Anleitung zur Nutzung des Tails-Live-Betriebssystems für sichere Kommunikation, Recherche, Bearbeitung und Veröffentlichung sensibler Dokumente

7. Auflage

Hefte zur Förderung des Widerstands gegen den technologischen Angriff

Band I: Tails – The amnesic incognito live system

capulcu productions, ISSN (Online) 2701-9977
7. überarbeitete Auflage, 11. März 2021
V.i.S.d.P. E. Schmidt, Am Zuckerberg 14, 21984 Silikontal

Anleitung zur Nutzung des Tails-Live-Betriebssystems für sichere Kommunikation, Recherche, Bearbeitung und Veröffentlichung sensibler Dokumente

Eine digitale Version dieser Anleitung sowie redaktionell bearbeitete Anmerkungen, Änderungen und Neuerungen findet ihr unter `https://capulcu.blackblogs.org`. Die Verbindung zur Webseite erfolgt verschlüsselt.

Wir freuen uns über Feedback. Den *Schlüssel* zu unserer Mail-Adresse findet ihr auf unserer Webseite. Wir drucken hier zur Überprüfung der Echtheit den *Fingerprint* dieses Schlüssels ab:

`capulcu@nadir.org AF52 0854 7EF1 711A F250 57CB D0D0 A3C5 DF30 9590`

Tails ist ebenfalls mit einem Schlüssel signiert. Den Schlüssel der Tails-Entwickler*innen findet ihr auf der Seite `https://tails.boum.org`. Wir drucken hier den zugehörigen Fingerprint ab:

`tails@boum.org A490 D0F4 D311 A415 3E2B B7CA DBB8 02B2 58AC D84F`

Inhalt

Einführung

Repressionsorgane interessieren sich seit einiger Zeit verstärkt für das „Digitale“. Hausdurchsuchungen bedeuten eigentlich immer, dass alles, was nach Rechner, Smartphone, Datenträger jeder Art etc. aussieht, danach beschlagnahmt ist. An einigen Grenzen (z.B. der USA) kommt es vor, dass der/die Grenzer*in nach dem Passwort für Accounts in sozialen Netzen fragt. Diverse Armeen dieser Welt überschlagen sich beim Aufstellen von „Cyberwar“-Einheiten. Spätestens seit den Veröffentlichungen von Edward Snowden ist bekannt, dass die Geheimdienste NSA und GCHQ (aber selbstverständlich auch andere Geheimdienste, z.B. der BND) in großem Umfang Daten aus dem Netz saugen - wenn es geht, dann sogar automatisiert, bis hin zum massenweisen „Hacken“ von Rechnern[1].

Wir empfehlen angesichts dieser Situation, den Kopf nicht in den Sand zu stecken, sondern die vorhandenen technischen Möglichkeiten zum Selbstschutz voll auszuschöpfen. *Tails* ist ein großer Schritt in diese Richtung. Das Live-Betriebssystem ist ein eigenständiges Betriebssystem, was von DVD oder USB-Stick gestartet werden kann, ohne es zu installieren. Euer Standard-Betriebssystem auf der Festplatte wird nicht angefasst.

Tails hilft bei der Bearbeitung von sensiblen Text-, Grafik- und Tondokumenten. Tails verwendet beim Surfen, Mailen und Chatten automatisch die Anonymisierungssoftware *Tor* und verändert zusätzlich die sogenannte „MAC-Adresse“ eurer Netzwerkkarte. Was das ist und wozu das von Nutzen ist, erklärt euch die Einführung dieser Anleitung.

Tails hinterlässt bei richtiger Nutzung keine Spuren auf dem Rechner - eure Festplatte bleibt unberührt. Ein eventuell (auf Betriebssystemebene) eingeschleuster Schadcode kann sich auf einer Live-DVD oder einem schreibgeschützten Live-USB-Stick als Start-Medium nicht „festsetzen“ und euch beim nächsten Rechnerstart nicht mehr behelligen. Tails ist allerdings Software - gegen eine manipulierte Hardware kann es nicht schützen. In der letzten Auflage fandet ihr dazu das Kapitel „BIOS schützen“. Dort hatten wir euch gezeigt, wie ihr Manipulationen an eurem BIOS oder Bootloader feststellen könnt. Die Anleitung war sehr technisch und erforderte das Flashen der Hardware eures BIOS. In Zukunft wird dies wesentlich einfacher möglich sein. Wir hatten gehofft, eine Anleitung dazu in dieser Auflage zu haben, müssen euch aber leider auf die nächste Auflage vertrösten.

Konkrete Blockade digital-totalitärer Erfassung

Wer sich gegen die Verletzung von Persönlichkeitsrechten durch das Ausspionieren jeglicher Netzdaten, gegen DNA-Datenbanken und (Drohnen-)Kameraüberwachung politisch aktiv zur Wehr setzt, sollte auch bei der Preisgabe seiner Alltagsdaten nicht nur sparsamer, sondern vor allem strategisch (und damit ganz anders als üblich) vorgehen.

Insbesondere das Zusammenführen unserer verschiedenen Aktivitäten, Interessen, Neigungen, Einkäufe, Kommunikationspartner*innen, (...) zu einer integralen „Identität“ ist die Grundlage für die Mächtigkeit von schnüffelnden Analysewerkzeugen - egal, ob sie ökonomisch-manipulativen, politischen oder repressiven Absichten entspringen. Das im Folgenden beschriebene Live-Betriebssystem Tails hilft Nicht-Expert*innen, mit annehmbarem Aufwand dieses „integrale Ich“ auf unterschiedliche digitale Identitäten zu verteilen. Um Identitäten zu verbergen, kann es hilfreich sein, mit mehreren vertrauenswürdigen Personen einen Mail-, Chat-, Blog-, oder Forums-Account gemeinsam zu nutzen. Wichtig ist in jedem Fall, die Anonymisierungssoftware *Tor* zu nutzen. Das erledigt Tails für euch.

Zur (Wieder-)Erlangung eines Mindestmaßes an Privatheit und Daten-Souveränität raten wir darüber hinaus zur Verschlüsselung aller Inhalte, zum lokalen Speichern eurer Daten (ohne Cloud), zur Facebook-Verweigerung, zur gezielten Drosselung der Teilhabe am digitalen Dauersenden (das möglichst „unsmarte“[2] Mobiltelefon so oft es geht zu Hause lassen) und zum Offline-Einkauf mit Barzahlung. Im Netz möglichst wenig Spuren zu hinterlassen muss zu den Grundfertigkeiten einer jeden Aktivist*in gehören. Tor muss unser Standardwerkzeug werden und Tails hilft uns, (unter anderem) bei der Nutzung von Tor möglichst wenig Fehler zu machen.

Verglichen mit dem, was wir an Selbstbestimmtheit bereits verloren haben, ist der Aufwand für ein abgeändertes Alltagsverhalten minimal, auch wenn es vielen von uns „unbequem“ erscheint. Die „bequeme“ Alternative hingegen bedeutet Kontrollierbarkeit, Vorhersagbarkeit, Manipulierbarkeit und erhöhtes Repressions-Risiko – nicht nur für euch, sondern auch für diejenigen, mit denen ihr kommuniziert.

Wozu ein Live-Betriebssystem (auf DVD oder USB-Stick)?

Die wichtigsten Gründe für die Verwendung eines Live-Betriebssystems wie Tails sind dessen Vergesslichkeit und Unveränderbarkeit.

