahren.23


Das Backup-Konzept von Signal App ist dreistufig:


3. Ein vollständiges Backup inklusive aller Chatinhalte kann man unter Android nur lokal auf einer SD-Karte speichern und auf ein neues Smartphone übertragen.

23https://signal.org/blog/private-contact-discovery/
Für hohe Sicherheitsanforderungen bietet Signal App einige zusätzliche Optionen in der Sektion Datenschutz in den Einstellungen:

- Die Bildschirmsperre bei Inaktivität kann dagegen schützen, dass ein Angreifer bei kurzzeitigem Zugriff auf das entsperrte Smartphone eine Signal Desktop Instanz initialisiert, um die Kommunikation mitzulesen. (Das BKA hat einen vergleichbaren Angriff bei WhatsApp gegen einen Terrorverdächtigen bereits aktiv eingesetzt.)

- Die Anrufe (Audio und Video) können immer über einen Signal Proxy geleitet werden, um dem Kommunikationspartner nicht die eigene IP-Adresse zu verraten.

- Die Anzeige der Signal Anrufe in der Call History kann abgeschaltet werden, damit die Metadaten über Signal Anrufe nicht in der Cloud von Google landen.

Signal App für Android verwendet keine Google Services für Push Notifications bei neu eintreffenden Nachrichten. Aus Sicht der Privatsphäre ist das erfreulich, bringt aber bei einigen Nutzern das Problem, dass sie keine Notifications bei neuen Nachrichten erhalten sondern immer in der App nachschauen müssen, ob es etwas Neues gibt. Um dieses Problem zu vermeiden, müssen folgende Vorraussetzungen erfüllt sein:

- Die Signal App muss auch Hintergrund aktiv bleiben dürfen und sollte nicht durch Stromsparmaßnahmen abgeschaltet werden.

- Für die Signal App müssen im Hintergrund Internetaktivitäten erlaubt sein.

Ein Support Artikel erläutert die Einstellungen für verschiedene Android Phones.  

Signal App verwendet keine eigenen Server für die Infrastruktur sondern die Clouds von Microsoft, Google, Amazon und Cloudflare. Die Software nutzt Features wie Azure Confidential Computing oder SGI Secure Enclave, um die sensiblen Daten gegenüber dem Cloud Provider zu schützen.

Signal-Desktop installieren und verwenden

Um Signal als Messenger zu verwenden, benötigt man zwingend ein Smartphone, auf dem man die Signal App installiert und seinen Hauptaccount mit der Telefonummer registriert. Auf bis zu fünf Desktop PCs oder Laptops können zusätzliche Clients eingereicht werden, die mit allen Funktionen parallel zum Smartphone genutzt werden können.

Installation

- Für Windows gibt es auf der Download Seite ein EXE-Datei, die man nach dem Download startet, um die Anwendung Signal-Desktop zu installieren.

- Für Debian basierte Linux Systeme steht ein Repository zur Verfügung, welches man zur Installation und Aktualisierung verwenden kann. Als erstes ist der Signatursschlüssel des Repositories in den APT-Keyring einzufügen und das Repository als Paketquelle anzulegen. Dann kann man die Anwendung signal-desktop installieren:

  ```
  > sudo su
  # curl -s https://updates.signal.org/desktop/apt/keys.asc | apt-key add -
  # echo "deb [arch=amd64] https://updates.signal.org/desktop/apt xenial main" > /etc/apt/sources.list.d/signal-xenial.list
  # apt update
  # apt install signal-desktop
  # exit
  ```

24 https://support.signal.org/hc/de/articles/360007318711-Problembehebung-bei-Benachrichtigungen
25 https://signal.org/de/download/
9.2. INSTANT MESSAGING

- Für alle anderen Linux Systeme gibt es ein Snap-Paket, das neben Signal-Desktop auch alle notwendigen Bibliotheken enthält. Um dieses Paket zu nutzen, muss man zuerst Snap installieren (falls nicht vorhanden) und den Rechner neu starten.

  Für Fedora Nutzer erledigen das die folgenden Befehle:

  ```
  > sudo dnf install snapd
  > sudo ln -s /var/lib/snapd/snap /snap
  ```

  Nach dem Neustart kann man das Snap-Paket signal-desktop installieren:

  ```
  > sudo snap install signal-desktop
  ```

**Signal-Desktop verwenden**


Nach dem Scan des QRCode fragt das Smartphone nach der PIN für die Registrierungssperre, die man hoffentlich in den Datenschutzeinstellungen aktiviert hat.


Dann kann man Signal parallel auf dem Desktop und dem Smartphone nutzen. Das Hauptfenster (Abb. 9.7) ist spartanisch und bietet nicht alle Funktionen wie auf dem Smartphone. Man kann chatten, Dateien senden oder verschlüsselt telefonieren. Als erstes könnte man an als Test sich selbst eine kleine Nachricht schicken.

![Abbildung 9.7: Hauptfenster von Signal-Desktop](image-url)
Daten löschen, wenn der Account nicht mehr auf dem PC verwendet wird

Wenn man den Signal Account nicht mehr auf dem Desktop PC oder Laptop verwenden möchte, sollte man unbedingt alle auf der Festplatte gespeicherten Daten löschen. Signal-Desktop bietet in den Einstellungen mit einem dicken roten Button die Möglichkeit, diese Daten sicher zu entfernen.

9.2.3 Messenger Telegram


In den Einstellungen zur Privatsphäre kann man die Anzeige der eigenen Telefonnummer beim Gegenüber verbieten. Das schützt gegen Stalking auf anderen Kanälen und kann ein bisschen Anonymität gegenüber Kommunikationspartnern oder in Gruppenchats bieten. Da Telegram bei Terrorismusverdacht mit Behörden kooperiert, ist ein Pseudonym kein Sicherheitsfeature für politische Aktivisten, die mit staatlicher Verfolgung rechnen.

If Telegram receives a court order that confirms you’re a terror suspect, we may disclose your IP address and phone number to the relevant authorities.

Wenn der Angreifer eine Vermutung hat, zu welcher Gruppe von Personen ein Pseudonym gehört, könnte er bis zu 1.000 Telefonnummern im Adressbuch eingeben. Wenn die Telefonnummer im Adressbuch steht, wird sie auch in Chats unter dem Pseudonym angezeigt und über die Adressbuch-API kann der Angreifer den Namen herausfinden (s.o.)

Den Zugriff auf das Adressbuch zum Finden von neuen Kontakten kann unter Privatsphäre - Dateneinstellungen deaktiviert werden und das ist DRINGEND empfehlenswert.


Nach der Registrierung sollte man die **zweistufige Bestätigung** für das Hinzufügen neuer Geräte aktivieren. Es wurden bereits mehrfach staatliche Angriffe nachgewiesen, welche die Multi-Device Unterstützung ausnutzten, um unbemerkt Chats mitzulesen, die nicht Ende-zu-Ende verschlüsselt waren. Die zweistufige Registrierung aktiviert man in den Einstellungen unter **Privatsphäre und Sicherheit**. Es wird ein zusätzliches Passwort für die Registrierung von Desktop Clients für den Account festgelegt.
**KAPITEL 9. INSTANT MESSAGING UND TELEFONIE**

*Mehr… und anschließend auf Geheimen Chat starten.*


Für besonders brisante geheime Chats bietet Telegram *selbstlöschende Nachrichten*, die nach einer einstellbaren Zeit nach dem Lesen gelöscht werden.


![Abbildung 9.10: Verifizierung der Verschlüsselung für Audio- und Videotelefonie](image)

**Telegram Gruppen** können bis zu 200.000 Mitglieder enthalten. Teilnehmer mit Admin Status können mit einem Klick ein Telefonkonferenz mit den Gruppenteilnehmern starten und kontrollieren, wer sprechen darf. Teilnehmer können mit eine Handzeichen auf sich aufmerksam machen.

Es gibt keine Ende-zu-Ende Verschlüsselung für Telegram Gruppenchats. Trotzdem ist das Mitlesen für externe Dritte ohne Unterstützung des Betreibers nicht trivial, wie die Versuche des BKA bei der Infiltrierung rechtsextremer Gruppenchats zeigen.

Hinweis: Wenn man den Zugriff auf das Adressbuch für Telegram blockiert hat, muss man Bekannte zuerst zur Telegram Kontaktliste hinzufügen, bevor man sie in eine Gruppe einladen kann.

**Telegram Kanäle** sind eines der besonderen Social Media Features des Messengers. Man kann diese Kanäle nutzen, um einem breiten Publikum seine Meinung vorstellen oder um Millionen Follower bei Protesten zu informieren ohne eine Beschränkung auf 200 Zeichen.


- In Russland werden auf diesem Weg immer wieder Informationen über Korruption in unterschiedlichen Behörden publiziert.
- 2020 wurden diese Kanäle bei den Protesten in Hongkong gegen China und in Weißrussland gegen den Wahlbetrug genutzt, um Millionen Anhänger zu mobilisieren.
- In Deutschland bieten viele Online Medien einen Telegram Kanal, um Hinweise auf neue Artikel zu posten. Telegram bietet sich somit als News Aggregator an, der schnell und übersichtlich über Neigkeiten informiert, ähnlich wie RSS Feeds früher.
Hinweis: Die in den Kanälen geposteten Links zu den vollständigen Artikeln enthalten häufig Tracking-Parameter in den URLs. Man sollte den Browser zum Öffnen der Links also privacy-freundlich konfigurieren, um die Tracking-Parameter zu entfernen.

- Außerdem nutzen rechtsextreme Gruppen und viele Anhänger von Verschwörungstheorien dieses Medium, nachdem sie bei Facebook und Twitter wegen Verbreitung von Hass oder Fake News rausgeflogen sind.

Weil Telegram bei rechten Gruppen usw. populär ist, gilt der Messenger zunehmend als schmutzig. Dem gegenüber steht die Einschätzung von Europol\(^\text{26}\), dass Telegram sich erfolgreich bemüht, Terror- und Hasspropaganda und Aufrufe zu Straftaten zu entfernen:

> Telegram is no place for violence, criminal activity and abusers. The company has put forth considerable effort to root out the abusers of the platform by both bolstering its technical capacity in countering malicious content and establishing close partnerships with international organisations such as Europol.

Im Nov. 2020 wurden 17.975 Kanäle und Bots gelöscht, im Dez. 2020 waren es 17.279…


- Der Messenger unterliegt nicht dem NetzDG, das den Betreiber zur Lösung (politischer) unliesamer Inhalte verpflichten würde wie Facebook, Twitter oder TikTok. Telegram kooperiert freiwillig bei der Verherrlichung von Terrorismus und Gewalt.

- Auf iPhones ist die Freiheit aber ein bisschen weniger freizügig als anderswo. Weil Apple ein bisschen prüde ist, werden einige Kanäle auf iPhones nicht angezeigt:

  ![Diese Gruppe kann nicht angezeigt werden, weil sie zur Verbreitung pornographischer Inhalte verwendet wurde.](image)

- Wenn man (zufällig) illegale Inhalte findet, kann man sie mit wenigen Klicks dem Abuse Team melden. Man öffnet die Channel Einstellungen und klickt auf mehr… (Abb 9.11). Im zweiten Schritt kann man angeben, warum man den Kanal (oder Bot) meldet.

Telegram Nearby ist ein Social Feature, das man eher bei Dating Apps wie Tinder vermuten würde. Man kann unter Kontakte - Leute in der Nähe finden nach Personen und lokalen Gruppen suchen, die ihren Standort für diese Funktion freigegeben haben. (In den Gruppen bieten fliegende Händler oft Waren an, die sonst schwer zu bekommen sind.)

Wenn man selbst seinen Standort für die Leute in der Nähe freigibt, dann können Leute in der Umgebung auch den Standort ermitteln. Telegram zeigt nur die Entfernung an, aber mittels Triangulation (ein paar Meter nach rechts gehen und nach links) kann man den Standort interpolieren. Für Heise ist das ein Security Bug\(^\text{27}\) aber Telegram kommentierte:


\(^{27}\)https://heise.de/-5004687
People in the Nearby section intentionally share their location, this feature is disabled by default. It’s expected that determining the exact location is possible under certain conditions.

Telegram Bots sind ein weiteres, populäres Feature des Messengers. Ein Bot ist ein Chatpartner, der auf simple Kommando reagieren kann oder automatisiert Informationen liefert. Es ist keine grandiose, neue Erfindung, das gab es schon im letzten Jahrhundert bei IRC, aber aktuell sind Bots vor allem bei Telegram wieder populär geworden.

Ein einfaches, simples Beispiel ist der News Bot der ARD Tagesschau:

1. Einen Bot findet man über die Suche nach Kontakten in der Telegram App oder als Link auf Webseiten und man startet einen Chat, wie mit anderen Chatpartnern.

2. /start ist das erste Kommando, das jeder Bot kennt und bei Beginn des Chats ausführt. Es zeigt meist eine kurze Einführung und am unteren Rand ein paar Buttons für weitere Kommandos für die nächsten Schritte

3. /help ist ein weiteres Kommando, das jeder Bot kennen muss und dass man ihm immer schicken kann, wenn man nicht weiter weiß.
Abbildung 9.12: Personen und Gruppen in der Umgebung suchen

Dieser einfache Bot versteht also die Kommandos /news, /push und /feedback.

Der Bot der ARD Tagesschau ist ein sehr einfaches Beispiel. Es gibt wesentlich ausgefeiltere Bots, die komplette Shopsysteme emulieren inklusive Auswahl aus den Angeboten, Bewertung der Verkäufer, Bezahlung usw. In diesen Shops kann man auch Dinge finden, die nach dem Betäubungsmittelgesetz illegal sind, gefälschte Dokumente oder Waffen... man muss nur lange genug suchen und darf natürlich nicht auf Fakes hereinfallen. Es bildet sich ein neues Darknet ähnlich wie bei den illegalen Marktplätzen auf Tor Onion Services, welches allerdings auch zukünftig von der Policy der Telegram Betreiber abhängig ist.

Die Sicherheit illegaler Handelsplätze für Drogen oder Waffen ist bei Telegram wesentlich geringer als im Darknet (beisprw. Tor Onion Services), da ein zentraler Ansprechpartner als Betreiber existiert, der unter Umständen auch mit der Strafverfolgung kooperiert. Im Okt. 2020 wurden mehrere Chat Kanäle der Drogenszene mit mehr als 8.000 Nutzern vom BKA übernommen. Die Chatverläufe konnten analysiert werden, es gab mehrere Festnahmen und das BKA hat eine Informationsseite in den übernommenen Gruppen
Telegram Passport wurde 2018 als Ende-zu-Ende verschlüsselter Cloud Speicher eingeführt. Man kann Dokumente hochladen (Ausweiskopie, Führerschein… o.ä.) Diese Dokumente können von einem Webdienst angefragt werden und der Nutzer hat die Möglichkeit, die angeforderten Daten mit wenigen Klicks via Telegram zu verschicken. (In Deutschland ist das ein eher unüblicher Vorgang und wird hier wenig genutzt werden.)

Außerdem kann Telegram Passport als Identity Provider für den Login genutzt werden:

9.2.4 Messenger basierend auf [matrix]


Im Gegensatz zu anderen Messengern wirbt [matrix] nicht damit, dass Nutzer die volle Kontrolle über ihre Kommunikation behalten. Der Vorteil ist laut [matrix] Werbung:

There is no single point of control or failure in a Matrix conversation which spans multiple servers: the act of communication with someone elsewhere in Matrix shares ownership of the conversation equally with them.

juristisch in seiner Reichweite befindet. Sollten die Inhalte der Nachrichten Ende-zu-Ende verschlüsselt sein, können trotzdem detaillierte Metadaten der Kommunikation für die Kommunikationsanalyse abgerufen werden. (Wer, wie häufig, mit wem...?)


Die Ende-zu-Ende Verschlüsselung ist Teil des Sicherheitskonzeptes von [matrix] und standardmäßig aktiviert. Für eine hohe Sicherheitsansprüche gibt es folgende Optionen:

1. Verifizierung der Kommunikationspartner: Die Verifizierung der Partner soll sicherstellen, dass man wirklich mit dem gewünschten Gegenüber verbunden ist, und erfolgt durch Scannen von QR-Codes bei einem persönlichen Treffen oder mit Emoji, die man über einen getrennten Kommunikationskanal (out-of-band) prüfen muss.


Neben den Smartphone Clients, deren Krypto-Implementierung jemand im Rahmen eines Audits nach Vorliegen der finalen Version untersuchen könnte, gibt es eine Browserversion als Desktop Client oder für den Einsatz auf einem Webserver. Aufgrund konzeptioneller Schwächen kann man bereits ohne Prüfung der finalen Version sagen, dass eine Webversion nicht für hohe Sicherheitsansprüche geeignet ist:

- Das Webserver-basierte Chat Clients für die Sicherheitsansprüche politischer Aktivisten, Menschrechtsaktivisten o.ä. generell nicht geeignet sind, hat Patrick Ball 2012 in einem Essay bei Wired am Beispiel von Cryptocat dargelegt.\(^\text{28}\)


### 9.2.5 Chatten mit Jabber/XMPP


Bei der Ende-zu-Ende Verschlüsselung gibt es mehrere Alternativen:


Im Vergleich zu den im Punkt Sicherheit führenden Messengern hinkt Jabber/XMPP bei der Umsetzung moderner Sicherheitsfeatures hinterher. Die Ursachen dafür liegen in der förderlichen Serverstruktur und der Community-basierten Entwicklung. Gerade diese

\(^{28}\)http://www.wired.com/2012/08/wired_opinion_patrick_ball/all/

\(^{29}\)https://cheatsheetseries.owasp.org/cheatsheets/HTML5_Security_Cheat_Sheet.html
beiden Punkte sind für Open Source Dogmatiker die Pluspunkte von Jabber/XMPP und werden vehement verteidigt, ohne die Nachteile bezüglich Sicherheit zu erwähnen.

Einige Beispiele für kryptographische Schwächen bei Jabber/XMPP:


Threema und Signal App nutzen CA-Pinning, um diese Angriffe zu verhindern.


Bei Threema und Signal App werden diese Daten ausschließlich auf den Clients gespeichert. Die Server Betreiber haben keine Informationen über Kontaktlisten, Mitgliedschaften in Gruppenchats, Profilfotos o.ä. Das schränkt die Flexibilität bei der Verwendung unterschiedlicher Geräte ein zugunsten der Sicherheit.


Bei Jabber/XMPP sind bisher alle Versuche einer Ende-zu-Ende Verschlüsselung unvollständig und können nicht sicherstellen, dass die gesamte Kommunikation zwischen zwei oder mehreren Partnern sicher verschlüsselt wird.


Man sollte daraus nicht die Schlussfolgerung ziehen, dass XMPP unbrauchbar ist. Wer Spaß daran hat, kann es weiterhin verwenden, wenn der Sicherheitslevel ausreichend ist. Bei der Diskussion über Alternativen sollte man aber nicht dogmatisch auf Open Source und förderale Strukturen bestehen, ohne die Mängel in der Kryptografie einzugestehen.

9.2.6 Messenger Wire

Wire ist in erster Linie eine gute Collaboration Plattform für Unternehmen. Das in Berlin arbeitende Entwicklerteam gehört zur Wire Swiss GmbH, die die Server der Infrastruktur betreut und eine Tochterfirma der Wire Group Holdings GmbH in München (DE) ist.


Das Whitepaper postuliert, dass unter Android der Schutzwall gegen Zugriffe auf die gespeicherten Daten durch anderen Apps ausreichend ist, und empfiehlt auf PCs und Laptops die Verschlüsselung der Festplatte (was aber auf Mehrbenutzersystemen nicht gegen Zugriffe durch Dritte schützt).

Außerdem speichert Wire die Metadaten der Kommunikation dauerhaft unverschlüsselt in der europäischen Amazon Cloud. Im Privacy Statement findet man keinen Hinweis auf diese Mini-VDS und keine Hinweis, wie lange die Metadaten gespeichert werden. (Für Unternehmen mit Compliance Anforderungen und eigenen Servern ist das nicht relevant.)

Haben wir 20 Jahre gegen die Vorratsdatenspeicherung bei E-Mails gekämpft, um sie dann bei einem Messenger aus technischen Gründen ohne Widerstand zu akzeptieren?

Vor einigen Jahren war Wire der deutsche Shooting Star unter den Krypto-Messengern, aber die Versprechungen auf förderale Infrastruktur der Server wurden auf unbekannte Zeit verschoben und Vorteile gegenüber WhatsApp sind gering. Als Argument könnte

9.2. INSTANT MESSAGING

man anerkennen, das die Adressbücher nicht an Datensammler weitergegeben werden.

Wire Enterprise ist der bevorzugte Messenger der Bundesregierung und vom BSI für VS-NfD zugelassen. Wire ist eine gute Collaboration Plattform für Unternehmen.

9.2.7 Einige weitere Messenger (unvollständig)


Facebook Messenger ist keine Alternative zu WhatsApp. Man kann zwar eine Ende-zu-Ende Verschlüsselung aktivieren, aber trotzdem kann Facebook bei Bedarf die verschlüsselten Chats mitlesen. Dabei wird nicht die Krypto gebrochen sondern auf Anforderung eine unverschlüsselte Kopie der Nachricht an Facebook gesendet.

Die Verschlüsselung erfolgt mit OpenPGP und der Schlüsselaustausch per Autocrypt. Warum Autocrypt kein sicherer Schlüsseltausch ist, kann man im Kapitel E-Mail Verschlüsselung mit OpenPGP nachlesen. Diese Verschlüsselung bietet nur geringe Sicherheit, konzeptionell bedingt nur some Protection Most of the Time. Mit anderen Worten: sie wird genau dann nicht funktionieren, wenn man sie gebraucht hätte, also wenn sich ein ernsthafter Angreifer für die Inhalte der Chats interessiert.

Mit der Erweiterung countermitm versucht Delta-Chat, die Schwächen des Autocrypt Schlüsseltausches etwas abzumildern. Es wird damit die Möglichkeit zur Verifizierung von Schlüsseln eingeführt und Man-in-the-Middle Angriffe auf verifizierte Schlüssel werden verhindert.

Bei der E-Mail Kommunikation fallen viele Metadaten beim Provider an.

E-Mail ist das am häufigsten genutzte Medium für Textnachrichten. Als Realitätscheck ein Vergleich mit den genannten Messenger Diensten:

- Die Grundlage für die seit vielen Jahren hohe Nutzung von E-Mail bilden offene Protokolle, die eine förderbare Serverlandschaft von vielen Anbietern auf Basis von Open Source Software erlauben.
- E-Mails werden in der Regel unverschlüsselt gesendet. Die großen E-Mail Provider wie Google oder Microsoft lesen ungeniert mit. Auch wenn man selbst einen privacy-freundlichen E-Mail Provider nutzt, ist man nicht gegen das Mitlesen nicht geschützt, weil:

  Google has most of my emails, because it has all of yours.

- Der Austausch von Schlüsseln für OpenPGP oder S/MIME muss per Hand erfolgen, es gibt keinen vertrauenswürdigen Automatismus. Außerdem müssen die Schlüssel per Hand verifiziert werden.


9.3 Videokonferenzen mit Jitsi Meet


- Die Verwendung von WebRTC muss möglich sein und der OpenH264 Codec muss zur Verfügung stehen, was nicht bei allen Firefoxen Standard ist.
- Um Firefox etwas zu zähmen, könnte man die minimale user.js verwenden.
- Wenn man eine restriktive Firefox Konfiguration für spurenarmes Surfen verwendet, kann man unter about:profiles ein neues Profil erstellen, starten und dann passend konfigurieren (inklusive Lesezeichen für die bevorzugten Konferenz Server).

Wenn man dieses Profil beispiw. videokonferenz genannt hat, kann man es direkt mit folgendem Kommando starten oder als ein Starter-Icon auf dem Desktop anlegen:
9.3. VIDEOKONFERENZEN MIT JITSI MEET

> firefox -P videokonferenz --no-remote

Bevor man sich mit Elan in eine Videokonferenz stürzt, kann man auf der WebRTC Testseite\(^{31}\) prüfen, ob Kamera, Mikrofon und Verbindungsaufbau korrekt funktionieren. Das vermeidet nervende Diskussionen zu Beginn der Konferenz, weil etwas nicht funktioniert.

**Jitsi Meet Videokonferenz Server**

Es gibt viele öffentlich verfügbare Jitsi Meet Instanzen\(^{32}\). Hier eine kleine Auswahl an Empfehlungen für Server, die von vertrauenswürdigen IT-Professionals betrieben werden und hinsichtlich Sicherheitsfeatures wie DNSSEC, moderne TLS Ciphern, Server Konfiguration und Aktualität der Software auf dem Stand der Technik sind:

1. Single Server Instanzen ermöglichen Konferenzen mit bis zu 8-10 Teilnehmern:
   - Jitsi Meet Server der Nitrokey GmbH: [https://meet.nitrokey.com](https://meet.nitrokey.com)
   - Jitsi Meet Server von Golem.de: [https://meet.golem.de](https://meet.golem.de)
   - Jitsi Meet Server von M. Kuketz: [https://www.kuketz-meet.de](https://www.kuketz-meet.de)

2. Einige spenden-finanzierten Servercluster sind auch für größere Videokonferenzen mit 50-70 Teilnehmern geeignet:
   - Jitsi Cluster vom Freifunk München: [https://meet.ffmuc.net](https://meet.ffmuc.net)
   - Jitsi Meet Server der Horizon44 GmbH: [https://sichere-videokonferenz.de/](https://sichere-videokonferenz.de/)


Abbildung 9.14: Videokonferenz beim mailbox.org starten

\(^{31}\)[https://test.webrtc.org](https://test.webrtc.org)

Kapitel 10

Anonymisierungsdiensste

Anonymisierungsdiensste verwischen die Spuren im Internet bei der Nutzung herkömmlicher Webdienste. Die verschlüsselte Kommunikation verhindert auch ein Belauschen des Datenverkehrs durch mitlesende Dritte. Diese Dienste sind für den anonymen Zugriff auf Websites geeignet und ermöglichen auch unbeobachtete, private Kommunikation via E-Mail, Jabber, IRC...


10.1 Warum sollte man diese Dienste nutzen?

Anonymisierungsdienste verstecken die IP-Adresse des Nutzers und verschlüsseln die Kommunikation zwischen Nutzer und den Servern des Dienstes. Außerdem werden spezifischer Merkmale modifiziert, die den Nutzer identifizieren könnten (Browser-Typ, Betriebssystem...).


2. Standortbestimmung: Die Anbietern von Webdiensten können den Standort des Nutzers nicht via Geolocation bestimmen. Damit ist es nicht möglich:
   - die Firma identifizieren, wenn der Nutzer in einem Firmennetz sitzt.
   - bei mobiler Nutzung des Internet Bewegungsprofile zu erstellen.

3. Belauschen durch Dritte: Die verschlüsselte der Kommunikation mit den Servern des Anonymisierungsdienstes verhindert ein Mitlesen des Datenverkehrs durch Dritte in unsicheren Netzen. (Cafes, WLANs am Flughafen oder im Hotel, TKÜV…)

10.1. WARUM SOLLTE MAN DIESE DIENSTE NUTZEN?

IP-Adressen zur tagtäglichen Rasterfahndung nutzt. Facebook gibt täglich 20-30 IP-Adressen an US-Behörden, AOL übergibt 1000 Adressen pro Monat…

5. **Zensur:** Der Datenverkehr kann vom Provider oder einer restriktiven Firewall nicht manipuliert oder blockiert werden. Anonymisierungsdienste ermöglichen einen unzensierten Zugang zum Internet. Sie können sowohl die “Great Firewall” von China und Mauretanien durchtunneln sowie die in westeuropäischen Ländern verbreitete Zensur durch Kompromittierung des DNS-Systems.

6. **Repressionen:** Blogger können Anonymisierungsdienste nutzen, um kritische Informationen aus ihrem Land zu verbreiten ohne die Gefahr persönlicher Repressionen zu riskieren. Für Blogger aus Südafrika, Syrien oder Burma ist es teilweise lebenswichtig, anonym zu bleiben. Iran wertet Twitter-Accounts aus, um Dissidenden zu beobachten.

7. **Leimruten:** Einige Websites werden immer wieder als Honeypot genutzt. Ein Beispiel sind die Leimrute des BKA. In mehr als 150 Fällen wurden die Fahndungseiten von LKAs oder des BKA als Honeypot genutzt und die Besucher der Webseiten in Ermittlungen einbezogen. Surfer wurden identifiziert und machten sich verdächtig, wenn sie sich auffällig für bestimmte Themen interessierten.


9. **Belauschen durch den Dienst:** Im Gegensatz zu einfachen VPNs oder Web-Proxys schützen die hier vorgestellten Anonymisierungsdienste auch gegen Beobachtung durch die Betreiber des Dienstes selbst. Die mehrfache Verschlüsselung des Datenverkehrs und die Nutzung einer Kette von Servern verhindert, dass einzelne Betreiber des Dienstes die genutzten Webdienste einem Nutzer zuordnen können.

---

1[http://heise.de/-1704448](http://heise.de/-1704448)
10.2 Tor Onion Router


Tor nutzt ein weltweit verteiltes Netz von 6.000-7.000 aktiven Nodes. Aus diesem Pool werden jeweils 3 Nodes für eine Route ausgewählt. Die Route wechselt regelmäßig in kurzen Zeitabständen. Die zwiebelartige Verschlüsselung sichert die Anonymität der Kommunikation. Selbst wenn zwei Nodes einer Route kompromittiert wurden, ist eine Beobachtung durch mitlesende Dritte nicht möglich. Da die Route durch das Tor Netzwerk ständig wechselt, müsste ein großer Teil des Netzes kompromittiert worden sein, um einen Nutzer zuverlässig deanonymisieren zu können.

Abbildung 10.1: Das Prinzip von Tor Onion Router

Tor ist neben Surfen auch für IRC, Instant-Messaging, den Abruf von Mailboxen oder Anderes nutzbar. Dabei versteckt Tor nur die IP-Adresse! Für die sichere Übertragung der Daten ist SSL- oder TLS-Verschlüsselung zu nutzen. Sonst besteht die Möglichkeit, dass Bad Exit Nodes die Daten belauschen und an Userkennungen und Passwörter gelangen.

Der Inhalt der Kommunikation wird 1:1 übergeben. Für anonymes Surfen bedarf es weiterer Maßnahmen, um die Identifizierung anhand von Cookies, der HTTP-Header, ETags aus dem Cache oder JavaScript zu verhindern. Das TorBrowserBundle ist für anonymes Surfen mit zu nutzen.

Verschiedene Sicherheitsforscher demonstrierten, dass es mit schnüffelnden Bad Exit Nodes relativ einfach möglich ist, Daten der Nutzer zu sammeln.

- Dan Egerstad demonstrierte, wie man in kurzer Zeit die Account Daten von mehr als 1000 E-Mail Postfächern erschnüffeln kann, u.a. von 200 Botschaften.2

- Auf der Black Hack 2009 wurde ein Angriff auf die HTTPS-Verschlüsselung beschrieben. In Webseiten wurden HTTPS-Links durch HTTP-Links ersetzt. Innerhalb von 24h konnten mit einem Tor Exit Node folgende Accounts erschnüffelt werden: 114x Yahoo, 50x GMail, 9x Paypal, 9x Linkedin, 3x Facebook.3

2012 haben mehrere russische Extis-Nodes diesen Angriff praktisch umgesetzt.

- Die Forscher um C. Castelluccia nutzten für ihren Aufsatz Private Information Disclosure from Web Searches (The case of Google Web History) einen schnüffelnden Tor Exit Node, um private Informationen von Google Nutzern zu gewinnen.4

---

2http://heise.de/-95770
4http://planete.inrialpes.fr/projects/private-information-disclosure-from-web-searches/
• Um reale Zahlen für das Paper *Exploiting P2P Applications to Trace and Profile Tor Users* zu generieren, wurden 6 modifizierte Tor Nodes genutzt und innerhalb von 23 Tagen mehr als 10.000 User deanonymisiert.\(^5\)

Man kann davon auszugehen, dass die Geheimdienste verschiedener Länder ebenfalls im Tor-Netz aktiv sind und sollte die Hinweise zur Sicherheit beachten: sensible Daten nur über SSL-verschlüsselte Verbindungen übertragen, Warnungen nicht wegllicken, Cookies und JavaScript deaktivieren... Dann ist Tor für anonyme Kommunikation geeignet.

Tor bietet nicht nur anonymen Zugriff auf verschiedene Services im Web. Die *Tor Onion Services* bieten Möglichkeiten, anonym und zensurresistent zu publizieren.

**Finanzierung von TorProject.org**


Für die verbleibenden 61% der insgesamt 4,6 Mio. Dollar wurden 2020 folgende Geldgeber genannt:

- 15,4% von einer Behörde des schwedischen Außenministeriums
- 13,4% von der Mozilla Foundation
- 6,2% von der US-amerikanischen Stiftung Media Democracy Fund
- 4,1% von der Organisation Handshake Open Source Pledge
- 11,9% Einzelspenden

**Tor ist eine Triple-Use-Technik**

Anonymisierungsdienste und Kryptografie allgemein sind Triple-Use-Techniken. Am Beispiel von Tor Onion Router kann man es deutlich erkennen:

1. Ganz normal Menschen nutzen Tor, um ihre Privatsphäre vor Datensammlern und staatlicher Überwachung / Repressalien zu schützen. Dieses Szenario steht oft im Mittelpunkt der Diskussion mit Aktivisten, ist aber vielleicht die kleinste Gruppe.


Unmittelbar nach den Wahlen begannen massive Proteste, auf welche die Regierung mit Gewalt und Blockaden von Internetdiensten reagierte. Tor war mit den Bridges in der Lage, die Blockaden zu umgehen. Aber die Statistik zeigt, dass es in Weißrussland keine nennenswerte Zunahme der Nutzung von Tor während der Proteste gab. Vor, während und nach dem Höhepunkt der Proteste gab es weniger als 6.000 Tor-Clients in Weißrussland.

Signal App und Telegram konten die Internetsperren gleichfalls umgehen und oppositionelle Telegram Kanäle wie *Nexta* hatten zeitweise mehr als 2 Mio. Follower.

\(^5\) [http://hal.inria.fr/inria-00574178/en/](http://hal.inria.fr/inria-00574178/en/)


![Mevada.A Botnetz von metrics.torproject.org](https://metrics.torproject.org)

**Abbildung 10.2: Mevada.A Botnetz von metrics.torproject.org**

Außerdem nutzen Drogenhändler u.a. die Technik der Tor Onion Sites (Tor Hidden Services), um ihre Waren anzubieten. Im Rahmen der Operation Onymous konnte das FBI mehr als 400 Drogenmarktplätze abgeschalten werden. Das FBI hatte dabei technische Unterstützung von der Carnegie Mellon University bei der Deanonymisierung von Tor Onion Sites.

Die Nutzung von Anonymisierungsdiensten durch Kriminelle betrifft nicht nur Tor. Im Jahresbericht 2015 befürchten die Analysten von Europol, dass Kriminelle zukünftig das Invisible Internet Project (I2P) oder OpenBazaar statt Tor Onion Sites nutzen könnten, was die Verfolgung erschweren würde.

3. Geheimdienste nutzen Tor in erheblichen Umfang, um Kommunikation geheim zu halten. Außerdem ist Tor eine Waffe im Arsenal der CIA und des US-Cybercommand. Im Frühjahr 2014 auf dem Höhepunkt der Ukraine-Krise wurde beispielsweise ein Botnetz in Russland hochgefahren, dass der russischen Gegenseite ernsthafte Probleme bereitet hat. In Bild 10.3 sieht man den Anstieg der Tor Nutzer in Russland (aber nicht international), der typisch für ein aktiviertes Botnetz ist.

Die russische Regierung hat offiziell 4 Mio. Rubel für einen Exploit geboten um die beteiligten Tor Nodes zu deanonymisieren. Der russische Militärdienstleister Kalashnikow hatte den Auftrag übernommen, konnte aber keine Ergebnisse liefern.

Die vom Journalisten Y. Levine veröffentlichte FOIA Dokumente belegen, das insbesondere die CIA Tor Onion Router aktiv als Werkzeug bei Kampagnen zur Destabilisierung unbequemer Länder nutzt:

*The documents showed Tor employees taking orders from their handlers in the federal government, including hatching plans to deploy their anonymity tool in countries that the U.S. was working to destabilize: China, Iran, Vietnam, Russia.*

Die Nutzung von Tor Onion Router ist ein **Spiegel der gesellschaftlichen Probleme**:

1. Das in der UN-Menschenrechtscharta und der Europäische Menschenrechtskonvention deklarierte Recht auf unbeobachtet, private Kommunikation ist durch die staatlich organisierte Massenüberwachung und kommerzielle Datensammlungen praktisch abgeschafft. Bundesinnenminister Friedrich empfiehlt Selbstschutz, weil die technischen Möglichkeiten zur Ausspähung nun einmal existieren (die Bankrott-erklärung der Politik), und Tor ist ein Technik zum Selbstschutz.
10.2. TOR ONION ROUTER

2. Kriminalität wie Wirtschaftskriminalität, Eigentumsdelikte, Drogenkriminalität... oder ganz allg. *Handlungen im Widerspruch zu geltenden Gesetzen* sind gesellschaftliche Phänomene, für die man nicht den technischen Hilfsmitteln die Schuld geben kann.


Durch diese unterschiedlichen Interessen entstehen skurrile Situationen, wenn das FBI der Carnegie Mellon University 1 Mio. Dollar zur Verfügung stellt, um Tor Onion Services für die Operation Onymous zu deanonymisieren⁷, die Universität die wiss. Ergebnisse auf der BlackHat Konferenz aber nicht publizieren darf⁸, um die US-Cyberoperationen in Russland nicht zu gefährden, und die Entwickler bei TorProject.org auf Vermutungen angewiesen sind⁹, um die Bugs zu fixen, damit sie politischen Aktivisten wie Wikileaks eine vertrauenswürdige Infrastruktur bereit stellen können.

10.2.1 Security Notes

Die Sicherheit von IP-Anonymisierern wie Tor Onion Router ergibt sich nicht allein aus der Qualität der Software und der Kryptografie. Durch Fehler bei der Nutzung oder durch falsche Konfiguration kann die Anonymität komplett ausgehebelt werden.

- Wer in seinem Standardbrowser nur die Proxy-Einstellungen anpasst um Tor zu verwenden, ist auch nicht sicher anonym. Eine Deanonymisierung ist mit WebRTC oder Java-Applets möglich. Cookies und andere Trackingfeatures können langfristig ebenfalls zu einer Deanonymisierung des Surfverhaltens führen.


---

⁷https://blog.torproject.org/blog/did-fbi-pay-university-attack-tor-users
⁹https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack/
Einige nicht-anonyme Peer-2-Peer Protokolle wie BitTorrent übertragen die IP-Adresse des eigenen Rechners zusätzlich in Headern des Protokoll-Stacks ähnlich wie bei ICE. Damit ist es ebenfalls möglich, User zu deanonymisieren. Eine wiss. Arbeit zeigte, wie 10.000 BitTorrent Nutzer via Tor deanomisiert werden konnten.

Der Assistent zur Einrichtung eines E-Mail Account in Thunderbird umgeht die Proxyeinstellungen beim Abrufen der Autoconfig Datei mit den Servereinstellungen und sendet dabei die eigene E-Mail Adresse an den Provider. Der E-Mail Provider erhält damit die echte IP-Adresse zusammen mit der E-Mail Adresse und man ist deanonymisiert, bevor man die erste E-Mail geschrieben oder empfangen hat.


Schlussfolgerungen:

- TorProject empfiehlt für anonymes Surfen ausdrücklich das TorBrowserBundle. Das ist eine angepasste Version des Browser Mozilla Firefox zusammen mit dem Tor Daemon. Nur diese Konfiguration kann als wirklich sicher nach dem aktuellen Stand der Technik gelten. Die vielen Sicherheitseinstellungen dieser Softwarekombination kann man nur unvollständig selbst umsetzen.

- Für alle weiteren Anwendungen sind die Anleitungen der Projekte zu lesen und zu respektieren. Nur die von den Entwicklern als sicher deklarierten Anwendungen sollten mit Tor genutzt werden.

- Verwenden Sie ausschließlich die Originalsoftware der Entwickler.

10.2.2 Anonym Surfen mit dem TorBrowserBundle

Das TorBrowserBundle enthält einen modifizierten Firefox als Browser sowie den Tor Daemon und ein Control Panel. Die Webseite stellt das TorBrowserBundle für verschiedene Betriebssysteme und in unterschiedlichen Sprachen zur Verfügung.

HINWEIS: man sollte die englische Version des TorBrowsers (en-US) herunter zu laden. In den letzten Jahren gab es immer wieder aufgrund von Bugs im TBB die Möglichkeit, Hinweise auf die Lokalisierung des Browser zu finden, z. B via Javascript `date.toLocale()` Funktion (Bug #5926) oder via Informationen aus dem HTTP Accept-Language Header (Bug #628) oder via `resource://` URI (Bug #8725). Wenn man die deutsch lokalisierte Version des TorBrowsers nutzt, gibt man möglicherweise einen Hinweis auf die bevorzugte Sprache, und das möchte man natürlich vermeiden.


Installation

Das Archiv ist nach dem Download zu entpacken, keine Installation nötig.
10.2. TOR ONION ROUTER


• Unter Linux entpackt man das Archiv mit dem bevorzugten Archiv-Manager oder erledigt es auf der Kommandozeile mit:

  ```
  > tar -xaf tor-browser- *
  ```

Danach kann man das TorBrowserBundle starten, indem man das Startscript auf der Kommandozeile aufruft oder mit einem Klick im Dateimanager startet:

  ```
  > tor-browser_en-US/start-tor-browser.desktop
  ```

Mit einem kleinen Kommando kann man den TorBrowser im Startmenü des Desktops in der Programmgruppe `Internet` hinzufügen, um den Start zu vereinfachen:

  ```
  > tor-browser_en-US/start-tor-browser.desktop --register-app
  ```

• Für Debian und Ubuntu Derivate gibt es außerdem den *TorBrowser Launcher*, der sich um Download, Verifikation und Installation des TorBrowserBundles kümmert. Das Paket kann man mit dem bevorzugten Paketmanager installieren:

  ```
  > sudo apt install torbrowser-launcher
  ```

In der Regel wird auch gleich ein Tor Daemon installiert. Diesen Tor Daemon braucht man evtl. nur für den ersten, initialen Download des TorBrowserBundle. Es ist aber kein Sicherheitsgewinn, wenn man das TorBrowserBundle via Tor herunter lädt und man kann diesen Tor Daemon gleich wieder entfernen, da das TorBrowserBundle eine aktuellere Version von Tor enthält.

  ```
  > sudo apt purge tor
  ```

In der Programmgruppe `Internet` findet man zwei neue Menüpunkte. Wenn man den Menüpunkt *TorBrowser Launcher Settings* wählt, öffnet sich das in Bild 10.4 gezeigte Fenster. Den *Download over System Tor* kann man deaktivieren, man sollte die englische Version des TorBrowsers herunterladen und außerdem kann man einen Mirror wählen, falls die Webseite von TorProject.org nicht erreichbar ist. Ein Klick auf den *Install Button* lädt das TorBrowserBundle herunter, verifiziert die OpenPGP Signatur und installiert den TorBrowser. Zum Starten verwendet man zukünftig den Menüpunkt *TorBrowser* in der Programmgruppe `Internet`.