Nach dem Herunterfahren des Rechners sind alle Daten, die ihr zuvor nicht explizit auf einen (externen) Datenträger gesichert habt, wieder weg. Der ohnehin vergessliche Arbeitsspeicher eures Rechners wird beim Herunterfahren zusätzlich mit Zufallszahlen überschrieben und die Festplatte bleibt von der Tails-Sitzung unberührt[3]. Das bedeutet, es gibt keine Systemdateien, die verraten, welche USB-Sticks ihr benutzt habt, keine versteckten Rückstände eurer Internetrecherche, keinen Hinweis auf „zuletzt bearbeitete“ Dokumente und keine Überbleibsel einer Bildbearbeitung. Euer „normales“ Betriebssystem (auf der Festplatte) dieses Rechners bleibt unverändert. Der Rechner trägt auch keine Spur, die darauf hindeutet, dass es diese Tails-Sitzung gegeben hat.

Um bei sensibler Arbeit wirklich sicher zu gehen, dass tatsächlich nichts zurückbleibt, sollte sich das Tails Live-Betriebssystem entweder auf einem unveränderlichen Datenträger befinden (z.B. auf einer gebrannten DVD oder einem USB-Stick mit mechanischem Schreibschutzschalter[4]), oder aber (per Startoption toram - siehe Kapitel „Tails starten“) vollständig in den Arbeitsspeicher des Rechners geladen werden. Dann könnt ihr nämlich den Datenträger, auf dem sich Tails befindet, nach dem Hochfahren des Rechners noch vor Arbeitsbeginn auswerfen/abziehen.

Einschränkend muss an dieser Stelle hinzugefügt werden, dass zuvor Beschriebenes nicht auf Rechner zutrifft, die bereits manipulierte Firmware in ihrem BIOS aufweisen (siehe Kapitel „Warnung: Grenzen von Tails“). Daher raten wir davon ab,

1 The Intercept, Glenn Greenwald, Ryan Gallagher, 12.3.2014 `https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/`

2 Ein Mobiltelefon ohne WLAN und Bluetooth ist ein besserer Schutz.

3 Es sei denn, ihr speichert explizit einzelne Dateien auf die interne Festplatte. Davon raten wir ab!

4 USB-Sticks mit mechanischem Schreibschutzschalter sind leider nur selten im Offline-Handel erhältlich. Herstellerin solcher Sticks ist u.a. die Firma Trekstore.

5 Am sichersten ist die Nutzung eines Rechners mit entfernter Festplatte (siehe Kapitel „Tails als Quasi-Schreibmaschine“). Als alternatives Betriebssystem bietet sich Debian, Parabola oder Qubes OS an.

Computer mit Tails zu nutzen, auf denen ihr auch Windows oder Mac verwendet[5]. In Anbetracht der Entschlüsselungsbehörde ZITiS, existierender und neuer Polizeiaufgabengesetze raten wir dringend dazu, die Festplatte auszubauen (siehe Kapitel „Tails als Quasi-Schreibmaschine“).

Tails basiert auf der Linuxdistribution *Debian* und ist keine selbst entworfenes System. Sicherheitsupdates und die Weiterentwicklung der ganzen Software wird größtenteils von Debian übernommen. Es ist erklärter Anspruch der Tails-Entwickler*innen, die Modifikationen an Debian auf das Nötige zu beschränken. Das hat den netten Nebeneffekt, dass bei Fragen zur Software die Dokumentation von Debian (oder dem ebenfalls debianbasierten Ubuntu oder Mint) in vielen Fällen auch weiterhilft. Tails besteht also zum großen Teil aus bekannter Software, die nur anders konfiguriert wurde - wenn überhaupt.

Da Tails mittlerweile ein sehr umfangreiches und vielseitig einsetzbares Live-System ist und die (derzeit nur in englischer und französischer Sprache vollständige) Dokumentation auf der Webseite `https://tails.boum.org` entsprechend reichhaltig ist, versuchen wir hiermit, eine verdichtete, aber trotzdem verständliche Einführung für Computer-Nicht-Expert*innen zur Verfügung zu stellen.

Wir werden im Folgenden auf drei Nutzungsmodelle für Tails eingehen. Die Anleitungen dazu überschneiden sich untereinander:

a) Tails als System für sensible Arbeiten auf einem Rechner mit Internetzugang. Hier lernt ihr den Umgang mit den von Tails zur Verfügung gestellten Programmen. Die Verbindung zum Netz erledigt ein weitgehend automatisierter und einfach zu bedienender Netzwerk-Manager. Die Oberfläche sieht eurem normalen Betriebssystem auf der Festplatte sehr ähnlich - egal, ob ihr Windows, Mac-OS X oder ein Linux-Betriebssystem nutzt, ihr werdet euch bei Tails schnell zurecht finden.

b) Tails als „Quasi-Schreibmaschine“ für hoch-sensible Arbeiten auf einem völlig abgeschotteten Rechner ohne Netz, bei dem Festplatte(n), WLAN- und Bluetooth-Adapter ausgebaut sind. Hier lernt ihr den Umgang mit besonders sensiblen Dokumenten. Das kann die Bearbeitung von Texten, Fotos, Tonaufnahmen oder die Erstellung ganzer Bücher sein. Hier darf nichts schief gehen. Deshalb raten wir in solchen Fällen zu einem Rechner mit beschränkten Fähigkeiten *(keine Festplatte, keine Internetverbindung, kein WLAN, kein Bluetooth)*, der euch zudem nicht persönlich zugeordnet werden kann.

c) Persistenz: Tails als Reise- und Alltagssystem. Hier lernt ihr, wie ihr auf einem USB-Stick, auf dem ihr *Tails* installiert habt, eine zusätzliche (verschlüsselte) Daten-Partition[6] einrichtet. Auf dieser Partition bleiben Einstellungen, Mails oder andere Daten dauerhaft gespeichert. In dieser Nutzungsart ist der Tails- Stick nicht mehr *unveränderbar*[7] und Tails nicht mehr vollständig *vergesslich*.

Im Vergleich zu **a**) und **b**) ist Nutzungsmodell **c**) also explizit unsicherer! Im Vergleich zu eurem Alltagsrechner auf der Festplatte aber in der Regel viel sicherer, denn Tails lenkt weiterhin jede Kommunikation von für Tails konfigurierte Anwendungen mit der Außenwelt verschlüsselt durch das Anonymisierungsnetz Tor. Wer also einen Reiselaptop mit Netzzugang nutzt, aber z.B. seinen Aufenthaltsort beim Mailen und Chatten nicht verraten will, und dennoch bequemen Zugriff auf seine bisherigen Mails und Dokumente benötigt, der sollte Tails als sicherere Alternative zu einem Standard-Betriebssystem in Erwägung ziehen. Diese Methode beschreiben wir im Kapitel „Persistenz“.

Systemvoraussetzungen und Betriebsarten von Tails

Tails läuft auf den meisten Rechnern, die einen „64-Bit“ Prozessor besitzen[8]. Ihr benötigt einen Rechner mit einem internen oder externen Laufwerk, das DVDs lesen und *booten* (starten) kann, oder aber einen Rechner, der von einem USB-Stick booten kann.

Zusätzlich sollte euer Rechner für einen fehlerfreien Betrieb über einen Arbeitsspeicher (RAM) von mindestens 2-4 GB verfügen[9]. Tails läuft auf allen halbwegs aktuellen PCs und Laptops, nicht jedoch auf Smartphones (ARM-Prozessoren) oder PowerPCs (ältere Apple-Rechner).

Zumindest in zwei Fällen empfehlen wir Tails mit der Startoption **toram** zu benutzen. Dann wird das gesamte Betriebssystem von Tails mit allen Anwendungsprogrammen zu Beginn in den Arbeitsspeicher geladen. Dazu sollte euer Rechner über mindestens 2 GB Arbeitsspeicher verfügen.

1. Wenn ihr einen Tails-USB-Stick ohne mechanischen Schreibschutzschalter benutzt. Mit der Startoption können diese Datenträger nach dem Start[10] von Tails entfernt werden, noch bevor ihr mit der Arbeit beginnt. Damit sind diese Datenträger vor einem eventuellen Angriff (eingeschleust über das Internet oder andere Datenträger) sicher.
2. Wenn ihr eine Tails-DVD benutzt und in eurer Sitzung Daten auf CD oder DVD brennen wollt. Mit der Startoption kann die Tails-DVD nach dem Hochfahren des Rechners herausgenommen werden. Damit ist das Laufwerk während der Sitzung frei.

Wie bekomme ich Tails?

Prinzipiell gibt es zwei Möglichkeiten:

1. Die einfachste (wenn auch nicht sicherste[11]) Variante ist, auf eine bereits überprüfte Version von Tails einer vertrauenswürdigen Person zurückzugreifen. Du brauchst:
   - 1 anderes Tails (USB-Stick)
   - 1 USB-Stick (mindestens 8 GB)
   - 1/2 Stunde zum Installieren
2. Eine andere (technisch aufwendigere) Variante ist, die jeweils aktuelle Version von Tails *herunterzuladen und zu überprüfen*, um daraus eine „bootfähige“ Tails-DVD oder einen USB-Stick zu erstellen. Du brauchst dazu:
   - 1 USB-Stick (mindestens 8 GB) oder 1 DVD
   - 1 Stunde zum Herunterladen von Tails (1.1 GB)
   - 1/2 Stunde zum Installieren

6 Ein Datenträger kann in mehrere getrennte Partitionen aufgeteilt sein.
7 Der Datenträger wird dazu ohne Schreibschutz genutzt.
8 Diese Einschränkung besteht seit Tails Version 3.0.
9 Bei weniger als 2 GB Arbeitsspeicher kann der Rechner manchmal „einfrieren“. Der Grund dafür ist, dass Tails nicht auf die sogenannte Auslagerung-Partition (SWAP) der Festplatte zurückgreifen darf: Ein Auslagern von Daten und Programmen auf die Festplatte würde nachvollziehbare Datenspuren hinterlassen!
10 Sobald sich der Rechner mit der Tails-Arbeitsoberfläche meldet (nach Boot- und Start-Bildschirm).
11 Das System könnte manipuliert sein.

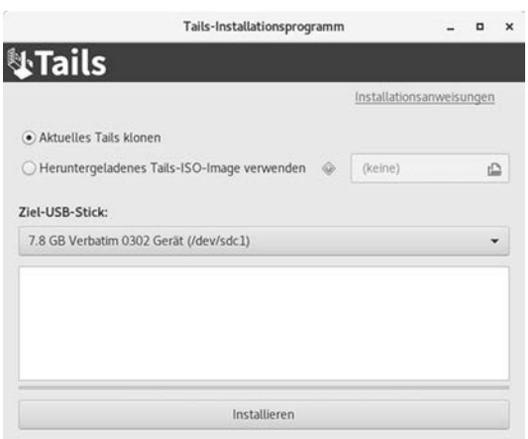
Falls euch (wider Erwarten) etwas nicht gelingen sollte, holt euch Hilfe, denn das sollte kein Grund sein, auf die Benutzung von Tails zu verzichten!

Variante 1: Installation von einem anderen Tails

Mit dem im folgenden Abschnitt beschriebenen „Tails Installer“ ist das Erzeugen eines neuen oder weiteren Tails-Stick einfach. Im darauf folgenden Abschnitt „Tails Upgrader“ lernt ihr, wie ihr euer Tails automatisch aktuell haltet.

Tails Installer

Wenn ihr schon ein lauffähiges Tails-System auf einem USB-Stick oder einer DVD habt und einen weiteren USB-Stick (keine DVD) erstellen wollt, könnt ihr den *Tails Installer* verwenden. Den „Tails Installer“ findet ihr unter `Anwendungen ► Tails ► Tails Installer`. Wenn ihr ihn startet, erhaltet ihr den folgenden Bildschirm, auf dem ihr zwischen zwei Möglichkeiten auswählen könnt:



- „Aktuelles *Tails* klonen“ wählt ihr aus, wenn ihr die Tails-Version des laufenden Systems auf einen anderen USB-Stick übertragen wollt. **Alle Daten auf dem anderen USB-Stick werden dabei gelöscht.** Es wird ausschließlich das Tails-System übertragen, nicht eventuell vorhandene Daten der Tails-Persistenz.
- „Heruntergeladenes *Tails*-ISO-Image verwenden“ wählt ihr aus, wenn auf dem zu beschreibenden USB-Stick bereits ein Tails-System vorhanden ist und ihr dieses mit einem heruntergeladenen ISO-Abbild einer neueren Tails-Version überschreiben möchtet.

Spätestens, nachdem ihr euch für eine Funktion entschieden habt, müsst ihr den USB-Stick einstecken, der das neue Tails-System erhalten soll. Um nicht versehentlich den falschen USB-Stick zu löschen, solltet ihr darauf achten, dass außer dem originalen und dem zukünftigen Tails-Stick keine anderen USB-Sticks oder SD-Karten eingesteckt sind. Ist dies der Fall, wird in diesem Fenster als „Zielmedium“ nur eine Option - euer eingesteckter USB-Stick - vorhanden sein (siehe Abbildung). Andernfalls muss der gewünschte USB-Stick als Zielmedium ausgewählt werden. Nachdem ihr nun auf „Tails installieren“ geklickt habt, müsst ihr noch einmal bestätigen, dass ihr auch wirklich diesen Stick überschreiben möchtet. Danach kann die Erstellung des neuen Sticks ein paar Minuten in Anspruch nehmen. Ausschließlich bei der Option „Von ISO aktualisieren“ müsst ihr zusätzlich noch das zu verwendende, bereits heruntergeladene Live-System-ISO-Abbild auswählen.

Tails Upgrader

Bei jedem Start von Tails wird direkt, nachdem die Verbindung zu dem Tor-Netzwerk hergestellt wurde, überprüft, ob die aktuelle Tails-Version verwendet wird.

> *Es ist wichtig, immer die aktuelle Version zu verwenden, da regelmäßig Sicherheitslücken in den von Tails verwendeten Programmen entdeckt werden, die im schlimmsten Fall dazu führen, dass eure Identität, eure IP-Adresse, etc. nicht verschleiert werden. Durch ein Tails-Upgrade werden diese Sicherheitslücken gestopft und meist auch andere Features optimiert.*

Falls ihr Tails mit DVD verwendet oder Tails manuell auf den USB-Stick gespielt habt ohne die Verwendung des Tails Installers, bekommt ihr die Meldung „You should do a manual Upgrade“. Das heißt, ihr solltet manuell eine neue Version von Tails herunterladen, überprüfen und auf DVD brennen oder auf einen USB-Stick installieren.