![Abbildung 10.4: Start des TorBrowser](image-url)
Wenn die Downloadseite für das TorBrowserBundle gesperrt ist, dann findet man unter GetTor alternative Downloadmöglichkeiten. Man kann z.B. per Jabber/XMPP oder E-Mail eine Nachricht mit dem gewünschten Betriebssystem (windows, linux, osx) an den Account gettor@torproject.org schicken und bekommt eine Liste alternativer Downloadlinks.

Abbildung 10.5: Alternative Downloadlinks via Jabber/XMPP abrufen

Beim ersten Start öffnet sich zuerst das Control Panel. Hier kann man bei Problemen Einstellungen zur Umgehung von Firewalls konfigurieren (z.B. wenn eine Firewall nur Verbindungen zu bestimmten Ports passieren lässt) oder man kann den Tor Daemon mit Klick auf den Button Verbinde ohne weitere Konfiguration starten.

Größe des Browserfensters

Der TorBrowser startet mit einer festgelegten Größe des Browserfensters. Die Fensterbreite sollte ein Vielfaches von 200px sein (max. 1000px) und die Höhe ein Vielfaches von 100px. Die Fenstergröße wird gleichzeitig als Bildschirmgröße via JavaScript bereitgestellt. Da die innere Größe des Browserfensters und die Bildschirmgröße als Tracking-Feature genutzt werden, sollte man die voreingestellte Größe des Browserfensters nicht(!) ändern.

Sicherheitseinstellungen


1. 2016 wurde auf der Tor Mailingliste ein Javascript Bug gepostet, den das FBI aktiv mit Exploits ausnutzte, um einen Trojaner zu installieren, der Tor Nutzer deanony-

10 https://gettor.torproject.org/
11 https://blog.torproject.org/blog/day-action-stop-changes-rule-41
misiert. Der Einsatz wurde auf der vom FBI beschlagnahmten Onion Site Giftbox nachgewiesen.\textsuperscript{13}

2. 2015 verwendete das FBI einen Zero-Day-Exploit im TorBrowser, um einen Trojaner zu installieren und die Tor-Nutzer damit zu deanonymisieren. Welcher Lücke im Firefox dabei ausgenutzt wurde, ist nicht bekannt. Mozilla und TorProject.org haben sich bemüht, aber die Informationen zur ausgenutzten Lücke wurden unter Hinweis auf die Nationale Sicherheit als geheim eingestuft.\textsuperscript{14}

3. Im Sommer 2013 wurden tausende Tor-Nutzer mit dem FBI-Trojaner \textit{Magneto} infiziert. Der Exploit zur Installation des Trojaners nutzte einen JavaScript Bug im TorBrowser aus. Der installierte Trojaner sendete die IP-Adresse, die MAC-Adresse und den Namen des Rechners an einen FBI Server, um Tor-Nutzer zu deanonymisieren.\textsuperscript{15}

4. Aus den Snowden-Dokumenten geht hervor, dass die NSA das TorBrowserBundle auf Basis von Firefox 10 esr über einen Bug in E4X, einer XML Extension für JavaScript, automatisiert angreifen und Nutzer deanonymisieren konnten.\textsuperscript{16}

Die Tor-Entwickler haben den Tradeoff zwischen einfacher Benutzbarkeit und Sicherheit in den Default-Einstellungen zugunsten der einfachen Benutzbarkeit entschieden. Es wird aber anerkannt, dass diese Einstellungen ein Sicherheitsrisiko sind. In den FAQ steht:

\begin{quote}
There's a tradeoff here. On the one hand, we should leave JavaScript enabled by default so websites work the way users expect. On the other hand, we should disable JavaScript by default to better protect against browser vulnerabilities (not just a theoretical concern!).
\end{quote}

Beim Start wird man darauf hingewiesen, dass man die Sicherheitseinstellungen anpassen kann. TorBrowser startet standardmäßig mit dem niedrigsten Sicherheitslevel \textit{Standard}, um das Surferlebnis möglichst wenig einzuschränken. Bei Bedarf kann man den

\begin{footnotesize}
\begin{enumerate}
\item[14] https://motherboard.vice.com/read/the-fbi-is-classifying-its-tor-browser-exploit
\item[16] http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity
\end{enumerate}
\end{footnotesize}
Abbildung 10.7: Sicherheitslevel im TorBrowser anpassen

Sicherheitslevel erhöhen.

Für sicherheitsbewusste Nutzer ist der umgekehrte Weg empfehlenswert. Man kann standardmäßig im höchsten Sicherheitslevel Safest surfen und wenn es ein Login bei einer Webseite erfordert, auf den mittleren Level Safer wechseln. Fast alle Websites, die einen Login erfordern (E-Mail Provider u.ä.), kann man mit dem Level Safer problemlos nutzen.


HTTPS Security

sslstripe Angriffe durch Bad Tor Exit Nodes, die 2009 auf der Black Hack Konferenz demonstriert wurden, sind auch 2020 noch ein aktuelles Problem.

Als Schutz gegen diese Angriffe enthält der TorBrowser das Add-on HTTPSEverywhere, welches anhand von Regeln die Umschreibung von HTTP Adressen auf HTTPS für viele populäre Webseiten erzwingt (aber nicht für alle Webseiten, die HTTPS unterstützen).

Konzeptuell bietet die Verwendung von Regeln, die von Servern herunter geladen werden, einige Angriffsmöglichkeiten, die den Entwicklern von HTTPSEverywhere

Abbildung 10.8: HTTPSEverywhere: Sicherheitswarnung vor Regelsätzen von Unbekannten

Aber sind die Regelsätze der Default Downloadserver der EFF.org vertrauenswürdig? Selbst wenn man der Qualität bei den Maintainern der Regelsätze vertraut, kann man nie zu 100% ausschließen, dass ein Hacker an diesem Punkt ansetzt und etwas manipuliert...

Alternative: Seit Firefox 78.5 ESR funktioniert der HTTPS-only-Mode zufriedenstellend gut. Damit wird bei Eingabe URL eine Umschreibung auf HTTPS für alle Webseiten erzwungen, die TLS Verschlüsselung unterstützen. Außerdem wird mmixed content auf Webseiten, die via HTTPS geladen wurden, komplett blockiert. Wenn kein Upgrade auf eine HTTPS Verbindung möglich ist, wird eine Warnung angezeigt und man könnte die unverschlüsselte HTTP Seite trotzdem aufrufen, wenn man es wirklich will und das Risiko akzeptiert.

Man könnte daher das Add-on HTTPSEverywhere in der Add-on Verwaltung deaktivieren (also: deaktivieren(!) und nicht entfernen, sonst ist es nach dem nächsten Update vom TorBrowser wieder aktiv) und unter about:config folgende Optionen aktivieren:

dom.security.https_only_mode = true
security.mixed_content.upgrade_display_content = true

Ein Trackingdienst kann nicht erkennen, ob der Nutzer https://www.privacy-handbuch.de eingegeben hat oder ob die verkürzte Eingabe von privacy-handbuch.de durch den HTTPS-only-Mode umgeschrieben wurde. Aber es ergibt sich ein kleiner Unterschied zum Verhalten des originalen TorBrowsers, da die Entwickler bei TorProject.org entschieden haben, für passive mixed content (Bilder, CSS, Fonts...) auf HTTPS Webseiten kein Upgrade auf HTTPS zu versuchen und es nicht blockieren. Daraus ergibt sich aber kein individuelles Trackingmerkmal, da auch andere Nutzer diese Einstellungen nutzen.

AdBlocker und Trackingprotection

Der TorBrowser enthält keinen AdBlocker und alle Trackingprotection Features von Firefox sind vollständig deaktiviert. Es ist das Konzept vom TorBrowser, Werbung und Trackingscripts nicht zu blockieren sondern durch Anonymität die Privatsphäre zu gewährleisten.

• Das Anonymitätskonzept des TorBrowser verhindert, dass Nutzer individuell erkannt und beim Surfen verfolgt werden können.

• Viele Webseiten finanzieren sich durch Werbung. TorProject.org möchte in diesem Punkt keine Konfrontation, um die Akzeptanz des Browsers nicht zu belasten.
Es ist empfehlenswert, dem Konzept von TorProject.org zu folgen. Ein AdBlocker ist leicht erkennbar und unterschiedliche Filterlisten können als Merkmal für das Fingerprinting dienen. Es ist nahezu unmöglich, eine Anonymitätsgruppe mit identischen Filterlisten aufzubauen.

**Cookies und EverCookies**

Um Trackingcookies und EverCookies muss man sich beim TorBrowser keine Gedanken machen. Das von den Entwicklern umgesetzte Sicherheitskonzept *Cross-Origin Identifier Unlinkability* schützt zuverlässig gegen Tracking und Deanonymisierung mit Cookies oder EverCookies ohne das Surferlebnis nennenswert zu beeinträchtigen.

- Für jede aufgerufene Domain wird automatisch ein Surf-Container erstellt. Dieser Container enthält in einer abgeschotteten Umgebung alle Daten, die von einer Website lokal im Browser gespeichert werden (Cookies, HTML5-Storage, IndexedDB, Cache, TLS Sessions...). Diese Daten bilden dann den sogenannten Context.


- Beim Neustart oder wenn man den Menüpunkt *Neue Identität* der Zwiebel in der Toolbar wählt, werden alle Container gelöscht. Für eine Neue Identität wird außerdem eine neue Route durch das Tor Netzwerk mit einem anderen Tor Exit Node genutzt.

Abbildung 10.9: Neue Identität im TorBrowser wählen

Man sollte dem Anonymitätskonzept des TorBrowser folgen und gelegentlich alle Cookies und andere lokalen Daten löschen, indem man auf die Zwiebel neben der URL-Leiste klickt und Neue Identität wählt. Insbesondere nach einem Login auf einer Webseite ist es empfehlenswert, die Spuren zu beseitigen.

**PDFs und andere Dokumente**

Auf der Downloadseite des TorBrowserBundles findet man unten einige Sicherheitshinweise\(^\text{17}\), unter anderem zu PDFs und anderen Dokumenten:

*Don’t open documents downloaded through Tor while online*

*You should be very careful when downloading documents via Tor (especially DOC and PDF files) as these documents can contain Internet resources that will be downloaded outside of Tor by the application that opens them. This will reveal your non-Tor IP!*

*If you must work with DOC and/or PDF files, we strongly recommend either using a disconnected computer, downloading the free VirtualBox and using it with a virtual machine image with networking disabled, or using Tails.*

\(^{17}\text{https://www.torproject.org/download/download}\)

Um nicht immer daran denken zu müssen, mit der rechten Maustaste auf einen PDF-Link zu klicken und Speichern unter... zu wählen, kann man die Einstellung im TorBrowser für PDF-Dokumente zu ändern und auf Speichern setzen.

Die via Tor herunter geladenen Dokumente kann man in einem besonderen Ordner speichern. Dann behält man den Überblick und weiß, dass man diese Dokumente nur öffnen darf, wenn man den Netzwerkstecker gezogen hat oder die WLAN-Verbindung ausgeschaltet wurde.

Hinweis: Man kann eine PDF Datei von Wanzen säubern, indem man die heruntergeladenen Dateien auf einem Rechner ohne Internetverbindung in einem PDF-Viewer öffnet und in eine neue PDF-Datei ausdruckt. Dabei werden sichtbare Fotos neu gerendert und unsichtbar eingebettete Wanzen entfernt.

10.2.3 TorBrowser für Android Smartphones

Tor Browser für Android wird von TorProject.org entwickelt und ist wie die Desktop Version eine Kombination von sicher konfiguriertem Browser und Tor Onion Router.

OrBot ist der offizielle Tor Client für Android. Er kann den Datenverkehr für alle oder einzelne Apps über das Tor Netzwerk leiten und damit die IP-Adresse verstecken.

Für anonymes Surfen sollte man nur die von Torproject.org empfohlene App verwenden, die Browser und Tor Onion Router kombiniert. Nur mit einem modifizierten und sicher konfiguriertem Browser kann die Anonymität gewährleistet werden.

Viele Apps senden umfangreiche Daten an Werbenetzerweke und an die Anbieter der Dienste. Die Daten enthalten in der Regel eine eindeutige Tracking-ID, außerdem werden auch Standortdaten und weitere Informationen versendet. Das betrifft die Apps von Facebook und Twitter, verschiedene Dating-Apps, einfache Wetter-Apps und auch die App zur Mediathek des ZDF. (M. Kuketz hat in seinem Blog weitere Beispiele analysiert.)


Es gibt nur sehr wenige Apps, die in Kombination mit OrBot für anonyme Kommunikation geeignet sein könnten. Dazu zählen:

- K9Mail mit OpenKeyChain könnten mit Anonymisierungsdiensten für anonyme E-Mail Kommunikation genutzt werden.

- Mit Conversations oder Chatsecure könnte man evtl. anonym jabbern.

10.2.4 OnionBrowser für iPhones

Der Onion Browser von Mike Tigas ist die von TorProject.org empfohlene App für anonymes Surfen auf dem iPhone. Es ist ebenfalls eine Kombination von Browser und Tor.

18https://www.kuketz-blog.de/
KAPITEL 10. ANONYMISIERUNGSDIENSTE

Beim ersten Start nach der Installation fragt der Onion Browser, ob er sich direkt mit dem Tor Netzwerk verbinden soll oder ob Bridges genutzt werden sollen, weil der Zugang zum Tor Netzwerk zensiert wird. Bridges sind ein extra Theme und in Europa nicht nötig. Danach wird abgefragt, welcher Sicherheitslevel standardmäßig genutzt werden soll.

- Den unsicheren Level sollte man nicht nutzen, weil er wirklich unsicher ist. Damit ist der Onion Browser ungeeignet, um Youtube oder Youporn Videos zu konsumieren.
- Im Level moderat ist Javascript allgm. erlaubt, aber es sind einige Techniken wie XHR, Websockets, WebRTC und Videos verboten. Außerdem werden auf Webseiten mit HTTPS Verschlüsselung keine unverschlüsselten Inhalte geladen.
- Wenn man den höchsten Level sicher wählt, dann macht das Surfen einfach keinen Spaß, weil Javascript, Videos usw. komplett verboten werden.

Mit einem Klick auf das Icon oben links im OnionBrowser kann für die aktuell dargestellte Webseite individuelle Einstellungen für den Sicherheitslevel definieren.

![Abbildung 10.10: OnionBrowser: Sicherheitslevel für eine Webseite anpassen](image)


10.2.5 Sicherheitskonzept für hohe Ansprüche

Tor Onion Router schützt den Datenverkehr auch gegen Angriffe potenter Geheimdienste wie die NSA. Es ist nach dem aktuellen Stand der Technik nahezu unmöglich, die Verschlüsselung mathematisch zubrechen und Nutzer zu deanonymisieren.

Angriffe zur Deanonymisierung von Tor Nutzern konzentrieren sich daher üblicherweise auf die Client Anwendung (z.B. den Webbrowser). In mehreren bekannten Fällen wurde durch Ausnutzung von Security Bugs im TorBrowser ein kleiner Trojaner auf dem Rechner von Zielpersonen installiert, der IP- und MAC-Adressen des Rechners ermittelt und an einen Server des Angreifers sendet.

Das FBI verwendet seit mehrere Jahre den Magneto Trojaner, der auf Webseiten platziert wird und nach Infektion des Systems via TorBrowser die Daten an einen Server der Science Applications International Cooperation sendet, die u.a. mit dem FBI kooperiert.
10.2. TOR ONION ROUTER

- Der Server des Projektes *Freedom Hosting* wurde vom FBI in Frankreich lokalisiert und ein direkter Zugriff in Kooperation mit dem Datacenter vor Ort eingerichtet.

  Der Magneto Trojaner wurde in mehrere Onion Sites eingebaut und die Besucher deanonymisiert. Neben Webangeboten mit kinderpornografischem Material waren auch der E-Mail Service TorMail und die Bitcoin Börse OnionBank betroffen (2013).\(^{19}\)

- Der Onion Service *Playpen* zur Verteilung von KiPo wurde vom FBI übernommen und noch zwei Wochen weiter betrieben. In dieser Zeit wurde der Trojaner auf der Webseite platziert und 8.700 Besucher aus 120 Ländern deanonymisiert (2015).\(^{20}\)

- Der Onion Service *Giftbox* wurde vom FBI übernommen, wie üblich den Trojaner installiert und die Besucher deanonymisiert... (2016).\(^{21}\)

  Bei den Beispielen ging es um echt schmutzige Dinge, die in Gerichtsverhandlungen bekannt wurden und mit denen das FBI seine Erfolge feierte. Rein technisch gesehen kann nicht nur das FBI diese Angriffe durchführen sondern auch andere, potente Angreifer.

  Wenn **hohe Sicherheitsanforderungen** gestellt werden, muss die Verschlüsselung des Datenverkehrs mit dem Tor Daemon (oder einem VPN-Client) in einer Umgebung erfolgen, die von der/den Arbeitsumgebungen mit den Internet Anwendungen getrennt ist.

![Diagramm von Tor Onion Router](image)

**Arbeitsumgebung(en)** stellen die Anwendungen wie TorBrowser, E-Mail Client, Messenger usw. dem Nutzer zur Verfügung. Es sind mehrere Arbeitsumgebungen möglich.

In den Arbeitsumgebungen wird für Anwendungen, die Verbindungen ins Internet aufbauen dürfen, sowie für System Updates ein SOCKS5 Proxy konfiguriert (Proxy: Tor Daemon). Es wird aber KEIN globaler Proxy gesetzt, um unerwünschte Verbindungen zu vermeiden.

**Trusted LAN** ist ein gekapseltes Netz, welches keine direkte Verbindung ins Internet oder in andere lokale Netzwerke ermöglicht. Es gibt keine Gateways in andere Netze!

**Die Firewall** sorgt dafür, dass nur zulässige Daten den Tor Daemon erreichen. Bei der Nutzung von Tor Onion Router darf nur TCP-Traffic die Firewall passieren, der direkt an die **SocksPorts** des Tor Daemon addressiert ist.

**Der Tor Server** (non-Exit Tor Node) ist als Tor Relay Node (non-Exit) konfiguriert mit limitierter Bandbreite (für Cover Traffic) und verschlüsselt alle Daten, die aus dem Trusted LAN kommen und ins Internet fließen sollen. Aus den Arbeitsumgebungen gibt es keinen Weg daran vorbei.

Ein kleines Konfigurationsbeispiel mit den Optionen für einen non-Exit Tor Node:

```
# Tor Client für Arbeitsumgebungen
SocksPort <Trusted-LAN-IP>:9050

# Tor Relay für Cover Traffic
Address <IP> oder <DynDNS>
```

---

\(^{19}\)https://www.wired.com/2013/09/freedom-hosting-fbi/


KAPITEL 10. ANONYMISIERUNGSDIENSTE

Nickname <frei wählbar>

ORPort 9001
DirPort 9030

ExitPolicy reject *:*

# Limits für Bandbreite (anpassen)
RelayBandwidthRate 500 KB
RelayBandwidthBurst 800 KB
AccountingMax 1024 GB
AccountingStart month 1 00:00

ContactInfo Max Mustermann <max@mustermann.tld>

Wenn man beim Angreifermodell davon ausgeht, dass die Arbeitsumgebungen kompromittiert werden könnten, darf man den Arbeitsumgebungen keinen Zugriff auf den Tor ControlPort geben (nur SocksPorts!). Es gibt einige Control-Kommandos, welche die Anonymität gefährden können. Zur Vereinfachung der Tor Server Administration könnte man den ControlPort lokal freischalten:

# für lokale Admin-Tools
ControlPort 127.0.0.1:9051
CookieAuthentication 1
CookieAuthFile /var/lib/tor/control_auth_cookie
CookieAuthFileGroupReadable 1
DataDirectoryGroupReadable 1

StreamIsolation ist ein weiteres Feature, das man aktivieren kann. Für Internet Anwendungen mit Login Kenntnung werden mehrere SocksPorts zur Verfügung gestellt. Der Traffic für diese Ports wird isoliert und über unterschiedliche Routen durch das Tor Netz geleitet, um eine Deanonymisierung durch Korrelationen zu vermeiden.

# SocksPort mit StreamIsolation
SocksPort <Trusted-LAN-IP>:9101 IsolateDestAddr IsolateDestPort
SocksPort <Trusted-LAN-IP>:9102 IsolateDestAddr IsolateDestPort
SocksPort <Trusted-LAN-IP>:9111 IsolateDestAddr
SocksPort <Trusted-LAN-IP>:9112 IsolateDestAddr

Für den TorBrower wird StreamIsolation NICHT empfohlen, aber Thunderbird könnte z. B. Port 9101 verwenden, ein Messenger Port 9111, wget den Port 9112...

Der Router braucht evtl. einen DynDNS Namen und ein Port-Forwarding für den konfigurierten ORPort und DirPort des Tor Daemon (für den Cover Traffic).

Wenn eine Arbeitsumgebung kompromittiert wird, kann der Angreifer nur IP-Adressen aus einem privaten Netzwerkbereich ermitteln und den Nutzer nicht deanonymisieren.

Möglicherweise könnte ein Angreifer mit einem Trojaner zur Online-Durchsuchung persönliche Daten wie Kontonummern oder Kreditkartennummern o.ä. finden, die zur Deanonymisierung führen können? Darüber muss man selbst nachdenken!

Auch die beste Technik kann nicht vor Fehlern beim eigenen Verhalten schützen. So wurde Ross Ulbricht 2011 als Betreiber des Darknet Marktplatzes Silk Road identifiziert, weil er in einem Forum Werbung für sein Projekt postete und dabei eine Bitcoin Adresse angab. Durch Analyse der Blockchain wurden weitere Bitcoin Adressen ermittelt, die zu einer Bitcoin Börse führten, wo er eine GMail Adresse mit seinem realen Namen angegeben hatte. (Wieder so ein schmutziges Beispiel, falls jemand bessere Beispiele hat... )
10.2. TOR ONION ROUTER

Warum ist Cover Traffic sinnvoll? Ein Beispiel: Es gab einen Studenten, der eine Bombendrohung per E-Mail an seine Universität sendete. Der Sender-IP im Header E-Mail verwies auf einen Tor Exit Node. Das Log des zentralen HTTP-Proxy der Universität zeigt nur eine Verbindung ins Tor Netzwerk, die aus der Bibliothek der Universität kam. In der Bibliothek nutzte zum fraglichen Zeitpunkt nur ein Student das Uni-Netz - FAIL.

10.2.6 Anonyme E-Mail Accounts

Es ist wenig sinnvoll, einen bisher ganz normal genutzten E-Mail Account plötzlich anonym zu nutzen. Es haben sich in den letzten Monaten genug Daten angesammelt, die die Identifizierung des Nutzers ermöglichen. Der erste Schritt sollte also die Einrichtung eines neuen E-Mail Accounts sein, der ausschließlich via Tor Onion Router genutzt wird.


Bei der anonymen Nutzung von E-Mail Accounts sind bestehen zwei Anforderungen:

1. Anonymität: Es dürfen keine Lücken bei Anonymisierung bestehen.
2. Sicherheit: Verschlüsselung mit OpenPGP sollte möglich sein.

Derzeit gibt es keinen E-Mail Client, der für die Nutzung mit Tor von TorProject.org überprüft und für gut befunden wurde. Die eigenmächtigen Nutzung einer Anwendung mit Tor als SOCKS5 Proxy ohne qualifizierte Prüfung durch Experten ist nicht ratsam, wie Thunderbird oder diverse Jabber Clients zeigen. Anonymität ist damit nicht gesichert.

Mit dem TorBrowser das Webinterface des E-Mail Providers nutzen

Eine Alternative ist die Nutzung des Webinterfaces eines E-Mail Providers mit dem TorBrowser. Dabei sollte der E-Mail Provider einen Tor Onion Service anbieten oder vergleichbare Lösungen, um die Gefahren durch Bad Exit Nodes zu reduzieren.

Die Verwendung eines Browsers erschwert die Verschlüsselung der E-Mails mit OpenPGP. Man könnte irgendwie versuchen, die Inhalte der E-Mails mit Copy/Paste zu verschlüsseln und entschlüsseln, wie bei Webformularen beschrieben, aber das macht kein Spaß. Besser wäre es, wenn der E-Mail Provider OpenPGP im Webinterface unterstützt.


Da die GUIs der Mailprovider sehr intensiv mit Javascript arbeiten, muss man den mittleren Sicherheitslevel Safer im TorBrowser aktivieren, damit alles funktioniert.


• Mit kleinen Einschränkungen könnte man auch mailbox.org für die anonyme Nutzung mit dem TorBrowser empfehlen, wenn man die angebotenen Features aktiviert:
  - Der Tor Node von mailbox.org kann ähnlich wie ein Onion Service mittels MapAddress Konfiguration verwendet werden. Im Installationsverzeichnis des TorBrowsers die Datei “Browser/TorBrowser/Data/Tor/torrc mit einem Texteditor öffnen und folgende Einträge am Ende hinzufügen:
KAPITEL 10. ANONYMISIERUNGSDIENSTE


– Anonyme Bezahlung ist per Cash (Brief oder Überweisung) möglich.

• Es gibt weitere E-Mail Provider, die die Voraussetzungen erfüllen. Die Liste ist nicht abschließend sondern soll einige Hinweise geben, worauf man achten kann.

Thunderbird 68.x und Tor Onion Router???

Thunderbird 68.x ist nicht für anonyme E-Mails geeignet. Das Add-on TorBirdy ist nicht kompatibel mit Thunderbird 68+ und niemand hat die Gefahren der neuen Features von Thunderbird 68.x in Kombination mit Tor Onion Router analysiert, siehe Bugticket 31341.

Alas, I think it might be a while until torbirdy gets an update – it involves somebody looking at Thunderbird 68 to see what new privacy invasive problems they put into it.

Man kann in Thunderbird einen Proxy verwenden und die nötigen Einstellungen für Tor Onion Router eintragen, aber das reicht nicht. Eine Sicherheitsanalyse der Features von Thunderbird 2011 zeigte einige Gefahren auf, die zur Deanonymisierung führen können. Mit dem Add-on TorBirdy, das maßgeblich von Jacob Appelbaum initiiert wurde, konnten diese Risiken gebannt werden. Für Thunderbird 68.x wäre eine neue Analyse nötig und eine neue, angepasste Version des Add-on TorBirdy, die es nicht gibt.

E-Mail Accounts mit der Tor Live-DVD TAILS verwalten

Die Tor Live-DVD TAILS ermöglicht die Verwendung von Thunderbird zur Verwaltung anonymer E-Mail Accounts. Die Live-DVD enthält einen modifizierten Thunderbird, der die Features von dem Add-on TorBirdy umsetzt, das seit einiger Zeit nicht mehr weiterentwickelt und nicht an aktuelle Thunderbird Versionen angepasst wird. Außerdem verhindert das Sicherheitskonzept von TAILS Verbindungen ins Netz, die nicht via Tor anonymisiert werden.

Da man Thunderbird nicht bei jedem Start der Live-DVD neu konfigurieren möchte, sollte man die persistente Speicherung der Daten von Thunderbird und GnuPG aktivieren.


2. Dann ist die Live-DVD neu zu starten und im Boot Greeter ist der persistente Speicher einzubinden. Dafür ist die Eigabe des Passwortes nötig.


4. Als E-Mail Provider sind jene zu bevorzugen, die Tor Onion Services für IMAP, POP3 und SMTP anbieten, um die Gefahr durch börsartige Tor Exit Nodes zu minimieren.
E-Mail Accounts mit Whonix verwalten

Whonix ist ein System, das aus zwei virtuellen Computern (VMs) besteht. In der Arbeits-VM sind diverse Internetprogramme installiert und in der zweiten Tor-VM läuft Tor Onion Router. Die Arbeits-VM sendet den gesamten Datenverkehr an die Tor-VM. Von dort wird alles durch das Tor Netzwerk geleitet und anonymisiert.

Die Entwickler empfehlen die Nutzung des TorBrowsers, um E-Mail die Kommunikation im Webinterface eines E-Mail Providers zu verwalten.


Spam-Blacklisten

Viele große E-Mail Provider sperren Tor-Nodes bei der Versendung von E-Mails via SMTP aus. Sie nutzen Spam-Blacklisten, in denen Tor-Relays häufig als “potentiell mit Bots infiziert” eingestuft sind. Wenn der E-Mail Provider eine dieser DNSBL nutzt, sieht man als Anwender von Tor nur eine Fehlermeldung beim Senden von Mails. Der Empfang funktioniert in der Regel reibungslos.

Um diese Probleme zu vermeiden, sollte man einen privacy-freundlichen E-Mail Provider nutzen, der Sender-IPs aus dem Header der versendeten E-Mails entfernt.

GoogleMail und Anonymisierungsdienste

GoogleMail (oder GMail) mag eine anonyme Nutzung der kostenfreien Accounts nicht. Kurz zusammengefasst kann man sagen, dass Google entweder eine IP-Adresse der Nutzer haben möchte oder die Telefonnummer. Stellungnahme des Google account security team zu einer Anfrage der Tor Community:

Hello,

I work for Google as TL of the account security system that is blocking your access.

Access to Google accounts via Tor (or any anonymizing proxy service) is not allowed unless you have established a track record of using those services beforehand. You have several ways to do that:

1) With Tor active, log in via the web and answer a security quiz, if any is presented. You may need to receive a code on your phone. If you don’t have a phone number on the account the access may be denied.

2) Log in via the web without Tor, then activate Tor and log in again WITHOUT clearing cookies. The GAPS cookie on your browser is a large random number that acts as a second factor and will whitelist your access.

Once we see that your account has a track record of being successfully accessed via Tor the security checks are relaxed and you should be able to use TorBirdy.

Hope that helps,
Google account security team
Außerdem werden nach einem Bericht von Wired 22 zukünftig alle E-Mails der GMail Ac-
counts in das NSA-Datacenter in Bluffdale kopiert.

10.2.7 Anonym Bloggen
Es gibt viele Gründe, um anonym zu Bloggen. Auf die möglichen Gründe möchte ich nicht
weiter eingehen und mich auf einige technische Hinweise für die Umsetzung beschränken.

Die einfachste Variante:

- Man braucht einen anonymen Browser, am besten das TorBrowserBundle. Gut ge-
eignet ist beispielsweise TAILS, da diese neben einem fertig konfigurierten Browser
 für anonymes Surfen auch die nötigen Tools zur Anonymisierung von Bildern und
 Dokumenten enthalten und keine Spuren auf dem PC hinterlassen.
- Man braucht eine anonyme E-Mail Adresse, die nur in Zusammenhang mit dem Blog
 verwendet wird (für die Registrierung und als Kontaktadresse). Dabei ist es nicht
 nötig, einen E-Mail Client zu konfigurieren. Man kann die E-Mails im Webinterface
 des Providers mit dem TorBrowser lesen.
- Man braucht einen Bloghoster, der anonyme Registrierung oder Registrierung mit
 Fake-Daten ermöglicht und anonym z.B. mit Paysafecard bezahlt werden kann.
 Wordpress.com ist empfehlenswert oder die kostenfreie Variante von Twoday.net. Für
 politische Aktivitäten ist der Bloghoster blackblogs.org geeignet. Um ein Blog bei diese-
mem Hoster zu eröffnen, benötigt man eine E-Mail Adresse von einem Technik Kol
 lektiv. Auf der Policy Seite von blackblogs.org finden man eine die Liste von ak
 zeptierten E-Mail Providern. Diese E-Mail Provider bieten kostenlose Postfächer für
 politische Aktivisten. Um ein Postfach zu erstellen, muss man seine Gründe darlegen,
 aber man muss seine Identität nicht aufdecken.
- Registrierung und Verwaltung des Blogs sowie das Schreiben von Artikeln können
 komplett im Browser durchgeführt werden. Dabei ist stets der Anonymisierungs-
dienst zu nutzen. Man sollte darauf achten, dass man nicht hektisch unter Zeitdruck
 schnell mal einen Beitrag verfasst. Dabei können Fehler passieren.
- Im Blog veröffentlichte Bilder und Dokumente sind stets vor dem Upload zu an-
onymisieren. Vor allem Bilder von Digitalkameras enthalten eine Vielzahl von Infor-
mationen, die zur Deanonymisierung führen können. Fotos von Freunden oder Be-
kannten sollte man nicht veröffentlichen, da durch Freundschaftsbeziehungen eine
 Deanonymisierung möglich ist.
- Jede Blogsoftware bietet die Möglichkeit, den Zeitpunkt der Veröffentlichung von
 neuen Artikeln festzulegen. Das sollte man nutzen und neue Artikel nicht sofort ver-
 öffentlichen sondern einige Stunden später freigeben, wenn man nicht online ist.
- Stilometrie (Deanonymisierung anhand des Schreibstils) ist inzwischen fester Be-
 standteil geheimdienstlicher Arbeit. Es ist mit (teil-) automatisierten Verfahren mög-
l ich, anonyme Texte einem Autor zuzuordnen, wenn der Kreis der Verdächtigen ein-
geschränkt ist und genügend Textproben der Verdächtigen vorliegen. Mit Ruhe und
 Konzentration beim Verfassen von Blogartikeln ist es möglich, seinen individuellen
 Schreibstil zu verstellen und stilometrische Angriffe zu erschweren.

10.2.8 Anonymes Instant-Messaging
Verschlüsselte Chats und Instant Messaging in Kombination mit Anonymisierungsdiens-
ten wie Tor sind auch für potente Geheimdienste wie die NSA ein Alptraum. Es gibt keine
Metadaten, OTR-Verschlüsselung kann noch nicht gebrochen werden und eine Zuordnung

22http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1
23https://blackblogs.org/policy/
von Traffic zu IP-Adressen wird durch die Anonymisierungsdienste verhindert.

Leider gibt es nur wenige Messenger, die für die Kombination mit Tor geeignet sind:

- Populäre Messenger, die eine Telefonnummer und ein Smartphone für den Hauptaccount erfordern, sind natürlich ungeeignet (trivial).

- Messenger, die Interactive Connection Establishment (ICE) für Audio- und Videochats verwenden, sind auf PCs/Laptops ebenfalls ungeeignet, weil ICE agressiv versucht, eine Peer-2-Peer Verbindung mit oder ohne Proxy herzustellen und dabei die eigene IP-Adresse dem Kommunikationspartner mitteilt und via UPnP ein Loch in den Router bohren will. Somit kann ein Anruf zur Deanonymisierung führen.
  ICE ist Bestandteil von WebRTC und der libjingle (XMPP, WhatsApp).

- DNS Leaks sind ein häufiges Problem bei Messenger, die nicht ausdrücklich für die Nutzung via Tor Onion Router vorbereitet wurden.

Folgende Anwendungen können für Instant Messaging via Tor genutzt werden:

**Briar** (nur Android) bringt Tor bereits mit und ist für anonyme Nutzung optimiert.

**qTox** (PCs/Laptops) bzw. der **TRIfA** Tox Client für Android können mit Tor genutzt werden, weil das Protokoll keine verräterischen Informationen überträgt.

Dabei ist darauf zu achten, dass der anonyme genutzte Account erst dann angelegt wird, wenn der Proxy via Tor konfiguriert wurde. Evtl. muss man zuerst einen Dummy Account erstellen, damit man die Einstellungen modifizieren kann und danach den richtigen Account.

UDP und IPv6 Support sind entgegen der Empfehlung bei der Konfiguration von Tor als Proxy zu deaktivieren, da beides von Tor nicht unterstützt wird (Abb: 10.11).

**Abbildung 10.11: qTox Proxy Konfiguration für Tor Onion Router**

**Jabber/XMPP** mit Tor zu verwenden, war vor einige Jahren populär. Der XMPP Client muss dabei folgende Anforderungen erfüllen:

1. Es muss ein SOCKS5 Proxy mit Remote DNS Resolving (ohne DNS-Leaks) konfigurierbar sein, um die Daten durch den Anonymisierungsdienst zu schicken.
2. Die Tor Hidden Service Adresse des Jabber Servers muss als Verbindungsserver konfigurierbar sein. Wenn Tor Onion Router genutzt wird, empfehlen wir nachdrücklich die Jabber/XMPP Server, die eine Tor Hidden Service Adresse anbieten. Damit vermeidet Gefahren durch bösertige Tor Exit Nodes. Angriffe von bösertigen Tor Exit Nodes auf Jabber/XMPP wurden bereits nachgewiesen.
KAPITEL 10. ANONYMISIERSDienste


10.2.9 Gajim (Linux) und Tor Onion Router

Gajim ist unserer Meinung nach NICHT für die Kombination mit dem Tor Onion Router geeignet. Es ist eine Proxy Konfiguration für Tor vorbereitet, aber Gajim enthält Bugs, welche die Anonymität und Sicherheit bei der Verwendung von Tor gefährden.

Wir haben Gajim 0.16.5 unter Ubuntu 16.04 kurz getestet (Stand: Nov. 2016). Gajim für Windows verhält sich möglicherweise etwas anders. Evtl. ist die *libjingle* nicht enthalten? Vielleicht kann man sich ähnlich wie bei Pidgin einen Gajim für Linux selbst bauen?

**DNS-Leaks:** Gajim überlässt die Auflösung von Hostnamen in IP-Adressen nicht dem SOCKS Proxy, sondern macht es selbst und umgeht dabei die Proxy Einstellungen. Diese DNS-Leaks sind ein Security Bug und können die Anonymität gefährden. Im TorProject Wiki findet man folgende Empfehlung, das Problem zu umgehen:

> To prevent this you have to take the hostname of your jabber-server you want to connect to and resolve its IP, e.g. with *tor-resolve* and paste the IP address into Account -> Connection -> Custom Hostname and Port. Now you’re safe (probably)

Vor einigen Jahren war diese Empfehlung vielleicht ok, die IP-Adresse (oder die Tor Hidden Service Adressen) des XMPP Servers als Verbindungsserver einzutragen. Neumodisch aufgemotzte Jabber Server bieten aber mehrere Services unter unterschiedlichen Hostnamen. Wenn man mit dem Account verbunden ist, kann man sie unter *Aktionen - Dienste durchsuchen* abrufen. Der Jabber Server von conversations.im bietet z.B. die in Abbildung 10.12 zu sehenden Dienste.

Man müsste also auch die IP-Adressen der Services `conference.conversations.im`, `proxy.conversations.im` usw. ermitteln und lokal auf dem Rechner fest vorgen, um DNS-Leaks für diese Hostnamen ebenfalls zu vermeiden (könnte man unter Linux in `/etc/hosts` machen). Aber die Services können sich jederzeit ändern, der Admin könnte neue Services hinzugefügt und automatisch an die Clients verteilen... Man müsste es ständig beobachten und bei Bedarf anpassen. Unsicher.


**ICE:** Gajim für Linux enthält eine Implementierung der *libjingle* für Audio- und Videochats. Wenn ein Angreifer eine Einladung zu einem Audio Chat schickt, dann versucht das *Interactive Connectivity Establishment* (ICE) der *libjingle* auf unterschiedlichen Wegen, irgendwie eine Verbindung für einen Audio Channel herzustellen und umgeht dabei auch die Proxy Einstellungen. *Auch wenn man Tor als Proxy konfiguriert hat, versucht ICE mit oder ohne Tor irgendwie die Verbindung zum*
Angreifer herzustellen. Das kann den Nutzer deanonymisieren. (Dieses Verhalten ist kein Bug sondern ein Feature, dass in der Spezifikation so vorgeschrieben ist).

Ein Beispiel: Unter anderem schickt Gajim eine SSDP Discovery Message ins LAN, um einen UPnP-fähigen Router zu finden, der die externe IP-Adresse liefern könnte:

```
M-SEARCH * HTTP/1.1
Host: 239.255.255.250:1900
Man: "ssdp:discover"
ST: urn:schemas-upnp-org:service:WANIPConnection:1
MX: 3
User-Agent: gajim GSSDP/0.14.14
```

Wenn der Angreifer innerhalb des gleichen lokalen Netz sitzt (innerhalb des Firmennetzwerk, bei Starbucks o.ä.), dann hat man damit verloren. Wenn der Angreifer diese SSDP Discovery Message unmittelbar als nach einer Einladung zu einem Audio Chat sieht, dann weiß er, an welchem Rechner das anonyme Gegenüber sitzt.

Wenn Gajim zufällig einen UPnP-fähigen Router findet, dann ist man auch gegenüber einem Angreifer aus dem Internet deanonymisiert. Bei vielen Heimroutern ist UPnP standardmäßig aktiviert, um die Usability zu verbessern.

Unser Test ist nicht gründlich und ist nicht abschließend. Wir haben ein bisschen rumgespielt und mit Wireshark den Datenverkehr beobachtet, das ist kein Security Audit! Insbesondere haben wir keine Zeit gehabt, wirklich im Code nachzuschauen. Wir haben genug Probleme gefunden, um vor der Kombination Gajim+Tor zu warnen.

10.2.10 Dateien anonym tauschen via Tor

OnionShare ist ein kleines Tool, um in Kombination mit dem TorBrowserBundle Dateien zu tauschen. Es ist eine ideale Ergänzung zu TorMessenger oder Ricochet, denen die Möglichkeit zum Tauschen von Dateien (noch) fehlt.

24https://onionshare.org
1. Der Absender benötigt OnionShare und den Tor Daemon des TorBrowserBundles, um die Dateien zum Download bereitzustellen. OnionShare stellt einen Tor Hidden Service bereit, unter dem die Dateien abgerufen werden können.

2. Der oder die Empfänger benötigen nur den TorBrowser, um die bereitgestellten Dateien herunterzuladen. Den Link zum Download bekommen die Empfänger über einen anderen sicheren Kanal, z. B. via TorMessenger oder Ricochet.

Installation von OnionShare:

• Für Windows und MacOS stehen auf der Download Website Setup Dateien zur Installation bereit.

• In den Linux Distributionen Ubuntu und Fedora ist Onionshare enthalten und kann mit dem bevorzugten Tool zur Softwareverwaltung installiert werden.

• Für alle anderen Linux Distributionen muss man OnionShare selbst compileren. Eine Anleitung findet man auf der Webseite.

Nach dem Start von OnionShare kann man im Hauptfenster Dateien zur Liste der gespeicherten Dateien hinzufügen und den Service starten. Der Tor Daemon des TorBrowserBundle wird genutzt, um den Hidden Service bereitzustellen, das TorBrowserBundle muss also gestartet werden, bevor man die Dateien zum Download freigeben kann.