Habt ihr jedoch euer Tails mit dem Tails Installer auf einen USB-Stick gespielt, habt ihr nun Glück, denn in diesem Fall macht der Tails Upgrader für euch die Arbeit. Ihr werdet gefragt, ob ihr ein Upgrade sofort oder später durchführen wollt. Wenn ihr auf „Upgrade Now“ klickt, wird das Upgrade automatisch heruntergeladen und überprüft. Dies erspart euch die aufwendigere Überprüfung der Checksumme, die ihr durchführen solltet, wenn ihr ein ISO-Abbild herunterladet. Wenn der Download-Vorgang beendet ist, wird das Upgrade auf eurem USB-Stick installiert. Nach einem Neustart ist das Tails-System auf dem aktuellen Stand. Daten auf einer eventuell vorhandenen Tails-Persistenz sind davon nicht betroffen und bleiben weiterhin bestehen. Falls ein Stick mit Schreibschutzschalter verwendet wird, müsst ihr diesen natürlich für die eine Sitzung, in der ihr das Upgrade durchführt, auf „beschreibbar“ stellen.

Bekommt ihr allerdings nach dem Start von Tor die Meldung „Nicht genügend Speicher vorhanden, um nach Aktualisierungen zu suchen“, hat euer Rechner zu wenig Arbeitsspeicher oder ihr habt schon speicherhungrige Programme wie LibreOffice oder den Tor-Browser gestartet. In diesem Fall kann es helfen, nach einem Neustart und der Meldung „Tor ist bereit“ zunächst keine weiteren Programme zu starten.

Variante 2, Schritt 1: Tails herunterladen und überprüfen

Tails liegt auf dem Server `https://tails.boum.org` zum Download bereit. Leider ist es möglich, dass ein*e Angreifer*in die Daten auf dem Weg zu euch abfängt und modifiziert. Im Kapitel „Warnung: Grenzen von Tails“ haben wir einen Angriff diskutiert, bei dem sich die Angreifer*in in die Datenströme hängt, um sie zu *kontrollieren* und/oder zu *manipulieren*. Aus diesem Grund ist insbesondere beim Herunterladen von Software darauf zu achten, ihre „Echtheit“ zu überprüfen. Andernfalls kann euch leicht ein manipuliertes Tails untergeschoben werden. Wir zeigen euch, wie die Überprüfung und Erstellung eines Tails-Startmediums eigenständig erledigt werden kann. Dieser Teil der Anleitung mag euch kompliziert erscheinen - aber ihr dürft ihn nur dann ignorieren, wenn euch eine Person eures Vertrauens eine „geprüfte“ Tails-Version gegeben hat.

Ihr braucht drei Dateien, die ihr vom Tails-Server runterladen müsst:

1. Das Image der Tails-Software selbst.

2. Die Signatur, welche die Echtheit bestätigt.
3. Den Public-Key der Tails-Entwickler*innen, mit dem die Signatur gemacht wurde.

Wir beschreiben im Folgenden, wie ihr eine solche Modifikation sicher identifizieren könnt und deshalb auch sicher sein könnt, dass die Daten, die ihr runtergeladen habt, auch die richtigen sind. Wir adressieren Linux- und MacOS-X-Nutzer*innen. Windows-Nutzer*innen müssen wir auf die Anleitung auf `https://tails.boum.org` verweisen.

Zunächst wollen wir kurz auf digitale Signaturen und den Unterschied von ISO- und IMG-Dateien etwas eingehen.

Digitale Signaturen

Durch digitale Signaturen kann die „Echtheit" einer Software überprüft werden. Hierfür wird der öffentliche PGP-Schlüssel des Entwickler*innen-Teams benötigt, mit dem die Software unterschrieben wurde. Die Unterschrift garantiert, dass es sich um eine unveränderte Version der bezogenen Software handelt.

Wenn ihr euch z.B. die aktuelle Version der Live-DVD Tails besorgt, findet ihr im Download-Bereich eine entsprechende Signatur, mit der ihr die „Echtheit" der Software überprüfen könnt. Dafür benötigt ihr noch den PGP-Schlüssel der Entwickler*innen, der ebenfalls auf der Download-Seite erhältlich ist. Nach erfolgreichem Import dieses Schlüssels könnt ihr über grafische Tools oder über eine sogenannte Kommandozeile die Authentizität der Software überprüfen. Wie dies funktioniert, stellen wir euch im Folgenden vor.

Theoretisch wäre es durch einen Man-in-the-Middle-Angriff trotzdem noch möglich, euch eine falsche Signatur und eine dafür angepasste Software sowie einen falschen Schlüssel zu übermitteln. Ein Weg, dies zu umgehen, ist, die Software und deren Signatur über verschiedene Netzwerke zu besorgen - z.B. einmal von eurer Arbeit aus, dann von eurem Anschluss zu Hause und ein zusätzliches Mal über Tor.

Die Echtheit eurer heruntergeladenen Tails-Version solltet ihr über die PGP-Signatur der Tails-Entwickler*innen überprüfen.

Der Unterschied von ISO- und IMG-Dateien

Wenn es darum geht, Kopien von Linux-Distributionen aus dem Internet herunterzuladen, ist es üblich, dass die Software in einer archivierten (zusammengepackten) Form zum Download bereitgestellt wird.

Dies bedeutet, dass jeder Teil der Software heruntergeladen wird, und daher keine Notwendigkeit besteht, nach fehlenden Dateien zu suchen. Des Weiteren stellt es auch sicher, dass die Dateien nicht manipuliert wurden, wenn die Prüfsumme und Signatur stimmen.

Die verschiedenen Dateiformate können jedoch verwirrend sein, deshalb wollen wir kurz auf die Unterschiede zwischen ISO- und IMG-Dateien eingehen, damit sie nach dem Herunterladen richtig behandelt werden.

ISO und IMG sind beides Archivierungsformate, die hauptsächlich zum Erstellen eines Abbildes von Datenträgern benutzt werden. Jede Datei enthält eine Kopie des Inhalts des Originaldatenträgers, von dem das Archiv erstellt wurde, sowie Informationen über die Dateistruktur des Datenträgers. Sie wurden entwickelt, um die Archivierung des Datenträgers zu vereinfachen und das Erstellen einer exakten Kopie zu erleichtern. Während es jedoch nur eine Version des ISO-Formats gibt, gibt es IMG in zwei Versionen: komprimiert und unkomprimiert.

Das ISO-Dateiformat ist ein internationales Standarddateiformat, das entwickelt wurde, um ein Disc-Image, einschließlich seines Dateisystems, in einer einzigen Datei zu enthalten. Das ISO-Format wurde als Mittel zur Archivierung von Discs entwickelt und hat sich als solches zu einer Standardmethode für die Verteilung von Software, wie z.B. Linux-Installations-CDs, entwickelt, die Benutzer*innen herunterladen und selbst brennen können. ISO wird verwendet, um CD- und DVD-Images zu erstellen. Wenn ihr also Tails auf eine DVD brennen wollt, müsst ihr ein ISO-Image wählen.

Das IMG-Dateiformat wurde entwickelt, um eine Sicherungskopie einer Diskette in einer einzigen Datei zu erstellen. Seit dem Niedergang der Disketten wird das IMG-Format für die Erstellung von Image-Dateien für Festplatten oder andere Datenträger wie USB-Sticks oder anderen Flashlaufwerken verwendet. Wollt ihr also Tails auf einem USB-Stick installieren, so müsst ihr ein IMG-Image herunterladen.

Download und Verifikation im Webbrowser/Torrent-Client

Tails bietet drei Mechanismen, mit denen Nutzer*innen das über einen Spiegel-Server eines Drittanbieters heruntergeladene ISO-/IMG-Image verifizieren können:

1. Verifizierung durch JavaScript-Code auf der Download-Seite.
2. Verifizierung durch automatische Prüfsummenprüfung in BitTorrent-Clients.
3. Manuelle Prüfung über die Kommandozeile.

> *Bei den ersten beiden Mechanismen handelt es sich allerdings um aus unseren Augen unzureichende Maßnahmen. Das Prüfen der OpenPGP-Signatur wird als optionale Verifizierungstechnik dargestellt, die möglicherweise zusätzlich zu den anderen beiden Techniken und idealerweise über das Web-of-Trust von OpenPGP erfolgt. Wir raten, die Signatur unbedingt zu prüfen.*

Bei der Verifizierung durch JavaScript-Code auf der Download-Seite lädt das JavaScript zunächst eine Bildbeschreibungsdatei (IDF) von `https://tails.boum.org/install/v2/Tails/amd64/stable/latest.json`. Anschließend wird überprüft, ob die Prüfsumme des von euch heruntergeladenen Bildes in der IDF vorhanden ist. Dabei wird sich auf kryptografische Informationen verlassen, die von der Website über HTTPS abgerufen werden. Für Ziele, Umsetzung und Angriffsmöglichkeiten verweisen wir auf das Design-Dokument[12].

Ganz ähnlich verhält es sich bei einem BitTorrent-Download. Die Torrent-Datei, die über HTTPS von der Tails-Website heruntergeladen wird, enthält eine Prüfsumme des Bildes. BitTorrent-Clients verifizieren diese Prüfsumme automatisch, wenn der Download beendet ist.

Im folgenden Abschnitt beschreiben wir, wie die Signatur geprüft werden kann. Wenn ihr eine der oben beschriebenen Möglichkeiten benutzt habt, um die Datei herunterzuladen, dann entfällt Schritt 2.

Download und Verifikation auf der Kommandozeile

Für Eingaben per Kommandozeile müsst ihr zunächst ein *Terminal* öffnen. Die Kommandozeilen in diesem Heft sind alle ohne Silbentrennung gedruckt; d.h., ihr müsst alle Minus-Zeichen auch am Zeilenende eintippen. Des Weiteren findet ihr diese

12 `https://tails.boum.org/contribute/design/download_verification/`

Anleitung auch auf unserer Webseite `https://capulcu.blackblogs.org`, sodass ihr die Kommandos auch dort mit der Maus in die Zwischenablage kopieren und im Terminal einfügen könnt. Die Kommandozeilen-Eingabe wird jeweils mit der Eingabetaste [ENTER] abgeschlossen. Ein \ am Ende der Zeile zeigt an, dass das Kommando auf der nächsten Zeile fortgesetzt wird.

Linux

1. Tails-Schlüssel von der Kommandozeile herunterladen und importieren:

   ```
   wget https://tails.boum.org/tails-signing.key
   gpg --import tails-signing.key
   ```

   Die Ausgabe sollte wie folgt aussehen:

   ```
   gpg: key 0xDBB802B258ACD84F: public key "Tails \
    developers (offline long-term identity key) \
    <tails@boum.org>" imported
   gpg: Total number processed: 1
   gpg: imported: 1 (RSA: 1)
   ```

   (wenn du den Schlüssel das erste Mal importierst) oder

   ```
   gpg: key 0xDBB802B258ACD84F: "Tails developers \
    (offline long-term identity key) \
    <tails@boum.org>" not changed
   gpg: Total number processed: 1
   gpg: unchanged: 1
   ```

   (wenn der Schlüssel bereits importiert war)

   Wir überprüfen nun, ob der importierte Key echt, d.h. unverändert ist:

   ```
   gpg --fingerprint 0xDBB802B258ACD84F | grep \
    fingerprint
   Key fingerprint = A490 D0F4 D311 A415 3E2B B7CA \
    DBB8 02B2 58AC D84F
   ```

   Die Ausgabe bei euch muss identisch sein, andernfalls ist etwas schief gegangen.

   In diesem Fall löscht den falschen Key mit

   ```
   gpg --delete-key DBB802B258ACD84F
   ```

   und versuche diese Prozedur von einem anderen Internet-Anschluss aus nochmal. Auf keinen Fall mit dem falschen Key weitermachen!

2. Tails herunterladen: (>1GB - das dauert eine Weile) Um ein ISO-Image herunterzuladen, geht auf folgende Seite: `https://tails.boum.org/install/dvd-download/index.en.html`. Ladet dort die Software hinter dem Link „Download the Tails 4.8 ISO image (1.2 GiB).“ herunter. Um eine IMG-Image herunterzuladen, geht auf folgende Seite: `https://tails.boum.org/install/download/index.en.html`. Ladet dort die Software hinter dem Link „Download the Tails 4.8 USB image (1.2 GiB).“ herunter. Beim Schreiben dieses Textes ist 4.8 die aktuelle Version, das wird sich natürlich im Laufe der Zeit ändern.

3. Tails-Signatur herunterladen:

   Auf den gleichen Seiten findet ihr den Link „Download the Tails 4.8 OpenPGP signature“, ladet diese herunter.

4. Tails mit der Signatur überprüfen:

   Jetzt zum magischen Schritt: Die Überprüfung der Signatur und damit die Sicherstellung, ob die Tails-Software modifiziert wurde oder nicht.

   ```
   gpg --verify tails-amd64-4.8.iso.sig \
    tails-amd64-4.8.iso
   ```

   Die Ausgabe sollte nach zusätzlichen GPG-Statusmeldungen wie folgt aussehen:

   ```
   gpg: Signature made Mon 25 Apr 2016 07:02:56 PM CEST
   gpg: using RSA key 0x98FEC6BC752A3DB6
   gpg: Good signature from "Tails developers \
    (offline long-term identity key) <tails@boum.org>"
   gpg: aka "Tails developers <tails@boum.org>"
   gpg: WARNING: This key is not certified with a \
    trusted signature!
   gpg: There is no indication that the signature \
    belongs to the owner.

   Primary key fingerprint: A490 D0F4 D311 A415 3E2B \
    B7CA DBB8 02B2 58AC D84F
   Subkey fingerprint: BA2C 222F 44AC 00ED 9899 3893 \
    98FE C6BC 752A 3DB6
   ```

   ACHTUNG: Überprüfe, ob „Good signature ...“ erscheint. Wenn dem so ist, und nur dann**(!)**, fahre fort. Andernfalls entferne die heruntergeladenen Dateien, z.B. mit dem Kommando

   ```
   rm tails-amd64-4.8.iso
   ```

   , wechsle den Ort bzw. die Internetverbindung, und lade Tails erneut herunter.

   Wenn du fertig bist, kannst du folgendem Kommando das Terminal schließen.

   ```
   exit
   ```

Mac

Während bei allen Linux-Distributionen das Programm *GPG* bereits installiert ist, müssen MacOSX-Nutzer*innen einmalig das Programm *GnuPG for OSX*[13] herunterladen.