Abbildung 10.13: OnionShare Hauptfenster

Wenn die Option Den Server automatisch anhalten aktiviert, dann wird der Tor Hidden Service nach dem ersten erfolgreichen Download sofort wieder beendet. Das ist ein Sicherheitsfeature, da es im Tor Netz auch bösertige Nodes gibt, die neue Tor Hidden Services testen und teilweise auch angreifen.\textsuperscript{25}

Wenn der Service erfolgreich gestartet ist, kann man die Tor Onion URL in die Zwischenablage kopieren und an den oder die Empfänger schicken, am besten via Instant Messenger. Der oder die Empfänger können die Adresse dann im TorBrowser aufrufen und die bereitgestellten Dateien als ZIP-Archiv herunterladen.

1-Click-Hoster

1-Click-Hoster sind eine weitere mögliche Alternative. Mit dem TorBrowserBundle kann man anonym Dateien bei einem 1-Click-Hoster hochladen und den Download-Link verteilen.

• Auf diesen Hostern sind die Uploads nur eine begrenzte Zeit verfügbar (1-4 Wochen):
  – https://1fichier.com (Uploads werden nach 15 Tagen gelöscht)

\textsuperscript{25}https://www.schneier.com/blog/archives/2016/07/researchers_dis.html
10.2. TOR ONION ROUTER

- https://www.transferbigfiles.com (bis zu 20GB für registrierte Nutzer)
- https://www.filefactory.com (benötigt Javascript und eine E-Mail Addr.)

- Für Langzeit-Hosting kann man folgende Dienste verwenden:
  - https://nofile.io (Verschlüsselung möglich - BETA)
  - https://www.mediafire.com (Registrierung für Uploads nötig)

BitTorrent über einen Anonymisierungsdienst ???

Die naheliegende Variante ist es, BitTorrent über einen Anonymisierungsdienst wie Tor zu nutzen, um die eigene IP-Adresse zu verstecken. Das funktioniert nur begrenzt. Das BitTorrent-Protokoll überträgt die IP-Adresse des Clients auch im Header der Daten und es ist relativ einfach möglich, die Teilnehmer zu deanonymisieren. Im Moment hat die Abmahn-Industrie den Weg noch nicht gefunden. Im Blog von TorProjekt.org findet man eine ausführliche Erläuterung, warum BitTorrent via Tor NICHT anonym ist.

Anonyme Peer-2-Peer Netze

Einige Projekte für anonymes, unbeobachtetes Filesharing:

• I2P Snark: Das Invisible Internet Project bietet anonymes Filesharing innerhalb des Netzes. Eine kurze Einführung findet man im Kapitel zum Invisible Internet.


10.2.11 Tor Onion Services

Das Tor Netzwerk ermöglichst nicht nur den anonymen Zugriff auf herkömmliche Angebote im Web sondern auch die Bereitstellung anonymer, zensurresisternder und schwer lokalisierbarer Angebote auf den Tor-Nodes.

Der Zugriff auf die Tor Hidden Services (Neu: Tor Onion Services) ist nur über das Tor Netzwerk möglich. Eine kryptische Adresse mit der Top-Level Domain .onion dient gleichzeitig als Hashwert für ein System von Schlüsseln, welches sicherstellt, dass der Nutzer auch wirklich mit dem gewünschten Dienst verbunden wird. Die vollständige Anonymisierung des Datenverkehrs stellt sicher, dass auch die Betreiber von Onion Sites technisch anonym bleiben und nur sehr schwer ermittelt werden können.

Es gibt zwei Versionen für Tor Onion Services:

Onion Services v2 werden derzeit standardmäßig verwendet. Diese Onion Service verwenden kryptografische Funktionen, die teilweise veraltet sind. Es wird SHA1 verwendet, DH-Schlüsseltausch und Public Key Kryptografie auf Basis RSA mit 1024 Bit langen Schlüsseln. Die Onion Adressen sind 16 Zeichen lang:

vwakviie2ienjx6t.onion

Hinweis: Onion Services v2 sind DEPRECATED und werden mit Tor Daemon Version 0.4.6 und TorBrowser ab Okt. 2021 nicht mehr unterstützt werden.

26https://blog.torproject.org/blog/bittorrent-over-tor-isnt-good-idea
Onion Services v3 stehen ab Tor Version 3.2 zur Verfügung (Stable Release v3.2.9 Jan. 2018). Die Onion Services V3 verwenden aktuelle kryptografischen Funktionen (SHA3, ECDHE mit ed25519 und Public Key Kryptografie auf Basis elliptischer Kurven mit curve25519). Die Onion-Adressen sind mit 56 Zeichen wesentlich länger:

4acth47l6kzvkeWtm6q7ib2s3ufpo5sdbnzjpbi7utijcltosqemad.onion

Stealth Onion Services erfordern einen zusätzlichen Schlüssel für den Aufbau einer Verbindung. Die Informationen in den Hidden Service Directories über mögliche Zugangspunkte zu diesen Onion Services sind verschlüsselt, so dass bösartige Dritte diese Onion Services nicht ausspionieren oder angreifen können. Wer sich mit diesen Onion Sites verbinden möchte, braucht einen zusätzlichen Key, um die Informationen über die Zugangspunkte zu dechiffrieren.

Authorisierte Nutzer erhalten den Key zum Entschlüsseln der Informationen vom Betreiber über einen unabhängigen, sicheren Kanal. Der Betreiber kann dabei bis zu 50 unterschiedliche Schlüssel für verschiedene Personen generieren. Die Nutzer können diesen Key in der Konfigurationsdatei torrc des Tor Daemon eintragen:

HidServAuth <OnionAdresse> <Key>

Alternativ kann man den Schlüssel auch bei Aufruf einer Stealth Onion Adresse im TorBrowser eingeben und dort dauerhaft speichern, wenn die Abfrage erscheint.

Abbildung 10.14: Abfrage des schlüssels für eine Stealth Onion Site im TorBrowser

Tor Onion Services als sichere Alternative

Es gibt mehrere Angebote im normalen Web, die zusätzlich als Tor Hidden Service bzw. als Tor Onion Site anonym und unbeobachtet erreichbar sind. Wenn man Tor nutzt, sollte man diese Onion Services den normalen Webadressen vorziehen, da dann keine Gefahr durch Bad Tor Exit Nodes besteht.

- Die Suchmaschine Metager (deutsche Suchmaschine) ist erreichbar unter http://metagerv65pwclop2rsfzg4jwowpavpwd6grhhldgsuvwo6ii4akgyd.onion
- Die folgenden Webseiten können als Tor Onion Sites aufgerufen werden:
  - Die Webseite von TorProject.org ist unter folgender Adresse zu finden: http://2gzyxa5ihm7mgsghfjnx5brck2v4rvmdlkmu3zuzv5d3uyx4yclen53wd.onion
  - Weitere Onion Sites findet man unter https://onion.torproject.org bzw. http://xao2kxsmia2edq2n5zxc8uah6x6ox2t7bfjw6b5v6sxi7ezm4qb6qid.onion
  - Die Onion Sites des Debian Projektes findet man unter https://onion.debian.org
– Heise.de bietet einen sicheren Briefkasten auf Basis von Secure Drop für Tippgeber (sogenannte Whistleblower) unter der Adresse:
http://ayznmonmewb2tjvgfl7ym4t2726muprjvwckzs2vhf2hbarbbzydm7oad.onion
– …

• Die folgenden E-Mail Provider bieten POP3, IMAP und SMTP als Tor Onion Service:
– mailbox.org: xy5d2mmnh6jnroce4yk7njlkyafi7tkramseybu43rgsg5ywynelmad.onion
– Riseup.net: 5gdvpfoh6kb2iqbib371zjzk2dzzwra47m6pdueg2m656fovmhoptqd.onion
– ProtonMail ist unter https://protonriockexow.onion als v2 Onion Service erreichbar.

• Die folgenden Jabber-Server sind als Tor Onion Service erreichbar:
– Mailbox: xy5d2mmnh6jnroce4yk7njlkyafi7tkramseybu43rgsg5ywynelmad.onion
– systemli: razpihro3mgydaiykvxwa43rgsg5ywynelmad.onion
– securejabber: sidignlwz2odjhc5hfbueinmr23v5bubq2x43dskebh5sbq2qrxtd.onion
– jabberotr: im: ynmuxkkbbiy5gjidcydekipmhmpbq4fruxa2mhpccy35xjx55ayvjqxd.onion
– jabberstr: jukrlvyhgu2rtyhx75vhuwx3v5wvtyw3wvty75wvty.onion
– securejabber: sidignlwz2odjhc5hfbueinmr23v5bubq2x43dskebh5sbq2qrxtd.onion
– jabber.otr.im: ynnuxkbbiy5gjidcydekipmhmpbq4fruxa2mhpccy35xjx55ayvjqxd.onion
– dismail: 4colmnerbjz2xtjmqogehptb15upjzef57huilibbq3wfpsylub7yd.onion

• HKP-Keyserver für OpenPGP Schlüssel sind unter folgender Adresse erreichbar: http://zkaan2xfbuxia2wp7onfkbz6r5zdbvvxunvp5g2iebopbf4iqmpbd.onion

Tor Onion Services für E-Mail Kommunikation

Für unbeobachtete Kommunikation gibt es folgenden Dienste, die ausschließlich aus Tor Hidden Service genutzt werden können:

• Mail2Tor (kostenfrei, Gateway ins normale Web ist vorhanden)
http://mail2torjgmxgexntbrmhvgluavbj7ouul5yar6lybvjkxwqfl6xkwjd.onion

• TorBox (kostenfreier Hidden-only E-Mail Service)
http://torbox36ijlcevujx7mb4oiusvwgvmue7fn2cvutwa6kl6to3uyqad.onion

• Secmail.pro (kostenfrei, Gateway ins normale Web ist vorhanden)
http://secmail63sex4dfw6h2nsrbmzf2z6alwxe4e3adtkpd4pckkkht4jidad.onion


Debian GNU/Linux Hidden Software Repository

Für Debian GNU/Linux gibt es einen Mirror der Repositories als Tor Hidden Service unter der Adresse vwakviie2ienjx6t.onion. Außerdem gibt es den Apt-Transport-Tor, der die Nutzung des Hidden Service mit den ganz normalen Tools zur Softwareverwaltung ermöglicht. Um die Software des Systems anonym und von Dritten unbeobachtet zu verwalten und zu aktualisieren ist ab Debian jessie nur das Paket apt-transport-tor zu installieren:

```bash
> sudo apt install apt-transport-tor
```

Anschließend editiert man die Datei /etc/apt/sources.list und ersetzt die Server für Debian Paketquellen nach folgendem Muster:
KAPITEL 10. ANONYMISIERUNGSDIENSTE

Zukünftig nutzen alle Tools zur Softwareverwaltung (aptitude, Synaptic, KPackeikit, ...) den Tor Hidden Service für die Installation und Aktualisierung der Software.

Neben Debian bietet natürlich auch TorProject.org das Repository für alle unterstützten Distributionen als Onion Site an. Um den Tor Daemon regelmäßig zu aktualisieren, kann man folgendes Repository nutzen:

```
deb tor+http://sdscoq7snqtznauu.onion/torproject.org <DISTRIBUTION> main
```

<DISTRIBUTION> ist dabei durch den Codenamen der Distribution zu ersetzen, den man mit dem folgenden Kommando ermitteln kann:

```
> lsb_release -c
Codename: yakkety
```

Sonstiges

Ansonsten kenne ich kaum etwas, dass ich weiterempfehlen möchte. Meine “Sammlung” an reinen Tor Hidden Services enthält:

- 34x Angebote, die kinderpornografischen Schmutz zum Download anbieten (ausschließlich und teilweise zusätzlich zu anderen Inhalten). Das BKA hat eine etwas umfangreichere Liste mit 545 Seiten (Stand: 2012).  

- 3x Angebote zum Thema Rent a Killer. Ein Auftragsmord kostet offenbar nur 20.000 Dollar (wenn diese Angebote echt sind).  

- Ein Angebot für gefäkelte Ausweisdocumente (aufgrund der mit Photoshop o.ä. bearbeiteten Screenshots der Beispieldokumente auf der Webseite halte ich das Angebot selbst für einen Fake).  

- Mehrere Handelsplattformen für Drogen. (Das FBI kannte über 400 Plattformen zu diesem Thema.)  

- Einige gähnend langweilige Foren & Blogs mit 2-3 Beiträgen pro Monat.  

- Einige Index-Seiten mit Listen für verfügbare Hidden Services wie das legendäre HiddenWiki oder das neuere TorDirectory. In diesen Index Listen findet man massenweise Verweise auf Angebote mit Bezeichnungen wie TorPedo, PedoVideoUpload, PedoImages. Nach Beobachtung von ANONYMOUS sollen 70% der Besucher des HiddenWiki die Adult Section aufsuchen, wo dieses Schmutzzeug verlinkt ist.  

In dem Paper Cryptopolitik and the Darknet (2016) haben sich die Autoren D. Moore und T. Rid empirisch mit den Tor Onion Sites beschäftigt. Von den 2723 besuchten Onion Sites waren 1547 Onion Sites auf kriminelle, illegale Aktivitäten ausgerichtet.

Fake Onion Sites

Für Tor Onion Sites gibt es kein Vertrauens- oder Reputationsmodell. Es ist unbekannt, wer einen Tor Hidden Services betreibt und es ist damit sehr einfach, Honeypots aufzusetzen. Die kryptischen Adressen sind nur schwer verifizierbar. Das Problem von Anonymität und Reputation ist im Kapitel Nachdenken ausführlicher beschrieben.

27 http://heise.de/-2124930  
28 http://www.tandfonline.com/doi/abs/10.1080/00396338.2016.1142085
10.2. TOR ONION ROUTER

Abbildung 10.15: Original und Fake Onion Site der Suchmaschine Ahmia.fi

Juha Nurmi (Betreiber der Hidden Service Suchmaschine Ahmia.fi) veröffentlichte bereits zwei Warnungen im Juni 2015\textsuperscript{29} und Januar 2016\textsuperscript{30} mit 300 Fake Onion Sites, die den originalen Onion Sites täuschend ähnlich sehen. Diese Fake Sites leiten des Traffic der originalen Sites durch, modifizieren die Daten geringfügig oder erschnüffeln Login Credentials.

Auch Suchmaschinen mit Hidden Service Adressen wie DuckDuckGo (Tor) und Ahmia.fi waren betroffen, wie die Screenshots in Bild 10.15 zeigen. Die Fake Site sieht dem Original täuschend ähnlich, die Besucher werden mit den Suchergebnissen aber auf andere Fake Onion Sites gelenkt.

Teilweise sind die Adressen der Fake Sites den Originalen sehr ähnlich:

REAL: http://torlinkbgs6aabns.onion
FAKE: http://torlinksb7apugxr.onion

REAL: http://valhallaxmn3fydu.onion
FAKE: http://valhalla4qb6qccm.onion

\textsuperscript{29}https://lists.torproject.org/pipermail/tor-talk/2015-June/038295.html
\textsuperscript{30}https://lists.torproject.org/pipermail/tor-talk/2016-January/040038.html
KAPITEL 10. ANONYMISIERUNGSDIENSTE

REAL: http://vendor7zqdpt400.onion
FAKE: http://vendor7eewu66mcc.onion

Schlussfolgerung: Man sollte den kryptischen Hidden Service Adressen nur vertrauen, wenn man sie aus einer vertrauenswürdigen, verifizierten Quelle bekommt. Die Ergebnislisten einer Suchmaschine für Onion Sites sind dabei nur begrenzt zuverlässig, da die Betreiber der Fake Onion Sites natürlich auch SEO-Techniken nutzen, um vor den Orginalen platziert zu werden.

10.2.12 Tor Bad Exit Nodes

Ein sogenannter Bad-Exit-Node im Tor-Netz versucht den Traffic zu beschnüffeln oder zusätzliche Inhalte in eine (nicht SSL-gesicherte) Website einzuschmuggeln. Bedingt durch das Prinzip des Onion Routings holt der letzte Node einer Kette die gewünschten Inhalte. Diese Inhalte liegen dem Tor Exit Node im Klartext vor, wenn die Verbindungen zum Server nicht mit TLS verschlüsselt wurden.


Einige Beispiele für Bad Exits:


apple $232986CD960556CD8053CBECC47C189082B34EF09
CorryL $3163a22dc3849042f2416a785eaebe0e10c48
tortilla $acc9d3a6f5ffca67ff96efc579a001339422687
whistlersmother $e413c4ed88de25a4b69edf9be743f99ad083de
BlueMoon $d51cf2e4e65fd81f2381c53ce3dfs7795df86fca
TRHCourtney1...10 $786fe318d4af52fae078b3305b5ba15f30bc8d48
$AA254D3E276178DB8D955AD93B0562097AD802996
$F650611B117B575E0C5F5B5EFBB065B170CBE0F1
$ECA712A29A088032689A4A1B890E6928906E2
$276A31C32623C3FE8D745BBF9579D17C6DE77
$F0C518A71F4ED5AEE92E980256CD2FA49D9ECC59
$77DF35BBCDC2CD7DB17026FB60724A83A50502827
$BC75DFAC9E807FE9B0A43BBD11F46DB97964AC11

Unnamed $05842ce44dd12cc959f8f583b12537dd7158a
$F36a9380dc35f9448abb235da29abbeded541bc
$9ee320d484b6563bef4ae7f715fe63f55fadb0
$c595385ea8a4053b82746a3920aad4f1916865756
$0326d8412f874256536530e15f9bbd5a4c93738d
$8673eef87f3bf6e02193c6f502d68db7cd58128

2. Die folgenden Nodes wurden bei dem Versuch erwischt, SSL-Zertifikate zu falschen, um den verschlüsselten Traffic mithören zu können.
10.2. TOR ONION ROUTER

(a) *LateNightZ* war ein deutscher Tor Node, der 2007 beim man-in-the-middle Anriff auf die SSL-Verschlüsselung erwischt wurde.\(^{31}\)

(b) *ling* war ein chinesischer Tor Node, der im Frühjahr 2008 versuchte, mit gefälschten SSL-Zertifikaten die Daten von Nutzern zu ermitteln. Gleichzeitig wurde in China eine modifizierte Version von Tor in Umlauf gebracht, die bevorzugt diesen Node nutzte. Die zeitliche Korrelation mit den Unruhen in Tibet ist sicher kein Zufall.\(^{32}\)

(c) Im Sept. 2012 wurden zwei russische Tor Nodes mit den IP-Adressen 46.30.42.153 und 46.30.42.154 beim SSL man-in-the-middle Angriff erwischt.

(d) Im April 2013 wurde der russische Tor Node mit der IP-Adresse 176.99.10.92 beim SSL man-in-the-middle Angriff auf Wikipedia und auf IMAPS erwischt.\(^{33}\)


<table>
<thead>
<tr>
<th>Node</th>
<th>IP-Adresse</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bradiex</td>
<td>bcc93397b50c1ac75c94452964a5bcda01f47215</td>
</tr>
<tr>
<td>TorRelay3A2FL</td>
<td>ee25656d71db9a82c8efb8c4a99d9bec89f24a67</td>
</tr>
<tr>
<td>lolling</td>
<td>1f9803d6ade96771891262ac876feef1088cf9a</td>
</tr>
<tr>
<td>Unnamed</td>
<td>486efad8aef3360c07877dab7b969bf22d304256</td>
</tr>
<tr>
<td>ididedittheconfig</td>
<td>0450b15ffac9e310ab2a222adedf3ef354a65c23</td>
</tr>
<tr>
<td>UnFilTerD</td>
<td>ffd2075c29852c322e1984555c6dfbc6f1ee80</td>
</tr>
</tbody>
</table>

4. Im Oktober 2014 wurde ein Tor Exit Node aufgespürt, der Windows Binaries (z. B. DLLs oder EXE-Dateien) beim Download on-the-fly mit dem Trojaner OnionDuke infizierte, einer Variation der russischen Cyberwaffe MiniDuke. Der Trojaner sammelte Login Daten und spionierte die Netzwerkstruktur der Opfer aus. F-Secure konnten die ersten Infektionen mit OnionDuke auf Oktober 2013 datieren. Der Bad Exit Node wurde gefunden, weil ein Sicherheitsforscher gezielt nach diesem Angriff suchte.\(^{34}\)

5. Im April 2015 wurden 70 Bad Tor Nodes identifiziert, die den Hidden E-Mail Service angriffen hatten. Die Betreiber von SIGAINT warnen, dass es den Angreifern gelungen ist, den Hidden Service mit einem man-in-the-middle Angriff zu kompromittieren und möglicherweise Daten inklusive Login Credentials mitzulesen.\(^{35}\)

*I think we are being targeted by some agency here. That’s a lot of exit nodes. SIGAINT Admin*

Diese 70 Tor Nodes meldeten sich innerhalb eines Monats kurz vor dem Angriff als neue Tor Nodes im Netzwerk an. 31 weitere Nodes stehen noch in dem Verdacht, ebenfalls zu dieser Gruppe zu gehören, aber noch nicht aktiv angesprochen zu haben.

\(^{32}\)http://archives.seul.org/or/talk/Mar-2008/msg00213.html
\(^{33}\)https://trac.torproject.org/projects/tor/ticket/8657
\(^{34}\)http://heise.de/-2457271
\(^{35}\)https://lists.torproject.org/pipermail/tor-talk/2015-April/037549.html
6. Um passiv schnüffelnde Tor Exit Nodes in eine Falle tappen zu lassen, hat Chloe im Juni 2015 einen Honigtopf aufgestellt und 11 passiv schnüffelnde Exit Nodes aufgespürt. Zwei der elf Nodes hatten Guard Status.\footnote{https://chloe.re/2015/06/20/a-month-with-badonions/}


- freifunk.im
- jabber.ccc.de
- jabber.systemli.org
- jappix.org
- jodo.im
- pad7.de
- swissjabber.ch
- tigase.me


10. Europol betreibt seit Jahren ein Projekt mit dem Ziel to provide operational intelligence related to TOR. Die Formulierung lässt vermuten, dass ebenfalls passiv schnüffelnde Exit-Nodes genutzt werden.

### 10.2.13 Tor Good Exit Nodes

Im Abschnitt Tor Bad Exits sind einige Nodes genannt, denen man nicht trauen sollte. Diese Aufzählung kann natürlich nicht abschließend und vollständig sein.


Als Verteidigung können Nutzer in der Tor-Konfiguration Exit Nodes angeben, denen sie vertrauen und ausschließlich diese Nodes als Exit-Nodes nutzen. Welche Nodes vertrauenswürdig sind, muss jeder Nutzer selbst entscheiden, wir können nur eine kurze Liste als Anregung zum Nachdenken liefern.
10.2. TOR ONION ROUTER

- Torserver.net ist eine vertrauenswürdige Organisation, die Exit-Nodes betreibt.
- Der Tor Node Digitalcourage3ip1 wird vom Verein Digitalcourage e.V. betrieben.\footnote{https://digitalcourage.de/support/tor}
- Die Heinlein Support GmbH betreibt den Tor Node mailboxorg und empfiehlt die Konfiguration von MapAdresses in der torrc, so dass dieser Node als Exit Node für alle Mailbox.org Dienste genutzt wird.
- ...bitte selbst die Liste erweitern


Konfiguration in der torrc

In der Tor Konfigurationsdatei /etc/tor/torrc bzw. für das TorBrowserBundle in \texttt{<TorBrowserBundleVerzeichnis>/Browser/TorBrowser/Data/Tor/torrc} kann man die gewünschten Nodes mit folgenden Optionen konfigurieren:

\begin{verbatim}
StrictExitNodes 1
ExitNodes $9BDF3EEA1D3AA58A2EEA9E6CA58FB8A667288FC,$1A1DA6B9F262699A87F9A4F24EF48BS0148EB018,$31A993F413D0168117F76247E4F242095190B87,$A07FF746DBA56C3F916BBD404307396BFA862E0,$A3279B1AC705C9F3478947598CF05578B1E12DE1,$AB176B6575A99DCCCB7889184E62EF0B2E35751,$B7BE1D357621555FEB2BC9DAE0A157C706D738FE5,$85D4088148B1A6954C9BF8FFCA010E85E0A88FF0,$39659458160887CC8A46FAE627EE01EDEAAED07F,$0111BA9B604669E653FFDF5B503F3824A7AD66E0,$AD86CD1A49573D52A7B6F4A35750F161AAD89C88,$DC4124B158D1420C98C66F7B5E569C9DE98FE,$B060482C7847B888A564DEC9D04E14CB305C88B38,$88487BDD980BF6E72092EE690E8C510CA4A538C,$95DA61AEEF23A6C351028C1AA88A8593F659E60F,$95DA61AEEF23A6C351028C1AA88A8593F659E60F,$487092BA36F4675F2312AA09AC0393D85DAD6145
\end{verbatim}

Die erste Option gibt an, dass nur die im folgenden gelisteten Nodes als Exit verwendet werden dürfen. Für die Liste der Exits nutzt man die Fingerprints der Nodes, beginnend mit einem Dollar-Zeichen. Die Fingerprints erhält man von verschiedenen TorStatus Seiten. Diese Liste enthält die oben genannten Nodes und ist nur ein Beispiel. Für die praktische Nutzung ist sie viel zu klein, um eine hohe Anonymität zu gewährleisten.

\footnote{https://digitalcourage.de/support/tor}
10.3 Finger weg von unseriösen Angeboten

Neben Projekten, die sich wirklich um eine anonyme Lösung für Surfer bemühen, gibt es immer wieder Angebote, die unbedarfte Anwender ködern wollen.

Tor-Boxen

Sogenannte Tor-Boxen wie Anonabox oder SafePlug leiten als Router den gesamten Traffic eines Computers oder Heimnetzwerkes oder als Proxy nur den HTTP-Traffic durch Tor. Die Anbieter versprechen eine einfachste Installation und gleichzeitig die Anonymität des Tor-Netzwerkes. Aber manchmal ist einfach das Gegenteil von Anonym.

Anonymes Surfen erfordert in erster Linie eine sichere Browserkonfiguration. Wer mit einem beliebigen Browser (z. B. Internet Explorer, Google Chrome oder Safari) ohne privacy-freundliche Konfiguration im Internet surft, der kann sich die Nutzung von Tor sparen, damit surft man nicht anonym. Die einzige, von den Tor-Entwicklern empfohlene Variante zum anonymen Surfen ist die Nutzung des TorBrowserBundle.

The most crucial problem with a torifying proxy is that it uses a bring-your-own-browser system, as opposed to a hardened browser, and therefore is susceptible to browser-based privacy leaks. This is why it’s better to use the Tor Browser Bundle. (Quelle: Blog TorProject.org)

Web-Proxys

Web-Proxys mit HTTPS-Verschlüsselung sind ein probates Mittel, um Zensur im Internet zu umgehen. Sie sind aber als Anonymisierungsdienste unbrauchbar. Mit kruden HTML-Elementen oder JavaScript ist es möglich, die meisten Web-Proxys auszutricksen und die reale IP-Adresse des Nutzers zu ermitteln.

Die folgende Tabelle zeigt eine Liste bekannter Webproxys, die den Anonymitätstest der JonDos GmbH nicht bestehen:

<table>
<thead>
<tr>
<th>Betreiber</th>
<th>HTML/CSS</th>
<th>JavaScript</th>
<th>Java</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymouse</td>
<td>gebrochen</td>
<td>gebrochen</td>
<td>gebrochen</td>
</tr>
<tr>
<td>Cyberghost Web</td>
<td>gebrochen</td>
<td>gebrochen</td>
<td>gebrochen</td>
</tr>
<tr>
<td>Hide My Ass!</td>
<td>gebrochen</td>
<td>gebrochen</td>
<td>gebrochen</td>
</tr>
<tr>
<td>WebProxy.ca</td>
<td>gebrochen</td>
<td>gebrochen</td>
<td>gebrochen</td>
</tr>
<tr>
<td>KProxy</td>
<td>gebrochen</td>
<td>gebrochen</td>
<td>gebrochen</td>
</tr>
<tr>
<td>Guardster</td>
<td>gebrochen</td>
<td>gebrochen</td>
<td>gebrochen</td>
</tr>
<tr>
<td>Megaproxy</td>
<td>gebrochen</td>
<td>nicht verfügbar</td>
<td>nicht verfügbar</td>
</tr>
<tr>
<td>Proxify</td>
<td>gebrochen</td>
<td>gebrochen</td>
<td>gebrochen</td>
</tr>
<tr>
<td>Ebunma</td>
<td>gebrochen</td>
<td>gebrochen</td>
<td>gebrochen</td>
</tr>
</tbody>
</table>

Free Hide IP

Free Hide IP wird von Computerbild als Anonymisierungsdienst angepriesen.


ZenMate

ZenMate will ein VPN-artiger Anonymisierungsdienst sein, der eine einfach zu installierende Lösung für anonymes Surfen verspricht. Man muss auf der Webseite nur einmal kurz klicken, um einen Browser Add-on zu installieren. Es gibt eine kostenlose Version, die nur die IP-Adresse versteckt. Außerdem steht eine Premium Version zur Verfügung, die auch Tracking Elemente blockieren können soll, was aber nicht funktioniert (Abb. 10.16).

Abbildung 10.16: Tracking Protection in ZenMate funktioniert nicht

Schlussfolgerung: Das ist nu
Kapitel 11
Anonyme Peer-2-Peer Netzwerke

Anonyme Peer-2-Peer Netze nutzen die Infrastruktur des WWW, um in einer darüber liegenden, komplett verschlüsselten Transportschicht ein anonymes Kommunikationsnetz zu bilden. Der Datenverkehr wird mehrfach verschlüsselt über ständig wechselnde Teilnehmer des Netzes geleitet. Der eigene Rechner ist auch ständig an der Weiterleitung von Daten für andere Teilnehmer beteiligt. Das macht die Beobachtung durch Dritte nahezu unmöglich.

Es entsteht ein sogenanntes Darknet im Schatten des normalen Internet, das Google nicht kennt und in dem man sich weitgehend unbeobachtet bewegen kann, wie im Dunkel der Nacht.

Abbildung 11.1: Prinzip von anonymen Peer-2-Peer Netzen


Invisible Internet Project (I2P)


• Das Äquivalent zum Usenet ist Syndie. Es gibt öffentliche und private Diskussionsforen, die auf Syndicationservern gehostet werden.

• Es gibt zwei redundante Server für IRC.

• Für das Filesharing ist mit I2Psnark eine Adaption von BitTorrent vorhanden. Der Tracker von Postman ist das Äquivalent zur PirateBay im normalen Netz.

**Freenet**

Freenet bietet Schutz gegen das umfangreichste Angriffsmodell. Freie Kommunikation unter den Bedingungen totaler Überwachung ist das Ziel des Projektes. Es stellt die höchsten Anforderungen an die Nutzer und erzielt die langsamste Downloadgeschwindigkeit.

Im Unterschied zu I2P werden die Inhalte im Freenet redundant über alle Teilnehmer verteilt und verschlüsselt abgelegt. Es gibt keine Server für Webdienste, E-Mail usw. Der Zugriff auf die Inhalte erfolgt nicht über einfache URLs, sondern über komplexe Schlüssel, welche die Adressen der TOR Hidden Services als absolut harmlos erscheinen lassen. Einmal veröffentlichte Inhalte können im Freenet nicht mehr modifiziert werden, auch nicht vom Autor. Es ist jedoch möglich, aktualisierte Versionen zu veröffentlichen. Die Freenet Software stellt sicher, dass immer die aktuellste Version angezeigt wird.

Neben Webseiten gibt es F-Mail und mit Frost ein Äquivalent zum Usenet. Das Tauschen von Dateien erfolgt direkt im Browser mit einer Oberfläche, die die Freenet Software bereitstellt.

Unabhängig vom Open Freenet kann man mit vertrauenswürdigen Freunden ein eigenes Netz Friend-2-Friend Netzwerk konfigurieren, welches sich vollständig der Beobachtung durch unbefugte Dritte entzieht.

**Retroschare**


RetroShare ermöglicht die unbeobachtete Kommunikation in Gruppen, ohne zentrale Dienste im Internet zu nutzen. Die Kommunikation ist durch Dritte sehr schwer kompromittierbar, wenn jeder Teilnehmer die kryptografischen Schlüssel nur an vertrauenswürdige Freunde weitergibt. Wenn man allerdings diese Grundregel missachtet und die eigenen Schlüssel im Internet publiziert, um das private Netzwerk zu vergrößern, dann können sich auch unbefugte Dritte einschleichen.
11.1 Invisible Internet Project (I2P)


Neben der Möglichkeit, anonym zu surfen und Websites (sogenannte eepsites) anzubieten, sind weitere Anwendungen bereits fester Bestandteil von I2P. Es bietet anonyme E-Mail (Susimail, I2P-Bote), BitTorrent Downloads (I2Psnark), ein anonymes Usenet (Syndie) u.a.m.

11.1.1 Installation des I2P-Routers


**Windows:** Als erstes ist ein Java-Runtime-Environment (JRE) zu installieren. Das Installationsprogramm für Java gibt auf der Webseite www.java.com1. Der Installer möchte unbedingt die Ask-Toolbar für alle Browser installieren. Das sollte man deaktivieren, braucht man nicht.


**Ubuntu:** Die aktuellen Versionen von Ubuntu ab 18.04 enthalten den I2P-router in den Repositories. Mit dem bevorzugten Paketmanager kann man alles Nötige mit einem Kommando installieren:

> sudo apt install i2p

Für ältere Ubuntu kann man das PPA Repository der I2P Maintainer nutzen:

1https://www.java.com/de/
> sudo apt-add-repository ppa:i2p-maintainers/i2p
> sudo apt update
> sudo apt install i2p

**Debian:** Für Debian *stretch* gibt es ein Repository, das man mit folgenden Zeilen in der Datei `/etc/apt/sources.list` einbindet:

```plaintext
deb http://deb.i2p2.no/ stable main
deb-src http://deb.i2p2.no/ stable main
```

Außerdem ist der Signaturschlüssel des Repository `i2p-debian-repo.key.asc` herunterzuladen und in den Apt-Keyring einzufügen mit:

```plaintext
> wget https://geti2p.net/_static/i2p-debian-repo.key.asc
> sudo apt-key add i2p-debian-repo.key.asc
```

Danach kann man I2P und auch das Paket `i2p-keyring` für spätere Updates des Signaturschlüssels installieren:

```plaintext
> sudo apt install i2p i2p-keyring
```

Debian *buster* enthält den I2P Router in den Repositories der Distribution, mit dem Paketmanager kann man alles notwendige installieren ohne extra Repositories einzufügen:

```plaintext
> sudo apt install i2p
```

**Linux:** Als erstes ist Java (Paket: `default-jre`) mit der Paketverwaltung der Distribution zu installieren. Danach kann der I2P-Router installiert werden. Den Installer `i2pinstall-0.x.y.jar` findet man auf der Downloadseite des Projektes. Nach dem Download startet man den Installer und wählt die Sprache sowie das Verzeichnis für die Installation:

```plaintext
> java -jar i2pinstall-*.jar
```

In dem neu angelegten Installationsverzeichnis findet man das Script zum Starten/Stoppen des I2P-Routers:

```plaintext
> ~/i2p/i2prouter start
```


11.1.2 Konfiguration des I2P-Router

Standardmäßig ist der I2P-Router funktionsfähig vorkonfiguriert. Ein paar kleine Anpassungen können die Arbeit etwas verbessern.

Bandbreite anpassen


Netzwerkkonfiguration

Auf der Seite http://localhost:7657/confignet der Router Konsole sind die Einstellungen für die Einbindung in das I2P-Netz zu konfigurieren. Dabei gibt es zwei Möglichkeiten:

1. Wenn der eigene Rechner nicht vom Internet erreichbar ist, dann sind folgende Optionen zu aktivieren, damit der I2P-Router korrekt arbeitet:
   - **Versteckter Modus** ist zu aktivieren.
   - Optional kann der **Laptop Modus** aktiviert werden. Dann ändert sich Router-Identifikation bei Änderung der IP-Adresse.

2. Wenn der eigene I2P-Router vom Internet für andere Teilnehmer erreichbar ist, verbessert sich die Performance und Anonymität. In der Netzwerk Konfiguration des I2P-Routers sind dann folgende Optionen zu konfigurieren:
   - In den UDP-Einstellungen ist der Port anzugeben, für den die Weiterleitung auf dem DSL-Router konfiguriert wurde.
   - In den TCP-Einstellungen ist ebenfalls der Port zu konfigurieren und die Option automatisch erkannte IP-Adresse benutzen zu aktivieren.

Die Hinweise im Kapitel Konfiguration des DSL-Routers erläutern die notwendigen Einstellungen, damit Ihr Rechner vom Internet erreichbar ist. Auf dem DSL-Router ist ein Portforwarding zu Ihrem Rechner zu konfigurieren und die Firewall des Rechners ist anzupassen.

SusiDNS anpassen

Für die Zuordnung von Domainnamen mit der Toplevel Domain .i2p zu einem Service wird SusiDNS verwendet, ein dem DNS im Internet vergleichbares System. Wie in den Anfangszeiten des WWW erhält jeder I2P Router eine komplette Liste der bekannten eepsites: das addressbook.

Um neue eepsites oder Services in das addressbook einzufügen, verwendet I2P sogenannte subscriptions. Die eine standardmäßig vorhandene subscription wird relativ selten aktualisiert.

Um auf dem Laufenden zu bleiben, kann man weitere subscriptions zu abonnieren. Die Einstellungen für SusiDNS findet man in der Routerkonsole. Subscriptions kann man unter folgender Adresse einfügen: http://localhost:7657/susidns/subscriptions.jsp (Bild 11.3)

Folgende subscriptions bieten aktuelle Neuerscheinungen von eepsites:

http://stats.i2p/cgi-bin/newhosts.txt
http://i2host.i2p/cgi-bin/i2hostetag
http://tino.i2p/hosts.txt
11.1. INVISIBLE INTERNET PROJECT (I2P)

Abbildung 11.3: subscriptions für SusiDNS

11.1.3 Anonym Surfen mit I2P

Der I2P-Router stellt einen HTTP- und HTTPS-Proxy für den Webbrowser bereit. Die Default-Adressen dieser Proxys sind:

- Rechner: localhost
- HTTP-Proxy Port: 4444
- SSL-Proxy Port: 4445
- FTP-Proxy Port: 4444
- Gopher-Proxy Port: 4444

Der Proxy kann genutzt werden, um Webseiten im Invisible Internet aufzurufen (sogennannte eepsites, erkennbar an der Toplevel Domain .i2p).

JonDoFox nutzen

Das Firefox Profil JonDoFox ist für spurenarmes und sicheres Surfen optimiert. Es bietet neben JonDo und Tor eine Benutzerdefinierte Proxy Konfiguration, die man für I2P nutzen kann. Die Einstellungen zeigt Bild 11.4. Der JonDoFox verhindert zuverlässig eine Kompromittierung der Anonymität.

Firefox selbst konfigurieren

Ich würde empfehlen, für das Surfen im Invisible Internet ein separates Firefox-Profil zu erstellen. Dann ist es für spionierende Websites gänzlich unmöglich, im Cache oder in der Historie abgelegte Daten über das anonyme Surfen auszulesen. Den Profil-Manager von Firefox startet man mit folgendem Kommando:

> firefox -P

In dem sich öffnenden Dialog (Bild 11.5) kann man ein neues Profil anlegen und anschließend die Proxy-Einstellungen konfigurieren. In Zukunft wird Firefox bei jedem Start fragen, welches Profil genutzt werden soll.

Abbildung 11.4: Benutzerdefinierte Proxy-Konfiguration im JonDoFox

Abbildung 11.5: Firefox Profil-Manager

Wichtige Sicherheitseinstellungen für Firefox

Flash und Java Plug-ins sind unbedingt zu deaktivieren, da diese Plug-ins die Proxy-Einstellungen umgehen könnten. Um eine Deanonymisierung zu vermeiden, sind für einen aktuellen Firefox außerdem folgende Features unter der Adresse about:config zu deaktivieren:

- WebRTC kann durch UDP-Tunnel die reale IP-Adresse aufdecken (nur Firefox 18 und neuer):
  
  \[
  \text{media.peerconnection.enabled = false}
  \]

- Geolocation-API kann den realen Standort ermitteln:
  
  \[
  \text{geo.enabled = false}
  \]

- Phishing- und Malware Protection funktioniert für eepsites nicht, da die Webseiten des Darknet nicht in der Google Datenbank enthalten sind:
  
  \[
  \text{browser.safebrowsing.enabled = false}
  \]
11.1.1 INVISIBLE INTERNET PROJECT (I2P)

Abbildung 11.6: Firefox Proxy-Einstellungen für I2P

Suchmaschinen für I2P

Um sich in einem Netzwerk zu orientieren, braucht man eine Suchmaschine. Die Webseite plugins.i2p bietet viele Firefox Search Plugins für I2P. Wenn man die Webseite http://plugins.i2p/firefox aufgerufen hat, kann man die Suchmaschinen einfach durch Aufklappen der Liste der Suchmaschinen oben rechts im Firefox hinzufügen. Unter dem Trennstrich findet man die neuen Suchmaschinen, die diese Webseite zur Installation anbietet.


11.1.4 I2P Mail 1 (Susimail)


Es ist möglich, E-Mails in das normale Web zu versenden und auch von dort unter der Adresse <username>@i2pmail.org zu empfangen. Die Weiterleitung ins normale Internet kann bis zu 24h dauern und ist von den gewählten Einstellungen auf HQ Postmaster abhängig. Um für Spammer unattraktiv zu sein, haben die Entwickler von I2P die Anzahl der ins normale Web versendbaren Mails begrenzt. Es ist möglich, innerhalb von 24h bis zu 20 Empfängern beliebig viele E-Mail zu senden. Wer unbedingt mehr Leute per E-Mail kontaktieren will, kann mit einem Hashcash ein Kontingent von weiteren 20, 40 oder 80 Empfängern freischalten.

Routerkonsole nutzen

KAPITEL 11. ANONYME PEER-2-PEER NETZWERKE

Abbildung 11.7: Webinterface von Susimail

Es bietet eine simple Möglichkeit, Mails abzurufen und zu versenden. Komfortabler ist die Nutzung des bevorzugten E-Mail Clients, vor allem wenn man die Möglichkeiten zur Verschlüsselung der Nachrichten nutzen möchte.

Thunderbird konfigurieren

Der Susimail-Account kann mit jedem E-Mail Client genutzt werden.

```
SMTP-Server: localhost Port: 7659
POP3-Server: localhost Port: 7660
Login-Name: <username>
```

In Thunderbird ist als erstes ein neuer SMTP-Server anzulegen (Konten -> Postausgangs-Server (SMTP) -> Hinzufügen). Der Server erfordert eine Authentifizierung mit den Daten des Susimail Accounts.