Desweiteren verwenden Mac-Nutzer*innen das Kommando „curl -O“ statt „wget“ und zwar mit einem großen „O“ - keine Null! Ansonsten sind alle vier Schritte des vorherigen Abschnitts identisch.

Variante 2, Schritt 2: Tails auf USB-Stick installieren oder DVD brennen

Im Folgenden beschreiben wir, wie ihr Tails auf einen USB-Stick installiert oder auf DVD brennt.

Tails auf USB-Stick installieren

Wir empfehlen zur komfortablen Einrichtung eines Tails-USB-Sticks das Programm *Gnome-Disks* zu benutzen, welches unter anderem in Debian und Ubuntu zur Verfügung steht. Du benötigst einen USB-Stick mit mindestens 8 GB Speicherplatz. ACHTUNG: Alle eventuell vorhandenen Daten auf diesem Stick werden gelöscht![14] Weiter geht es für alle Linux-Varianten mit der Erstellung des Tails-USB-Sticks.

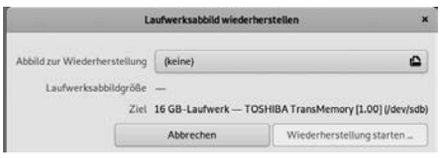
- Entferne alle möglicherweise an den Computer angeschlossenen USB-Sticks, die du nicht als Tails-Stick verwenden möchtest.
- Schließe den USB-Stick an den Computer an, der zukünftig Tails-Stick werden soll. Erinnerung: Alle Daten auf diesem Stick werden gelöscht!

13 `https://sourceforge.net/p/gpgosx/docu/Download/`

14 Ein*e Forensiker*in könnte die ehemaligen Daten problemlos wiederherstellen. Daher nutze keinen Stick, auf dem zuvor unverschlüsselte, sensible Daten gespeichert waren.

- Starte das Programm „Gnome-Disks“. Du findest es im Anwendungsmenü Hilfsprogramme unter dem Namen „Disks“ oder „Laufwerke“
- Wähle in der Laufwerksliste den USB-Stick aus, auf dem du Tails installieren willst.

- Klicke auf die 3 Striche in der Kopfleiste des Programms. Wähle dort „Laufwerksabbild wiederherstellen“ . Beim Klicken auf „Laufwerksabbild wiederherstellen“ öffnet sich ein Dateibrowser, navigiere in das „Persönlicher Ordner / Tor Browser“-Verzeichnis und klicke doppelt auf „4.8“ oder eine entsprechend neuere Version (NICHT „4.8.sig“).



- In dem Feld unter „Ziel“ kannst du nochmals kontrollieren, ob du den richtigen Stick ausgewählt hast.
- Klicke ganz unten auf „Widerherstellung starten“. Das dann erscheinende Fenster fragt dich um Bestätigung, weil alle Daten auf dem USB-Stick gelöscht werden.
- Wenn du dir sicher bist, klicke „Wiederherstellen“.
- Andernfalls klicke „Cancel“, und wechsle den USB-Stick.
- Der nachfolgende Prozess dauert eine Weile. Auf keinen Fall den Stick ziehen! Danach könnt ihr Gnome-Disks schließen.

Mac

Das Tails-Team empfiehlt für die Tails-Installation unter MacOS X die Verwendung von *Etcher*. Etcher könnte ihr euch auf der Tails-Seite herunterladen.[15]

- Ladet *Etcher* unter dem angegebenen Link herunter.
- Öffnet den Download (DMG Image).
- Schiebt das *Etcher*-Icon in den Programme-Ordner.
- Schließt das Fenster und werft das *Etcher*-Image aus.

Zur Installation von Tails geht ihr wie folgt vor:

- Steckt den USB-Stick ein, auf dem ihr Tails installieren wollt.
- Öffnet „Finder“ und wählt im Programme-Ordner *Etcher*.
- Klickt auf den „Select Image“-Button und wählt das heruntergeladene Tails-Image aus. Beachtet, dass es eine IMG Endung haben muss.
- Ist nur ein USB-Stick im Computer eingesteckt, erkennt *Etcher* ihn direkt. Ansonsten müsst ihr über den „change“-Button den richtigen Stick auswählen.
- Klickt `Flash` . *Etcher* installiert jetzt Tails auf dem USB Stick.

Tails auf DVD brennen

Wer keinen USB-Stick für das Tails-Betriebssystem benutzen möchte oder kann, muss sich mit einer DVD behelfen. Vorteil: Die einmal gebrannte DVD ist automatisch gegen nachträgliche Veränderung „schreibgeschützt“. Nachteil: Ihr müsst für jede aktuelle Tails-Version (etwa alle 2 Monate) eine neue DVD brennen. Dieser Abschnitt gilt sowohl für Linux als auch MacOSX.

Nachdem ihr nun davon ausgehen könnt, dass ihr eine korrekte Version von Tails besitzt (z.B. *tails-amd64-4.8.iso*), muss das Betriebssystem auf eine DVD gebrannt werden. Verwendet dafür am besten eine *nicht-wieder-beschreibbare* DVD mit der Bezeichnung „DVD+R“. Sie sollte auf keinen Fall die Bezeichnung „DVD+RW“ oder „DVD+RAM“ besitzen.

Linux

Tails könnt ihr euch unter Ubuntu oder Debian auf DVD brennen, indem ihr mit der *rechten Maustaste* aus die überprüfte Tails.iso-Datei (z.B. *tails-amd64-4.8.iso*) klickt und „Mit Brasero öffnen“ oder „Mit Xfburn öffnen“ auswählt. Mit einem Bestätigen über den Button `Abbild erstellen` wird Tails auf eine DVD gebrannt.[16]

Mac

Um Tails auf eine DVD zu brennen, müsst ihr das „Festplattendienstprogramm“ unter „Programme/Dienstprogramme“ öffnen und die Tails.iso Datei (z.B. *tails-amd64-4.8.iso*) dort hinein ziehen. Danach kann das Live-System über den Button `Brennen` auf eine DVD gebrannt werden.

Alternativ könnt ihr Tails auch über das „Festplattendienstprogramm“ durch `Images ► Brennen` dauerhaft auf eine DVD bringen.

Tails starten

Da einige Menschen, abhängig vom Rechner und dessen BIOS-Einstellmöglichkeiten, *Schwierigkeiten beim Booten* von einem der Startmedien haben, gehen wir kurz auf die häufigsten Fallstricke ein. Falls euch etwas nicht gelingen sollte, holt euch Hilfe. Denn das ist kein hinreichender Grund, auf die Benutzung von Tails zu verzichten!

---

15 `https://tails.boum.org/etcher/Etcher.dmg`

16 Für neuere Ubuntu-Versionen (nach 12.10) findet ihr eine Anleitung zum Erstellen der DVD unter folgender Webseite: `https://help.ubuntu.com/community/BurningIsoHowto`

Achtung! Der Tails-Datenträger muss vor dem Start eingelegt/eingesteckt sein - andernfalls würde ein „Fehlstart“ mit eurem Standard-Betriebssystem euren Computer starten. Bei Laptop kann das dazu führen, dass eure originale MAC-Adresse per WLAN in der Funkreichweite bekannt gemacht wird (siehe Kapitel „Tails ändert eure MAC-Adresse(n)“). Ein spezieller Recherche-Computer, aus dem ihr die Festplatte ausbaut und den ihr nur für Live-Systeme wie Tails nutzbar macht, löst das „Fehlstart“-Problem und verhindert zudem ein „versehentliches“ Speichern von Daten auf die Festplatte (siehe Kapitel „Tails Tails als „Quasi-Schreibmaschine“ für sensible Offline-Arbeiten“).