Danach kann ein neues POP3-Konto angelegt werden, welches diesen SMTP-Server für die Versendung nutzt. SSL- und TLS-Verschlüsselung sind zu deaktivieren. Der I2P-Router übernimmt die abhörsichere Übertragung.

```
In den Server-Einstellungen des Kontos sollte die Option “Alle x Minuten auf neue Nachrichten prüfen” deaktiviert werden! Die Admins von Susimail bitten darum, den Service nicht unnötig zu belasten.
```

Susimail mit Tor nutzen

An Stelle des I2P-Routers kann auch Tor für den Abruf und das Versenden von Nachrichten via I2P Mail genutzt werden. Folgende Hidden Services bieten ein SMTP-Gateway (Port: 7659) und POP3-Gateway (Port: 7660):

```
v6ni63jd2tt2keb5.onion
5rw56roa13f2riwj.onion
```

11.1. INVISIBLE INTERNET PROJECT (I2P)

Hinweise zur Nutzung von Susimail

Der Service wird von postman und mastijaner in der Freizeit aufgebaut und gepflegt. Sie bitten darum, folgende Hinweise zu beachten:


2. Um anonym zu bleiben, sollte man keine Mails an die eigene Mail Adresse im Web schreiben oder an Bekannte, mit denen man via E-Mail im normalen Web Kontakt hält.

3. Bitte Susimail nicht für Mailinglisten nutzen, die man nicht mitliest. Das Abmelden auf Mailinglisten bei Desinteresse nicht vergessen.


Englischer Orginaltext bei HQ Postman: http://hq.postman.i2p/?p=63

11.1.5 I2P Mail 2 (Bote)


I2P Bote ist keine Weiterentwicklung von Susimail und es soll es auch nicht ersetzen. Langfristig werden beide Projekte parallel existieren und kooperieren. Das Projekt bietet folgende Features:

• Bedienung im Webinterface der I2P-Routerkonsole.
• Erzeugen von Identitäten, Senden/Empfangen von E-Mails.
• SMTP- und IMAP-Gateway für die Integration in Thunderbird u.a.
• Anonyme Absender und Versenden über Zwischenstationen mit zeitlicher Verzögerung (Remailer-Konzept).
• Dateianhänge bis 500 kB werden unterstützt. Die Begrenzung der Größe der Dateianhänge ist aufgrund der redundanten Speicherung nötig. Die Nachrichten werden mit 20x Redundanz gespeichert und eine 1 MB große Mail würde 20 MB Speicherplatz in der DHT belegen.

Installation von I2P Bote

Um I2P Bote zu nutzen, ist die Installation von 3 Plug-ins für den I2P Router nötig. Auf der Seite I2P Dienste der Routerkonsole (unter http://localhost:7657/configclients.jsp) findet man ganz unten den Abschnitt für die Installation zusätzlicher Plug-Ins (Bild 11.8).

 Folgende Plug-Ins sind in dieser Reihenfolge zu installieren:

KAPITEL 11. ANONYME PEER-2-PEER NETZWERKE

Abbildung 11.8: Installation des Plug-in I2P Bote


Eigene Identität erzeugen

Der erste Schritt nach der Installation ist in der Regel die Erstellung einer eigenen Adresse. In der Navigationsleiste rechts wählt man "Identitäten" und den Button "Neue Identität".

Als Pflichtfeld ist nur ein Name anzugeben. Die Verschlüsselung belässt man am besten bei 256Bit-ECC. Diese Verschlüsselung liefert relativ kurze und starke Schlüssel. Die Mailadresse wird zur Zeit noch nicht genutzt.

Die kryptische Bote-Adresse ist an alle Partner zu verteilen oder zu veröffentlichen. In der Übersicht ist die Adresse nicht voll sichtbar. Wenn man auf die Identität klickt, erhält man eine vollständige Ansicht. Die gesammelten Adressen der Partner können in einem rudimentären Adressbuch verwaltet werden.

Abbildung 11.9: Neue Identität für I2P-Bote anlegen
11.1. INVISIBLE INTERNET PROJECT (I2P)

Konfiguration

Bevor man loslegt, sollte man einen Blick in die Konfiguration werfen und diese anpassen.


- Über Zwischenstationen senden: Wird diese Option deaktiviert ("AUS"), gehen versendete Nachrichten direkt in die DHT. Die Anonymität entspricht der normalen Anonymität bei der Nutzung von I2P.

Eine höhere Anonymität erreicht man, wenn die Nachricht vor dem Speichern in der DHT über 1...n Teilnehmer des I2P-Bote Netzes geleitet und dort jeweils um eine zufällige Zeitspanne verzögert wird. Die min. und max. Werte für die Verzögerung können konfiguriert werden. Ähnlich wie bei Remailern sinkt damit natürlich die Performance der Kommunikation.

- Durchleitung an Nicht-I2P-Adressen: Es ist möglich, Mails an Nicht-I2P-Bote Teilnehmer zu versenden. Die Nachrichten werden an die Bote-Adresse eines Durchleitungsdienstes versendet, der sich dann um die weitere Zustellung kümmert. Derzeit arbeitet HQ Postman an der Entwicklung dieses Services, der aber noch nicht arbeitsfähig ist.


Mails schreiben und empfangen

Das im Bild 11.10 gezeigte Formular für eine neue Mail öffnet sich mit Klick auf den Button "Neu".

Als Absender kann man Anonym wählen, oder eine der zuvor angelegten Identitäten. Wer Anonym wählt, sollte sich nicht wundern, dass er vom Empfänger als anonymer Unbekannter behandelt wird. Für vertrauliche Konversation muss man seinen Gegenüber verifizieren können.
KAPITEL 11. ANONYME PEER-2-PEER NETZWERKE

In die Felder An, Kopie oder Blindkopie sind die kryptischen Bote-Adressen der Empfänger einzutragen, der Rest sollte sich selbst erklären. Eingehende Mails findet man im Ordner Posteingang.

Adressbuch


Außerdem hilft das Adressbuch bei der Verifikation der Absender empfangener Nachrichten. Ein Absender ist eindeutig nur durch seine Bote-Adresse bestimmt. Der Name kann frei gewählt werden und kann auch mehrfach genutzt werden. Es könnte also jemand den Namen HungryHobo nutzen, um sich als Hauptentwickler von I2P-Bote auszugeben.


Abbildung 11.11: Inbox mit verifiziertem Absender

11.1.6 I2P IRC


Das I2P-Netz bietet zwei anonyme Chat-Server, die direkt über den I2P-Router erreichbar sind. Die Konfiguration der verschiedenen Clients wie XChat (Linux/UNIX), Kopete (KDE), Colloquy (MacOS) oder Mirc (Windows) ist einfach. Man nutzt als Chat-Server folgende Adresse und ist anonym:

Host: localhost
Port: 6668

Die wichtigsten Chat-Kommandos

Der Chat wird in der Regeln komplett durch Kommandos gesteuert. Alle Kommandos beginnen mit einem Slash. Eine kurze Liste der wichtigsten Kommandos:

/list Listet alle Diskussions-Channels auf, die auf dem Server verfügbar sind.
/join #channel Den Raum #channel betreten und mitdiskutieren.
/quit Den aktiven Raum verlassen oder vom Server abmelden.
/msg nick <text> Sendet eine Nachricht an den User nick.
/ignore nick Einen Troll ignorieren.
/help Beantwortet alle weiteren Fragen.
Im IRC ist man mit einem Nicknamen unterwegs. Die Nicknamen werden registriert und mit einem Passwort geschützt, damit kein Dritter einen bekannten Nicknamen nutzen kann, um sich eine Identität zu erschleichen.

Die Registrierung erfolgt mit folgendem Kommando:
/msg nickserv register <Password> fake-email-addr

Um einen registrierten Nicknamen zu nutzen, muss man sich identifizieren:
/msg nickserv identify <Password>

#anonops

Die Channels von Anonymous stehen auch auf den I2P-IRC Servern zur Verfügung. Für die Diskussionen in diesen Channels sollten sie die Regeln von Anonymous beherzigen:

Basics: Tauchen Sie in der Masse unter ohne ein besonders smarter Typ sein zu wollen. Es gibt keine Helden, die alt geworden sind, es gibt nur junge Helden und “tote” Helden.

Geben Sie keine persönlichen Informationen im public IRC preis.

- keine Anhaltspunkte im Nicknamen und Realnamen veröffentlichen
- keine persönlichen Informationen im Chat diskutieren
- keine Informationen über die Herkunft diskutieren (Land, Stadt usw.)
- keine Beschreibung von Tattoos, Piercings oder anderer Merkmale
- keine Informationen über Beruf und Hobbys
- keine Sonderzeichen wie äöü verwenden, die nur in Ihrer Sprache verfügbar sind
- veröffentlichen Sie nichts im normalen Netz, während Sie in einem anonymen Chat sind - es kann einfach korreliert werden
- posten Sie keine Bilder von Facebook im Chat, diese Bilder enthalten die persönliche ID
- verbinden Sie sich nicht Tag für Tag zur gleichen Zeit mit dem Chat

11.1.7 I2P BitTorrent

Der I2P-Router bietet auch eine angepasste Implementierung des BitTorrent Protokolls für anonymes Peer-2-Peer Filesharing. Im Gegensatz zur Nutzung von normalem BitTorrent über Tor ist die Implementierung des Invisible Internet Project anonym und die Nutzung ausdrücklich erwünscht. Der Dienst bietet Optimierungen mit speziellen Clients.

Die I2P-Router-Konsole bietet einen einfachen BitTorrent Client als Webinterface unter Torrents (http://localhost:7657/i2psnark).


**Hinweis zur Nutzung:** Es gehört beim Filesharing zum guten Ton, Dateien nicht nur zu saugen. Man stellt die heruntergeladenen Dateien auch anderen Teilnehmern zur Verfügung. Bei BitTorrent im normalen Netz gilt es als freundlich, wenn man heruntergeladene Dateien mindestens für 2 Tage zum Upload anbietet oder bis die Datenmenge des
Upload das 2,5fache des Downloads beträgt. Da die Geschwindigkeit im I2P-Netz wesentlich geringer ist, sollte man heruntergeladene Dateien mindestens für 1 Woche zum Upload anbieten.
11.2 DSL-Router und Computer vorbereiten

Um als vollwertiger Teilnehmer an einem anonymen Peer-2-Peer Netz teilzunehmen, muss der eigene Rechner vom Internet aus erreichbar sein. Nur dann können andere Teilnehmer des Netzes den eigenen Knoten kontaktieren. Als typischer Heimnutzer mit DSL-Anschluss sind einige Anpassungen nötig, damit der eigene Rechner aus dem Internet erreichbar ist.


<table>
<thead>
<tr>
<th>Application</th>
<th>Start</th>
<th>End</th>
<th>Protocol</th>
<th>IP Address</th>
<th>Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grp</td>
<td>8888</td>
<td>8888</td>
<td>Both</td>
<td>192.168.1.16</td>
<td>✔</td>
</tr>
<tr>
<td>gnut1</td>
<td>1080</td>
<td>1080</td>
<td>Both</td>
<td>192.168.1.16</td>
<td>✔</td>
</tr>
<tr>
<td>gnut2</td>
<td>2086</td>
<td>2086</td>
<td>Both</td>
<td>192.168.1.16</td>
<td>✔</td>
</tr>
</tbody>
</table>

Abbildung 11.12: Portforwarding auf dem Router


3. Außerdem muss die Firewall auf dem lokalen Rechner den ankommenden Datenverkehr der anderen Peer-2-Peer Teilnehmer auf den Ports durchlassen, für die eine Weiterleitung im Router konfiguriert wurde.

2http://heise.de/-1793625
Virtual Private Networks (VPNs)

Virtual Private Networks (VPNs) wurden entwickelt, um vertrauenswürdige Endpunkte über unsichere Netzwerke zu verbinden. Sinnvolle Anwendungen für VPNs sind:

- Verbindung von zwei oder mehreren Firmenstandorten über das Internet.
- Einbindung einzelner Außendienst Mitarbeiter (*Road Warrior*) in ein Firmennetz.
- Einbindung externer, industrieller Anlagen an zentrale Leitsysteme (z. B. Windkraftträger im Energiebereich, dezentrale Pumpwerke der Wasserversorgung o. ä.)
- Im privaten Bereich kann man VPNs verwenden, um in öffentlichen Wi-Fi Netzerken (Hotel, Flughafen, U-Bahn o. ä.) die Verbindung zu einem vertrauenswürdigen Zugangsprovider herzustellen. Das verhindert Firesheep-ähnliche Angriffe durch andere, möglicherweise böswillige Nutzer des Wi-Fi Hotspot.

Außerdem kann man mit VPNs geo-spezifische Sperren von IP-Adressen umgehen, indem man einen VPN Server in einem Land wählt, das nicht blockiert wird.

VPN Technologien

Die für ein VPN notwendige Software steht für unterschiedliche Standards als Open Source Software zur Verfügung:


**IPsec** arbeitet einen Level tiefer auf IP-Ebene und bietet daher eine höhere Robustheit gegen Lauschern, da auch die TCP-Header verschlüsselt werden. Es wird von Regierungsbehörden und Militär bis zur Geheimhaltungsstufe VS-Geheim verwendet.

IPsec ist ein sehr komplexes Protokoll, das die Lösung eines Problems auf mehreren unterschiedlichen Wegen ermöglicht. Diese Komplexität ist einer der Hauptkritikpunkte von N. Ferguson und B. Schneier in ihrer Evaluierung von IPsec.²

*In our opinion, IPsec is too complex to be secure. The design obviously tries to support many different situations with different options.*


---

¹[http://www.searchnetworking.de/definition/Firesheep-ein-interessantes-Firefox-Plugin](http://www.searchnetworking.de/definition/Firesheep-ein-interessantes-Firefox-Plugin)
²[https://www.schneier.com/academic/paperfiles/paper-ipsec.pdf](https://www.schneier.com/academic/paperfiles/paper-ipsec.pdf)
Iodine versteckt den VPN Traffic im DNS Datenverkehr, um VPN-Sperren zu umgehen. Der Datendurchsatz ist viel geringer, als bei anderen VPNs.

PPTP Microsofts Point-to-Point-Tunneling-Protocol (PPTP) ist konzeptuell kaputt und sollte nicht mehr verwendet werden.


12.1 VPN Dienste als Billig-Anonymisierer

Aus der Werbung eines VPN Providers:

Verbergen Sie Ihre Online-Identität und surfen Sie anonym im Netz!

Nein! VPNs wurden NICHT als Anonymisierungsdienste entwickelt. Der Einsatz als Billig-Anonymisierer ist aus folgenden Gründen nicht sinnvoll:

- VPNs anonymisieren lediglich die IP-Adresse eines Internetnutzers. Für Trackingdienste ist die IP-Adresse aber nur ein geringwertiges Trackingfeature. Durch die Verbreitung mobiler Internetnutzung mit ist der Wert dieses Merkmals weiter gesunken. Modernes Tracking verwendet Fingerprinting und EverCookies, gegen die VPNs nicht schützen. Somit ist durch VPNs keine Anonymität bei Surfen gegeben. (Richtige Anonymisierungsdienste wie Tor Onion Router adressieren dieses Problem durch eine einheitliche Browserkonfiguration (TorBrowserBundle), die eine Anonymitätsgruppe schafft, in der einzelne Surfer nicht unterscheidbar sind.)


Hermann/Wendolsky/Federrath haben bereits 2009 in dem Paper Popular Privacy Enhancing Technologies with the Multinomial Naïve-Bayes Classifier gezeigt, dass man die Nutzer eines OpenVPN Anonymisierers zu 95% durch Beobachtung des Traffics des VPN-Servers bzw. -Nutzers deanonymisieren kann ohne die Krypto zu knacken.

- Ein VPN Betreiber hat wie ein Internet Zugangsprovider Zugriff auf das gesamte Nutzungsverhalten. Das erfordert ein hohes Maß an Vertrauen in den VPN Betreiber, das bei vielen Betreibern nicht gerechtfertigt ist.

  - Der von Facebook betriebene VPN-Dienst Onavo spioniert seine Nutzer aus und speichert, welche Apps und Internetdienste die Nutzer verwenden. Damit kann Facebook frühzeitig Konkurrenten erkennen und Maßnahmen zur Sicherung der Marktes ergreifen.

  - Der VPN Dienst AnchorFree verwendet für das Angebot Hotspot Shield Fre JavaScript, um IFrames mit personalisierten Werbeanzeigen zu injizieren und außerdem den Standort des Nutzers zu tracken. Eindeutige Identifikationsmerkmale wie MAC-Adressen und IMEI-Nummern von Smartphones werden an Werbenetzerwerke weitergegeben, was die Nutzer gegenüber den Trackingdiensten natürlich deanonymisiert.

Statt einem Gewinn an Privatsphäre wird man als Nutzer solcher VPN Dienste noch mehr ausgespäht.

3https://epub.uni-regensburg.de/11919
5https://heise.de/-3795523
• Bei vertrauenswürdigen VPN Providern ist zu beachten, dass sie den Gesetzen des jeweiligen Landes folgen müssen. Da diese Dienste wie Zugangsprovider zum Internet arbeiten, kann sich daraus eine deutliche Absenkung der Sicherheit und Privatsphäre ergeben, wenn die Gesetze des Heimatlandes des VPN Anbieters eine Vorratsdatenspeicherung fordern oder Zugriff auf den Datenverkehr für Geheimdienste.

Der britische VPN-Dienst HideMyAss (Testsieger beim VPN Magazine\textsuperscript{6}) hat z. B. 2011 den LuzSec Hacker Cody Kretsin, der dem Anonymitätsversprechen von HideMyAss vertraute, an das FBI verraten. Dabei hat HideMyAss nur im Rahmen der gesetzlichen Vorgaben kooperiert. In einem Blog Artikel verteidigt HideMyAss die Deanonymisierung von Kretsin gegenüber dem FBI.\textsuperscript{7}

Es gibt keinen Grund, einem VPN Anonymisierer mehr zu vertrauen, als einem Internet Zugangsanbieter wie Telekom oder Vodafone oder...

### 12.2 Empfehlenswerte VPN-Provider

Einige VPN-Provider haben Tracker in ihren Apps integriert, was man für Android Apps bei Exodus Privacy erfragen kann, sie werben mit Anonymität beim Surfen, was oben breits zerlegt wurde, oder werben mit military grade security, weil AES256-GCM für die Verschlüsselung der Daten verwendet wird. Um solche VPN-Provider mit irrefühender Werbung sollte man einen Bogen machen.

(Für military grade security braucht man nicht nur sichere Cipher sondern auch sichere Speicherung der Schlüssel außerhalb der Arbeitsumgebung auf einem Hardware Security Modul und die VPN-Verschlüsselung muss ebenfalls außerhalb der Arbeitsumgebung erfolgen. Diese Anforderungen erfüllt kein bekannter VPN-Provider.)

Folgende VPN-Provider kann man für die Umgehung geo-spezifischer IP-Sperren, zur Vermeidung von Gefahren in öffentlichen WLANs (Hotel, ICE, Flughafen usw.) oder zur Verhinderung des Trackings von Reisetätigkeiten anhand wechselnder IP-Adressen empfehlen:

**Mullvad VPN** hebt sich durch seriöse Aussagen vom Großteil der VPN Anbieter ab.\textsuperscript{8}

• Mullvad VPN bietet weltweit verteilte OpenVPN und Wireguard Server für 5,- Euro pro Monat. Man sollte owned Server bevorzugen, bei denen der Anbieter die volle Kontrolle hat.
• Die Smartphone Apps von Mullvad VPN enthalten keine Tracker und fordert nur die minimal nötigen Berechtigungen.
• Man kann auf PCs die Standardsoftware für OpenVPN oder Wireguard nutzen.

**ProtonVPN** hebt sich durch einige Sicherheitsfeatures von anderen Anbietern ab.\textsuperscript{9}

• ProtonVPN bietet Server für OpenVPN und IPsec/IKEv2 mit starker Krypto.
• Es gibt einen kostenlosen Angebot und Premiumangebote für 4,- Euro (zwei Geräte, kein Streaming) 8,- Euro (inklusive Video Streaming) bis 24,- Euro monatlich.
• Es ist empfehlenswert, auf Smartphones die Apps von ProtonVPN zu nutzen. Es sind nur notwendige Freigaben erforderlich und keine Tracker enthalten aber dafür zusätzliche Sicherheitsfeatures wie den Netzwerk Kill Switch für Android oder Always-on-VPN für iPhones.
• Windows 10, MacOS (El Capitan) und Linux unterstützen IPsec/IKEv2 oder OpenVPN standardmäßig.

\textsuperscript{6}https://www.vpnmagazin.de/hidemyass-test
\textsuperscript{7}http://t3n.de/news/lulzsec-hacker-anonymizer-hidemyass-straftatverfolgung-332537
\textsuperscript{8}https://mullvad.net/de
\textsuperscript{9}https://protonvpn.com/de

- IVPN.net bietet Wireguard, OpenVPN und IPsec/IKEv2 Server in 32 Ländern, die eine sichere Verschlüsselung nach dem aktuellen Stand der Technik bieten.
- Bei der Registrierung werden keine Daten erfasst, kein Name, Telefonnummer oder E-Mail Addr. Es wird eine Account-ID generiert, die man kopieren muss.
- Für die Bezahlung bietet IVPN.net flexible Laufzeiten mit opt-in für eine automatische Verlängerung sowie anonyme Zahlung per Cash Brief. Beim Test gab es ein paar Probleme. Bezahlung mit einer Kreditkarte war nicht möglich. Der Support von IVPN kommentierte:

> We occasionally see the bank or financial institution associated with the credit or debit card block payments because it looks suspicious to them. We are located in Gibraltar, so this is not entirely unexpected.

Die Bezahlung mit Bitcoin schied wegen der hohen Mining Gebühren von 100-800% für die Zahlung aus. Bei In-App Bezahlung mit iPhones zahlt man 15% Aufschlag für die Provision an Apple.

Der erste VPN Provider, dem man vertrauen kann, ist man selbst mit eigener Technik.

- Wenn man einen kleine Rasberry PI oder Mini-Computer im eigenen Heimnetz betreibt, kann man ihn zu einem VPN Server mit OpenVPN oder Wireguard aufrüsten.
- Fritz!Boxen könnten out-of-the Box als VPN Server eingesetzt werden, wenn keine hohen Ansprüche an die Sicherheit der VPN-Verbindung gestellt werden.

Man könnte damit den Datenverkehr von Smartphones oder Laptops bei der Nutzung von öffentlichen WLANs in Hotels oder am Flughafen via VPN über den eigenen Router leiten, um die Gefahren in öffentlichen Wi-Fi Netzen zu verringern. Aber Fritz!VPN ist NICHT geeignet, um eine sichere Verbindung ins Firmennetz oder zwischen Standorten aufzubauen.

WARNUNG: Fritz!VPN verwendet die DH Group 2 mit 1024 Bit für den initialen Schlüsseltausch (Fritz!OS 7.20). Damit kann die VPN-Verbindung von Diensten wie der NSA seit Jahren on-the-fly aufgebrochen werden. (Aber wenn der Traffic an der anderen Seite der Fritz!Box wieder ins Internet purzelt, gewinnt ein Überwacher wenig durch Knacken des VPN. Man könnte die gleichen Informationen auch durch einfache Korrelationsanalyse gewinnen.)

HINWEIS: Mit iPhones ist ein Always-on-VPN NICHT realisierbar. Die VPN-Verbindung wird geschlossen, wenn kein Datenverkehr fließt. Man müsste das VPN also immer wieder aktivieren, bevor man eine App startet, deren Datenverkehr über den eigenen Router laufen soll (was man gelegentlich vergessen wird).

### 12.3 Verschiedene VPN Lösungen für Linux

Linux bietet Implantierungen für nahezu alle VPN-Lösungen. Im folgenden werden einige Konfigurationen für Linux Clients (Road Warrior) vorgestellt. Die Serverseite ist den IT-Profis vorbehalten und wird hier nicht behandelt.

#### 12.3.1 OpenVPN mit Linux

OpenVPN hat den Vorteil, dass es unter Linux auf Client Seite sehr einfach zu konfigurieren ist. Die nötige Software ist in Regel standardmäßig installiert oder wird nachinstalliert:
KAPITEL 12. VIRTUAL PRIVATE NETWORKS (VPNS)

Ubuntu: > sudo apt install openvpn network-manager-openvpn-gnome resolvconf
Fedora: > sudo dnf install openvpn NetworkManager-openvpn-gnome resolvconf

Die VPN-Provider oder die Administratoren der IT-Abteilung einer Firma können eine OpenVPN Konfigurationsdatei zum Download bereitstellen, die man nur importieren muss.

Unter Linux fügt man ein VPN im NetworkManager hinzu, der auch LAN- und WLAN-Verbindungen verwaltet. Nachdem man die OpenVPN Konfiguration von der Webseite des VPN-Providers herunter geladen hat, wählt man VPN hinzufügen und die Option Aus Datei importieren: …

Im folgenden Dialog muss man nur noch die Login Credentials für die Anmeldung angeben. Bei der Speicherung des Passworts für die Anmeldung gibt es mehrere Möglichkeiten:

1. Wenn man das Passwort nur für den aktuellen Nutzer speichert, wird es verschlüsselt im GNOME Keyring oder KWallet (KDE Desktop) gespeichert.
2. Wenn man es für alle Nutzer speichert, liegt es unverschlüsselt auf der Festplatte.
4. Bei einigen VPN Providern wie z. B. IVPN.net ist kein Passwort nötig, weil die zufällig generierte Userkennung nicht zu erraten ist und nur für das VPN verwendet wird.

Man kann das VPN mit einem Klick im NetworkManager Applet aktivieren, sobald man mit einem Netzwerk verbunden ist. Um diesen Vorgang zu automatisieren, könnte man in den Einstellungen für ein (WLAN) Netzwerk festlegen, dass immer ein bestimmtes VPN automatisch gestartet werden soll, wenn man sich mit diesem Netzwerk verbindet.

HINWEIS: in den Netzwerkeinstellungen im GNOME Kontrollzentrum ist diese Option nicht vorhanden. Wenn die Linux Distribution das GNOME Kontrollzentrum zur Konfiguration der Netzerwe bevorzugt, muss man den Konfigurationeditor des Network-Managers im Terminal aufrufen:

> nm-connection-editor

12.4 IPsec/IKEv2 VPN Client mit Windows 10


1. Eine IPsec VPN-Verbindung wird mit folgendem Cmdlet erstellt:

   PS C:\> Add-VPNConnection -AllUserConnection -Name "meinVPN"
   -ServerAddress 1.2.3.4 -TunnelType "Ikev2"
   -AuthenticationMethod "EAP" -RememberCredential

   • Es wird eine IPsec VPN Verbindung für alle Anwender erstellt.
   • Der Name kann frei gewählt werden. Er dient nur der Anzeige und wird in den folgenden Kommandos verwendet, im die VPN-Verbindung auszuwählen.
   • Der VPN-Server hat die IP-Adresse 1.2.3.4. Man kann auch einen DNS Namen angeben. Die DNS Namen der VPN Server findet man auf der Webseite des VPN-Providers.
12.5 DAS VPN EXPLOITATION TEAM DER NSA

- Die Authentifizierung beim Server erfolgt mit Username/Passwort (EAP).
- Die Login Credentials werden beim ersten Login abgefragt und dauerhaft gespeichert. Wenn man die Credentials nicht speichern möchte, kann man den letzten Parameter weglassen.

2. Standardmäßig vertraut Windows 10 den Certification Authorities (CAs) im Store, um die Identität des VPN-Servers anhand seines X509v3 Zertifikates zu bestätigen. Unter Umständen kann es nötig sein, das Root Zertifikat von der Webseite des VPN Providers herunter zu laden, wenn der VPN Provider aus Sicherheitsgründen eine eigene CA verwendet statt der bekannten Certification Authorities. Bei ProtonVPN muss man z. B. das Zertifikat der ProtonVPN Root CA herunterladen und dann mit folgendem Befehl in den Store importieren:

```
PS C:\> Import-Certificate -FilePath "C:\Users\XYZ\Download\ProtonVPN_ike_root.der" -CertStoreLocation Cert:\LocalMachine\Root
```

Um Man-in-the-Middle Angriffe zu erschweren, kann man das CA Root Zertifikat festlegen, mit dem das Zertifikat des VPN Server signiert sein muss (CA Pinning). Wenn man ProtonVPN verwendet, könnte man nach dem Import des Root Zertifikat mit folgenden Powershell Kommandos die CA für diese VPN Verbindung festlegen:

```
PS C:\> $ca = Get-ChildItem Cert:\LocalMachine\Root | ? Subject -EQ 'CN=ProtonVPN Root CA'
PS C:\> Set-VpnConnection -ConnectionName "meinVPN" -MachineCertificateIssuerFilter $ca
```

Der erste Befehl filtert das CA Root Zertifikat der Liste der vertrauenswürdigen CAs. Der zweite Befehl legt fest, dass dieses Root Zertifikat die Identität des VPN-Servers bestätigen muss.

3. Ein guter VPN Provider wird seine Server so konfigurieren, dass nur sichere Cipher für die Verschlüsselung verwendet werden. Wenn man den Admins des VPN-Servers diesbezüglich nicht vertraut, kann man mit folgendem Cmdlet die VPN Verbindung anpassen, um sichere Ciphersuiten gemäß NSA Suite-B-128 zu erzwingen:

```
PS C:\> Set-VpnConnectionIPsecConfiguration -ConnectionName "meinVPN" -CipherTransformConstants GCMAES128 -EncryptionMethod AES128 -PfsGroup ECP256 -DHGroup ECP256 -IntegrityCheckMethod SHA256 -AuthenticationTransformConstants SHA256128
```

4. Man kann festlegen, dass bestimmte Anwendungen nur via VPN genutzt werden. Es wird automatisch das VPN gestartet, wenn eine der definierten Anwendungen gestartet wird. Man definiert VPN-only Anwendungen mit folgendem Cmdlet:

```
PS C:\> Add-VpnConnectionTriggerApplication -ConnectionName "meinVPN" -ApplicationID <Path> | <Package Family Name>
```

Legacy Anwendungen werde dabei über den Path der EXE-Datei spezifiziert, moderne Anwendungen werden über den Package Family Name referenziert.

12.5 Das VPN Exploitation Team der NSA

Aus den Dokumenten, die Edward Snowden bei der NSA rausgetragen hat, ist bekannt, dass die in der NSA das OTP VPN Exploitation Team für die Angriffe auf VPNs zuständig ist. Es werden einige Angriffsvektoren beschrieben, die ambitionierte Hacker gegen VPNs einsetzen (nicht nur die NSA setzt diese Techniken ein, auch andere Länder wie Frankreich, China oder Russland haben erhebliche Kapazitäten auf dem Gebiet und Kriminelle Hacker jeglicher Art sind auch interessiert).

[10] https://protonvpn.com/download/ProtonVPN_ike_root.der
Angriffe auf die Verschlüsselung: In den Snowden-Dokumenten wird erwähnt, dass der NSA 2010 einen Durchbruch bei Angriffen auf Verschlüsselung gelang und 60% des weltweiten VPN-Traffic on-the-fly entschlüsselt werden konnte. 2015 wurde die Logjam Attack\(^{11}\) durch zivile Kryptoforscher publiziert, die die Erfolge der NSA erklären konnte. Dabei handelt es sich um einen pre-computation Angriff auf den Diffie-Hellman Schlüsseltausch.

Dieses Beispiel zeigt, dass staatliche Angreifer mehrere Jahre Informationsvorsprung bei der Kryptoanalyse haben. Man sollte deshalb keine Kryptografie einsetzen, die schon ein bisschen schwächelt.

Außerdem werden Man-in-the-Middle Angriffe und TLS-Downgrade Angriffe eingesetzt. Für beide Angriffe gibt es inzwischen Appliances.


- Bei TLS-Downgrade Angriffen stört der Angreifer den Aufbau der VPN-Verbindung immer wieder und bringt damit beide Seiten dazu, eine immer schwächere Verschlüsselung zu probieren. Wenn dann eine hinreichend schwächere Verschlüsselung ausgewählt wurde, die der Angreifer knacken kann, lässt er den Aufbau der Verbindung zu.

Appliances für TLS-Downgrade Angriffe sind military-grade Hardware hinsichtlich Geheimhaltung und Exportbeschränkungen. Ich kenne nur eine ältere Appliance, die RC4 Cipher on-the-fly brechen konnten. Auch bei der IETF hat man davon gehört und mit RFC 7465 die Verwendung von RC4 verboten. An dieser Stelle ein Dank an Jakob Appelbaum, der als erster darauf hinwies:

\[
\text{RC4 is broken in real time by #NSA - stop using it. (Nov. 2013)}^{12}\]

(In der zivilen Kryptoanalyse ist kein Ansatz bekannt, um RC4 Cipher on-the-fly zu brechen. RC4 gilt als schwacher Cipher und konnte mit der NOMORE Attack\(^ {13}\) in 7,5h geknackt werden, um HTTPS Cookies zu entschlüsseln, und in 1h bei WPA Passwörtern. RC4 on-the-fly brechen ist bisher NSA-only Level.)

Angriffe auf die kryptografischen Schlüssel sind die logische Alternative, wenn man die Verschlüsselung nicht brechen kann.

Pre-shared Keys (PSK) können alle VPNs zur Authentifizierung nutzen. Das Programm HappyDance der NSA hat die Aufgabe, diese Schlüssel zu knacken um den Datenverkehr als passive Lauscher zu entschlüsseln.

Dabei kommen drei Methoden zum Einsatz:

1. Die E-Mail Überwachung wird genutzt, um in den abgefangenen Mails nach Schlüsseln zu suchen, die als pre-shared Keys für die Authentifizierung bei VPNs geeignet sein könnten. Diese Schlüssel werden gesammelt und automatisiert genutzt. (Es gibt immer Admins, die diese Schlüssel per E-Mail verteilen.)


\(^{11}\)https://weakdh.org

\(^{12}\)https://twitter.com/ioerror/status/398059565947699200

\(^{13}\)https://www.rc4nomore.com
Pre-shared Keys sollte man nur für Testzwecke nutzen. Das StrongSwan Team warnt aufgrund der Snowden Dokumente vor dem Einsatz. Statt dessen sollte man X509v3 Zertifikate verwenden, auch wenn die Konfiguration damit komplizierter wird.

**Kompromittierung der VPN-Server oder -Clients** Das OTP VPN Exploitation Team der NSA setzt auch diese Methode gegen High-Value-Targets wie z. B. Banken ein, wenn Admins ihre VPNs professionell konfigurieren.


2. Anschließend installiert das NSP-Team ein Implantat (Rootkit), dass die VPN-Verschlüsselung des Datenverkehrs so stark schwächt, dass sie on-the-fly gebrochen werden kann, ohne das der Admin es jahrelang bemerkt.

Gelegentlich greift das TAO-Team die Server nicht direkt an sondern spielt über die Bande und kompromittiert zuerst die Computer Administratoren, um an Passwörter oder Keys zu gelangen ([Inside the NSA’s Secret Efforts to Hunt and Hack System Administrators](https://theintercept.com/2014/03/20/inside-nsa-secret-efforts-hunt-hack-system-administrators/)).
Kapitel 13

Domain Name Service (DNS)

DNS (Domain Name Service) ist das Telefonbuch des Internet. Eine kurze Erklärung:

1. Der Surfer gibt den Namen einer Website in der Adressleiste des Browsers ein. (z. B. https://www.privacy-handbuch.de)

2. Daraufhin fragt der Browser bei einem DNS-Server nach der IP-Adresse des Webservers, der die gewünschte Webseite liefern könnte. Üblicherweise wird der DNS-Server des Zugangsproviders gefragt, also z. B. Telekom, Vodafone...


5. Dann sendet der Browser seine Anfrage an die IP-Adresse des entsprechenden Servers und erhält als Antwort die gewünschte Webseite.


Möglichkeit zur Zensur


Aktuell wird die Sperrung von Webseiten in Iran, Türkei, Ukraine, Südkorea oder Vietnam beispielsweise nach diesem Muster umgesetzt und in Großbritannien gibt es konkrete Pläne für eine Zensurinfrastruktur auf Basis von DNS-Manipulationen. Für die Türkei
wurde auch nachgewiesen, dass die Nutzung alternativer DNS Server zur Umgehung der Zensur blockiert wird und DNS Anfragen auf Port 53 immer an die kompromittierten Server umgeleitet wird. Nur verschlüsseltes DNS ermöglicht eine Umgehung der Zensur.

13.1 DNSSEC Validierung

DNSSEC verbreitet sich langsam aber immer weiter als Sicherheitskomponente. Ein DNSSEC validierender DNS-Server kann die Echtheit der DNS Informationen anhand kryptografischer Signaturen verifizieren, Manipulationen erkennen und verwerfen, wenn der Betreiber der Domain die DNS-Daten signiert hat. Damit wird verhindert, dass Dritte die Daten manipulieren und den Surfer irgendwie umleiten (Zensur? Phishing?). Wie das konkret funktioniert, ist eine Menge Krypto-Voodoo.

DNSSEC ist außerdem eine Voraussetzung, um via DANE/TLSA die X509v3 Zertifikate für die TLS Verschlüsselung zu verifizieren oder um mit OPENPGPKEY bzw. SMIMEA kryptografische Schlüssel sicher zu verteilen.


Um diese Schwäche zu vermeiden, könnte man die DNSSEC Signaturen auch auf dem eigenen Rechner mit einem lokalen Resolver validieren.

- Windows bietet out-of-the-box noch keine Möglichkeit, DNSSEC zu nutzen.
- Die meisten Linux Distributionen verwenden inzwischen systemd-resolve für die DNS Namensauflösung. Um DNSSEC zu aktivieren, ist eine Config Datei dnssec.conf im Verzeichnis /etc/systemd/resolved.conf.d/ anzulegen mit folgendem Inhalt:

  [Resolve]
  DNSSEC=true

13.2 Verschlüsselung des DNS Datenverkehr

Das DNS-Protokoll enthält keine Authentifizierung die sicherstellt, dass man wirklich mit dem gewünschten DNS-Server verbunden ist. DNS-Anfragen könnten vom Provider auf eigene, möglicherweise kompromittierte DNS Server umgeleitet werden. In der Türkei wird dieses Feature seit mehreren Jahren zur Durchsetzung der Zensur umgesetzt.

Um diese Schwächen zu vermeiden, kann man den DNS-Datenverkehr zum Upstream DNS-Server verschlüsseln. Das stellt kryptografisch sicher, dass man wirklich mit dem gewünschten DNS-Server verbunden ist (Authentifizierung) und verhindert eine Manipulation durch Dritte auf der letzten Meile.

Die Verschlüsselung der DNS-Daten in Kombination mit ESNI (Encrypted Server Name Indication) in TLS 1.3 hat das Potential, die staatliche Infrastruktur zur Zensur des Internet in den meisten Ländern auszutricksen. Aus diesem Grund versuchen einige Länder, diese technischen Entwicklungen zu blockieren:

- Die Great Firewall von China blockiert TLS 1.3, um anhand der unverschlüsselt übertragenen Servernamen im TLS Handshake unerwünschte Webseiten zu blockieren.
- In Großbritannien wurde auf Druck der Internet Service Betreiber ein Deal mit Mozilla geschlossen, dass DNS-over-HTTPS nicht wie geplant standardmäßig aktiviert wird. Man rechnet damit, dass die meisten Nutzer nie etwas davon gehört haben.
KAPITEL 13. DOMAIN NAME SERVICE (DNS)


Um den Datenverkehr kryptografisch zu sichern, gibt es folgende Möglichkeiten:

DNSCrypt ist die älteste Technik für verschlüsseltes DNS und basiert auf DNS-curve von D.J. Bernstein. DNScrypt stellt mit kryptografischen Verfahren sicher, dass man wirklich den gewünschten DNS-Server verwendet und verschlüsselt die DNS Daten.


iPhones unterstützen verschlüsseltes DNS-over-TLS seit iOS Version 14.

DNS-over-HTTPS wurde im Sommer 2016 von Google initiiert. Es dient in erster Linie Umgehung von Zensur auf Basis von DNS Manipulationen und ist aufgrund des HTTP Overhead einig Millisekunden langsamer als normales DNS.

Es gibt einige Programme, die DNS-over-HTTPS beherrschen und damit die in den Systemeinstellungen konfigurierten DNS-Server umgehen können:

*dnscrypt-proxy* kann als lokaler DNS Resolver mit eingebautem Cache genutzt werden und auch DNS-over-HTTPS Server verwenden.

Firefox kann die DNS Einstellungen des Systems umgehen und DNS-over-HTTPS Server als Trusted Recursive Resolver (TRR) verwenden.

Thunderbird kann ebenfalls DNS-over-HTTPS Server als Trusted Recursive Resolver (TRR) verwenden. Es sind die gleichen Parameter wie bei Firefox in den erweiterten Einstellungen anzupassen.

DNS-over-HTTPS-over-Tor kann man machen, wenn ein sinnvolles Gesamtsicherheitskonzept es erfordert. Man kann beliebigen HTTPS Traffic durch Tor tunneln, um zu verhindern, dass der/die DNS-Server die eigene IP-Adresse protokollieren kann.

Man erreicht das gleiche Ziel aber auch ohne Performance Einbußen, indem man einen vertrauenswürdigen DNS-Server mit No-Logging-Policy verwendet.

Abgesehen von einigen Szenarien mit höchsten Sicherheitsanforderungen, für die es schwer fällt, ein plausibles Beispiel zu konstruieren, ist DoHoT meist Overkill.

Oblivious DNS-over-HTTPS wurde von Cloudflare im Dez. 2020 initiiert, weil es Vorbehalte in Europa gegen die Nutzung von Cloudflare als Default Trust-Recursive-Resolver (DoH) in Firefox gab. Derzeit läuft der Standardisierungsprozess.

Cloudflare ist nicht daran interessiert, welche Webseiten Lieschen Müller oder Pitschie Hufnagel aufrufen. Sie interessieren sich für eine globale Sicht, welche neuen Ideen gewinnen an Popularität, was ist der neue *heiße Shit* und was ist anderseits auf dem absteigenden Ast. Diese Informationen frühzeitig zu haben ist wertvoll, wie es Google mit seiner Suchmaschine demonstriert. Für Cloudflare besteht die Chance, als Default DNS-over-HTTPS Server für alle Firefox Nutzer millionenfach diese Daten zu sammeln, wenn sie die Bedenken der Privacy Community ausräumen können.
Aus technischer Sicht verwendet Oblivious DNS-over-HTTPS einfach Onion Routing mit nur einem Hop. Wenn die Betreiber der Hops nicht mit Cloudflare kooperieren, bleibt die Privatsphäre der Nutzer ähnlich gut geschützt, wie bei DoHoT mit wesentlich geringeren Einbußen bei der Performance.

Kann sein, dass ich mich täusche und ODoH ein neuer heißer Trend wird. Aber man muss nicht unbedingt Cloudflare DNS-Server nutzen. ;-)  

Hinweis für Wi-Fi Hotspots

Die Anmeldung für viele Wi-Fi Hotspots (zum Beispiel in Hotels, U-Bahn usw.) arbeitet in der Regel mit einer Manipulation des DNS für den Aufruf der Captive Portal Seite. Validierung mittels DNSSEC und Verschlüsselung mit DNScrypt, DNS-over-HTTPS oder DNS-over-TLS funktionieren daher an Wi-Fi Hotspots mit Login nicht.

Wer mit seinem Laptop einen Wi-Fi Hotspot nutzen möchte, muss den DNS-Server des Hotspot Betreibers verwenden und die lokale DNSSEC Validierung abschalten.


13.3 Vertrauenswürdige DNS-Server

Die meisten DNS-Server der Zugangs-Provider verwenden kein DNSSEC für die Validierung. Das könnte ein Grund (Sicherheit) für einen selbst gewählten DNS-Server sein.

Einige deutsche Kabelnetzprovider betreiben keine eigenen DNS-Server mehr sondern schicken ihre Kunden einfach zu Google-DNS (8.8.8.8) oder Cloudflare (1.1.1.1). Wenn man mit der Datenschutz Policy der Default DNS-Server der Provider nicht einverstanden ist, muss man sich auch selbst kümmern und die DNS-Server auf dem Router anpassen.

Das Sammeln, Auswerten und Verkaufen von DNS Daten der Kunden durch den Zugangsprovider ist in angelsächsischen Ländern üblich (USA, GB) aber in Deutschland nicht. Zensur durch DNS-Server spielt nach der Abwehr des ZugangsSchwG in Deutschland auch nur eine geringe Rolle, könnte in seltenen Fällen aber auch mal ein Grund sein.


Folgende DNS-Server mit No-Logging Policy, DNSSEC Validierung und Anti-Spoofing Schutz\(^1\) kann man als Alternative zu den Default DNS-Servern der Provider empfehlen:

- Freifunk München\(^2\) (normales DNS, DNS-over-TLS und DNS-over-HTTPS!)
  - IPv4: 5.1.66.255
  - IPv4: 185.150.99.255
  - IPv6: 2001:678:ed0:f000:: / dot.ffmuc.net

- Digitale Gesellschaft (CH)\(^3\) (Nur DNS-over-TLS und DNS-over-HTTPS!)

---

\(^1\)[https://www.grc.com/dns/dns.htm]
\(^2\)[https://ffmuc.net/wiki/doku.php?id=knb:dohdot]
\(^3\)[https://www.digitale-gesellschaft.ch/dns/]
KAPITEL 13. DOMAIN NAME SERVICE (DNS)

- IPv4: 185.95.218.42 / IPv6: 2a05:fc84::42 / dns.digitale-gesellschaft.ch
- IPv4: 185.95.218.43 / IPv6: 2a05:fc84::43 / dns.digitale-gesellschaft.ch

**Censurfridns Denmark** (aka. UncensoredDNS)
- IPv4: 91.239.100.100 / IPv6: 2001:67c:28a4::
- IPv4: 89.233.43.71 / IPv6: 2a01:3a0:53:53:: (mit DNS-over-TLS)

**Digitalcourage e.V.**
- IPv4: 5.9.164.112 / dns3.digitalcourage.de (nur für DNS-over-TLS!)

Die folgenden DNS-Server filtern Werbung, Tracking und Malware Domains. Alle drei Projekte werden von unabhängigen Einzelpersonen betrieben:

**dismail.de** (mit DNS-over-TLS)
- IPv4: 159.69.114.157 / IPv6: 2a01:4f8:c17:739a::2 / fdns2.dismail.de

**dnsforge.de** (mit DNS-over-TLS, DNS-over-HTTPS)
- IPv4: 176.9.93.198 / IPv6: 2a01:4f8:151:34aa::198 / dnsforge.de
- IPv4: 176.9.1.117 / IPv6: 2a01:4f8:141:316d::117 / dnsforge.de

**BlahDNS.com** (mit DNS-over-TLS, DNS-over-HTTPS, DNScrypt)
- Server DE: 78.46.244.143 / 2a01:4f8:c17:ec67::1 / dot-de.blahdns.com
- Server FI: 95.216.212.177 / 2a01:4f9:c010:43cc::1 / dot-fi.blahdns.com


### 13.4 DNS-Server der Big Player der IT Branche

Daneben gibt es einige kommerzielle DNS-Dienste von den Big Playern der IT-Branche, die damit werben, die länderspezifische Zensur von Zugangsprovider, wie es beispielsweise in der Türkei üblich ist, zu umgehen. Ein paar kleine Kommentare zu diesen Angeboten:

- Der Klassiker ist Google DNS. Google verspricht, dass die DNS-Server unter den IP-Adressen 8.8.8.8 und 8.8.4.4 nicht kompromittiert oder zensiert werden und bemüht sich erfolgreich um schnelle DNS-Antworten.


---

4[http://blog.uncensoreddns.org](http://blog.uncensoreddns.org)
5[https://digitalcourage.de/support/zensurfreier-dns-server](https://digitalcourage.de/support/zensurfreier-dns-server)
6[https://dismail.de/info.html](https://dismail.de/info.html)
7[https://dnsforge.de/](https://dnsforge.de/)
8[https://blahdns.com](https://blahdns.com)
9[https://policies.google.com/privacy?hl=de&gl=de](https://policies.google.com/privacy?hl=de&gl=de)
13.5. KONFIGURATION DER DNS-SERVER

kaum jemand leisten kann, die Wirtschaftsmacht Google zu blockieren. Damit wird auch die Sperrung alternativer DNS-Server deutlich erschwert, wie es in Deutschland im Rahmen des ZugErschwG geplant war.

- Quad9 mit Hauptsitz in der Schweiz ist technisch mit Google-DNS vergleichbar. Unter einheitlichen IP-Adressen stehen 100-200 DNS-Server zur Verfügung:

  Primary DNS:  9.9.9.9 / 2620:fe::fe / dns.quad9.net
  Secondary DNS: 149.112.112.112 / 2620:fe::9 / dns.quad9.net

Das Projekt verfolgt aber andere Ziele. Quad9 ist für die Anforderungen von Unternehmen optimiert. Im Vordergrund steht IT-Sicherheit. Durch die Verwendung von zeitnah aktualisierten Blocklisten sollen die Auswirkungen von Malware- und Phishing Kampagnen minimiert werden. Ein (temporäres) Overblocking ist nicht gewünscht, wird aber zugunsten der Sicherheit von Quad9 nicht ausgeschlossen.

Dafür arbeitet Quad9 mit 18+ Cyber Thread Intelligence Providern zusammen. Deren Erkenntnisse über Cyber-Angriffe werden gesammelt, um die Abwehr von kriminellen Angriffen und Wirtschaftsspionage auf DNS-Ebene zu konsolidieren. Im Gegenzug erhalten die Thread Intelligence Provider Zugriff auf den (anonymisierten) DNS-Traffic bei einem Angriff, um die Analyse zu beschleunigen.

Die Anforderungen privater Anwender an Privatsphäre und Zensurfreiheit spielen nur eine untergeordnete Rolle. Trotzdem sind auch private Anwender eingeladen, den Dienst zu nutzen. DNSSEC ist bei Quad9 Standard und außerdem sind DNS-over-TLS sowie DNS-over-HTTPS und (testweise) DNScrypt nutzbar.

- Am 01. April 2018 hat Cloudflare einen ähnlichen DNS Dienst gestartet. Unter den IP-Adressen 1.1.1.1 und 1.0.0.1 stehen weltweite sehr schnelle DNS-Server bereit, die hinsichtlich Geschwindigkeit Google DNS und Quad9 übertreffen.10

Privacy ist ein wichtiges Verkaufsargument und deshalb schwört auch Cloudflare, die Privatsphäre der Nutzer zu respektieren. Das Privacy Statement klingt sehr über spezifisch: Man wird keine Daten verkaufen, die IP-Adressen der Nutzer nicht auf die Festplatte schreiben und Logdaten max. 24h behalten. Cloudflare wird aber auswerten, welche Domains gesucht wurden und darauf aufbauend Analysen durchführen, die viel Geld wert sind, wenn große Mengen an Daten einfließen, die für die weltweite Internetnutzung repräsentativ sind.

Cloudflare behauptet nicht, das der DNS Service zensurfrei ist. Im Blog Artikel wird darauf hingewiesen, dass man mit den DNS-Servers via DoT oder DoH die länderspezifischen Sperren wie z. B in der Türkei umgehen kann, aber man kann davon ausgehen, das Cloudflare die Anforderungen der US-Administration umsetzen wird. DNSSEC ist aktiv, außerdem ist DNS-over-TLS und DNS-over-HTTPS nutzbar.

13.5 Konfiguration der DNS-Server

Für die Konfiguration der DNS-Server gibt es mehrere Möglichkeiten mit unterschiedlichen Vor- und Nachteilen.

DNS-Server auf dem Router konfigurieren

Die bevorzugten DNS-Server könnte man im eigenen LAN im Router konfigurieren, indem man auf der Konfigurationsseite für die Verbindung zum Internet Provider die bevorzugten DNS-Server eingibt.

Vorteil: via DHCP werden diese DNS-Server automatisch an alle Rechner im LAN und WLAN verteilt, sobald sie sich neu mit dem Router verbinden. Es sind keine weiteren

---

10 https://1.1.1.1/de/
Konfigurationen an Rechnern oder Smartphones nötig.

Nachteil: Router unterstützen in der Regel kein DNS-over-TLS, DNS-over-HTTPS oder DNScrypt um sicherzustellen, dass man wirklich mit dem gewünschten DNS-Server verbunden ist. Lediglich die Fritz!OS Version 7.20+ kann DNS-over-TLS.

Aber: mit der Fritz!Box Software 7.20 und 7.21 gibt es aufgrund von Bugs Probleme, wenn DNS-over-TLS verwendet wird. Der AVM Support schreibt:

*Mit FRITZ!OS 7.20 bzw. 7.21 kann es zu einem Problem mit der Funktion DNS over TLS (DoT) kommen.*

*Die Internetverbindung selbst wird von der FRITZ!Box zwar hergestellt, Internetseiten oder andere Ziele können jedoch nicht dargestellt oder erreicht werden, wenn diese DNS-over-TLS aktiv ist.*

*Es hat sich herausgestellt, dass die Funktion durch einen Neustart der FRITZ!Box wieder hergestellt werden kann, jedoch tritt das Verhalten nach unbestimmter Zeit wieder erneut auf, ein weiterer Neustart wäre dann wieder nötig.*

*Wir empfehlen, bis zum Erscheinen des Fixes die Funktion nicht zu nutzen.*

DNS-Server in den Netzwerkeinstellungen konfigurieren

Alternativ kann man die DNS-Server auf jedem Computer einzeln in den Einstellungen für die Netzwerkverbindung im Betriebssystem des PCs oder Laptops konfigurieren.

Unter Linux kann man z. B. mit dem NetworkManager Applet für jede Verbindung einzeln konfigurieren, welche DNS-Server verwendet werden sollen. Wenn man öfters mit dem Laptop unterwegs ist, kann man also im eigenen LAN zuhause andere Einstellungen nutzen als in bekannten WLANs oder bei Wi-Fi Hotspots, wo man den DNS-Server des Hotspot Betreibers nutzen muss, um die Captive Portalseite aufrufen zu können.

In dem Applet in der Taskleiste des Desktop wählt man den Menüpunkt *Verbindungen bearbeiten*. In dem sich öffnenden Fenster kann man für jede Internet-Verbindung (LAN, WLAN...) die DNS-Server konfigurieren. Der NetworkManager kümmert sich dann darum, dass die gewünschten Einstellungen beim Herstellen der Internetverbindung aktiviert werden. (Ist ein umständlich bei neuen WLANs, funktioniert aber.)

Die Einstellungen sind auf den Reitern IPv4 UND IPv6 anzupassen! Für IPv6 muss man keine DNS-Server konfigurieren, kann man aber machen. Es reicht, die Methode der Konfiguration auf Automatisch (DHCP), nur Adressen zu setzen. Für IPv4 muss man die Methode der Konfiguration auf Automatisch (DHCP), nur Adressen setzen und 2-3 DNS-Server eintragen. (Bild 13.1)

Verschlüsseltes DNS nutzen

Wenn man DNS-over-TLS, DNS-over-HTTPS oder DNScrypt einsetzen möchte, muss man einen DNS Daemon lokal auf dem Rechner installieren bzw. konfigurieren, der als DNS-Proxy agiert und den DNS-Traffic zum Upstream Server verschlüsselt.

**Windows** unterstützt in der Standardinstallation noch kein verschlüsseltes DNS. Interessierte Nutzer können den *Simple DNSCrypt Daemon* verwenden.\(^{11}\)


\(^{11}\)https://simplednscrypt.org
13.5. KONFIGURATION DER DNS-SERVER

Abbildung 13.1: Konfiguration der DNS-Server im NetworkManager (Linux)

**Linux** Distributionen verwenden überwiegend `systemd-resolve` für die DNS Namensauflösung, systemd Version > 245.2-1 (Ubuntu 20.04+, Fedora 32+) beherrscht DNS-over-TLS und man kann es aktivieren, indem man eine Datei `upstream.conf` im Verzeichnis `/etc/systemd/resolved.conf.d/` speichert. Ein Beispiel für die Quad9 Server:

```
[Resolve]
DNS=9.9.9.9#dns.quad9.net
DNS=149.112.112.112#dns.quad9.net
DNSOverTLS=yes
```

Es können mehrere DNS-Server angegeben werden. Die Adresse eines Servers besteht aus der IP und dem Namen des Servers für die TLS Authentifizierung.

Außerdem darf sich der NetworkManager nicht in die Konfiguration der DNS Server einmischen! Dafür speichert man eine Konfigurationsdatei `nodns.conf` im Verzeichnis `/etc/NetworkManager/conf.d/` mit folgendem Inhalt:

```
[main]
dns=none
systemd-resolved=false
```

Hinweis: diese Konfiguration ist nicht für Road Warrior geeignet, die unterwegs WiFi Hotspots mit Login Webseite in Hotels oder am Flughafen nutzen wollen.

**Android** Smartphones können DNS-over-TLS out-of-the-box. Die Option heißt *Privates DNS* und verbirgt sich in den erweiterten Einstellungen für *Netzwerk & Internet*. Hier kann man den Namen des gewünschten DoT-Servers eintragen (Abb. 13.2).

Die initiale Ermittlung der IP-Adresse des DNS-over-TLS Servers erfolgt mit dem Standard-Resolver, danach wird auf DNS-over-TLS umgeschaltet.

Mit dieser Methode lässt sich auch ein Trackingblocker für Android realisieren, indem man einen DNS Server mit Werbe- und Trackingfilter auswählt.
Abbildung 13.2: Android: DNS-over-TLS aktivieren


Kapitel 14

Daten verschlüsseln

Dass die Verschlüsselung von Daten der Erhaltung der Privatsphäre dient, bemerkt man spätestens, wenn ein USB-Stick verloren geht. Wird ein Laptop gestohlen, möchte man die Fotosammlung sicher nicht im Internet sehen.


Als Whistleblower sind besondere Anforderungen an die Datensicherheit zu stellen. Neben der sicheren Aufbewahrung kommt es auch darauf an, keine Spuren auf den Rechnern zu hinterlassen. Im Fall Bradley Mannings konnten Forensiker viele Daten wiederherstellen.

Die kurzen Beispiele zeigen, dass unterschiedliche Anforderungen an eine Verschlüsselung bestehen können. Bevor man wild anfängt, alles irgendwie zu verschlüsseln, sollte man sich Gedanken über die Bedrohung machen, gegen die man sich schützen will:

1. **Schutz sensibler Daten** wie z. B. Passwortlisten, Revocation Certificates o.ä. erfordert die Speicherung in einem Container oder verschlüsselten Archiv, welches auch im normalen Betrieb geschlossen ist.

2. **Schutz aller persönlichen Daten** bei Verlust oder Diebstahl von Laptop oder USB-Stick erfordert eine Software, die transparent arbeitet ohne den Nutzer zu behindern und bei korrekter Anmeldung möglichst automatisch den Daten-Container öffnet (beispielsweise Veracrypt für Windows/linux oder dm-crypt für Linux).

3. **Backups auf externen Medien** enthalten in der Regel die wichtigen privaten Daten und sollten ebenfalls verschlüsselt sein. Dabei sollte die Wiederherstellung auch bei totalem Datenverlust möglich sein. Es ist nicht sinnvoll, die Daten mit einem PGP-Schlüssel zu chiffrieren, der nach einem Crash nicht mehr verfügbar ist.


5. Wer eine **Manipulation der Systemdaten** befürchtet, kann seinen Rechner komplett verschlüsseln (z. B. mit dm-crypt für Linux).

6. **SDSRDDs** kann man nutzen, wenn Sicherheit absolute Priorität hat, Geld keine Rolle spielt und man sich nicht auf eine Softwarelösung verlassen möchte. SDSRDDs sind
SSD Festplatten mit integrierter Verschlüsselung, Token-Authentifizierung (also nicht mit Keyloggern angreifbar) und eingebautem Mechanismus zur Selbstzertörung, der remote via SMS oder bei unerlaubten Zugriff ausgelöst werden kann.

14.1 Konzepte der vorgestellten Tools

Um die vorgestellten Tools sinnvoll einzusetzen, ist es nötig, die unterschiedlichen Konzepte zu verstehen.


Cryptomator, Boxcryptor arbeiten Verzeichnis-basiert. Es gibt zwei Verzeichnisse:

1. Das Verzeichnis A mit den verschlüsselten Daten wird auf den Datenträger geschrieben bzw. in die Cloud synchronisiert.
2. Ein zweites Verzeichnis B oder ein virtuelles Laufwerk bietet den transparenten Zugriff auf die entschlüsselten Daten.

Veracrypt, dm-crypt arbeiten Container-basiert. Es ist zuerst ein verschlüsselter Container fester Größe zu erstellen, der dann wie ein Datenträger in das Dateisystem eingebunden werden kann. Als Container können komplette USB-Sticks, ganze Partitionen der Festplatte oder (große) Dateien genutzt werden.


Veracrypt - mit doppeltem Boden

Veracrypt ist ein Nachfolger des legendären Truecrypt. Es beseitigt einige Schwächen, die bei einem Audit von Truecrypt aufgedeckt wurden und wird als Open Source weiterentwickelt. Mit mit zuluCrypt gibt es eine 100% kompatible Linux Software.


Während ein einfacher Container leicht als verschlüsselter Bereich erkennbar ist, kann der doppelte Boden innerhalb eines Containers ohne Kenntnis des zweiten Schlüssels nicht nachgewiesen werden. Ist man zur Herausgabe der Schlüssel gezwungen, kann man versuchen, nur den Schlüssel für den äußeren Container auszuhändigen und die Existenz

1https://www.veracrypt.fr/en/Home.html
2https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf
14.2 Gedanken zur Passphrase


1. Bei der Initialisierung wird eine kleine Menge von zufälligen Zufallszahlen generiert, die als Schlüssel für die symmetrische Verschlüsselung mit AES256-XTS o.ä. dient.

2. Dieser Schlüssel aus zufälligen Zufallszahlen wird mit einer Passphrase verschlüsselt und im Header der verschlüsselten Daten gespeichert.

3. Beim Zugriff auf die Daten wird zuerst der Schlüssel aus Zufallszahlen mit der Passphrase entschlüsselt und danach für den Zugriff auf die Daten genutzt.

Es ist nach derzeitigem Stand der zivilen Kryptoanalyse unmöglich, die symmetrische Verschlüsselung wie AES-XTS oder Twofisch oder... mit mathematischen Methoden zu knacken, wenn hinreichend zufällige Zufallszahlen als Schlüssel verwendet werden.

Alle bekannten Angriffe auf moderne Datenverschlüsselungen konzentrieren sich darauf, die Passphrase zu erraten, um damit Zugriff auf den Schlüssel für die symmetrische Verschlüsselung zu bekommen und somit die geschützten Daten lesen zu können.

Die Stärke und Länge der Passphrase ist somit der entscheidende Faktor für die Sicherheit der Datenverschlüsselung und gleichzeitig auch oft das schwächste Glied in der Kette. Eine Passphrase, welche die gleiche Stärke gegen Brute-Force Angriffe wie AES128 hätte, müsste beispiw. aus mindestens 12 zufälligen generierten Wörtern bestehen (Diceware):

"stuff plastic young air easy husband exact install web stick hurt embody"

Das ist schon etwas kompliziert zu merken und in der täglichen Benutzung ganz schön umständlich. In der Regel werden die meisten Anwender einfachere Passphrasen wählen und damit ist die Passphrase der schwächsten Punkt der Verschlüsselung.

Wie findet man eine ausreichend starke Passphrase?

Ein 6-stelliges Passwort zu knacken, kostet 0,10 Euro. Eine 8-stellige Kombination hat man mit 300 Euro wahrscheinlich und mit weniger als 800 Euro sicher geknackt. Um eine 15-stellige Kombination aus zufälligen Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen oder eine Diceware Passphrase aus 6 Wörtern mit 50% Wahrscheinlichkeit zu knacken, würden auch die Computer der NSA viele Jahre benötigen.

Für eine gute Passphrase sollte man mindestens 12 zufällige Zeichen verwenden (Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen) oder eine Diceware Passphrase mit mindestens 5 Wörtern. Für eine gute Passphrase sind mind. 65 Bit Entropie nötig.

- Passwortspeicher wie KeepasXC enthalten einen Generator für wirklich zufällige Zeichenkombinationen oder auch Diceware Passphrasen.
Ein Passwortspeicher wie KeepassXC o.ä. ist aber evtl. nicht immer verfügbar, wenn man Zugriff auf Datenträger braucht (sollte man bedenken).

- Ein memorierbares Passwortsystem hat den Vorteil, dass man nicht von Tools abhängig ist und bei einem Crash des Computers kein aktuelles Backup braucht.

Die **Akronym-Methode** verwendet die Anfangsbuchstaben der Wörter von einem leicht merkbaren Satz ableiten und den variablen Anteil aus der Verwendung:

- Merksatz: *Die Sonne schien am ganzen Sonntag nur für uns.*
- Passwort für USB-Sticks: *DSsgSn4u-STICK*
- Passwort für Systemplatte: *DSsgaSn4u-BOOT*

Die **Collage-Methode** verwendet ein Wort in mehreren Übersetzungen und lässt die Vokale weg. Variable Anhängsel sind ebenfalls möglich:

- Ergebnis: *Result=42* könnte folgendes Passwort ergeben: *rgbns:Rslt=42*
- *Pferd?Horse!Cheval* könnte folgendes Passwort ergeben: *Pfrd?Hrs!Chvl*

- Beim **Diceware** Verfahren werden zufällige Kombinationen aus Wörtern aus einer Liste verwendet statt zufälliger Zeichenkombinationen. Wortkombinationen kann man sich leichter merken als sinnlose Zeichenkombinationen.

Für den klassischen Weg zur Erstellung einer Diceware Passphrase benötigt man eine Wortliste (beispw. die *DeReKo Liste* mit den häufigsten deutschen Wörtern laut Leibnitz Institut) und einen Würfel. Für jedes Wort würfelt man 5x und erhält damit einen Zahlenkombination. Diese Zahlenkombination sucht man in der Wortliste und wiederholt den Vorgang für 5-7 Wörter.

```
26431 gebilde
53612 schmal
42221 macht
66123 zauber
34641 karwoche
```

Ein Sonderzeichen zur Worttrennung kann man sich aussuchen. Und die gewürfelte Diceware Passphrase ist dann: *gebilde-schmal-macht-zauber-karwoche*.

Wenn man keine Würfel im Haushalt findet, könnte man auch Online würfeln.

- Beim **Challenge-Response** Verfahren mit Yubikeys wird ein simples, einfaches Passwort an den Yubikey geschickt (Challenge), der mit HMAC-SHA ein starkes Passwort ableitet (Response), das für den Zugriff auf den Schlüssel für die symmetrische Verschlüsselung verwendet wird.

Challenge-Response mit Yubikeys muss von der Software unterstützt werden:

- KeepassXC Datenbanken für Passwörter können damit geschützt werden.
- dmcrypt/LUKS bietet Unterstützung für Challenge-Response mit Yubikeys.

Um den Yubikey für Challenge-Response vorzubereiten, ist die nötige Software zu installieren. Linuxer finden das Yubico Personalisation Tool in den Repositoroes:

```
> sudo apt install yubikey-personalisation
```

Dann wird der zweite PW-Slot des Yubikey für den Challenge-Response initialisiert:

```
> ykpersonalize -2 -ochal-resp -ochal-hmac -ohmac-lt64 -oserial-api-visible
```

---

3 https://www.privacy-handbuch.de/download/diceware-dereko.txt
4 https://online-wuerfel.de/5-wuerfel
14.2. GEDANKEN ZUR PASSPHRASE

Herausgabe von Passwörtern an Strafverfolgungsbehörden

Zur Herausgabe von Passwörtern im Fall einer Beschlagnahme des Rechners oder eines verschlüsselten Datenträgers gibt es immer wieder Missverständnisse. In Deutschland geltenden folgenden gesetzlichen Regelungen:

- Richten sich die Ermittlungen gegen den Besitzer des Rechners oder Datenträgers, muss man keine Passwörter herausgeben, da man sich selbst nicht belasten muss.

- Richten sich die Ermittlungen gegen Dritte, ist man als Zeuge zur Herausgabe von Schlüsseln und Passwörtern zur Unterstützung der Strafverfolgung verpflichtet.

Es gibt nur zwei Ausnahmen:

1. Man kann sich auf das Recht zur Zeugnisverweigerung berufen, um Verwandte ersten Grades nicht belasten zu müssen.

2. Man kann oder glaubhaft(!) versichert, dass man sich selbst belasten würde.

Im Zweifel sollte man einen Anwalt konsultieren, wenn man in dieser Situation ist.


Bei Einreise in die USA sind die Grenzbehörden berechtigt, elektronische Geräte (Laptops und Smartphones) zu durchsuchen. Eine Herausgabe von Passwörtern kann ohne Durchsuchungsbeschluss nicht erzwungen werden, aber die Behörden können das Gerät zur weiteren Untersuchung einziehen, wenn man das Passwort nicht herausgeben will. Die EFF.org rät, mit einer leeren, unverschlüsselten Festplatte einzureisen und ein datenloses Handy zu nutzen.⁶

Den Polizeibehörden ist bekannt, dass es starke Verschlüsselung für Festplatten gibt, die im ausgeschalteten Zustand nicht geknackt werden kann. Deshalb sind die Festnahme Spezialisten des SEK u.ä. darin geschult, bei einer Festnahme (Polizei-Sprech: Zugriff) die Computer im eingeschalteten Zustand zu übernehmen und ein Backup der unverschlüsselten Daten anzufertigen.

- Ross Ulbricht (der Betreiber von Silk Road 2.0) wurde festgenommen, während er seinen Tor Hidden Service administrierte. Das FBI konnte den eingeschalten Laptop übernehmen und als Beweis die aktiven Login-Sessions auf den Servern des Drogenhandelsplatzes sicherstellen. Das war sicher kein Zufall sondern beabsichtigt.

- Der deutsche Betreiber eines illegalen Waffenhandels im Deep Web konnte bei der Festnahme mit dem Fuß das Stromkabel aus seinem batterielosen Laptop reißen und die Verschlüsselung damit aktivieren. Das SEK hatte aber zweifellos den Auftrag, bei der Festnahme den Laptop im eingeschalteten Zustand sicherzustellen.⁷

---

⁵[http://www.heise.de/newsticker/meldung/99313](http://www.heise.de/newsticker/meldung/99313)
14.3 Dokumente verschlüsselt speichern

Es gibt mehrere Anwendungen, die Dokumente verschlüsselt speichern können. Das Öffnen der Dokumente ist dann nur möglich, wenn das notwendige Passwort angegeben wird. Die verschlüsselte Speicherung ist bei vertraulichen Daten sinnvoll wie Steuererklärungen, Mitgliederlisten für politisch aktive Vereine... usw.


LibreOffice Dokumente verschlüsselt speichern

LibreOffice bietet die Möglichkeit, Dokumente mit AES256 verschlüsselt zu speichern, indem man beim Speichern die Option *Mit Kennwort speichern* aktiviert. Außerdem können die Dokumente mit OpenPGP verschlüsselt gespeichert werden (Abb. 14.1).

![Abbildung 14.1: Verschlüsselte Speicherung in LibreOffice aktivieren](image)

Im folgenden Dialog kann man den/die OpenPGP Schlüssel auswählen oder ein Kennwort für das Öffnen der verschlüsselten Datei festlegen. Um keine Spuren auf der Festplatte zu hinterlassen, sollte man den Schutz aktivieren, bevor das Dokument erstmalig gespeichert wird und bevor sensitive Daten in das Dokument geschrieben werden.

**PDF Dokumente**

Der PDF-Standard definiert ein Berechtigungsmodell, das auch die verschlüsselte Speicherung von Dokumenten ermöglicht. Dieser Standard ist aber *Broken by Design*. Ein Angreifer kann das PDF Dokument modifizieren, so dass ihm beim Öffnen des Dokumentes der vertrauliche Inhalt via Internet zugesendet wird.\(^8\)

\[\text{We analyze the security of encrypted PDF and show how an attacker can exfiltrate the content without having the corresponding keys.}\]

Die kryptografischen Signaturen im PDF Standard sind ebenfalls kaputt by Design.

\(^8\)https://www.pdf-insecurity.org/
14.4 Quick and Dirty mit GnuPG

Eine Möglichkeit ist die Verschlüsselung einzelner Dateien oder Verzeichnisse mit GnuPG. Die grafischen Tools GPA (GNU Privacy Assistant) oder Kleopatra bieten dafür im Menü den Punkt Datei - Datei verschlüsseln/signieren und Datei - Datei entschlüsseln/prüfen.

Noch einfach geht es, wenn man im bevorzugten Dateimanager mit der rechten Maustaste auf eine Datei klickt und in dem Kontextmenü den Punkt Datei verschlüsseln wählt. Es startet ein Assistent, der durch die Auswahl der Schlüssel usw. führt.

Abbildung 14.2: Kleopatra GnuPG GUI: Assistent zur Verschlüsselung von Dateien


Sollen mehrere Dateien in einem Container verschlüsselt werden, erstellt man ein Verzeichnis und kopiert die Dateien dort hinein. Anschließend verpackt man dieses Verzeichnis mit WinZip, 7zip o.ä. in einem Archiv und verschlüsselt dieses Archiv.

Zum Entschlüsseln reicht in der Regel ein Klick (oder Doppelklick) auf die verschlüsselte Datei. Nach Abfrage der Passphrase für den Schlüssel liegt das entschlüsselte Orginal wieder auf der Platte.

GnuPG für WINDOWS

Diese simple Verschlüsselung klappt allerdings unter WINDOWS nicht auf Anhieb. Es ist zuerst das Programmpaket gpg4win⁹ zu installieren.

⁹https://www.gpg4win.org
KAPITEL 14. DATEN VERSCHLÜSSELN

14.5 dm-crypt/LUKS für Linux

dm-crypt/LUKS ist fester Bestandteil des Linux-Kernels und in allen Linux Distributionen gut integriert. Die Verschlüsselung wird auch von Regierungen und Geheimdiensten zum Schutz vertauerlicher und geheimer Daten eingesetzt. dm-crypt/LUKS ist FIPS-2 zertifiziert, wird vom BSI regelmäßig evaluiert und ist in Deutschland bis VS-GEHEIM zugelassen (allerdings ab VS-NfD nur mit Smartcards als Zugriffsschutz und nicht mit Passwormern).

dm-crypt/LUKS verschlüsselt Blockdevices (Festplattenpartitionen, USB-Sticks oder Imagedateien) und arbeitet vollständig transparent. Es können bis zu 8 unterschiedliche Passphrasen + Schlüsseldateien als Credentials für den Zugriff auf einen Container definiert werden. Außerdem können Veracrypt Container geöffnet werden.


Abbildung 14.3: Datenträger verschlüsseln unter Linux

Im nächsten Schritt wird man nach der Passphrase gefragt, die man wie üblich 2x eingeben muss. Diese Passphrase wird im Slot 0 im LUKS Header gespeichert. Die Verwendung von mehreren, unterschiedlichen Passphrasen oder Keyfiles als Schlüssel wird in dieser einfachen Variante für Mausschubser nicht unterstützt. Dafür muss man die Kommandozeile nutzen.

Wenn man den verschlüsselten USB-Stick am Linux Rechner anschließt, wird man nach der Passphrase für den Zugriff auf die Daten gefragt und der Datenträger wird geöffnet.

14.5.1 Linux System komplett verschlüsseln

Neben der einfachen Verschlüsselung von Datenträgern bieten alle Linux Distributionen bei der Installation die Möglichkeit, das komplette System mit Ausnahme der Boot-Partition zu verschlüsseln, wenn man die Festplatte komplett löscht und den Logical Volume Manager (LVM) für die neue Installation aktiviert. Für die Verschlüsselung des gesamten System mit dm-crypt/LUKS ist dann nur ein kleines Häckchen zu setzen.

Beim Linux Mint Installer findet man die Option in den Erweiterten Funktionen…. Bei anderen Linux Distributionen sieht es irgenwie ähnlich aus.
14.5.2 Für Genießer in der Konsole mit cryptsetup


```
# luksformat -t ext4 /dev/sdb1
```

Das ist alles. Der Vorgang dauert ein wenig und es wird 3x die Passphrase abgefragt. Ein Keyfile kann dieses Script nicht nutzen!

Am Beispiel einer verschlüsselten Containerdatei werden die einzelnen Schritte beschrieben, welche das Script <em>luksformat</em> aufruft. Soll eine Partition (Festplatte oder USB-Stick) verschlüsselt werden, entfallen die Schritte 1 und 8. Das als Beispiel genutzte Device /dev/loop5 ist durch die Partition zu ersetzen, beispielsweise /dev/hda5 oder /dev/sdb1.


```
# dd if=/dev/zero of=geheim.luks bs=1M count=100
# losetup -f /dev/loop0
# losetup /dev/loop0 geheim.luks
```

2. Die ersten 2 MByte sind mit Zufallswerten zu füllen. Das Füllen der gesamten Datei würde sehr lange dauern und ist nicht nötig:

```
# dd if=/dev/urandom of=/dev/loop0 bs=1M count=2
```

3. Anschließend erfolgt die LUKS-Formatierung mit der Festlegung der Verschlüsselung. Die Option <em>-y</em> veranlaßt eine doppelte Abfrage des Passwortes, das <em>keyfile</em> ist optional

```
```

Abbildung 14.4: Linux Mint bei der Installation komplett verschlüsseln
KAPITEL 14. DATEN VERSCHLÜSSELT

# cryptsetup luksFormat -c aes-xts-plain64 -s 256 -h sha512
   -y /dev/loop0 [ keyfile ]

4. Das verschlüsselte Device wird dem Device-Mapper unterstellt. Dabei wird das zu-
vor eingegebene Passwort abgefragt. Das Keyfile ist nur anzugeben, wenn es auch im
vorherigen Schritt verwendet wurde. Der <name> kann frei gewählt werden. Unter
/dev/mapper/<name> wird später auf den verschlüsselten Containern zugegriffen:

   # cryptsetup luksOpen /dev/loop0 <name> [ keyfile ]

5. Wer paranoid ist, kann das verschlüsselte Volume mit Zufallszahlen füllen. Der Vor-
gang kann in Abhängigkeit von der Größe der Containerdatei sehr lange dauern:

   # dd if=/dev/urandom of=/dev/mapper/<name>

6. Ein Dateisystem wird auf dem Volume angelegt:

   # mkfs.ext3 /dev/mapper/<name>

7. Das Volume ist nun vorbereitet und wird wieder geschlossen:

   # cryptsetup luksClose <name>

8. Die Containerdatei wird ausgehängt:

   # losetup -d /dev/loop0

Verschlüsselte Container öffnen/schließen

Um eine verschlüsselte Partition auf einem USB-Stick auf der Kommandozeile zu öffnen,
sind zwei Schritte als root nötig.

1. Im ersten Schritt wird das verschlüsselte Device dem Device-Mapper zu unterstellt.
Der name kann frei gewählt werden. Zusätzlich kann man ein Keyfile nutzen.

   > sudo cryptsetup open --type luks /dev/sdc1 <name> [keyfile]
   Enter LUKS passphrase:

2. Danach kann es mit mount in das Dateisystem eingehängt werden, z.B. nach /mnt.

   > sudo mount /dev/mapper/<name> /mnt

   Das Schließen des Containers erfolgt in umgekehrter Reihenfolge. Dabei werden alle
   Keys für den Zugriff auf den Container im Kernel sicher gelöscht (wipe).

   > sudo umount /mnt
   > sudo cryptsetup close <name>

   Das Öffnen einer Containerdatei auf der Kommandozeile erfordert drei Schritte als root.
Als erstes ist die verschlüsselte Imagedatei als Loop Device einhängen. Das Loop-Device
kann dann wie eine verschlüsselte Partition behandelt werden.

   > sudo losetup /dev/loop0 geheim.luks
   > sudo cryptsetup open --type luks /dev/loop0 <name> [keyfile]
   Enter LUKS passphrase:
   > sudo mount /dev/mapper/<name> /mnt

   Das Schließen des Containers erfolgt in umgekehrter Reihenfolge.
14.5. DM-CRYPT/LUKS FÜR LINUX

```bash
> sudo umount /mnt
> sudo cryptsetup close <name>
> sudo losetup -d /dev/loop0
```

cryptsetup kann auch Truecrypt und Veracrypt Container öffnen. Auf einem aktuellen Linux System muss man also keine zusätzliche Software installieren, wenn man gelegentlich Truecrypt/Veracrypt Container öffnen möchte. Eine Truecrypt verschlüsselte Partition auf dem USB-Stick öffnet man in zwei Schritten:

```bash
> sudo cryptsetup [Optionen] open --type tcrypt /dev/sdc1 <name>
Enter passphrase:
> sudo mount /dev/mapper/<name> /mnt
```

Als [Optionen] können zusätzlich folgende Parameter angegeben werden:

- -veracrypt verwendet man für Container im Veracrypt Format.
- -key-file kann man mehrfach nutzen, um Schlüsseldateien anzugeben.
- -tcrypt-hidden öffnet den Hidden Container im Truecrypt Volume.
- -tcrypt-system ist für Systempartitionen mit Boot Manager zu nutzen.
- -readonly muss man nicht erklären.

Wenn man eine Containerdatei öffnen möchte, dann ist die Datei zuerst als Loop Device einzuhängen. Das Loop-Device kann dann wie eine verschlüsselte Partition behandelt werden.

```bash
> sudo losetup /dev/loop1 geheim.tc
> sudo cryptsetup [Optionen] open --type tcrypt /dev/loop1 <name>
Enter passphrase:
> sudo mount /dev/mapper/<name> /mnt
```

Das Schließen des Container erfolgt wie oben bei LUKS.

Passwörter verwalten

Mit root-Rechten ist es möglich, bis zu 7 zusätzliche Passwörter für das Öffnen eines Containers festzulegen oder einzelne Passwörter wieder zu löschen.

Um die Passwörter einer verschlüsselten Imagedatei geheim.img zu verwalten, ist die Imagedatei zuerst als Loop-Device einzuhängen, beispielsweise als /dev/loop5. Dieser Schritt entfällt für verschlüsselte Partitionen:

```bash
# losetup /dev/loop5 geheim.luks
```

Das Hinzufügen eines Passwortes und damit eines neuen Keyslots erfolgt mit folgendem Kommando, wobei als <device> beispielsweise /dev/loop5 für die eingebundene Imagedatei oder /dev/sda5 für eine Festplattenpartition anzugeben ist. Das Keyfile ist optional. Mit der Option –key-slot wählt man einen bestimmten Slot von 0...7 aus.

```bash
# cryptsetup --key-slot <slot> luksAddKey <device> [ keyfile ]
```

Ein Keyslot und das zugehörige Passwort können mit folgendem Kommando wieder entfernt werden:

```bash
# cryptsetup luksKillSlot <device> <slot>
```

Als <slot> ist die Nummer des Keyslots anzugeben, eine Zahl von 0...7. Es ist also nötig, sich zu merken, welches Passwort auf welchen Keyslot gelegt wurde. Eine Übersicht, welche Keyslots belegt und welche noch frei sind, liefert luksDump:
KAPITEL 14. DATEN VERSCHLÜSSELN

# cryptsetup luksDump <device>
LUKS header information for <device>
...
Key Slot 0: DISABLED
Key Slot 1: ENABLED
   Iterations:
   Salt:

   Key material offset:
   AF stripes:
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED

Komfortabel beim Login

Mit Hilfe des Modules pam-mount ist es möglich, das Anmeldepasswort zu nutzen, um standardmäßig beim Login einen oder mehrere Container zu öffnen. Insbesondere für verschlüsselte /home Partitionen ist dies sinnvoll und komfortabel.

Folgende Konfigurationen sind für einen Crypto-Login anzupassen:

1. PAM-Konfiguration: Dem PAM-Dämon ist mitzuteilen, dass er das Modul `mount` zu verwenden hat und das Login-Passwort zu übergeben ist. Gut vorbereitete Distributionen wie Debian und aktuelle Ubuntu(s) benötigen nur einen Eintrag in den Dateien `/etc/pam.d/login`, `/etc/pam.d/kdm` und `/etc/pam.d/gdm`:

   @include common-pammount

2. pam-mount Modul: Das Modul wird konfiguriert in der XML-Datei `/etc/security/pam_mount.conf.xml`. Am Anfang der Datei findet man eine Section für Volumes, die beim Login geöffnet werden sollen. Im ersten Beispiel wird bei allen Logins die verschlüsselte Partition `/dev/hda4` als `/home` eingebunden:

   <volume fstype="crypt" path="/dev/hda4" mountpoint="/home" />

   Das zweite Beispiel zeigt die Einbindung einer verschlüsselten Containerdatei `/geheim.luks` als HOME für den User Pitschie. Die Containerdatei wird nur geöffnet, wenn Pitschie sich anmeldet.

   <volume user="pitschie" fstype="crypt" path="/geheim.luks"
       mountpoint="/home/pitschie" options="loop" />

3. fstab: Da beim Booten keine Partition nach `/home` gemountet werden soll, ist evtl. der entsprechende Eintrag in der Datei `/etc/fstab` zu löschen.

SWAP und `/tmp` verschlüsseln

Das `/tmp`-Verzeichnis und der SWAP Bereich können unter Umständen persönliche Informationen enthalten, die im Verlauf der Arbeit ausgelagert wurden. Wenn eine komplette Verschlüsselung des Systems nicht möglich ist, sollte man verhindern, dass lesbare Datenrückstände in diesen Bereichen verbleiben.