Bootreihenfolge im BIOS ändern

Um euren Rechner in die Lage zu versetzen, ein Betriebssystem von DVD bzw. vom USB-Stick booten („starten“) zu können, müsst ihr in der Regel die „Boot-Reihenfolge“ im sogenannten BIOS ändern. Das BIOS ist das Basis-Betriebssystem eines Rechners, das grundlegende Rechnerfunktionen an-/ausschaltet und festlegt, in welcher Reihenfolge beim Start auf welchen Datenträgern nach bootfähigen Betriebssystemen gesucht werden soll. Die meisten Rechner bieten nur ein englischsprachiges BIOS-Menü.

1. Datenträger einlegen/-stecken und Computer starten.
2. Unmittelbar nach dem Start eine der Tasten F1, F2, DEL, ESC, F10 oder F12 gedrückt halten (auf einen Hinweis auf dem kurz erscheinenden Startbildschirm achten), um in das BIOS-Setup zu gelangen. Folgende Liste zeigt die *wahrscheinlichsten* Tasten, um zu den BIOS-Einstellungen zu gelangen:

Acer	Esc, F12, F9
Asus	Esc, F8
Dell	F12
Fujitsu	F12, Esc
HP	Esc, F9
Lenovo	F12, Novo, F8, F10, Return
Samsung	Esc, F12, F2
Sony	F11, Esc, F10
Toshiba	F12
andere	F12, Esc

3. Suche im Menü nach „Edit Boot Order“ (Boot-Reihenfolge ändern).
4. Setze den Eintrag „DVD“ oder aber einen der Einträge „removable drive“, „external USB disk“ oder „USB media“ an den Anfang der Liste der zu durchsuchenden Geräte. Auf jeden Fall vor den Listeneintrag eurer internen Festplatte „HD“oder „harddisk“.
5. Danach mit „Save changes and exit“ das BIOS verlassen und den Betriebssystemstart fortsetzen. Jetzt sollte der Rechner die geänderte Boot-Reihenfolge berücksichtigen.

Booten „fremder Systeme“ zulassen

Falls Tails trotz geänderter Boot-Reihenfolge nicht startet, und der Tails-Stick bzw. die Tails-DVD korrekt erstellt wurde (was einfach durch einen Test an einem anderen Computer zu überprüfen ist), dann überprüft bei neuerem Computer, ob ihr im BIOS eine der folgenden Funktionen finden und auswählen könnt:

- Enable Legacy mode
- Disable Secure boot
- Enable CSM boot
- Disable UEFI
- Disable Fastboot

Wenn Tails nicht vom USB-Stick startet

- Bootreihenfolge im BIOS überprüfen – sucht das BIOS wirklich auf einem externen USB-Gerät, bevor die Festplatte durchsucht wird?
- Ältere Rechner (vor 2001) sind teilweise nicht in der Lage, von USB zu „booten“.
- Andere externe USB-Geräte zum Start abziehen.
- Verwende einen anderen USB-Anschluss – Das BIOS mancher Rechner überprüft bei der Suche nach bootfähige Datenträgern nicht alle der vorhandenen USB-Anschlüsse.
- Überprüfe, ob der Stick wirklich „bootfähig“ ist. Führe erneut die Schritte zum „Brennen“ des USB-Sticks durch. Es genügt nicht, die Dateien auf den Stick zu „kopieren“.

Mac booten

Beim Hochfahren eures Macs müsst ihr die *Alt*-Taste oder die *C*-Taste gedrückt halten, damit anschließend die Tails-DVD als Startmedium bestimmt wird (oft wird sie fälschlicherweise als Windows-CD angezeigt). Alternativ könnt ihr sie auch unter Systemeinstellungen ► Startvolume auswählen. Bei Mac-Laptops ist das Track-Pad unter Tails oft nicht richtig nutzbar. In diesem Fall hilft eine externe USB-Maus.

Tails booten

Nachdem der Computer den Datenträger als Boot-Medium erkannt hat, erscheint wenige Sekunden später der **Boot-Bildschirm**. Bei den meisten Computern genügt es, die voreingestellte Auswahl *Live* mit der Enter-Taste zu bestätigen oder zehn Sekunden zu warten. Nur wenn *Tails* danach keine sichtbaren Startbemühungen unternimmt, solltet ihr in einem neuen Start-Versuch die Option *Tails (Troubleshooting Mode)* auswählen.

Zusätzliche Boot-Optionen

Um (eine) zusätzliche Boot-Option(en) auszuwählen, müsst ihr hingegen bei Erscheinen des Boot-Bildschirms

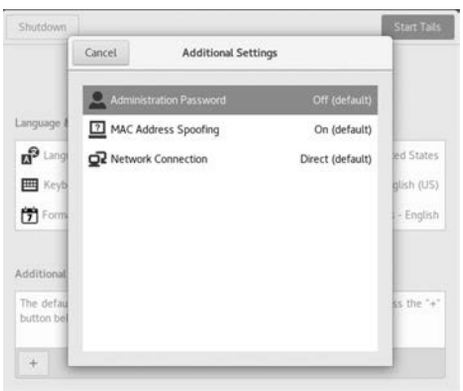
1. die *Tabulator*-Taste drücken und
2. ein *Leerzeichen* eingeben. Dann die jeweilige(n) Boot-Option(en) (jeweils durch ein Leerzeichen getrennt) eingeben und mit *Enter* abschließen:

toram Lädt *Tails* komplett in den Arbeitsspeicher (mindestens 2-4 GB). Empfehlenswert, wenn ihr **a**) einen USB-Stick ohne Schreibschutzschalter als *Tails*-Boot-Medium verwendet oder **b**) eine *Tails*-DVD nutzt, das DVD-Laufwerk aber zum Brennen von Daten in der Sitzung benötigt.

Tails-Startbildschirm

Nach erfolgreichem Boot-Vorgang erscheint folgender Startbildschirm:

Die Default-Spracheinstellung ist englisch mit US-Tastaturlayout. Mit einem Klick auf „Language“ könnt ihr bequem diese Spracheinstellung anpassen, muss es detaillierter sein, könnt ihr unter „Keyboard Layout“ und „Formats“ (z.B. Anzeigeformat von Datum und Uhrzeit) entsprechende Auswahlen treffen. Unter „Additional Settings“ findet ihr einen `+`-Button, klickt ihr darauf, erscheinen weitere Konfigurationsmöglichkeiten:



Administrationspasswort Das benötigt ihr, wenn ihr euren Bildschirm vorübergehend sperren wollt oder für ein Programm Administrations-Rechte braucht. Dies ist z.B. notwendig für das Installieren eines Druckers oder den Zugriff auf die interne Festplatte des Rechners. Ihr könnt euch im dann folgenden Dialog ein beliebiges Passwort ausdenken (und merken!). Es behält seine Gültigkeit nur für diese eine *Tails*-Sitzung.

Manipulation der MAC-Adresse Wenn der Netzzugang nur bestimmten Computern gewährt wird und ihr auf die zusätzliche Sicherheit einer geänderten MAC-Adresse verzichten könnt, könnt ihr das standardmäßig eingeschaltete Spoofing ausschalten.