Das Verzeichnis `/tmp` kann man im RAM des Rechners ablegen, wenn dieser hinreichend groß dimensioniert ist. Mit dem Ausschalten des Rechners sind alle Daten verloren.
Um diese Variante zu realisieren bootet man den Rechner im abgesicherten Mode, beendet die grafische Oberfläche (X-Server) und löscht alle Dateien in /tmp. In der Datei /etc/fstab wird folgender Eintrag ergänzt:

```
tmpfs /tmp tmpfs nosuid,noexec 0 0
```

Die Bereiche SWAP und /tmp können im Bootprozess als verschlüsselte Partitionen mit einem zufälligen Passwort initialisiert und eingebunden werden. Mit dem Ausschalten des Rechners ist das Passwort verloren und ein Zugriff auf diese Daten nicht mehr möglich.

**Achtung:** Suspend-to-RAM und Suspend-to-Disk funktionieren mit einer verschlüsselten SWAP-Partition noch nicht.

**Debian GNU/Linux**

Debian und Ubuntu enthalten ein Init-Script, welches eine einfache Verschlüsselung von SWAP und /tmp ermöglicht, wenn diese auf einer eigenen Partition liegen.

In der Datei /etc/crypttab sind die folgenden Zeilen einzufügen, wobei /dev/hda5 und /dev/hda8 durch die jeweils genutzten Partitionen zu ersetzen sind:

```
cryptswp /dev/hda5 /dev/urandom swap
crypttmp /dev/hda8 /dev/urandom tmp
```

In der Datei /etc/fstab sind die Einträge für swap und /tmp anzupassen:

```
/dev/mapper/cryptswp none swap sw 0 0
/dev/mapper/crypttmp /tmp ext2 defaults 0 0
```

Anschließend ist der Rechner neu zu booten und beide Partitionen sind verschlüsselt.

**Achtung:** Die Partition für /tmp darf kein Dateisystem enthalten! Soll eine bereits verwendete /tmp-Partition verschlüsselt werden, ist diese erst einmal nach dem Beenden des X-Servers(!) zu dismounten und zu überschreiben:

```
# umount /tmp
# dd if=/dev/zero of=/dev/hda8
```

### 14.5.3 Hardware Token verwenden (Nitrokey, Yubikey)

Die Passphrase ist der schwächste Punkt bei der Verwendung moderner Verfahren zur Verschlüsselung von Datenträgern, insbesondere wenn man im täglichen Gebrauch einfach zu merkende Passphrasen geringer Komplexität bevorzugt.

Im folgenden werden einige Möglichkeiten vorgestellt, die Sicherheit der Verschlüsselung durch Verwendung von Hardware Token (Nitrokey, Yubikey, USB-Stick) zu verbessern. Bei allen Varianten ist folgendes Grundkonzept empfehlenswert:

1. Es wird ein verschlüsselter Container erstellt (Festplattenpartition, USB-Stick, Containerdatei). Dabei wird eine echt knackige, komplexe Passphrase verwendet, die einem Brute-Force Angriff hochpotenter Angreifer mehrere Jahre standhält.

   Diese Passphrase benötigt man im nächsten Schritt zum Hinzufügen von Hardware Token und sie dient als Backup zum Öffnen des Containers, wenn das HW Token verloren geht. Sie wird off site in einem Tresor hinterlegt (digital oder auf Papier).


3. Wenn man zwei oder mehr HW Token zum Öffnen des Container definiert hat (mind. ein Backup Token!), könnte man die initiale Passphrase im Keyslot 0 auch löschen:

   ```bash
   > cryptsetup luksKillSlot <device> 0
   ```
**Variante A: LUKS mit Nitrokey**

Der Nitrokey ist eine GnuPG Smartcard im Format eines USB-Sticks. Es können natürlich auch andere GnuPG Smartcards wie Yubikey oder GnuK verwendet werden.

Die Idee ist einfach erklärt: Es wird die Keyfile für das Öffnen des LUKS Containers verwendet, das mit dem OpenPGP Key des Nitrokey verschlüsselt wurde. Zum Öffnen des Containers wird das Keyfile mit gpg2 entschlüsselt und via Pipe an cryptsetup übergeben. Eine kurze Anleitung, die sich auf das Wesentliche beschränkt:

1. Ein frischer Nitrokey ist erstmal einzurichten (Schlüssel erzeugen, PIN ändern usw.)
2. Da die folgenden Operationen als root durchgeführt werden, ist der OpenPGP Schlüssel des Nitrokey zu exportieren und im Schlüsselring von root zu importieren. Außerdem ist ein re-bind des privaten Schlüssel der Nitrokey Smartcard anzustoßen:
   
   ```
   > gpg2 --export "User-ID" > /tmp/luks-pgp-key.pgp
   > sudo gpg2 --import /tmp/luks-pgp-key.pgp
   > sudo gpg2 --card-status
   > rm /tmp/luks-pgp-key.pgp
   ```
3. Es wird ein Keyfile mit Zufallszahlen erzeugt (z. B. `/root/.gnupg/luks-key.bin`):

   ```
   > sudo dd if=/dev/urandom of=/root/.gnupg/luks-key.bin bs=512 count=8
   ```
4. Das Keyfile wird als Schlüssel für den Container in nächsten freien Keyslot eingefügt. Es wird dabei eine gültige Passphrase für das Öffnen des Containers abgefragt:

   ```
   > sudo cryptsetup luksAddKey <device> /root/.gnupg/luks-key.bin
   ```
5. Das Keyfile wird mit GnuPG verschlüsselt und das Orginal sicher gelöscht:

   ```
   > sudo gpg2 --encrypt --recipient /root/.gnupg/luks-key.bin
   > sudo shred -u /root/.gnupg/luks-key.bin
   ```
6. Zum Öffnen des Container werden folgende Kommandos verwendet, die man sich als Script ablegen kann. `<device>` und `<mount-point>` sind anzupassen. `<name>` kann beliebig gewählt werden und dient nur zur Identifikation im Devicemapper:

   ```
   > sudo su
   # gpg2 --decrypt /root/.gnupg/luks-key.bin.gpg | cryptsetup open <device> <name>
   # mount /dev/mapper/<name> <mount-point>
   # exit
   ```

   Mit KDialog oder Zenity könnte man das Script grafisch aufpeppen und einen Starter auf den Desktop legen. Kreativität und Spieltrieb sind dabei keine Grenzen gesetzt. Wenn man das grafisch aufgepeppte Script ohne ein Terminal im Hintergrund nutzen möchte, dann muss man die Option `--no-tty` bei dem gpg2 Kommando hinzufügen:

   ```
   > gpg2 --no-tty --decrypt /root/.gnupg/luks-key.bin.gpg | cryptsetup ...
   ```

**Full Disc Encryption:** Wenn man bei der Installation das System vollständig verschlüsselt hat, kann man den Nitrokey auch zum Öffnen des Root-Containers beim Booten verwenden. Die Firma Purism stellt ein Script bereit, das alle notwendigen Schritte automatisiert. Man muss nur das Script `smartcard-key-luks` herunter laden, den public Key als Datei bereitstellen, das Script aufrufen und danach den Rechner neu starten:
14.5. DM-CRYPT/LUKS FÜR LINUX

> gpg2 --armor --export "User-ID" > pub-key-fuer-luks.asc

> sudo install -d /usr/local/sbin (falls das Verzeichnis noch nicht existiert)

> sudo wget -o /usr/local/sbin/smartcard-key-luks https://source.puri.sm/pureos/packages/smartcard-key-luks/-/raw/master/smartcard-key-luks

> sudo chmod +x /usr/local/sbin/smartcard-key-luks

> sudo smartcard-key-luks pub-key-fuer-luks.asc

Reboot - Fertig!

Für Arch Linux User gibt es die Alternative *initramfs-sencrypt* bei Github.com.¹⁰

**Variante B: LUKS mit Yubikey**

Die Firma Yubico bietet mit *yubikey-luks* eine Software zur Nutzung ihrer Yubikeys als Schlüssel für einen LUKS Container, die mit einem Challenge-Response Verfahren arbeitet.


1. Die Software kann mit dem bevorzugten Paketmanager installiert werden:

   > sudo apt install yubikey-luks yubikey-personalisation

2. Der zweite PW-Slot des Yubikey wird für Challenge-Response vorbereitet:

   > ykpersonalize -2 -ochal-resp -ochal-hmac -ohmac-lt64 -oserial-api-visible

3. Das Challenge-Response Passwort wird in einen freien Keyslot des LUKS Containers eingetragen. Es gibt ein Script, dass die Aufgabe übernimmt. Es wird dabei 2x das neue Challenge Passwort für den Yubikey und eine gültige Passphrase für das Öffnen des LUKS Containers abgefragt:

   > sudo yubikey-luks-enroll -d <device> -s <key-slot>

Falls man den Überblick verloren hat, welche Keyslots im LUKS Container noch frei sind, kann man sich die Belegung mit folgendem Kommando anzeigen lassen:

   > sudo cryptsetup luksDump
   LUKS header information for <device>
   ...
   Key Slot 0: ENABLED
   Key Slot 1: DISABLED
   ...
   Key Slot 7: DISABLED


¹⁰https://github.com/fuhry/initramfs-sencrypt
**Full Disc Encryption:** Wenn man bei der Installation das System vollständig verschlüsselt hat, kann man den Yubikey auch zum Öffnen des Root-Containers beim Booten verwenden.

Dafür ist die Partition mit dem verschlüsselten Root-Container zu ermitteln und der Yubikey als Hardware Token zum Öffnen hinzuzufügen, wie oben beschrieben. Die folgenden Schritte funktionieren auf einem Debian System und davon abgeleiteten Derivaten:

1. Zuerst das BACKUP der Daten aktualisieren, falls man es etwas kaputtspielt!

2. Am einfachsten identifiziert man den Root-Container mit einem Blick in die Datei `/etc/crypttab`. In der ersten Zeile das zweite Element ist die Kennung für das `<device>`, welches für das Kommando `yubikey-luks-enroll` zu verwenden ist.

3. Danach ist die Datei `/etc/crypttab` anzupassen. In der (ersten) Zeile für den Root Container ist das Schlüsselwort `luks` mit dem vollständigen Pfad zu `ykluks-keyscript` zu ergänzen, also ...

   ```
   cryptroot UUID=xxxx ... luks,keyscript=/usr/share/yubikey-luks/ykluks-keyscript ...
   ```

   Also: aus der Zeile...

   ```
   cryptroot UUID=xxxx ... luks
   ```

   ...wird diese Zeile:

   ```
   cryptroot UUID=xxxx ... luks,keyscript=/usr/share/yubikey-luks/ykluks-keyscript
   ```

   Alle anderen Parameter bleiben so erhalten, wie bei der Installation konfiguriert.

4. Danach ist noch das Bootimage neu zu bauen mit:

   ```
   > sudo update-initramfs -u
   ```

5. Wenn man den Rechner neu bootet, kann man statt der bisherigen (hoffentlich starken und komplexen) Passphrase, die man bei der Installation vergeben hat, auch den Yubikey anschließen und das einfachere Challenge Passwort eingeben.

**14.5.4 LUKS-Nuke - hinterhältige Datenzerstörung**

LUKS Nuke bietet die Möglichkeit, eine vollständig verschlüsselte Installation von Debian basierten Distributionen auf die zukünftige Entsorgung der Festplatte vorzubereiten.


(Einsatzmöglichkeiten für ein solches Feature sind der Fantasie des Lesers überlassen.)

LUKS Nuke wurde für Kali Linux entwickelt, einer Linux Distribution für Offensive Security (Penetration). In dieser Distribution installiert man das Paket aus den Repositories:

```
> sudo apt install cryptsetup-nuke-password
```  

Im zweiten Schritt werden die Nuke Passphrase konfiguriert, die man 2x eingeben muss, und im Hintergrund automatisch alle notwendigen Systemanpassungen eingerichtet:

```
> sudo dpkg-reconfigure cryptsetup-nuke-password
```  

LUKS Nuke löst bei Eingabe der Nuke Passphrase statt der korrekten Passphrase zum Öffnen des Systemcontainers alle Keyslots im LUKS Header, so das die Daten nicht mehr entschlüsselt werden können. Wenn man ein Backup des LUKS Header off-site speichert, kann man mit einer Linux Live-DVD die Daten wieder lesbar machen.
1. Ein Backup des LUKS Header erstellt man mit folgendem Kommando:

   > sudo cryptsetup luksHeaderBackup --header-backup-file luksheader.bck <device>

   Bei Kali Linux ist das <device> üblicherweise /dev/sda5, bei anderen Distributionen ist es evtl. anzupassen. Das Backup kann man verschlüsseln und off-site ablegen.

2. Für ein Restore des alten LUKS Headers bootet man eine Linux Live-DVD und stellt den Header mit den Schlüsseln mit folgendem Kommando wieder her:

   > sudo cryptsetup luksHeaderRestore <device> --header-backup-file luksheader.bck

   Da Kali Linux auf Debian basiert, kann man das Paket cryptsetup-nuke-passphrase auch auf anderen Linux Distributionen installieren, die von Debian abgeleitet sind. Dafür könnte man die Kali Live-DVD starten und das Paket mit folgendem Kommando herunterladen:

   > apt download cryptsetup-nuke-password

   Anschließend transferiert man das Paket auf das eigene System und installiert es mit:

   > sudo dpkg -i cryptsetup-nuke-password.deb

   Dann die Konfiguration der Nuke Passphrase und Anpassung des Systems - FERTIG:

   > sudo dpkg-reconfigure cryptsetup-nuke-password

   (Getestet mit Debian 10 - für alle anderen Distributionen keine Gewährleistung.)

14.6 zuluCrypt für Linux

zuluCrypt ist eine 100% kompatible Open Source Alternative zu Veracrypt für Linux Nutzer und kann in aktuellen Linux Distributionen mit den üblichen Tools zur Paketverwaltung installiert werden.

Die Verwendung von zuluCrypt statt cryptsetup ist empfehlenswert, wenn man öfters mit Containerdateien arbeitet, wenn man Features für hohe Sicherheitsanforderungen verwendet (Passphrase+Keyfile als Credentials oder Hidden Volumes) oder Datenträger verschlüsseln möchte, die bei Bedarf auch unter Windows geöffnet werden können.

Neben Truecrypt und Veracrypt beherrscht das Tool auch dm-crypt/LUKS Verschlüsselung und unterstützt alle Features im GUI und nicht nur auf der Kommandozeile.

Als kleine Besonderheit kann zuluCrypt verschlüsselte Container in einer Videodatei verstecken (Steganografie). Dabei wird dm-crypt zur Verschlüsselung verwendet.

Das zuluCrypt Paket besteht aus vier Komponenten:

- zuluCrypt-gui ist das universelle GUI Tool zum Erstellen von verschlüsselten Containerdateien und Datenträgern sowie zum Öffnen und Schließen der Container.
- zuluCrypt-cli ist ein Tool für die Kommandozeile mit gleichem Funktionsumfang.
- zuluMount-gui dient zum Öffnen und Schließen der Container.
- zuluMount-cli macht das gleiche auf der Kommandozeile.

In der Regel wird man wahrscheinlich mit dem zuluCrypt GUI arbeiten. Es verwaltet einerseits die geöffneten Container in einem übersichtlichen Hauptfenster und kann anderseits auch Datenträger verschlüsseln und verschlüsselte Containerdateien erstellen. Dabei werden alle Features von Truecrypt, Veracrypt und dm-crypt/LUKS unterstützt inklusive Hidden Volumes (Veracrypt) und Passwort + Keyfiles als Credentials.
14.7 Backups verschlüsseln


1. Die persönlichen Daten oder einzelne Verzeichnisse mit häufig geänderten Dateien könnte man regelmäßig mit einer Kopie auf einem verschlüsselten Datenträger synchronisieren (USB-Stick, externe Festplatte). Da nur Änderungen übertragen werden müssen, geht es relativ schnell.

2. Einzelne, in sich geschlossene Projekte könnten platzsparend als komprimiertes verschlüsseltes Archiv auf einem externen Datenträger abgelegt werden.

3. Größere abgeschlossene Projekte könnten auf einem optischen Datenträger dauerhaft archiviert werden.

14.7.1 Schnell mal auf den USB-Stick

Inzwischen gibt es preiswerte USB-Sticks mit beachtlicher Kapazität. Aufgrund der einfachen Verwendung sind sie für Backups im privaten Bereich gut geeignet. Für große Datenmengen kann man auch eine externe USB-Festplatte nutzen. Wer eine Beschlagnahme der Backupmedien befürchtet, findet vielleicht eine Anregung bei true-random\(^\text{11}\).


\(^\text{11}\)http://true-random.com/homepage/projects/usbsticks/small.html
14.7. BACKUPS VERSCHLÜSSELN

Die von verschiedenen Herstellern angebotenen Verschlüsselungen sind oft unsicher. USB-Datentresore mit Fingerabdruckscanner lassen sich einfach öffnen. Einige USB-Sticks mit Verschlüsselung verwenden zwar starke Algorithmen (in der Regel AES256), legen aber einen zweiten Schlüssel zur Sicherheit auf dem Stick ab, der mit geeigneten Tools ausgescannt werden kann und Zugriff auf die Daten ermöglicht. Selbst eine Zertifizierung des NIST ist keine Garantie für saubere Implementierung.

Unison-GTK


Nach dem ersten Start wählt man Quell- und Zielverzeichnis für das Default-Profil. Es ist möglich, mehrere Profile anzulegen. Bei jedem weiteren Start erscheint zuerst ein Dialog zur Auswahl des Profiles (Bild 14.6).

Nach Auswahl des Profiles analysiert Unison die Differenzen und zeigt im Hauptfenster an, welche Aktionen das Programm ausführen würde. Ein Klick auf Go startet die Synchronisation.

**Achtung:** Unison synchronisiert in beide Richtungen und eignet sich damit auch zum Synchronisieren zweier Rechner. Verwendet man einen neuen (leeren) Stick, muss auch ein neues Profil angelegt werden! Es werden sonst alle Daten in den Quellverzeichnissen gelöscht, die im Backup nicht mehr vorhanden sind.

Neben der Möglichkeit, lokale Verzeichnisse zu synchronisieren, kann Unison auch ein Backup auf einem anderen Rechner via FTP oder SSH synchronisieren.

**rsync**

Das Tool rsync ist in allen Linux-Distributionen enthalten und insbesondere für Scripte einfach verwendbar. Es synchronisiert die Dateien eines Zielverzeichnisses mit dem Quellverzeichnis und überträgt dabei nur die Änderungen. Ein Beispiel zeigt das Sichern der E-Mails und Adressbücher von Thunderbird:

12 [http://heise.de/-270060](http://heise.de/-270060)
13 [http://heise.de/-894962](http://heise.de/-894962)
14 [http://www.cis.upenn.edu/bcpierce/unison/](http://www.cis.upenn.edu/bcpierce/unison/)
KAPITEL 14. DATEN VERSCHLÜSSELN

Abbildung 14.7: Hauptfenster von Unison-GTK

rsync -av --delete $HOME/.thunderbird /backup_dir/

Der Befehl legt im \texttt{backup\_dir} ein Verzeichnis \texttt{.thunderbird} an und kopiert alle Daten in dieses Unterverzeichnis. Sollte das Verzeichnis \texttt{.thunderbird} im Backup Verzeichnis bereits vorhanden sein, werden nur die Änderungen übertragen, was wenige Sekunden dauert.

Eine zweite Variante zum Sichern des gesamten \texttt{$HOME$} inklusive der versteckten Dateien und exklusiv eines Verzeichnisses (mp3) mit großen Datenmengen:

\begin{verbatim}
rsync -av --delete --include=$HOME/. --exclude=$HOME/mp3 $HOME /backup_dir/\end{verbatim}

Die Option \texttt{--delete} löscht im Orginal nicht mehr vorhandene Dateien auch in der Sicherungskopie. Weitere Hinweise liefert die Manualpage von rsync.

Standardmäßig sichert rsync keine versteckten Dateien und Verzeichnisse, die mit einem Punkt beginnen. Diese Dateien und Verzeichnisse müssen mit \texttt{--include} angegeben werden. Im Beispiel werden alle versteckten Verzeichnisse und Dateien mit gesichert.

Ein Script, welches alle nötigen Verzeichnisse synchronisiert, ist schnell gestrickt. Eine backup-freundliche Struktur im \texttt{$HOME$}-Verzeichnis erleichtert dies zusätzlich.

Grsync

Grsync ist ein grafischen Interface für rsync. Auch dieses Tool ist in allen Linux/Unix Distributionen enthalten.


14.7.2 Online Backups

Neben dem Backup auf einem externen Datenträger kann man auch Online-Speicher nutzen. Bei TeamDrive.com, DataStorageUnit.com, ADrive.com, rsync.net u.v.a.m. gibt es Angebote ab 3,- Euro monatlich. Wer einen eigenen (V)Server gemietet hat, kann seine
14.7. BACKUPS VERSCHLÜSSELN

Abbildung 14.8: Hauptfenster von Grsync

Backups auch dort ablegen. Um die Verschlüsselung der Daten vor dem Upload muss man sich immer selbst kümmern.

Ein Online-Backup ist praktisch, wenn man mit Laptop in ein Land wie die USA reist. Bei der Einreise werden möglicherweise die Daten der Laptops gescannt und auch kopiert. Die EFF.org empfiehlt, vor der Reise die Festplatte zu "reinigen". Man könnte ein Online-Backup erstellen und auf dem eigenen Rechner die Daten sicher(!) löschen, also shred bzw. wipe nutzen. Bei Bedarf holt man sich die Daten wieder auf den Laptop. Vor der Abreise wird das Online-Backup aktualisiert und lokal wieder alles gelöscht.

Mit dem Gesetzentwurf zum Zugriff auf Bestandsdaten der Telekommunikation (BR-Drs. 664/12) vom 24.10.2012 räumt die Bundesregierung den Geheimdiensten und Strafverfolgern die Möglichkeit ein, ohne richterliche Prüfung die Zugangsdaten zum Online-Speicher vom Provider zu verlangen. Um die gespeicherten Daten, die meist aus dem Bereich privater Lebensführung stammen, angemessen vor dem Verfassungsschutz zu schützen, ist man auf Selbsthilfe und Verschlüsselung angewiesen.

An ein Online-Backup werden deshalb folgende Anforderungen gestellt:

• Das Backup muss auf dem eigenen Rechner ver- und entschlüsselt werden, um die Vertraulichkeit zu gewährleisten.

• Es sollten nur geänderte Daten übertragen werden, um Zeitbedarf und Traffic auf ein erträgliches Maß zu reduzieren.


15 https://www.eff.org/deeplinks/2008/05/protecting-yourself-suspicionless-searches-while-t
16 https://www.boxcryptor.com
17 https://cryptomator.org

**Duplicity für Linux**

*Duplicity* ist ein Backuptool für Linux/Unix speziell für die Nutzung von Online-Speicherplatz. Es bietet transparente Ver- und Entschlüsselung mit OpenPGP und überträgt nur geänderte Daten, um Traffic und Zeitbedarf minimal zu halten.

Debian und Ubuntu stellen in der Regel alles Nötige für die Installation in den Repositories bereit. `aptitude` spült es auf die Platte:

> sudo aptitude install duplicity

Duplicity ist ein Kommandozeilen Tool. Ein verschlüsseltes Backup schiebt man mit folgendem Kommando auf den Server:

> duplicity Verzeichnis Backupadresse

Vom lokalen Verzeichnis wird ein Backup erstellt, mit OpenPGP symmetrisch verschlüsselt und unter der Backup Adresse abgelegt. Ein vorhandenes Backup wird aktualisiert. Das Passwort für die Verschlüsselung wird entweder beim Start des Programms abgefragt oder es wird die Environment Variable `PASSPHRASE` verwendet. Um das Backup mit cron zu automatisieren, kann man ein kleines Shellscript schreiben:

```
#!/bin/sh
PASSPHRASE="gutes_passwort"
duplicity Verzeichnis Backupadresse
```

Möchte man statt der symmetrischen Verschlüsselung einen OpenPGP-Key nutzen, verwendet man die Option `--encrypt-key` mit der ID oder Mail-Adresse des OpenPGP Key. Diese Option kann mehrfach angegeben werden, um mehreren Teilnehmern ein Restore des Backups zu erlauben.

> duplicity --encrypt-key="0x12345670" Verzeichnis Backupadresse

Die **BackupAdresse** kodiert das Übertragungsprotokoll, den Server und das Verzeichnis auf dem Server. Duplicity kann mit vielen Protokollen umgehen. BackupAdressen haben folgenden Aufbau:

- Alle Anbieter von Online-Speicherplatz unterstützen webdav oder die SSL-verschlüsselte Übertragung mit webdavs:
  ```
  webdavs://user[:password]@server.tld/dir
  ```
- Amazon S3 cloud services werden unterstützt:
  ```
  s3://server/bucket_name[/prefix]
  ```
- Man kann sein IMAP-Postfach für das Backup nutzen, möglichst mit SSL-verschlüsselter Verbindung. Diese Variante ist nicht sehr performant viele Mail-Provider sehen das nicht gern:
  ```
  imaps://user[:password]@mail.server.tld
  ```
- Das sftp-Protokoll (ssh) ist vor allem für eigene Server interessant. Loginname und Passwort werden ebenfalls in der Adresse kodiert. Statt Passwort sollte man besser einen SSH-Key nutzen und den Key mit ssh-add vorher freischalten.
**14.7. BACKUPS VERSCHLÜSSELN**

ssh://user[:password]@server.tld[:port]/dir

- scp und rsync können ebenfalls für die Übertragung zum Server genutzt werden:
  
  scp://user[:password]@server.tld[:port]/dir
  rsync://user[:password]@server.tld[:port]/dir

  Das Verzeichnis ist bei rsync relativ zum Login-Verzeichnis. Um einen absoluten Pfad auf dem Server anzugeben, schreibt man 2 Slash, also //dir.


  > mkdir /home/user/restore
  > duplicity Backupadresse /home/user/restore

  Weitere Informationen findet man in der manual page von *duplicity*. 
Kapitel 15

Daten löschen

Neben der sicheren Aufbewahrung von Daten steht man gelegentlich auch vor dem Problem, Dateien gründlich vom Datenträger zu putzen. Es gibt verschiedene Varianten, Dateien vom Datenträger zu entfernen. Über die Arbeit der einzelnen Varianten sollte Klarheit bestehen, anderenfalls erlebt man evtl. eine böse Überraschung.

15.1 Dateien in den Papierkorb werfen

Unter WIN wird diese Variante als Datei(en) löschen bezeichnet, was etwas irreführend ist. Es wird überhaupt nichts beseitigt. Die Dateien werden in ein spezielles Verzeichnis verschoben. Sie können jederzeit wiederhergestellt werden. Das ist kein Bug, sondern ein Feature.


15.2 Dateien sicher löschen (Festplatten)

Um sensible Daten sicher vom Datenträger zu putzen, ist es nötig, sie vor dem Löschen zu überschreiben. Es gibt diverse Tools, die einzelne Dateien oder ganze Verzeichnisse shredern können.


- Unter Linux kann KGPG einen Reißwolf auf dem Desktop installieren. Dateien können per Drag-and-Drop aus dem Dateimanager auf das Symbol gezogen werden, um sie zu shreadern.

- Für Liebhaber der Kommandozeile gibt es shred und wipe für Linux. Einzelne Dateien kann man mit shred löschen:

  > shred -u dateiname

Für Verzeichnisse kann man wipe nutzen. Das folgende Kommando überschreibt rekursiv (Option -r) alle Dateien in allen Unterverzeichnissen 4x (Option -q) und löscht anschließend das gesamte Verzeichnis.
15.3 Dateireste nachträglich beseitigen


Nach der Installation ist Bleachbit als Administrator bzw. root zu starten und nur die Option Free disk space zu aktivieren (Bild 15.1). Außerdem ist in den Einstellungen ein schreibbares Verzeichnis auf jedem Datenträger zu wählen, der gesäubert werden soll. Anschließend startet man die Säuberung mit einem Klick auf den Button Clean.

Abbildung 15.1: Bleachbit

Die Säuberung einer größeren Festplatte dauert einige Zeit. Dabei werden nur die als frei gekennzeichneten Bereiche überschrieben, das Dateisystem bleibt intakt.

1http://bleachbit.sourceforge.net/download
15.4 Dateien sicher löschen (SSDs)

Die für Festplatten empfohlenen Tools funktionieren nicht mit Flash basierten Solid State Disks (SSDs). Um die Speicherzellen zu schonen, sorgt die interne Steuerelektronik dafür, dass für jeden Schreibvorgang andere Zellen genutzt werden. Ein systematisches Über­schreiben einzelner Dateien ist nicht möglich. Mehr Informationen liefert die Publikation Erasing Data from Flash Drives.\(^2\)

Für SSDs ist die TRIM Funktion zu aktivieren. Dabei werden den Speicherzellen eines Blocks einige Zeit nach dem Löschen der Datei auf den Ursprungszustand zurück gesetzt. Weitere Maßnahmen zum sicheren Löschen sind nicht nötig.

**Windows** aktiviert TRIM standardmäßig, wenn bei der Installation eine SSD Festplatte gefunden wurde. Mit folgendem Befehl kann man prüfen, ob TRIM aktiv ist:

```
> fsutil behavior query disabledeletenotify
```

Wenn ein Wert = 0 ausgegeben wird, ist Trim aktiviert. Wird ein Wert = 1 ausgegeben (weil man eine SSD nachträglich eingebaut hat oder den AHCI Mode im BIOS erst nachträglich aktiviert), aktivieren sie die Trim Funktion mit dem Kommando:

```
> fsutil behavior set disabledeletenotify 0
```

Mit *fsutil* wird das Trimmen lediglich aktiviert. Ob es wirklich funktioniert, kann man mit dem kleinen Tool *trimcheck*\(^3\) prüfen. Das Tool ist in einem Verzeichnis auf dem Datenträger abzulegen, den man testen möchte, und als Administrator zu starten.

**Linuxer** haben für das Trimmen der Datenträger drei Möglichkeiten:

1. Standardmäßig verwenden in dem meisten Linux Distributionen **Batched TRIM**. Einmal pro Woche werden alle eingebauten SSDs gesäubert. Mit folgendem Kommando kann man prüfen, ob die Säuberung aktiv ist:

```
> sudo systemctl status fstrim.timer
```

Für unverschlüsselte Datenträger wird es in */etc/fstab* aktiviert, indem man die Mountoption *discard* hinzufügt:

```
UUID=[NUMSLETTER] / ext4 discard,noatime,errors=remount-ro 0 1
```

Bei LUKS verschlüsselten Datenträgern ist **Online TRIM** in */etc/crypttab* zu aktivieren, indem man die Mountoption *discard* hinzufügt:

```
sda2-crypt /dev/sda2 none luks,discard
```

Nach dem Ändern der Mountoptionen in */etc/fstab* oder */etc/crypttab* ist es eine gute Idee, die initramfs Images neu zu bauen:

```
> sudo update-initramfs -u -k all
```

\(^2\)https://www.usenix.org/events/fast11/tech/full_papers/Wei.pdf

\(^3\)https://github.com/CyberShadow/trimcheck
15.5 Gesamten Datenträger säubern (Festplatten)


Für die erste IDE-Festplatte:

\[\text{name} \text{wipe} -kq /dev/hda\]

Für SATA- und SCSI-Festplatte:

\[\text{name} \text{wipe} -kq /dev/sda\]

Wenn die Live-DVD das Tool `wipe` nicht enthält, kann man alternativ `dd` (disk doubler) nutzen. Um die erste IDE-Festplatte einmal mit NULL und dann noch einmal mit Zufallszahlen zu überschreiben, kann man folgende Kommandos nutzen:

\[\text{name} \text{dd if=/dev/zero of=/dev/hda} \]
\[\text{name} \text{dd if=/dev/urandom of=/dev/hda} \]

(Einmal mit NULLEN überschreiben reicht, alles andere ist paranoid.)

15.6 Gesamten Datenträger säubern (SSDs)

Das komplette Löschen einer SSD-Platte oder eines USB-Sticks funktioniert am besten, wenn der Datenträger den ATA-Befehl SECURE-ERASE unterstützt. Diese Funktion muss allerdings durch den Datenträger bereitgestellt werden. Unter Linux kann man das Tool `hdparm` nutzen, um diese Funktion aufzurufen.

Als erstes ist zu prüfen, ob SECURE-ERASE unterstützt wird:

\[\text{name} \text{sudo hdparm -I /dev/sdX}\]

Das Ergebnis muss einen Abschnitt `Security` enthalten und muss auf `not frozen` stehen. Falls die Ausgabe `frozen` liefert, wird SECURE-ERASE im Bios des Rechners blockiert.

`Security`:

\[
\begin{align*}
\text{Master password revision code} & = 64060 \\
\text{supported} & \quad \text{not enabled} \\
\text{not locked} & \quad \text{not frozen} \\
\text{expired: security count} & \quad \text{supported: enhanced erase}
\end{align*}
\]

\(^4\)http://www.dban.org/
Dann kann man ein Passwort setzen und den Datenträger vollständig löschen:

```bash
> sudo hdparm --user-master u --security-set-pass GEHEIM /dev/sdX
> sudo hdparm --user-master u --security-erase GEHEIM /dev/sdX
```

Falls der Datenträger SECURE-ERASE nicht unterstützt, bleibt nur das einfache Über-

schreiben des Datenträgers. Dabei werden aber nicht alle Speicherzellen garantiert ge-

löscht. Unter Linux auf der Kommandozeile wieder mit:

```bash
> dd if=/dev/zero of=/dev/sdc
```

### 15.7 Datenträger zerstören

Den Datenträger physisch zu zerstören, ist die ultimative Form der Datenvernichtung. Man kann es selbst versuchen mit Bohrmaschine und Flex in der Kellerwerkstatt oder man übergibt die Daten an professionellen Serviceanbieter, der das fachmännisch erledigt.


Hinweis: Der Postversand innerhalb Deutschlands ist vom BSI für vertrauliche Daten bis zur Geheimhaltungsstufe VS-NfD (Nur für Dienstgebrauch) zugelassen.

\(^5\)https://shop.nitrokey.com/de_DE/shop/product/nitrosred-datentragervernichtung-on-demand-106
Kapitel 16

Daten anonymisieren

Fotos, Office Dokumente, PDFs und andere Dateitypen enthalten in den Metadaten viele Informationen, die auf den ersten Blick nicht sichtbar sind, jedoch vieles verraten können.

**Fotos** von Digitalkameras enthalten in den EXIF-Tags oft eine eindeutige ID der Kamera, Zeitstempel der Aufnahmen, bei neueren Modellen auch GPS-Daten. Die IPTC-Tags können Schlagwörter und Bildbeschreibungen der Fotoverwaltung enthalten. XMP Daten enthalten den Autor und der Comment üblicherweise die verwendete Software.

**Office Dokumente** enthalten Informationen zum Autor, letzte Änderungen, Kommentare von anderen Bearbeitern, verwendete Softwareversion u.v.a.m.

Es ist manchmal interessant, wenn man die letzten Änderungen rückgängig machen kann und sieht, welche Formulierungen oder Zahlen zuletzt geändert oder angepasst wurden. Office Dokumente sollte man **NIE** veröffentlichen!

**PDF Dokumente** enthalten ebenfalls viele Metadaten. Besonders geschwätzig sind PDFs, die mit Microsoft Office generiert wurden. Sie enthalten nicht nur beschreibende Metadaten für das Dokument sondern evtl. auch URLs, von denen Bilder eingebunden wurden, Kommentare, Lesezeichen usw.

Ein Beispiel: professionelle Personalmanager schauen sich bei online zugesendeten Bewerbungen routiniert die Metadaten der Dokumente an. Wenn der Autor des Dokumentes nicht der Bewerber selbst war sondern bspw. bewerbungsmappe.de, hat man Hinweise, wo die Vorlage herkommt und kann diese Informationen in die Bewertung einfließen lassen.

Vor dem Upload von Fotos und anderen Dateien ins Internet ist es ratsam, diese überflüssigen Informationen zu entfernen. Es gibt mehrere Firmen, die sich auf die Auswertung dieser Metadaten spezialisiert haben. Ein Beispiel ist die Firma Heypic, die die Fotos von Twitter durchsucht und anhand der GPS-Koordinaten auf einer Karte darstellt. Auch Strafverfolger nutzen diese Informationen. Das FBI konnte einen Hacker mit den GPS-Koordinaten im Foto seiner Freundin finden\(^1\).

Der *StolenCameraFinder*\(^2\) sucht anhand der KameraID in den EXIF-Daten alle Fotos, die mit dieser Digital-Kamera gemacht wurden (Smartphone Kameras werden nicht unterstützt). Da die Kamera ID mit hoher Wahrscheinlichkeit eindeutig einer Person zugeordnet werden kann, sind viele Anwendungen für diese Suche denkbar. Die verbesserte Version *CameraForensics*\(^3\) ist nur für Strafverfolgung verfügbar.

---

\(^1\)[http://www.tech-review.de/include.php?path=content/news.php&contentid=14968]  
\(^2\)[http://www.stolencamerafinder.com]  
\(^3\)[https://www.cameraforensics.com]
16.1 Fotos und Bilddateien anonymisieren

- **Irfan View**[^4] (Windows) kann in Fotos mit Öffnen und Speichern die Metatags entfernen. Im Batchmode kann man die Funktion Konvertieren nutzen, um mehrere Bilder mit einem Durchgang zu bearbeiten. Man konvertiert die Fotos von JPEG nach JPEG und gibt dabei in den Optionen an, dass keine EXIF, XMP und IPTC Daten erhalten bleiben sollen.

![Abbildung 16.1: Informationen in Fotos löschen mit Irfan View](image)

- **exiv2** (für Linux) ist ein nettes kleines Tool zum Bearbeiten von EXIF, XMP und IPTC Informationen in Bilddateien. Es ist in den meisten Linux Distributionen enthalten und kann mit dem bevorzugten Paketmanager installiert werden:

  ```
  > sudo apt install exiv2
  ```

  Nach der Installation kann man z. B. Fotos auf der Kommandozeile säubern:

  ```
  > exiv2 rm foto.jpg
  ```


16.2 PDF-Dokumente säubern


[^4]: http://www.heise.de/download/irfanview.html
[^5]: https://www.privacy-handbuch.de/handbuch_43b.htm
Für Windows gibt es z. B. den Hexonic PDF Metadaten Editor⁶, um die restlichen Metadaten aus PDF Dokumenten zu entfernen. Nach dem Download und evtl. der Installation kann man das Tool starten und die zu säubernden PDF-Dokumente laden.

Unter Linux kann man die Metainformationen mit den Tools exiftool und qpdf entfernen. Beide Programme kann man mit dem bevorzugten Paketmanager installieren:

> sudo apt libimage-exiftool-perl qpdf

Nachdem das PDF mit einem PDF Viewer in eine neue PDF Datei datei-print.pdf gedruckt wurde, um die Metadaten von eingebetteten Bildern zu beseitigen, können alle Metadaten mit exiftool auf leere Werte gesetzt werden. Danach wird das PDF Dokument mit qpdf behandelt, damit die reversiblen Rückstände verschwinden:

> exiftool -all:all= datei-print.pdf
     Warning: [minor] ExifTool PDF edits are reversible.
     1 image files update

> qpdf --linearize datei-print.pdf datei-clean.pdf

> rm datei-print.pdf

exiftool arbeitet in-place und modifiziert die Input Datei direkt, qpdf liest eine Input Datei und schreibt das Ergebnis in eine neue Output Datei.

Mit folgendem Kommando kann man dann die Metadaten prüfen:

> exiftool -all:all datei-clean.pdf

....
MIME Type : application/pdf
PDF Version : 1.5
Linearized : Yes
Page Mode : UseOutlines
Page Count : 4

Man könnte sich auch ein kleines Script schreiben, um den Aufruf zu vereinfachen. Das folgende Mini-Script pdf-meta-clean.sh (mit ein bisschen Fehlerbehandlung) wird mit dem Dateinamen der zu reinigenden PDF-Datei aufgerufen. Es macht seine Arbeit und danach sind die Metadaten weg. (Es wird kein Backup der originalen Datei behalten!)

#!/bin/bash

if [ -z "$1" ]; then
    echo "Usage: 'basename $0' <Dateiname>"
    exit 1
fi

if [ ! -f "$1" ]; then
    echo "FEHLER: Die Datei $1 ist nicht vorhanden!"
    exit 1
fi

FILETYPE='mimetype -b "$1"'
if [ "$FILETYPE" != "application/pdf" ]; then
    echo "FEHLER: Datei $1 ist keine PDF Datei!"
    exit 1
fi

if [ ! -w "$1" ]; then
    echo "FEHLER Die PDF Datei $1 kann nicht modifiziert werden!"
    exit 1
fi

if [ -z 'which exiftool' ]; then
    echo "FEHLER: Das Programm exiftool ist nicht installiert!"
    exit 1
fi

if [ -z 'which qpdf' ]; then
    echo "FEHLER: Das Programm qpdf ist nicht installiert!"
    exit 1
fi

exiftool -all:all= "$1"
TFILE='mktemp'
 cp "$1" "$TFILE"
qpdf --linearize "$TFILE" "$1"
rm "$TFILE"
exit 0

Nach dem Download könnte man das Script nach /usr/local/bin kopieren und als ausführbar markieren:

> sudo cp Download/pdf-meta-clean.sh /usr/local/bin/pdf-meta-clean
> sudo chmod +x /usr/local/bin/pdf-meta-clean

 Dann kann man folgendes Kommado aufrufen, um eine PDF-Datei zu reinigen:

> pdf-meta-clean dateiname.pdf
Kapitel 17

Daten verstecken

Geheimdienste orakeln seit Jahren immer wieder, dass Terroristen über versteckte Bot-
schaften in Bildern kommunizieren. Telepolis berichtete 2001 und 2008 kritisch-ironisch
über Meldungen von Scotland Yard, wonach islamische Terroristen ihre Kommunikation
in pornografischen Bildern verstecken würden. Stichhaltige Belege für die Nutzung von
Steganografie konnten bisher nicht geliefert werden. Andere Journalisten hinterfragten
die Meldungen weniger kritisch:

“Bislang ist zwar noch nicht bewiesen, ob die Terrorverdächtigen die Bilder - bei einem
Verdächtigen wurden 40.000 Stück gefunden - nur zum persönlichen Vergnügen heruntergeladen
haben oder ob tatsächlich ein Kommunikationsnetzwerk aufgebaut wurde.” (Welt Online1, wieder
einmal viel heiße Luft.)

Wie funktioniert diese Technik, über die Zeit Online bereits 1996 berichtete und können
Nicht-Terroristen das auch nutzen?

Ein Beispiel

Statt Bits und Bytes werden in diesem Beispiel Buchstaben genutzt, um das Prinzip der Ste-
ganografie zu erläutern. Nehmen wir mal an, Terrorist A möchte an Terrorist B die folgende
kurze Botschaft senden:

Morgen!

Statt die Nachricht zu verschlüsseln, was auffällig sein könnte, versteckt er sie in dem
folgenden, harmlos aussehenden Satz:

Mein olles radio geht einfach nicht!

Wenn der Empfänger weiss, dass die eigentliche Botschaft in den Anfangsbuchstaben
der Wörter kodiert ist, wäre es ganz gut, aber nicht optimal.

keine GEZ!” Er wird aufmerksam und mit ein wenig Probieren kann der die Botschaft ex-
trahieren. Also wird Terrorist A die Nachricht zusätzlich verschlüsseln, nehmen wir mal
eine einfache Caesar-Verschlüsselung mit dem Codewort KAWUM, es entsteht:

Ilpcmg!

und ein neuer, halbwegs sinnvoller Satz wird konstruiert und verschickt.

1http://www.welt.de/politik/article2594337/
KAPITEL 17. DATEN VERSTECKEN

17.1 Allgemeine Hinweise

Das Beispiel verdeutlicht, welche Voraussetzungen für die Nutzung von Steganografie zum Austausch von versteckten Botschaften gegeben sein müssen:

- Sender und Empfänger müssen sich darüber verständigt haben, wie die Nutzdaten versteckt werden.
- Das Passwort für die Verschlüsselung muss ausgetauscht werden.
- Die Modalitäten für den Austausch der Trägermedien müssen geklärt werden. Wo kann der Empfänger die Fotos mit den versteckten Botschaften finden?

Wenn diese Voraussetzungen geklärt sind, kann es losgehen

1. Der Absender schreibt seine Botschaft mit einem einfachen Texteditor.
4. Der Empfänger muss wissen, wo er aktuelle Nachrichten finden kann. Fotos oder Audiodateien, in denen der Empfänger eine Botschaft vermutet, sind herunterzuladen.
5. Danach kann der Empfänger versuchen, die geheime Botschaft aus dem Trägermedium zu extrahieren. Dabei ist das gleiche Tool wie beim Verstecken zu verwenden. Wenn er alles richtig macht und das korrekte Passwort verwendet, wird die Textdatei extrahiert und kann mit einem einfachen Texteditor gelesen werden.

Unsichtbare Markierungen, Wasserzeichen

Man kann Steganografie Tools auch nutzen, um unsichtbare Wasserzeichen an Bildern oder Audiodateien anzubringen.

Wenn Fotos oder Videos nur einem kleinen Kreis von Personen zugänglich gemacht werden sollen, dann können individuelle Wasserzeichen steganografisch in den Dateien versteckt werden. Sollten diese Fotos oder Videos in der Öffentlichkeit auftauchen, kann das Leck anhand des unsichtbaren steganografischen Wasserzeichens ermittelt werden.

17.2 steghide

Um die Datei `geheim.txt` zu verschlüsseln und in dem Foto `bild.jpg` zu verstecken, ruft man es mit folgenden Parametern auf (mit dem Parameter `-sf` kann optional eine dritte Datei als Output verwendet werden, um das Original nicht zu modifizieren):

```
> steghide embed -cf bild.jpg -ef geheim.txt
Enter passphrase: Re-Enter passphrase: embedding "geheim.txt" in "bild.jpg"... done
```

Der Empfänger extrahiert die geheimnisvollen Daten mit folgendem Kommando (mit dem Parameter `-xf` könnte ein anderer Dateiname für die extrahierten Daten angegeben werden):

```
> steghide extract -sf bild.jpg
Enter passphrase: wrote extracted data to "geheim.txt".
```

Außerdem kann man Informationen über die Coverdatei bzw. die Stegodatei abfragen. Insbesondere die Information über die Kapazität der Coverdatei ist interessant, um abschätzen zu können, ob die geheime Datei reinpasst:

```
> steghide info bild.jpg
Format: jpeg
Kapazität: 12,5 KB
```

### 17.3 stegdetect


Der Name `stegdetect` ist eine Kurzform von `Steganografie Erkennung`. Das Programm ist nicht nur für den Nachweis der Nutzung von steghide geeignet, sondern erkennt anhand statistischer Analysen auch andere Tools.

Auch `stegdetect` ist ein Tool für die Kommandozeile. Neben der zu untersuchenden Datei kann mit einem Parameter `-s` die Sensitivität eingestellt werden. Standardmäßig arbeitet stegdetect mit einer Empfindlichkeit von 1.0 ziemlich oberflächlich. Sinnvolle Werte liegen bei 2.0...5.0.

```
> stegdetect -s 2.0 bild.jpg
F5(***)
```

Im Beispiel wird eine steganografische Manipulation erkannt und vermutet, dass diese mit dem Tool F5 eingebracht wurde (was nicht ganz richtig ist, da steghide verwendet wurde).

**Frage:** Was kann man tun, wenn auf der Festplatte eines mutmaßlichen Terroristen 40.000 Bilder rumliegen? Muss man jedes Bild einzeln prüfen?

**Antwort:** Ja - und das geht so:

1. Der professionelle Forensiker erstellt zuerst eine 1:1-Kopie der zu untersuchenden Festplatte und speichert das Image z. B. in `terroristen_hda.img`

2. Mit einem kurzen Dreizeiler scannt er alle 40.000 Bilder in dem Image:

```
http://www.outguess.org/download.php
```
KAPITEL 17. DATEN VERSTECKEN

> losetup -o $((63*512)) /dev/loop0 terroristen_hda.img
> mount -o ro,noatime,noexec /dev/loop0 /mnt
> find /mnt -iname "*.jpg" -print0 | xargs -0 stegdetect -s 2.0 >> ergebnis.txt

(Für Computer-Laien und WINDOWS-Nutzer sieht das vielleicht nach Voodoo aus, für einen Forensiker sind das jedoch Standardtools, deren Nutzung er aus dem Ärmel schüttelt.)

3. Nach einiger Zeit wirft man einen Blick in die Datei ergebnis.txt und weiß, ob es etwas interessantes auf der Festplatte des Terroristen gibt.
Kapitel 18

Betriebssysteme

Der Widerstand gegen Ausforschung und Überwachung sowie der Kampf um die Hoheit über den eigenen Computer beginnt bei der Auswahl des Betriebssystems. Einige stichpunkttartige Gedanken sollen zum Nachdenken anregen.

18.1 Microsoft Windows

Mit Windows 8.0 hat Microsoft begonnen, dass bei Smartphones akzeptierte Device-based Tracking auch bei PCs einzuführen. Ähnlich wie Google bei Android will Microsoft als eine der größten Tracking Familien im Internet seine Datenberge erweitern.


In Windows 10 wurde das Device-based Tracking weiter ausgebaut. Es wird für jeden Account auf dem Rechner eine Unique Advertising ID generiert. Diese ID wird auch Dritten zur eindeutigen Identifikation zur Verfügung gestellt. In der neuen Privacy Policy von Microsoft (Juli 2015) steht außerdem:

We will access, disclose and preserve personal data, including your content (such as the content of your emails, other private communications or files in private folders), when we have a good faith belief that doing so is necessary...

Privaten Daten, die Microsoft in der Standardkonfiguration sammelt:

• Persönliche Interessen, die sich aus dem Surfverhalten ergeben sowie aus den per Apps gesammelten Daten werden an Microsoft gesendet (eine Sport-App sendet die bevorzugten Teams, eine Wetter-App die häufig angefragten Städte... usw.)

• Standortdaten aller Geräte mit Windows werden an MS übertragen. Es wird bevorzugt GPS oder die WLANs der Umgebung genutzt, um den Standort so genau wie möglich zu bestimmen.

• Kontaktdaten der Freunde und Bekannten werden an MS übertragen, wenn man Tools von Microsoft als Adressbuch nutzt.


• Der Windows Defender übermittelt alle installierten Anwendungen an Microsoft.

• Mit der digitalen Assistentin Cortana wird in der Standardkonfiguration eine Art Abhörozentrals eingerichtet, die das Wohnzimmer direkt mit Microsoft verbindet.
• Das Schreibverhalten wird analysiert und an Microsoft gesendet. Das Profil der typischen Tastenanschläge könnte zukünftig für die Identifikation bei Texteingaben in Webformularen oder Chats genutzt werden (Stichwort: Keystroke Biometrics¹).

• Die eindeutige UUID, die Windows bei der Kommunikation mit Microsoftservern sendet (z. B. bei Softwareupdates), wird vom NSA und GCHQ als Selektor für Taylorred Access Operations (TAO) verwendet, um gezielt die Computer von interessanten Personen oder Firmen anzugreifen. Microsoft ist seit 2007 Partner im PRISM Programm der NSA.

• Als besonderes Highlight gehören auch die automatisch generierten Recovery Keys der Festplattenverschlüsselung Bitlocker zu den Daten, die MS in seiner Cloud sammelt und NSA/FBI/CIA zur Verfügung stellt. (Crypto War 3.0?)

Mit Windows 10 Pro oder Enterprise kann man den Upload des Recovery Key verhindern², indem man den Rechner einmal komplett verschlüsselt (mit Key Upload), dann die Verschlüsselung deaktiviert (damit muss das System wieder komplett entschlüsselt werden), den alten Recovery Schlüssel löscht und nochmal den Rechner komplett verschlüsselt. Erst beim zweiten Versuch wird man gefragt, ob man den Recovery Key evtl. lokal sichern möchte. Das kostet Zeit und ist auch wieder ein echtes Dark Pattern in der Benutzerführung.

Wenn man es schafft, einen Benutzeraccount ohne Cloud Anbindung einzurichten und in den Einstellungen unter Datenschutz die Privacy Features aktiviert, kann man die Sammelleidenschaft von Windows 10 etwas reduzieren aber nicht vollständig abstellen.³


_Aus Sicht des BSI geht der Einsatz von Windows 8 in Kombination mit einem TPM 2.0 mit einem Verlust an Kontrolle über das verwendete Betriebssystem und die eingesetzte Hardware einher. Daraus ergeben sich für die Anwender, speziell auch für die Bundesverwaltung und kritische Infrastrukturen, neue Risiken.

_T. Baumgärtner von Microsoft(!) erklärte in einer Antwort:_

_Das betrifft aber nur bestimmte Behörden, der Verfassungsschutz oder der BND sollten das System natürlich besser nicht nutzen._

_..._  
_Für normale Nutzer bietet das TPM 2.0 ein enormes Plus an Sicherheit._

Ähmm...

### 18.1.1 Telemetrie in Windows 10

Windows 10 reagiert auf 1.000 - 1.200 Ereignisse, die einen Logmeldung triggen, welche dann an die Microsoft Telemetrie Server übertragen wird. Microsoft Office sendet noch mehr Daten. Bei dem Paket MS Office Pro Plus lösen 23.000 - 25.000 Ereignisse eine Datenübertragung an Telemetrie Server aus. 20-30 Teams arbeiten an der Auswertung, wobei Microsoft keinen Gesamtüberblick hat, welche Produkte welche Daten senden.⁴

---

¹[https://de.wikipedia.org/wiki/Tippverhalten/](https://de.wikipedia.org/wiki/Tippverhalten/)
²[https://theintercept.com/2015/12/28/recently-bought-a-windows-computer-microsoft-probably-has-your-encryption-key/](https://theintercept.com/2015/12/28/recently-bought-a-windows-computer-microsoft-probably-has-your-encryption-key/)
Das BSI hat für Windows 10 die Telemetriedaten in der Analyse SiSyPHuS Win10 genauer untersucht (preiswürdiger Titel). Dabei kommt das BSI zu dem Ergebnis, dass die Übertragung der Telemetriedaten in Windows 10 Basic nicht durch die Konfiguration von Einstellungen vollständig deaktivierbar ist.

Als Schutz gegen die Datensammelwut empfiehlt das BSI, die Verbindungen zu den Windows Telemetrie Servern auf DNS Ebene zu blockieren. Diese Blockade muss außerhalb des Windows Betriebssystems erfolgen, da der Windows Defender die übliche Nutzung Nutzung der Datei %windir%\system32\drivers\etc\hosts zur Blockade von Trackingserver auf DNS Ebene für diesen Zweck blockiert.

Man kann folgende Lösungen nutzen:


2. Wenn man im lokalen Netz einen zentralen DNS-Resolver betreibt, kann man die DNS Namensauflösung für die Telemetrie Server an dieser Stelle blockieren und im DNS Resolver eine Sperrliste konfigurieren.


Die Regel für eine iptables Firewall definiert man nach folgendem Muster:

```shell
iptables -A OUTPUT -p udp --dport 53 -m string --hex-string "[03local09]telemetry[09]microsoft[03]com" -algo bm -j DROP
```

Das Blockieren der IP-Adressen der Telemetrieserver ist nicht sinnvoll, da es sich dabei um Cloud Dienste mit wechselnd IP-Adressen handelt.

Die vom BSI untersuchte Version von Windows 10 sendete Daten an folgende Server:

```
geo.settings-win.data.microsoft.com.akadns.net
db5-eap.settings-win.data.microsoft.com.akadns.net
settings-win.data.microsoft.com
db5.settings-win.data.microsoft.com.akadns.net
asimov-win.settings.data.microsoft.com.akadns.net
db5.vortex.data.microsoft.com.akadns.net
v10-win.vortex.data.microsoft.com.akadns.net
geo.vortex.data.microsoft.com.akadns.net
v10.vortex-win.data.microsoft.com
v10.events.data.microsoft.com
v20.events.data.microsoft.com
us.vortex-win.data.microsoft.com
eu.vortex-win.data.microsoft.com
vortex-win-sandbox.data.microsoft.com
alpha.telemetry.microsoft.com
oca.telemetry.microsoft.com
ceuswatcab01.blob.core.windows.net
ceuswatcab02.blob.core.windows.net
eaus2watcab01.blob.core.windows.net
eaus2watcab02.blob.core.windows.net
weus2watcab01.blob.core.windows.net
weus2watcab02.blob.core.windows.net
```

Zukünftige Windows Versionen können weitere oder andere Server nutzen.

### 18.1.2 Virescanner sind Snakeoil

Für 90% der Windows Nutzer ist ein Virescanner ein unverzichtbares Sicherheitstool aber nur 7% der Security Experten halten zusätzliche Virenscanner neben dem standardmäßig installierten Windows Defender für sinnvoll. Warum sind Sicherheitsexperten so skeptisch und bezeichnen diese Produktgruppe als Schlangenöl?

1. Virenscanner sind eine komplexe Software, die immer wieder selbst schwere Fehler enthält, die von einem Angreifer ausgenutzt werden können. Insbesondere die Parser für komplexe, exotische Dateiformate enthalten immer wieder Fehler.\(^5\)\(^6\)\(^7\)\(^8\)

Da ein Virenscanner tief im System verankert ist und vollen Zugriff auf alle Systemkomponenten hat, kann ein Angreifer durch Ausnutzen von Bugs im Virenscanner das System vollständig kompromittieren ohne das der Anwender etwas bemerkt.

Außerdem wird die Implementierung von Sicherheitsfeatures durch Softwareentwickler (z. B. die konsequente Umsetzung von ASLR) durch Virenscanner behindert, wie der Robert O’Callahan berichtete. Er rät zur De-Installation.\(^9\)

Schlussfolgerung: Virenscanner machen den Rechner unsicher.\(^10\)

2. Viele Virenscanner brechen die TLS Transportverschlüsselung der Webbrowser und E-Mail Clients, um die verschlüsselten Inhalte zu scannen. Es ist ein klassischer man-

\(^5\)https://www.heise.de/-3250784
\(^6\)https://www.heise.de/-3159436
\(^7\)https://www.heise.de/-3149913
\(^8\)https://www.heise.de/-2824437
\(^9\)https://www.heise.de/-3609009
in-the-middle Angriff mit Zustimmung der Anwender. Damit wird die Sicherheit der TLS Verschlüsselung massiv geschwächt.\footnote{https://www.heise.de/-2482344} \footnote{https://www.heise.de/-3095024}


AV-Hersteller sind grob fahrlässig bei HTTPS Interception.\footnote{https://www.heise.de/-3620159}

3. Mit der Installation eines Virescanners gibt der Nutzer praktisch die Hoheit über die Installation von Software teilweise auf. Es ist die Aufgabe eines Virenscanners, Software zu entfernen, die der Hersteller der Software für unpassend hält. Das kann auch zur Deinstallation von Software genutzt werden, die man nicht nutzen soll.

4. In der Regel verwenden Mainstream Viren keine 0day Exploits, um die Systeme zu kompromittieren. Die relativ teuren Angriffe mit 0day Exploits werden nur für gezielte Angriff auf besondere Ziele eingesetzt, und nicht bei Viren. Computer Viren nutzen in Regel längst bekannte Lücken in der Software aus, die in verschiedenen Quellen nach der Beseitigung durch den Softwarehersteller publiziert wurden.

Regelmäßige Updates der verwendeten Software und sichere Konfiguration des Systems schützen besser gegen die Angriffe mit Viren, als ein Virenscanner.

Hinweis: zur sicheren Konfiguration gehört als erstes, dass man die Einstellungen der Benutzerkontensteuerung auf die höchste Sicherheitsstufe stellt. Es ist bedauerlich, dass Microsoft dieses Sicherheitsfeature nicht standmäßig aktiviert.

5. Gegen potente Angreifer, die ein Target gezielt mit staatlich subventionierten Trojanern angreifen, können (und wollen?) kommerzielle Virenscanner nicht schützen. Das konnte man anhand der Veröffentlichungen zur NSA-Cyberwaffe \textit{Regin} verfolgen.

- Als erstes hat Fox-IT den Trojaner \textit{Regin} bei der Analyse des Einbruchs bei Belacom gefunden. Es wurde aber nichts veröffentlicht und die Signaturen wurden nicht in die Datenbank für Kunden aufgenommen. Ronald Prins von Fix-IT sagte nach der Veröffentlichung von \textit{Regin} durch The Intercept im Nov. 2014: 

  \begin{quote}
  We didn’t want to interfere with NSA/GCHQ operations. Everyone seemed to be waiting for someone else to disclose details of Regin first, not wanting to impede legitimate operations related to global security.
  \end{quote}

- Dann wurde der Trojaner \textit{Regin} von Symantec analysiert und auch nichts veröffentlicht. V. Thakur von Symantec sagte im Nov. 2014 als Entschuldigung:

  \begin{quote}
  We had been investigating Regin since last year, but only felt comfortable publishing details of it now.
  \end{quote}


- Erst nachdem The Intercept im Nov. 2014 ankündigte, über \textit{Regin} zu berichten, haben die Anti-Virus Firmen reagiert und die Öffentlichkeit informiert.

### 18.2 Apple MacOS

Wenn man die Apple Datenschutzrichtlinie liest, erkennt man, das MacOS sich nicht als Betriebssystem eignet, wenn man seine Privatsphäre nicht mit Apple teilen möchte:

\begin{footnotesize}
\begin{itemize}
\item \footnote{https://www.heise.de/-2482344}
\item \footnote{https://www.heise.de/-3095024}
\item \footnote{https://www.heise.de/-3620159}
\end{itemize}
\end{footnotesize}
Wir erheben Daten wie namentlich Beruf, Sprache, Postleitzahl, Vorwahl, individuelle Geräteidentifizierungsmerkmale, Weiterleitungs-URL sowie Ort und Zeitzone, wo Apple Produkte verwendet werden, damit wir das Verhalten unserer Kunden besser verstehen und unsere Produkte, Dienste und Werbung verbessern können.

Damit begann die heute allgegenwärtige Datensammlung im Gerät und für diese Innovation wurde Apple mit dem BigBrother 2011 geehrt.


Verantwortlich für diese Aktivitäten ist der trustd Daemon, dessen Kommunikation nicht mit den üblichen Mitteln blockiert oder gefiltert werden kann.

Apple kontrolliert damit, welche Programme man ausführen darf und kann unerwünschte Programme blockieren. Das ist vermutlich eine (krude) Idee, um die Sicherheit von MacOS zu verbessern. Es gibt Apple die Möglichkeit, unerwünschte Programme anhand einer Blacklist zu blockieren. Aber es nimmt den Nutzern die Kontrolle über die Software, die sie verwenden wollen.

Es werden dabei nicht nur die Nutzer kontrolliert. Apple ist damit auch in einer Machtposition, die eigenen Richtlinien und Moralverstellungen gegenüber den Entwicklern von Software und Betreibern von Diensten durchzusetzen, wie Apple es beim iPhone AppStore bereits mehrfach mit der Androhning demonstrierte, die App aus dem Store löschen:

- ProtonMail wurde gezwungen, In-App Bezahlungen anzubieten (von denen Apple 30% Provision kassiert) und musste die Option zu den gleichen Konditionen anbieten wie auf der Webseite. ProtonMail CEO Andy Yen nannte es: Mafia Methoden.

- Bei ProtonVPN musste der Hinweis aus der Beschreibung der iPhone App entfernt werden, dass das VPN zur Umgehung von Zensur geeignet ist.


(Apple bestreitet, die Lösung der belarussischen Kanäle gefordert zu haben. Aber Pavel Durov schreibt, dass die Formulierung keine andere Interpretation zulässt.)

Mit dem AppStore für iPhones kontrolliert Apple exklusiv die Software auf 25% der weltweit genutzten Smartphones und nutzt diese Machtstellung zur Durchsetzung von Regeln, die in anderen Ökosystemen undenkbar wären. Mit den Innovationen in MacOS 11 (Big Sur) schafft sich Apple diese Möglichkeit auch für die PCs und Laptops mit MacOS.


Apple ist seit Oktober 2012 Partner im PRISM Programm der NSA.

18.3 Linux Distributionen

Es gibt eine Vielzahl von Linux Distributionen, so dass man als potentieller Anwender erst einmal vor der Qual der Wahl steht: Debian und Derivate, OpenSuSE, OpenMandriva, Fedora, Gentoo für Bastler, Minidistributionen wie Puppy oder Fortress Linux als gehärtete
Variante, KaliLinux... Ich kenne nicht alle Distributionen daher nur einige Gedanken.

Alltagstaugliche Distributionen mit Debian Abstammung:


- **Xubuntu** oder **Kubuntu** sind für Linux Einsteiger gut geeignet. Die gute Hardware Unterstützung für neue Technik kombiniert mit einfacher Standardinstallation umfangreicher Software inklusive Multimedia, klarem Bedienkonzept des Desktop ohne irgendwelche Cloud Anbindungen oder Übertragung von Daten an Dritte sowie Full-Disc-Encryption bei der Installation erleichtern den Einstieg.

  Den privacy-invasiven Crash Reporter von Ubuntu und das Report Submission Tool *whoopsie*, das täglich den Server daisy.ubuntu.com kontaktiert, kann man nach der Installation problemlos mit der bevorzugten Paketverwaltung entfernen. Im Terminal erledigt man das mit:

  ```
  > sudo apt purge whoopsie apport
  ```

  Die Deinstallation überflüssiger Software ist ein Sicherheitsfeature. Ein Bug im Crash Reporter *apport* konnte beispielsweise jahrelang dazu genutzt werden, um den Rechner aus der Ferne zu kompromittieren.\(^\text{14}\)

  Wenn man gerade mit dem Paketmanager spielt, könnte man auch folgendes Paket installieren, um Angriffe über TMP-Dateien zu erschweren:

  ```
  > sudo apt install libpam-tmpdir
  ```

- **Mint Linux** möchte das bessere Ubuntu sein und bietet vor allem einen anderen Desktop, der sehr hübsch ist und Windows Umsteigern den Einstieg erleichtert. Allerdings ist Mint keine komplett selbstständige Distribution sondern schmarotzt bei Ubuntu, was öfters für Verstimmung bei Canonical sorgte und die Probleme mit der mangelhaften Versorgung für Sicherheitsupdates einschließt. Mit LMDE gibt es auch eine Variante, die auf Debian basiert.

Alltagstaugliche Distributionen mit RHEL Abstammung:

- **RHEL** (RedHat Enterprise Linux) ist eine kommerzielle Linux Distribution, für die man nur Updates bekommt, wenn man eine Lizenz kauft. RedHat konzentriert sich auf Sicherheit im kommerziellen Umfeld und bietet deshalb SELinux Integration und eine deutlich kleinere Software Auswahl als Debian (vor allem bei Multimedia).


- **Fedora** ist die Community Version von RedHat, für die man auch ohne Lizenz Updates bekommt. In der Verbreitung liegt Fedora hinter Ubuntu auf Platz 2.

  Um eine mit Ubuntu vergleichbare gute Unterstützung für Multimedia zu erhalten, kann man das RPMfusion Repository einbinden und die gewünschten Multimedia Pakete installieren (was allerdings auch Nachteile hinsichtlich Sicherheit bringt, wenn man `bad` oder `ugly` Codecs installiert). Man könnte den VLC-Player installieren:

  ```
  > sudo dnf install vlc
  ```

  Neue Fedora Versionen erscheinen halbjährlich. Updates werden für ein Jahr + ein paar Wochen bereitgestellt. Es gibt keine Long Term Support (LTS) Versionen wie bei Ubuntu Derivaten, so dass man ein System regelmäßig komplett aktualisieren muss.

Distributionen auf Basis von Arch Linux:


  Um Probleme bei Updates zu vermeiden, sollte man Rolling Release Distributionen regelmäßig aktualisieren, damit Änderungen am Gesamtsystem klein bleiben.

- **Manjaro** ist die aufgehübschte Version von Arch Linux, die sich mit einem eleganten Desktop insbesondere an Windows Umsteiger wendet.

Immutable (unveränderbare) Distributionen:

- **Silverblue** ist ein immutable Desktop System auf Basis von Fedora. Mit Toolbox können Container für verschiedene Arbeits- und Testumgebungen erstellt werden.

  - Ein Container ist keine abgeschlossene Umgebung wie eine VM. Ein neuer Container stellt anfangs die gleiche Umgebung wie der Host zur Verfügung. Man kann die Daten im Homeverzeichnis aus dem Hostsystem lesen aber Änderungen und neue Dateien sind nur innerhalb des Container verfügbar.
  
  - In einem Container kann man Software ganz normal installieren, compilieren, testen usw. Die zusätzliche Software steht nur im Container zur Verfügung.


Eine Linux Distribution für besondere Sicherheitsanforderungen:

- **Qubes OS** ist eine Besonderheit unter den Linux Distributionen. Alle Anwendungen laufen in mehreren getrennten virtuellen Maschinen mit einem Xen-basierten Hypervisor, der die Gastsysteme überwacht und ihnen nur begrenzt Zugriff auf die Hardware lässt. Qubes OS bietet:

  15https://rpmfusion.org/Configuration
18.4 Linux-taugliche Hardware

- Die deutsche Firma TUXEDO Computers bietet 100% Linux-compatible Laptops und PCs in vielen Varianten, darunter auch Notebooks im edlen Design.\(^\text{16}\)
- Die Business Laptops von Lenovo (X2x0, T4x0, T5x0) sind robust und kompatibel mit aktuellen Linux Distributionen. Man kann sie auch gebraucht noch gut verwenden.

**Hardware für besondere Sicherheitsanforderungen**

- **NitroPad X230**\(^\text{17}\) (12,5"Display, 1366x768) und **NitroPad T430**\(^\text{18}\) (14"Display, 1600x900) basieren auf etwas älteren, robusten Thinkpad Business Laptops und ermöglicht ein neues Sicherheitserlebnis. Die Hardwareausstattung ist konfigurierbar.
  - Die Integrität des Coreboot BIOS, des TPM und des Kernels des Betriebssystems kann mit einem Nitrokey Pro oder Nitrokey Storage verifiziert werden, der vor dem Booten eingesteckt wird und grün blinkt, wenn alles Ok ist.
  - Intel Management Engine (ME) ist aus Sicherheitsgründen entfernt.
  - Die Laptops werden werden wahlweise mit einem vorinstalliertem Ubuntu LTS oder QubesOS als Betriebssystem ausgeliefert. Eine vollständige Verschlüsselung der Festplatte ist dabei eingerichtet - sofort startfertig.


- **Die Purism Laptops** (Librem 14, Librem 15) und der **Purism Mini** bieten ebenfalls diese besonderen Sicherheitsfeatures:

\(^{16}\)https://www.tuxedocomputers.com
\(^{17}\)https://shop.nitrokey.com/de_DE/shop/product/nitropad-x230-67
\(^{18}\)https://shop.nitrokey.com/de_DE/shop/product/nitropad-t430-119
Es kommt ein reduziertes Coreboot BIOS zum Einsatz. Die Integrität des BIOS kann mit dem Librem Key verifiziert werden (BIOS Tamper Schutz).

Der Librem Key kann auch als Schlüssel für die Full-Disk-Encryption verwendet werden. Es ist ein modifizierter Nitrokey, der als OpenPGP- oder SSH-Schlüssel, als Passwortspeicher und OTP-Token für 2-Faktor-Auth. genutzt werden kann.

Hardware Kill Switches für Mikrofon, Kamera, Wi-Fi und Bluetooth schützen gegen Angriffe, die das Gerät in eine Spionage-Wanze verwandeln.

Das standardmäßig installierte Betriebssystem PureOS ist allerdings vernachlässigt. Es ist empfehlenswert, statt PureOS das gut gepflegte QubesOS zu installieren. Purism Laptops sind voll kompatibel mit QubesOS 4.0. Das wäre eine ideale Kombination von Hardware und Software für hohe Sicherheitsanforderungen.


### 18.5 NetBSD und OpenBSD

Diese beiden BSDs sind konsequent und ohne Kompromisse hinsichtlich Benutzerbarkeit auf Sicherheit optimiert. Wenn man mehrere Jahre Erfahrung mit mit einem UNIX-artigen System (z. B. Linux) gesammelt hat und hinreichend leidensfähig ist, dann kann man auch diese beiden Betriebssysteme einsetzen und sich an den Vorteilen erfreuen.

Die Optimierung auf Sicherheit gilt nur für das Betriebssystem, nicht für Anwendungen oder zusätzliche Bibliotheken. Gelegentlich werden Sicherheitsfeatures von Bibliotheken wie z. B. OpenSSL unterlaufen, denen das sichere Allocieren von Speicher bei NetBSD und OpenBSD zu langsam war und deren eigene Implementierung dann zum Heartbleed Bug führte.

Anwendungen wie X11, Mozilla Firefox oder Thunderbird lassen sich in der höchsten Sicherstufe von NetBSD und OpenBSD nicht installieren. In NetBSD muss man in der Datei /etc/mk.conf folgende Option setzen:

```
ALLOW_VULNERABLE_PKGAGES=yes
```

### 18.6 Risiko USB, Firewire und Thunderbolt


Sogenannte BadUSB Devices müssen kaum Sicherheitshürden überwinden und auch keine 0-day Exploits einsetzen. Sie können die vielfältigen technischen Features neu kombinieren, um unschöne Dinge anzustellen. USB-Geräte (z. B. USB-Sticks von Fremden) können neben der sichtbaren Funktion (z. B. als Speichermedium) weitere verdeckte Funktionen enthalten, die man nicht bemerkt. Sie können sich heimlich als USB-Tastatur ausgeben und Kommandos senden oder sich als Netzwerkkarten ausgeben und Daten umleiten.

---

19. https://puri.sm/posts/the-librem-key-makes-tamper-detection-easy/
18.6. RISIKO USB, FIREWIRE UND THUNDERBOLT


• Im Nov. 2016 hat Samy Kamkar mit PoisonTap[23] ein weiteres BadUSB Device vorgestellt. Wenn der Angreifer physischen Zugang zu einem Computer oder Laptop mit aktiviertem Passwortschutz hat (z. B. durch Bildschirmschoner) und auf dem Rechner noch ein Browser geöffnet ist, dann kann PoisonTab mit einigen kleinen Tricks die Online Accounts (E-Mail, Twitter, Facebook...) des Targets übernehmen, die mit diesem Browser genutzt wurden. Der Angreifer muss nur PoisonTab am USB Port anschließen und warten.

Ein besonderes Risiko sind USB-Sticks oder USB-Festplatten, die man bedenkenlos an unterschiedlichen Computern in verschiedenen Netzen nutzt.


• Einige spektakuläre Beispiele aus den Medien zeigen, dass es im Cyberwar üblich ist, Malware auf USB-Stick in schwer zugängliche Netzen zu transportieren. Dabei kann der USB-Stick extra präpariert werden oder man greift die schlecht gesicherten Rechner mehrere Targets zuhause an und hofft, dass der Trojaner von einem Wirt mit einem USB-Stick in das gesicherte Netzwerk getragen wird.


– Stuxnet wurde von einem Mossad Agenten mit einem USB-Stick in die Urananfallbereitungsanlage im Iran gebracht.


Bei Firewire (IEEE 1394) und Thunderbolt Schnittstellen ist das Risiko noch größer. Im Gegensatz zu USB wird bei diesen Schnittstellen keine Master-Slave Kommunikation genutzt. Über Firewire und Thunderbolt haben angeschlossene Geräte via DMA (Direct Memory Access) vollen Zugriff auf den Hauptspeicher des PC und können z. B. eine Kopie auslesen.

• 2008 wurde demonstriert, wie man den Windows Login mit einem Firewire Gerät umgehen kann. Microsoft sah keinen Handlungsbedarf, da die Funktionalität der Firewire Spezifikation entspricht. Es ist also kein Bug sondern ein Feature.


[22] https://www.youtube.com/watch?v=nuruzFqMglw
[24] https://heise.de/-1198049
• Die Datenverschlüsselung kann umgangen werden (für alle Produkte), da Keys aus dem Hauptspeicher ausgelesen werden können. Geheimdienste nutzen passende Tools routiniert, wenn sie physischen Zugriff auf den Zielrechner haben.

Hinweise zur Verbesserung der Sicherheit


2. Um Daten von USB-Sticks zu bearbeiten oder Fotos von der Digicam auf einer USB-Festplatte zu archivieren, kann man eine Live-DVD nutzen. Insbesondere sollte man eine Live-DVD nutzen, wenn man Daten aus der Firma zuhause bearbeiten und wieder mit in die Firma nehmen will.

3. Zum Aufladen von Geräten kann man USB-Ladegeräte nutzen. Man muss nicht alles, was wie ein USB-Stecker aussieht, in den Computer einführen. Das BSI warnt davor, E-Zigaretten via USB-Anschluss am Computer aufzuladen und rät zu einem USB-Ladegerät, da einige chinesische Produkte im Hintergrund Malware installieren.\(^{25}\)


5. Es gibt zahlreiche Freeware Tools, um USB-Schnittstellen unter Windows zu sperren. (z. B. den USB-Blocker\(^ {27}\) von securityXploded.com)

   - Für Windows stellt MS einen Support Artikel bereit: *Blockieren des SBP-2-Treibers und der Thunderbolt-Controller, um Bedrohungen für BitLocker zu reduzieren.*\(^ {28}\)
   - Unter Linux kann man prüfen, ob das System Firewire Schnittstellen beim Booten erkannt hat:

   ```bash
   > lspci | grep -i Firewire
   ```

   Wenn der Rechner Firewire Schnittstellen hat, dann kann man die Kernelmodule für diese Schnittstellen sperren. Man speichert eine Datei `firewire.conf` im Verzeichnis `/etc/modprobe.d/` mit folgendem Inhalt:

   ```
   blacklist firewire-ohci
   blacklist firewire-sbp2
   ```

   Danach führt man folgende Kommandos aus:

   ```
   > sudo depmod -ae
   > sudo update-initramfs -u
   ```

**USBGuard für Linux**

USBGuard für reglementiert die Nutzung von USB-Geräten. Es dürfen nur USB-Geräte genutzt werden, die in einer Whiteliste freigegeben wurden. Alle anderen USB-Spielzeuge werden blockiert. Das Tool ist in allen aktuellen Linux Distributionen enthalten und kann mit dem bevorzugten Paketmanager installiert werden:

   ```
   Debian: > sudo apt install usbguard
   Fedora: > sudo dnf install usbguard
   ```

---

\(^{25}\) https://heise.de/-3222811

\(^{26}\) https://dkopecek.github.io/usbguard/

\(^{27}\) http://securityxploded.com/windows-usb-blocker.php

\(^{28}\) https://support.microsoft.com/kb/2516445/de
Nach der Installation muss man einen initialen Regelsatz erzeugen, der zumindest eine via USB angeschlossene Tastatur und Maus freigibt (sonst spernt man sich aus). Es ist sinnvoll, auch weitere USB-Geräte anzuschließen, die man später nutzen möchte (Backup USB-Stick oder -Festplatte, Nitrokey usw.). Dann kann man mit folgendem Kommando die initiale Konfiguration erstellen, die alle angeschlossenen Geräte erlaubt und den Rest spernt:

```
> sudo usbguard generate-policy > rules.conf
```

Die erstellte Konfiguration muss man dann in das Konfigurationsverzeichnis `/etc/usbguard` kopieren und sichere Zugriffrechte für die Datei setzen:

```
> sudo cp rules.conf /etc/usbguard/rules.conf
> sudo chmod 0600 /etc/usbguard/rules.conf
```

In der Konfiguration `/etc/usbguard/usbguard-daemon.conf` sind kleine Anpassungen empfehlenswert, bevor man USBGuard verwendet:

- Mit strengen Regeln wird sichergestellt, dass alle Regeln auch für USB Spielzeuge angewendet, die bereits vor dem Booten angeschlossen wurden:

  ```
  PresentDevicePolicy = apply-policy
  PresentControllerPolicy = apply-policy
  ```

- Es kann allerdings vorkommen, dass man eine kaputte Tastatur mal austauschen muss. Mit strengen Regeln hat man sich dann ausge sperrt. Als etwas lockere Variante kann man alle Geräte zulassen, die beim Bootes des Rechners angeschlossen sind:

  ```
  PresentDevicePolicy = allow
  PresentControllerPolicy = apply-policy
  ```

Gegen Evil Maid Angriffe (jemand bootet den Rechner in Abwesenheit des Besitzers und nutzt ein BadUSB Device), schützt eine vollständige Verschlüsselung der Festplatte. Somit ist das Risiko durch etwas lockere Einstellungen überschaubar.

Danach kann man den USBGuard Daemon starten und für zukünftige Reboots aktivieren:

```
> systemctl start usbguard
> systemctl enable usbguard
```

Alle unbekannten USB-Geräte werden zukünftig blockiert. Wenn man ein ein neues USB-Spielzeug verwenden möchte, kann man es im Terminal freigeben. Dafür schließt man das Gerät an und lässt sich alle vorhandenen USB-Geräte anzeigen:

```
> sudo usbguard list-devices
...
29: block id 20a0:4107 serial "" name "Crypto Stick v1.2" hash "li65uJm8....
```

Die Nummer am Anfang der Zeile ist die ID, mit der man das Gerät freigeben kann:

```
> sudo usbguard allow-device 29
```

Wenn man das USB Spielzeug öfters verwenden möchte, kann man es dauerhaft freigeben, indem man die Option --permanent bzw. -p hinzufügt. Die Regel wird dann in die Datei `/etc/usbguard/rules.conf` eingetragen:

```
> sudo usbguard allow-device --permanent 29
```

Mit dem folgenden Kommando kann man eine Freigabe widerrufen, solange das USB Spielzeug noch angeschlossen ist:

```
> sudo usbguard allow-device --permanent 29
```

Wenn man eine permanente Freigabe löschen möchte und das USB Spielzeug nicht angeschlossen ist, kann man sich die Regeln anschauen und die Regel löschen:
Die umständliche Freigabe von unbekannten USB-Geräten auf der Kommandozeile und nur für den administrativen User ist etwas umständlich aber auch ein Sicherheitsfeature. Wer es etwas weniger streng haben möchte, kann auch anderen Nutzern die Modifikation der Regeln erlauben. Dafür ist folgende Option in der Konfigurationsdatei /etc/usbguard/usbguard-daemon.conf anzupassen:

```
IPCAllowedUsers = root username1 username2 ...
```

Die in der Liste genannten User können das Kommando usbguard wie beschrieben nutzen, um neue USB-Geräte zu erlauben oder Freigaben aufzuheben.

### 18.7 Linux Firewall konfigurieren

Es gibt sicherheitsorientierte Linux Distributionen wie RHEL oder QubesOS, die standardmäßig eine Firewall und ein GUI zur Konfiguration installieren, welche erstmal alle Verbindungsversuche von außen blockiert. Viele Mainstream Distributionen wie Ubuntu(s), Linux Mint, ARCH Linux oder Manjaro/KDE verzichten bei der Standardinstallation auf eine Firewall oder aktivieren sie nicht automatisch nach der Installation.

#### 18.7.1 Uncomplicated Firewall (UFW)

UFW ist eine einfach zu konfigurierende Firewall für Debian, Ubuntu(s), Linux Mint, ARCH Linux oder Manjaro, die man schnell installieren und in Betrieb nehmen kann. Linux Mint und Manjaro installieren die Firewall standardmäßig aber aktivieren sie nicht automatisch. In Debian und Ubuntu(s) erledigt man die Installation mit dem Kommando:

```
> sudo apt install ufw
```

Nachdem UFW installiert wurde, muss man die Firewall noch aktivieren:

```
> sudo ufw enable
```

Das Ergebnis ist eine Firewall, die alle Verbindungsversuche von außen blockiert aber für lokale Programme ist die Kommunikation nach außen ermöglicht. Für viele Anwender ist das wahrscheinlich ausreichend. Anpassungen sind möglich. Man kann einzelne Dienste freischalten, die von außen erreichbar sein sollen:

```
> sudo ufw allow ssh
```

Das Löschen der Freigabe erfolgt, indem man ein `delete` einfügt:

```
> sudo ufw delete allow ssh
```

Die Liste der vordefinierten Dienste kann man sich mit folgendem Kommando anschauen:

```
> sudo ufw app list
```

Wenn keine passenden vordefinierten Dienste vorhanden sind, kann man auch Ports angeben. Für den I2P Router kann man beispielsweise den Port 8888 freischalten: Die Liste der vordefinierten Dienste kann man sich mit folgendem Kommando anschauen:

```
> sudo ufw allow 8888
```

Man kann einzelne Dienst wie CUPS nur für das lokale Netzwerk freigeben:

```
> sudo ufw proto Tallow 631 from 192.168.1.0/24
```

Man kann ausgehende Protokolle sperren, die man nicht nutzen möchte:
Oder man könnte auch sehr restriktiv vorgehen, standardmäßig alle ausgehenden Dienste sperren und dann nur für einzelne Protokolle die Kommunikation nach außen erlauben:

```bash
> sudo ufw default reject outgoing
> sudo ufw allow out http
> sudo ufw allow out https
... 
> sudo ufw allow out dns to <ROUTER-IP>
```

Den DNS Traffic sollte man nicht vergessen. Road Warrior sollten auf die IP des Routers in der DNS Regel verzichten, wenn sie unterschiedliche Netze nutzen.

Den Status der Firewall kann man mit folgendem Kommando prüfen:

```bash
> sudo ufw status verbose
```

![Abbildung 18.2: GUFW Hauptfenster](image)

Es gibt ein grafisches Frontend GUFW, dass man mit dem bevorzugten Paketmanager installiert, wenn es noch nicht vorhanden ist, unter Debian/Ubuntu mit:

```bash
> sudo apt install gufw
```

GUFW kann mehrere Profile verwalten, wenn man auf dem Laptop zuhause andere Einstellungen verwenden möchte als unterwegs. Das Hinzufügen von Regeln ist einfach möglich, auch wenn die Regeln ein bisschen komplizierter sind.

### 18.7.2 RHEL Firewall

Bei RHEL wird standardmäßig der `firewalld` und ein GUI zur Verwaltung der Firewall Regeln installiert. `firewalld` unterscheidet zwischen einer temporären Runtime Konfiguration und einer permanenten Konfiguration. Wenn man Regeln dauerhaft speichern möchte, dann darf man nicht vergessen, auf die permanente Konfiguration umzuschalten.

`firewalld` unterscheidet zwischen Zonen, für die unterschiedliche Firewallregeln gelten können. Für jede Netzwerkschnittstelle kann festgelegt werden, welcher Zone sie zugewiesen ist. Es ist ein Tool, das sich gut für komplexe Server Architekturen eignet.

Die `firewalld` Konfiguration in Fedora erlaubt standardmäßig eingehende Verbindungen von außen auf den nicht-priviligierten Ports > 1024.
KAPITEL 18. BETRIEBSSYSTEME

Abbildung 18.3: RedHat Firewall Konfigurator

18.7.3 QubesOS Firewall

QubesOS enthält standardmäßig eine Firewall, die in einer eigenen VM läuft. In der Default Konfiguration können die Dienste in den Arbeits-VMs nicht erreicht werden aber aus den Arbeits-VMs heraus sind alle Verbindungen möglich.

In den Einstellungen zu jeder einzelnen VM kann man den Datenverkehr komplett blockieren, indem man Networking deaktiviert. Außerdem kann man restriktivere Firewall Einstellungen anwenden, indem man nur für bestimmte Protokolle ausgehende Verbindungen zulässt (Abb. 18.4).

18.8 WLAN Privacy Leaks

Wenn man mit dem Laptop unterwegs ist und WLANs in Internet Cafe’s, am Flughafen, in der Firma oder im Hotel nutzt, dann bekommt man die Netzwerkkonfiguration (eigene IP-Adresse, DNS-Server...) via DHCP-Protokoll zugeteilt. Damit hinterlässt man auf dem DHCP-Server Spuren, die C. Huitema von der IETF in der Studie Unique Identifiers in DHCP options enable device tracking zusammengefasst hat:

1. Die MAC-Adresse wird an den DHCP-Server übermittelt und ist eine weltweit eindeutige Kennung für die Hardware des Rechners (Netzwerkschnittstelle oder WLAN-Modul).

   • In IPv4 Netzen wird diese Kennung nur bis zum Router/Gateway übertragen. Im eigenen Home-Netz braucht man sich also keine Gedanken machen, aber in fremden WLANs (Hotel, Internetcafe’, Flughafen) ist davon auszugehen, dass die MAC-Adressen der Nutzer protokolliert werden.

29 [Link](https://tools.ietf.org/html/draft-huitema-perpass-dhcp-identifiers-00)
• In IPv6 Netzen wird die MAC-Adresse Bestandteil der IP-Adresse, wenn die Privacy Extension for IPv6 nicht aktiviert wurde. Damit wird die IP-Adresse zu einem personenbezogenen Merkmal und kann zur Wiedererkennung und zum Tracking genutzt werden.


3. Der konfigurierte Hostname und die DNS-Domain des Rechners wird an den DHCP-Server übermittelt.

Wenn man die automatische Anmeldung für die bevorzugte WLANs aktiviert hat, dann sendet der Laptop unterwegs (am Flughafen, im Hotel, in der U-Bahn...) ständig sogenannte Probes, um die Umgebung nach den bevorzugten WLANs zu scannen.

• Die Probes haben einen eindeutigen Fingerprint und können in gleicher Weise wie MAC-Adressen für das Tracking der Geräte verwendet werden, wie die Studie Why MAC Address Randomization is not Enough demonstrierte.30

• Mit den Probes auch eine Liste der bevorzugten WLANs gesendet, mit denen sich der Laptop automatisch verbinden würde (Preferred Network List, PNL). Diese Preferred Network List liefert Informationen über Orte, an denen sich der Besitzer des Laptops bevorzugt aufhält.

• Praktische Angriffe mit den Informationen aus den Probes hat die Security Firma Sensepost mit der Drohne Snoopy vorgestellt. Diese Drohne simuliert die SSID eines bevorzugten WLANs. Der Laptop meldet sich automatisch bei der Drohne an, der Internet Traffic läuft über die Drohne und kann dort analysiert werden. Es wurde z. B. demonstriert, wie Snoopy die Login Credentials für PayPal, Yahoo! usw. abreifen konnte.31

Um keine eindeutigen Spuren als Road-Warrior in Internet Cafe’s oder am Flughafen zu hinterlassen, kann man die MAC-Adresse faken, automatische Anmeldung für alle WLANs deaktivieren, PXE Boot im BIOS des Rechners deaktivieren und nichtssagenden

18.8.1 MAC-Adresse faken (Windows 10)

Windows 10 enthält alles, was man braucht, um die MAC-Adressen für WLAN-Verbindungen zu faken. Bevor(!) man sich unterwegs im Hotel, am Flughafen oder in der Berliner U-Bahn mit einem neuen WLAN verbindet, kann man die Randomisierung der MAC-Adresse aktivieren. Die Einstellungen werden alle in der Sektion Netzwerk und Internet auf dem Reiter Wi-Fi vorgenommen, siehe Bild 18.5.

1. Als erstes muss man unter Manage Wi-Fi settings die Randomisierung der MAC Adressen global einschalten, damit diese Funktion danach für einzelne WLANs konfiguriert werden kann. Außerdem wird immer eine zufällige MAC-Adresse für den Scan nach WLANs verwendet, wenn die Randomisierung global aktiviert wurde.


3. Die Option automatisch Verbinden sollte man für alle WLANs deaktivieren. Wenn die Option für ein oder mehrere WLAN Verbindungen aktiviert wurde, dann sendet der Rechner ständig sogenannte Probes, um aktiv nach diesen WLANs in der Umgebung zu suchen. Die Probes haben einen eindeutigen Fingerprint und können in gleicher Weise wie MAC-Adressen für das Tracking der Geräte verwendet werden.

4. Dann kann man sich mit dem WLAN verbinden.

Abbildung 18.5: MAC-Adresse faken für Windows 10

18.8.2 MAC-Adresse faken (Linux)

Der NetworkManager enthält alle nötigen Features, um die MAC-Adressen zu faken. Zusätzliche Tools sind nicht nötig. Beim Netzwerksscan wird standardmäßig eine zufällig
generierte MAC-Adressen verwendet. Beim Verbindungsaufbau verwendet der Networkmanager standardmäßig die echte MAC-Adresse.

Um beim Verbindungsaufbau eine Fake MAC zu verwenden, kann man die folgende Konfigurationsdatei unter `/etc/NetworkManager/conf.d/50-macchange.conf` speichern:

```ini
[connection-mac-randomization]
ethernet.cloned-mac-address=random
wifi.cloned-mac-address=stable
```

Für die Generierung der Fake MAC-Adressen gibt es zwei Möglichkeiten:

- **random**: es wird bei jedem Verbindungsaufbau eine neue Fake Adresse generiert.
- **stable**: es wird für ein WLAN immer der gleiche Fake verwendet aber für verschiedene WLANs unterschiedliche Fake Adressen. Das erleichtert meist den Login in bekannten Wi-Fi Hotspots, beispielsweise wenn man in einem Hotel immer die gleiche MAC Adresse verwenden muss. Es verhindert aber die Wiedererkennung anhand der MAC-Addr. in anderen WLANs.

In den Netzwerkeinstellungen kann man den Fake Mode anpassen und die **Duplizierte Adresse** vom oben konfigurierten Standardwert `stable` auf `random` setzen (Abb: 18.6).

![Abbildung 18.6: Fake Mode für MAC Adresse im NetworkManager anpassen](image)

Man kann die Fake Methode für ein WLAN auch individuell auf der Kommandozeile anpassen. Das erste Kommando zeigt eine Liste der Netzwerke an und das zweite Kommando ändert die Fake Methode für das WLAN mit dem Namen WIFIonICE auf `random`:

```bash
> nmcli connection show
...
> nmcli connection modify "WIFIonICE" wifi.cloned-mac-address random
```

### 18.8.3 Automatische Anmeldung für bevorzugte WLANs deaktivieren

Wenn man die **automatische Anmeldung** für WLANs aktiviert hat, sendet der Laptop unterwegs (am Flughafen, im Hotel, in der U-Bahn...) ständig sogenannte **Probes**, um die Umgebung nach den bevorzugten WLANs zu scannen.

...
Diese Probes haben einen eindeutigen Fingerprint und können in gleicher Weise wie MAC-Adressen für das Tracking der Geräte verwendet werden, wie die Analyse *Why MAC Address Randomization is not Enough* demonstrierte. In den Einstellungen der WLAN-Verbindungen muss man für alle konfigurierten WLANs die Option *Automatisch Verbinden* abschalten, um Probes unterwegs mit dem Laptop zu vermeiden (Abb: 18.7).

Abbildung 18.7: Automatische Anmeldung für WLANs deaktivieren

18.8.4 Hostname und DNS-Domain konfigurieren

Hostname und Domain kann man bei der Installation des Betriebssystems festlegen oder nachträglich ändern. Es gibt keine wirklich anonyme Empfehlung für diese Werte. Wir empfehlen die folgende nichts aussagende Werte, die auch von Live-DVDs wie TAILS u.a. verwendet werden:

Hostname: host
Domain: localdomain

Wenn man Linux verwendet, kann man den Hostnamen nachträglich mit folgenden Kommandos ändern:

```
> sudo hostname host
```

Um die DNS-Domain unter Linux nachträglich zu ändern, sind folgende Zeilen in der Datei `/etc/hosts` anzupassen:

```
127.0.0.1 host.localdomain host
::1 host.localdomain host
```

Man kann den NetworkManager auch dazu überreden, beim Aufbau einer Netzwerkverbindung keinen Hostnamen an den DHCP-Server zu senden. Dafür sind folgende Zeilen in der Datei `/etc/NetworkManager/NetworkManager.conf` einzutragen:

```
[ipv4]
dhcp-send-hostname=false
```
Kapitel 19

Smartphones


Braucht man das Ding wirklich oder ist es nur ein nettes Lifestyle Gadget? Für den Berliner Philosophen und Medientheoretiker Byung-Chul Han sind Smartphones das wesentliche Element zur Kontrolle der Bevölkerung im Zeitalter der Psychomacht:

_Jede Herrschaftstechnik bringt eigene Devotionalien hervor, die zur Unterwerfung eingesetzt werden. Sie materialisieren und stabilisieren die Herrschaft ... Das Smartphone ist eine digitale Devotionalie, ja die Devotionalie des Digitalen überhaupt. Es funktioniert wie der Rosenkranz. Beide dienen der Selbstprüfung und Selbstkontrolle. Like ist das digitale Amen. Das Smartphone ist nicht nur ein effizienter Überwachungsapparat, sondern auch ein mobiler Beichtstuhl. Facebook ist die Kirche, die globale Synagoge._

(Für manche Leute ist es Facebook, für andere Instagram oder Twitter oder... aber immer ist man online und auf der Jagd nach Likes.)


_Es entsteht ein fast vollständiges Modell. Mit der Beobachtung der Signale kann man ganze Firmen, ganze Städte, eine ganze Gesellschaft röntgen._

10 Jahre später sind die Vision von Greg Skibiski Wirklichkeit. Bewegungsdaten von Smartphones werden im Corona-Jahr 2020 routiniert verwendet, um die Bevölkerung zu durchleuchten und mehr oder weniger interessante Analysen zu veröffentlichen:

- Das Statistische Bundesamt analysiert die Veränderungen der Fahrgastzahlen der Deutschen Bahn nicht anhand der Verkäufe von Fahrrätschen und Platzkarten (was vielleicht naheliegend wäre) sondern anhand der Bewegungsdaten von Mobiltelefonen. Ergebnis: die Fahrgastzahlen sind 2020 um 50% niedriger als im Vorjahr.

- Zu Weihnachten und Silvester 2020 führt das Statistische Bundesamt eine außerplanmäßige Sonderauswertung der anonymisierten Mobilfunkdaten durch, um die Einhaltung der Coronabeschränkung durch die Bevölkerung zu prüfen.

In München und Stuttgart wurde die Einhaltung der Ausgangssperre zu Silvester 2020/21 anhand der Mobilfunkdaten beobachtet. In beiden Städten war die Mobilität in der Silvesternacht um rund 80% geringer als in den Vorjahren.

Man könnte den braven Bürger simulieren und das Smartphone zuhause lassen, wenn es nicht so schwer fallen würde, auf das kleine Gadget kurze Zeit zu verzichten.

Der CSU Politiker U. Brandl schlägt in einem Interview vor, auf die Anonymisierung der Mobilfunkdaten zu verzichten und die Bewegungsdaten aller Bürger der Polizei zur Auswertung und zur Durchsetzung von Ausgangsbeschränkungen zu Verfügung zu stellen, insbesondere um die Einhaltung der 15km-Regel durchzusetzen.\footnote{https://www.br.de/nachrichten/bayern/15-kilometer-regel-brandl-fordert-auswertung-von-handy-daten}

Wir müssen einfach mehr Mut haben, dass man die digitalen Möglichkeiten nutzt.

Man sollte sich darüber im Klaren sein, dass es gegen die Lokalisierung und Beobachtung von Bewegungsprofilen keinen technischen Schutz gibt.

19.1 Kommerzielle Datensammlungen

Bei den möglichen Gewinnen durch die Auswertung und Verarbeitung von Daten, die mit Smartphones und Apps gesammelt werden, wundert es nicht, dass viele Teilnehmer aggressiv bei den Datensammlungen beteiligt sind.

19.1.1 Datensammlungen der Smartphone Hersteller


Seit iOS Version 8 übertragen Apples Mobilgeräte automatisch die Liste der Telefonanrufe an Apple-Server (Telefonnummer, Datum/Uhrzeit, Dauer). Diese Datenspeicherung kann man nur verhindern, wenn man die iCloud komplett abschaltet.


19.1. KOMMERZIELLE DATENSAMMLUNGEN

Google Android: die tief im System verankerte Google Play Service App sendet alle 20min folgende Daten an Google:

- Telefonnummer und SIM-Kartennummer
- Gerätenummer (IMEI) und Seriennummer des Gerätes
- WLAN-MAC-Adresse und IP-Adresse
- Android-ID (E-Mail Adresse des Google Kontos)
- Standort (wenn die Standortverfolgung aktiv ist)


Auch Googles Smartphones übertragen seit April 2016 die gesamte Call History (Telefonnummer, Datum/Uhrzeit, Dauer). Zur Call History gehören auch die Metadaten verschlüsselter Anrufe mit Messenger Apps wie Signal, Telegram, Elements oder Videokonferenzen via Zoom App. In Googles Datenschutz Policy steht:

Wenn Sie unsere Dienste nutzen, um Anrufe zu tätigen und zu erhalten oder um Nachrichten zu senden und zu empfangen, erheben wir möglicherweise Telefonie-Informationen wie Ihre Telefonnummer, die Anrufernummer, die Nummer des Anrufers, die Zeit und Uhrzeit von Anrufen und Nachrichten, die Dauer, Routing-Informationen und die Art der Anrufe.

Die Call History wird wie alle anderen Daten für die Optimierung der Werbung verwendet und auch an Werbepartner weitergegeben. Anhand der Daten werden Vermutungen über sexuelle Vorlieben, politische Orientierung und andere Themen erstellt. Die Privacy Policy von Google beschreibt es als gaaaanz harmlos:

Diese Daten verwenden wir beispielsweise, um Ihnen ein YouTube-Video zu empfehlen, das Ihnen gefallen könnte.

Da Google seit 2009 Partner im PRISM Spionageprogramm der NSA ist, kann man wohl davon ausgehen, dass…

Neben Google können auch Apps die Call History absaugen, wenn sie die Berechtigung Reading SMS and Call Logs haben. Die Facebook App² nutzte natürlich diese Möglichkeit und sammelte die Call History von Smartphones ein, auf denen die App installiert war. Seit 2019 hat Google diese Berechtigung für Apps etwas eingeschränkt. Apps benötigen eine Erlaubnis von Google für den Zugriff auf die Call History.³

Es ist manchmal verwunderlich, wenn Leute seit 20 Jahren gegen die gesetzliche Verpflichtung zur Vorratsdatenspeicherung (bzw. Mindestspeicherpfllicht) kämpfen und bei ihren Lieblings-Lifestyle-Gadgets keine Probleme damit haben, wenn Apple oder Google die Kommunikationsdaten freiwillig auf Vorrat sammeln und Behörden zur Verfügung stellen.


Es werden nur die Standortortdaten an Server von Huawei übertragen, wenn man Apps aktiv nutzt, die auf den Standort zugreifen und dabei Informationen über WLANs in der Umgebung zur Verbesserung der Genauigkeit verwenden.

KAPITEL 19. SMARTPHONES

/e/ Android: Die googlefreien Smartphones der /e/ Foundation mit dem installierten Custom ROM /e/ verwenden standardmäßig keine Cloud Dienste und übertragen keine Daten an die /e/ Foundation. Um Cloud Funktionen zu nutzen, kann man einen Account bei der /e/ Cloud erstellen oder eine eigene Nextcloud Instanz nutzen.

Erfahrene Nutzer können das Costum ROM von /e/ auch auf einem vorhandenen Google Smartphone installieren und damit Google rauswerfen. Es werden aktuell 93 Android Smartphones unterstützt (Stand Okt. 2020).

19.1.2 Datensammlungen mit Smartphone Apps

Standortdaten: Tausende Apps sammeln überflüssigerweise Standort- und Bewegungsdaten der Nutzer. Der ehem. Bundesdatenschutzbeauftragte erwähnt beispielsweise eine App, die das Smartphone zur Taschenlampe macht und dabei den Standort an den Entwickler der App sendet (vielleicht lustig bis harmlos?)


Der norwegische Journalist M. Gundersen hat in einer Recherche die Datensammlung der Firma Venntel genau analysiert. Im Februar 2020 hat er auf einem neuen Smartphone 160 Apps installiert und dieses Smartphone ständig bei sich getragen. Keine der 160 Apps nannte die Firma Venntel in ihren Datenschutzklauseln.\(^7\)


Venntel informiert M. Gundersen auch darüber, dass seine Daten an die zahlenden Kunden der Firma weiterverkauft wurden, nannte aber keine Namen von Kunden.


\(^7\)https://nrkbeta.no/2020/12/03/my-phone-was-spying-on-me-so-i-tracked-down-the-surveillants
19.1. KOMMERZIELLE DATENSAMMLUNGEN

Für den Daten- und Überwachungsforscher Wolfie Christl hat diese Form der Überwachung eine völlig neue Qualität:

> Ich habe das Gefühl, dass viele nicht verstehen, dass dies völlig beispiellos ist und anders als das ist, was Edward Snowden im Jahr 2013 aufdeckte.

Fun Fact: Die NSA forderte im August 2020 die Mitarbeiter in der Spionage Community auf, auf den privaten Smartphones die Nutzung von Apps mit Standortverfolgung stark einzuschränken, weil auch andere Staaten diese Möglichkeiten nutzen.

**Browserverlauf:** Die Spiele der Hersteller iApps7 Inc, Ogre Games und redmicapps gehen in ihrer Sammelwut so weit, dass sie von Symantec als Malware eingestuft werden. Die Spiele-Apps fordern folgende Rechte um Werbung einzublenden:

- ungefährer (netzwerkbasierter) Standort
- genauer (GPS-)Standort
- uneingeschränkter Internetzugriff
- Browserverlauf und Lesezeichen lesen
- Browserverlauf und Lesezeichen erstellen
- Telefonstatus lesen und identifizieren
- Automatisch nach dem Booten starten

Auch Spiele von Disney verlangen sehr weitreichende Freigaben, so dass sie nur als Spionage-Tools bezeichnet werden können.

---
Adressbücher: Viele Apps beschränken sich nicht auf die Sammlung von Standortdaten und Anzeige von Werbung. Die folgenden Apps lesen die Kontaktdaten aus dem Adressbuch und senden sie ohne Freigabe durch den Nutzer an den Betreiber:

- die Social Networks Facebook, Twitter und Path
- die Location Dienste Foursquare, Hipster und Foodspotting
- die Fotosharing App Instagram
- die VoIP Software Viper sowie verschiedene Messaging Dienste
- ... 


Über die Firma Viper findet man kaum Angaben. Sitzt die Firma in Zypern, Israel, USA oder Weissrussland? Die auf der Webseite angegebene Kontakt-Adresse ist ein Briefkasten auf Zypern, Telefonnummern haben amerikanische Vorwahlen und die Domain versteckt sich hinter Domains by Proxy. Trotzdem haben bisher 50 Millionen Nutzer die Liste ihrer persönlichen Kontakte der Firma zur Verfügung gestellt.


Die Datenkonzerne werten die Daten natürlich parallel auch für ihre Interessen aus. So sammelt Facebook beispielsweise über diesen Weg große Mengen an Daten über Nichtmitglieder, die in sogenannten Schattenprofilen geführt werden.


- Prominentes Beispiel ist die MS Outlook App für iOS und Adroid. Das EU Parliaments IT department (DG ITECS) hat deshalb die Nutzung der MS Outlook

\(^9\)https://reports.exodus-privacy.eu.org/en/
\(^10\)https://reports.exodus-privacy.eu.org/en/reports/?filter=no_trackers
19.1. KOMMERZIELLE DATENSAMMLUNGEN

Abbildung 19.2: Die häufigsten Tracking Bibliotheken in Android Apps

App verboten. In dem Privacy Statement findet man den Hinweis, dass die Login Credentials für E-Mail Accounts (Username, Passwort) von Microsoft gesammelt werden und dass sich Microsoft die E-Mails von den Providern holt und verarbeitet:

Email Credentials: We collect and process your email address and credentials to provide you the service.

Email Data: We collect an process your email messages and associated content to provide you the service. […]

• M. Kuketz nennt in seinem Blog mit den E-Mail Apps BlueMail, TypeMail Mail.Ru, myMail u.a.m. weitere Beispiele. Mit der Einrichtung des E-Mail Accounts in der BlueMail App gibt man der Firma das Recht, in dem Mail Account zu schnüffeln:

When you link your email accounts (provided by third parties) to Blue Mail, you give Blue Mail permission to securely access your information contained in or associated with those accounts.

Außerdem beschnüffelt der BlueMail Server die E-Mails und wertet z. B. die Geolocation Tags in versendeten Fotos aus. Wer das nicht möchte, soll eine Kamera verwenden, die keine Geolocation Informationen in den Fotos speichert. Auch diese Schnüffelei wird juristisch korrekt im Privacy Statement benannt.

Vertrauenswürdige Alternativen für E-Mail Apps sind K9Mail oder FairEmail. Nach dem Wechsel auf eine vertrauenswürdige App sind die Passwörter für die betroffenen E-Mail Accounts zu wechseln!

12https://k9mail.app
13https://email.faircode.eu
KAPITEL 19. SMARTPHONES

19.2 Überwachung

Auch Strafverfolgungsbehörden und Geheimdienste nutzen die neuen Möglichkeiten zur Durchleuchtung der Gesellschaft:


- NSA/GCHQ sammeln täglich fast 200 Millionen SMS mit dem Programm DISHFiRE. Anhand der Datensammlung werden Kontaktbeziehungen (Identifizierung neuer Zielpersonen), Reisedaten, Finanztransfers (Konto- und Kreditkartennummern) u.a.m. analysiert.

- Das FBI nutzt das Tracking von Smartphones seit mehreren Jahren, wie Danger Room berichtete. Muslimische Communities werden systematisch analysiert, ohne dass die Personen im Verdacht stehen, eine Straftat begangen zu haben.¹⁴


- In der Ukraine wurden die Geofencing Daten von Handys bereits im Jan. 2014 zur Einschüchterung von Demonstranten genutzt. Teilnehmer einer Demonstration gegen den damals amtierenden Präsidenten bekamen eine SMS mit dem Inhalt:¹⁵

Sehr geehrter Kunde, sie sind als Teilnehmer eines Aufruhrs registriert.

Auch in Deutschland wird die Lokalisierung von Smartphones mittels Funkzellen auswertung zur Gewinnung von Informationen über politische Aktivisten genutzt:

- Die flächendeckende Auswertung von Handydaten im Rahmen der Demonstration GEGEN den (ehemals) größten Nazi-Aufmarsch in Europa in Dresden im Februar 2011 hat erstes Aufsehen erregt. Obwohl die Aktion von Gerichten als illegal erklärt wurde, werden die gesammelten Daten nicht gelöscht und weiterhin für die Generierung von Verdachtsmomenten genutzt.¹⁶


- Die breite Funkzellen auswertung in Berlin zur Aufklärung von Sachbeschädigungen wird als gängige Ermittlungsmethode beschrieben. Auf Anfrage musste die Polizei zugeben, dass diese Methode bisher NULL Erfolge gebracht hat.

- Die Nutzung der Stillen SMS zur Lokalisierung von Personen boomt gerade beim Verfassungsschutz:

  – 1. Halbjahr 2013: 28.500 Stille SMS versendet

¹⁵ https://www.heise.de/-2095284
¹⁶ https://www.heise.de/tp/artikel/34/34973/1.html
¹⁷ https://www.heise.de/tp/artikel/35/35043/1.html
19.3 AKTIVIERUNG ALS ABHÖRWANZE

– 1. Halbjahr 2014: 53.000 Stille SMS versendet
– 2. Halbjahr 2014: 142.000 Stille SMS versendet

Gleichzeitig stagniert die Nutzung der Stillen SMS bei Strafverfolgern (Polizei, BKA usw.) oder geht zurück. Man kann jetzt darüber spekulieren, was die Gründe für diese Aktivitäten des Verfassungsschutz sind.


Die Nutzung des Systems gegen Protestler wird ausdrücklich beworben:


19.3 Aktivierung als Abhörwanze


Aus Sicht des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist die effektivste Schutzmaßnahme ein Vermeiden des Mitführens von Handys bei Gesprächen mit sensitivem Inhalt, die Detektion jedweder Mobilfunkaktivität im Raum durch den vom BSI entwickelten Mobilfunkdetektor MDS sowie das Deaktivieren sämtlicher drahtloser Schnittstellen von Mobilfunkgeräten.

Der Missbrauch eines Smartphones als Abhörwanze ist nicht auf potente Geheimdienste beschränkt. Angreifer können auch Apps mit verdeckten Funktionen verwenden. Dafür gab es in der Vergangenheit bereits mehrere Beispiele:


Die Hamas hat anlässlich der WM ebenfalls eine App für Fußball Fans in der israelischen Armee entwickelt und außerdem mehrere Dating Apps für israelische Soldaten (Heart Breaker), die der Spionage dienten inklusive akustischer Räumüberwachung und Zugriff auf die Kamera.20

Ein Sicherheitsoffizier der IDF kommentierte:

Whatever you can do with your phone, a malicious app can do too.


Die Beispiele zeigen, dass man sich selbst nur schwer gegen eine mögliche Überwachung mit Smartphone Wanzen schützen kann. Selbst wenn man sein eigenes Smartphone zuhause lässt, dann hat möglicherweise ein Freund oder Kamerad sein Smartphone dabei und die Wanze belauscht nicht nur ihn sondern auch mich.

19.4 WLAN ausschalten, wenn nicht genutzt

Alle Smartphones (und Laptops!) haben ein WLAN Modul. Es ist bequem, wenn man nach Hause kommt oder wenn das Smartphone am Arbeitsplatz automatisch das WLAN nutzt statt der teuren Datenverbindungen des Mobilfunk Providers.

Wenn man mit aktiviertem WLAN Modul und automatischem Login für die bevorzugte WLANs unterwegs ist, dann sendet das Smartphone oder der Laptop regelmäßig aktive Probes, um die Umgebung nach den bevorzugten WLANs zu scannen. Dabei wird neben der weltweit eindeutigen MAC Adresse auch eine Liste der SSIDs der bevorzugten WLANs gesendet, mit denen sich das Smartphone automatisch verbinden würde (Preferred Network List, PNL). Diese Liste liefert Informationen über Orte, an denen sicher der Besitzer des Smartphones bevorzugt aufhält. (Home, Office...)

Mit geringem technischen Aufwand kann man diese Daten der aktiven WLAN Probes zum Tracking und für Angriffe nutzen:

1. Auf der re:publica 2013 wurde ein kostenfreies WLAN bereitgestellt. Dieses WLAN verfolgte alle WLAN-fähige Geräte (Laptops und Smartphones) der Besucher, unabhängig davon, ob die Geräte das WLAN nutzten oder nicht. Das Projekt re:log - Besucherstromanalyse per re:publica W-LAN visualisiert die Daten.21


19https://heise.de/-4075636
21http://apps.opendatacity.de/relog/


\[
p2p_disabled=1
\]

Es gibt bereits erste praktische Ansätze der Werbeindustrie, um die WLAN Probes der Smartphones zum Schnüffeln zu nutzen:

- Die Werbefirma Renew stellte zu den Olympischen Spielen 2012 in London 200 Abfallbehälter auf, die mit einem integrierten WLAN Access Point die Fußgänger anhand der MAC Adressen der Smartphones verfolgten. Innerhalb einer Woche wurde über 4 Mio. Geräte auf dem Weg durch die Londoner City verfolgt.\(^{24}\) We will cookie the street. (K. Memari, chief executive of Renew)

- **Ins Netz gegangen** (Pressemitteilung der BVG, PDF)\(^{25}\): Die Berliner Verkehrsbetriebe werden in Zusammenarbeit mit HOTSPLOTS auf den U-Bahnhöfen kostenfreien WiFi zur Verfügung stellen. Bis Ende 2016 sollen 76 U-Bahnhöfe mit den Access Points

---
\(^{23}\)http://www.sensepost.com/blog/7557.html
Die Bahnhöfe wurden so gewählt, dass rechnerisch 2/3 der täglich 1,5 Mio U-Bahn-Kunden erfasst werden können. Außerdem wird mit kostenfreiem WLAN auf den Buslinien 200 und 204 experimentiert.

Die Nutzung ist ganz einfach. Wenn man beim Warten auf die U-Bahn noch schnell mal... wählt man das BVG Wi-Fi und ruft eine Webseite auf. Nachdem man die Nutzungsbedingungen bestätigt und die erste Werbeseite gesehen hat, kann man kostenfrei Surfen usw. Es wird kein Name und E-Mail Adresse abgefragt.

Zukünftig meldet sich das Smartphone bei jedem Ein- und Aussteigen und bei jeder Durchfahrt durch den Bahnhof automatisch bei dem BVG Access Point an. In den Nutzungsbedingungen ganz unten (runterscrollen) findet man die Daten, die bei jedem (automatischen) Connect gespeichert werden:

- die eindeutige MAC-Adresse des Gerätes
- die zugewiesene IP-Adresse
- Zeitstempel des Login und Logout


Auf dem Flughafen Amsteram-Schiphol findet man folgendes Schild, das auf Wifi- und Bluetooth-Tracking hinweist (Abb: 19.4). Auf der Webseite des Flughafens findet man die Erklärung, dass das Wifi-Tracking genutzt wird, um die Anzahl und Bewegung der Reisenden in den unterschiedlichen Bereichen des Flughafens zu beobachten und damit die Anzeigen für die geschätzten Wartezeiten zu aktualisieren.


U. Spaan vom Handelsforschungsinstitut EHI schätzt, dass 20% der Einzelhändler in Deutschland derzeit (Feb. 2018) mit Trackingmethoden in Läden experimentieren.

Die Firma AdNear experimentiert mit Drohen, welche die Wi-Fi und Baseband Signale der Smartphones auswerten. Anhand der MAC Adresse der WLAN Module werden die Bewegungen der Nutzer verfolgt.

---

26. [https://www.heise.de/-3973727](https://www.heise.de/-3973727)
19.5 Tracking blockieren


Seit Herbst 2020 funktioniert diese Form der Filterung immer schlechter und wird löchrig. Die Trackingdienste nutzen Anti-Zensur Techniken, um die Filterung zu umgehen:


Wenn Anti-Zensur Techniken entwickelt werden, dann müssen wir uns nicht wundern, wenn auch die Trackingbranche diese Techniken verwendet, um Blockaden zu umgehen.

Für weniger hochentwickelte Apps funktioniert die Zensur auf DNS Ebene weiterhin. Für aktuelle Varianten von Android und iOS ist die Variante (2) empfehlenswert.


Nachteilig bei diesen Lösungen ist, dass man kein anderes VPN mehr nutzen kann.

(2) Aktuelle Android und iOS Versionen unterstützen die Konfiguration eines DNS-over-TLS oder DNS-over-HTTPS Server in den Systemeinstellungen. Wenn man einen DNS Server mit Blocklisten für Tracking und Werbung auswählt, werden Tracking- und Werbungserver auf DNS Ebene zensiert und man kann gleichzeitig ein VPN nutzen.

Android unterstützt seit Version 9 (Pie) DNS-over-TLS. Die Option heißt Privates DNS und verbirgt sich in den erweiterten Einstellungen für Netzwerk & Internet.


---

28https://reports.exodus-privacy.eu.org
iPhone unterstützen verschlüsseltes DNS seit iOS Version 14. Die Konfiguration ist ein bisschen umständlicher als bei Android aber machbar:

1. Man muss sich ein Konfigurationsprofil für den DNS Server herunterladen. Es gibt mehrere Webseiten, die Profile für einige DNS Server bereitstellen. Es ist aber empfehlenswert, ein signiertes Profil direkt vom Anbieter herunter zu laden, z. B. vom bekannten russischen DNS Anbieter AdGuard.\(^\text{30}\)
2. Dann ist das Konfigurationsprofil zu installieren: (Einstellungen -> Profil geladen)
   und die Warnung zu bestätigen, dass DNS Einstellungen modifiziert werden.

19.6 Zugriff auf Standortdaten einschränken

Im Dez. 2020 hat der norwegische Journalist M. Gundersen eine Recherche veröffentlicht, die demonstrierte, dass viele Apps Standortdaten sammeln und an irgendwelche Firmen im Wilden Westen verkaufen, die aus den aggregierten Daten detaillierte Bewegungsprofile erstellen. Das muss man aber nicht einfach so akzeptieren.

iPhone bieten in den Einstellungen unter Datenschutz -> Ortungsdienste die Möglichkeit, für jede App festzulegen, ob und wann sie den Standort abfragen darf (Abb: 19.6).

- Wenn kein Grund erkennbar ist, warum der Zugriff auf den Standort für die Funktionalität der App nötig sein sollte, dann wird der Zugriff gesperrt.
- Wenn man sich nicht sicher, ob es u.U. einmal sinnvoll sein könnte, der App Zugriff auf den Standort zu geben, wählt man Nächstes Mal fragen (z. B. Messenger).
- Für Navigations-Apps u.ä. ist es natürlich sinnvoll, dass die App während der Benutzung auf den genauen Standort zugreifen darf.

19.7 Krypto-Apps

Eine Warnung: Jede kryptografische Anwendung braucht einen vertrauenswürdigen Anker. Üblicherweise geht man davon aus, dass der eigene PC oder Laptop ein derartiger vertrauenswürdiger Anker ist, über den man volle Kontrolle hat. Bei Smartphones kann man nicht davon ausgehen, dass der Nutzer volle Kontrolle über die Software hat.

1. Mit dem Kill Switch\(^{31}\) hat Google die Möglichkeit, auf Android Handys beliebige Apps zu deinstallieren, zu installieren oder auszutauschen. Das iPhone\(^{32}\) und Windows Phone\(^{33}\) haben ebenfalls einen Kill Switch. Jede Crypto-Anwendung aus den Markets muss also als potentiell kompromittiert gelten. Sie kann genau dann versagen, wenn man den Schutz am nötigsten braucht.

2. Jede Crypto-Anwendung benötigt gute Zufallszahlen. Der Zufallszahlengenerator der Android Java VM war so beschmerzlich, dass man als Angreifer nicht die Kompetenz und Rechenleistung der Crypto-City von Fort Meade braucht. Ganz gewöhnliche Hacker konnten die Schwächen der Android Implementierung im Sommer 2013 nutzen, um Geldbörsen von Bitcoin Nutzern leer zu räumen\(^{34}\).

3. Smartphones sind leicht kompromittierbar:

\(^{31}\)https://mashable.com/2011/03/06/android-kill-switch
\(^{32}\)https://www.telegraph.co.uk/technology/3358134/Apples-Jobs-confirms-iPhone-kill-switch.html
\(^{33}\)https://www.heise.de/-1131297
\(^{34}\)https://www.heise.de/-1933714
KAPITEL 19. SMARTPHONES


- Auch das *Xposed Framework* kann mit einem ähnlichen Trick Kryptografie komplett aushebeln oder die Privacy-Einstellungen verschärfen (je nach Intention).

**OpenPGP-Verschlüsselung**

Man kann OpenPGP auch auf dem Smartphone nutzen, aber:

*Never store your private PGP key on your mobile phone... Mobile phones are inherently insecure.* (Mike Cardwell)

Der Yubikey NEO hat eine OpenPGP Smartcard, die via NFC genutzt werden kann. Der private Schlüssel wird dabei auf dem Yubikey gespeichert und verlässt diese Umgebung nie. Die PIN zur Freigabe des Schlüssels wird zusammen mit den zu entschlüsselnden oder zu signierenden Daten via NFC an den Yubikey gesendet und das Ergebnis der Kryptooperation wird zurück an das Smartphone gegeben.

1. Auf dem Android Smartphone benötigt man folgende Software, die man aus dem Google Play Store oder F-Droid Store installieren kann:

   - Das E-Mail Programm *K9mail* kann direkt mit OpenKeychain zusammenarbeiten und integriert Buttons zum Verschlüsseln bzw. Entschlüsseln von E-Mails.
   - Der Jabber/XMPP Client *Conversations* kann in Kombination mit OpenKeychain die Chats mit OpenPGP verschlüsseln, der private Key liegt dabei aber auf dem Smartphone. OTR- und OMEMO-Verschlüsselung sind auch möglich.

2. Den Yubikey NEO bereitet man am einfachsten mit Enigmail auf einem PC vor (siehe: OpenPGP Smartcards). Die OpenPGP Smartcard Funktion ist freizuschalten, die PIN und Admin-PIN ist zu ändern und die Schlüssel sind zu generieren.

3. Das neu erstellte Schlüsselpaar kann man aus Enigmail in eine Datei exportieren (geheimer + öffentlichen Schlüssel). Der geheime Schlüssel in dieser Datei enthält praktisch nur einen Verweis, welche Smartcard genutzt werden muss.

4. Diese Schlüsseldatei ist auf das Smartphone zu übertragen und in OpenKeychain zu importieren.


**19.8 Stille SMS ind IMSI-Catcher erkennen**


*I would bet money that there are governments that are spying in DC.* (C. Soghoian)


In Sicherheitskreisen vermutet man, das die IMSI-Catcher in den Regierungsvierteln in erster Linie der Beobachtung dienen, wer in den verschiedenen Einrichtungen ein- und ausgeht. Das Abhören von SMS und Telefonaten ist vermutlich eher nebensächlich. Das Smartphone ist eine Trackingwanze, die wir freiwillig mit uns umhertragen!

### 19.9 Juice Jacking Angriffe


In Deutschland sind diese Angriffe kaum bekannt, weil es nur wenige öffentliche Ladestationen gibt. International ist man schon weiter, sowohl bei der Bereitstellung öffentlicher Ladestationen an Flughäfen, in Hotels und öffentlichen Plätzen, als auch...


*Travellers should avoid using public USB power charging stations in airports, hotels and other locations because they may contain dangerous malware.*


Man kann natürlich seinen AC-Charger nutzen oder (wenn der Stecker mal nicht passt) eine Powerbank, die man via USB auflädt um damit dann das Smartphone zu laden.

Außerdem gibt es das USB Condom oder USB Data Blocker. Das sind kleine Adapter für USB-Stecker, in denen nur die Kontakte für die Energieversorgung verbunden sind aber nicht die Kontakte für Datenleitungen. Im deutschen Fachhandel gibt es diese Dinger noch nicht, aber man kann sie bei Amazon o.ä. Händlern mit internationaler Lieferung bestellen.

### 19.10 Das Hidden OS im Smartphone

In jedem Smartphone steckt neben dem End-User-Betriebssystem (Android, iOS, Windows Phone) und dem Linux Kernel ein weiteres, verstecktes Betriebssystem. Dieses Hidden OS läuft auf dem Baseband Prozessor und bearbeitet die Kommunikation mit den Mobilfunkstationen in Echtzeit. Es handelt sich dabei um ein Real-Time Betriebssystem. Der Markt
KAPITEL 19. SMARTPHONES

Abbildung 19.7: Warnung vor USB Charger Scam

wird von Qualcomm mit AMSS dominiert, die Software ist Closed Source.

Im Betrieb hat das Hidden OS die volle Kontrolle über die gesamte Hardware incl. Mikrofon und Kamera. Linux Kernel und End-User Betriebssysteme laufen als Slaves unter Kontrolle des Hidden OS.


- Weinmann stellte auf der DeepSec 2010 mit All Your Baseband Are Belong To Us einen Angriff vor, der mit einem nur 73 Byte großen Remote Code Execution Exploit eine Backdoor öffnete und das Smartphone in eine Abhörwanze verwandelte.38
- Mit den Hexagon challenges wurde auf der PacSec 2013 ein verbesserter Angriff auf das Hidden OS von Rals Phillip Weinmann vorgestellt.39

38 http://www.securitytube.net/video/5372
39 http://pacsec.jp/speakers.html

• Das GSMK-Team demonstrierte 2013 einen Over-the-Air Angriff auf Smartphones, bei dem zuerst das Hidden OS des Baseband Prozessors durch ein Over-the-Air Update kompromittiert und dann das Smartphone OS (iOS und Android) angegriffen wurde. Es wurden alle verfügbaren erfolgreich Smartphones kompromittiert.  

Compromised phones can then be used to record conversations or gain access to sensitive data. It would also be possible to monitor content being accessed through pwned smartphones.

Der Angriff ist relativ aufwändig und wird daher wahrscheinlich sehr selten eingesetzt, da es einfachere Möglichkeiten durch Verteilung kompromitterter Apps via Play Store oder ähnliches gibt.

---

41 https://www.theregister.co.uk/2013/03/07/baseband_processor_mobile_hack_threat/Malware-flingers%20can%20pwn%20your%20mobile%20with%20over-the-air%20updates