Netzwerkverbindung Wenn das Netz, in dem ihr euch befindet, Zugriffe einschränkt, dann wechselt hier auf „Tor-Brücke oder lokalen Vermittlungsserver konfigurieren“ - seid ihr unsicher, ob das passiert, probiert es erstmal mit der Standardeinstellung „Direkt mit dem Tor-Netzwerk verbinden (Vorgabe)“. Mit „Alle Netzwerkfunktionen deaktivieren“ könnt ihr alle Netzwerkadapter softwareseitig beim Start deaktivieren. Dies geschieht sinnvoller Weise, bevor *Tails* seine Netzwerkfunktionalität startet. So bleiben u.a. WLAN und Bluetooth still und können eure Anwesenheit in Funkreichweite anderer Geräte nicht mehr preisgeben. (Siehe dazu das Kapitel „*Tails* als Quasi-Schreibmaschine“).

Unsicherer Webbrowser Der unsichere Webbrowser ist ab *Tails* Version 4.8 standardmäßig deaktiviert, da er zur Deanonymisierung verwendet werden kann. Ein*e Angreifer*in könnte eine Sicherheitslücke in einer anderen Anwendung in Tails ausnutzen, um einen unsichtbaren unsicheren Browser zu starten und deine wahre IP-Adresse zu offenbaren. Das funktioniert auch, wenn du selbst den unsicheren Browser nicht verwendest. Beispielsweise könnte eine Angreifer*in eine Sicherheitslücke in Thunderbird ausnutzen, indem er oder sie dir eine Phishing-E-Mail schickt, die einen unsichtbaren Browser startet, eine Website aufruft und damit deine IP-Adresse enthüllt. Ein solcher Angriff ist sehr unwahrscheinlich, könnte aber von einem starken Angreifer, wie z.B. einer Regierung oder einem Hackerunternehmen, durchgeführt werden. Aus diesem Grund empfehlen wir und auch die *Tails*-Entwickler*innen:

- Aktiviere den unsicheren Browser nur, wenn du dich z.B. ein einem Internet-Cafe oder in einem Hotel bei einem Login-Portal anmelden musst, um eine Internetverbindung aufzubauen.
- Aktualisiere immer auf die neueste Version von Tails, um bekannte Schwachstellen so schnell wie möglich zu beheben.

Nachdem ihr den Schalter `Tails starten` angeklickt habt, meldet sich Tails mit der grafischen Oberfläche und den zwei Hauptmenüs **Anwendungen** und **Orte**. Damit Tails erkennt, ob ihr eine veraltete Version benutzt, wird zu Beginn eurer Sitzung (nach erfolgreich hergestellter Netzwerk-Verbindung) einmal nach Hause telefoniert. Ihr werdet ggfs. aufgefordert, per *Upgrade* eine neue Version einzuspielen.

Zur gleichzeitigen Arbeit mit mehreren Programmen sind zwei Arbeitsflächen voreingestellt - damit es auf einem kleinen Bildschirm nicht zu voll wird. Zieht den Mauszeiger in die linke obere Ecke, um eine Übersicht über den aktuellen Desktop, Arbeitsflächen und das Programmpanel zu bekommen.

Tails benutzt die graphische Oberfläche *Gnome*, deren Benutzung etwas Einarbeitung bedarf. Insbesondere ist die Standardeinstellung für das Scrollen MacOSX nachempfunden und damit genau andersrum, als wie von Windows und den meisten Linux-Betriebssystemen gewohnt.

Nur über Tor ins Netz

Wir gehen in diesem Kapitel darauf ein, wie Rechner im Netz kommunizieren, auf das Tor-Prinzip und dessen Nutzung sowie einige Fallstricke[17].

Das Internet Protocol und das Domain Name System

Das Domain Name System (DNS) ist mit einem Telefonbuch vergleichbar. Menschen greifen online über Domänennamen, wie de.indymedia.org oder tails.boum.org, auf Informationen zu. Rechner interagieren über IP-(Internet Protocol)-Adressen. Jedes Gerät, das mit dem Internet verbunden ist, hat eine eindeutige IP-Adresse, die von anderen Rechnern verwendet

17 https://tor.eff.org/download/download-easy.html.en#warning

wird, um das Gerät zu finden. DNS-Server machen es überflüssig, dass sich Menschen IP-Adressen wie `192.168.1.1` (in IPv4) oder komplexere neuere alphanumerische IP-Adressen wie `2400:cb00:2048:1::c629:d7a2` (in IPv6) merken müssen. Der Prozess der DNS-Auflösung beinhaltet die Umwandlung eines Hostnamens (Domänennamen) in eine computerfreundliche IP-Adresse. Wenn die IP-Addresse bekannt ist, kann diese auch direkt eingegeben werden um mit dem Host zu kommunizieren.

> *Wenn ihr eine Webseite laden wollt, muss eine Übersetzung erfolgen zwischen dem, was ihr in eurem Webbrowser eingebt und der maschinenfreundlichen Adresse, die notwendig ist, um die entsprechende Webseite zu finden.*

Identifizierung im Netz per IP- und MAC-Adresse

Ein großer Teil der digitale Kommunikation identifiziert die Kommunizierenden über die IP-Adresse. Ein *Router*, über den ihr ins Netz geht, bekommt eine IP-Adresse vom Internetanbieter zugewiesen. Die IP-Adresse wird bei jeder Netzaktivität über ein standardisiertes Protokoll (lesbar) mitgeschickt. Euer Surfen, Chatten oder Mailen ist (ohne Tor) mit der *Identität und Lokalität dieses Routers* nachvollziehbar verknüpft.

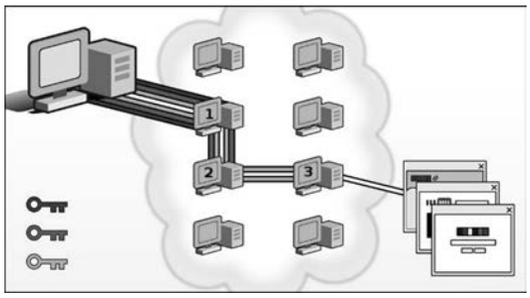
> *Wenn ihr keine zusätzlichen Vorkehrungen trefft, verrät die übertragene IP-Adresse den ungefähren geografischen Ort des Routers, über den ihr ins Netz geht.*

Zusätzlich besitzen alle Netzwerkadapter eine zusätzliche Kennung - die MAC-Adresse (Media-Access-Control, z.B. `B4:89:91:C1:F4:CE`). Jede Netzwerkschnittstelle (z.B. die WLAN-Karte oder das kabelgebundene LAN) eures Rechners meldet sich mit einer eigenen, eindeutigen (physikalischen) MAC-Adresse beim Router an. Beim aktuell (noch) verwendeten Internetprotokoll (IPv4) wird diese jedoch nicht „nach draußen“ (ins Netz) übertragen[18]. Aber: Wenn ihr z.B. per WLAN in einem öffentlichen Café ins Netz geht, kann der Betreiber oder ein Angreifer ohne technischen Aufwand eure MAC-Adresse mitprotokollieren. Damit ist dann eure Internet-Aktivität nicht mehr nur dem WLAN-Router des Cafés, sondern exakt dem von euch verwendeten WLAN-Adapter eures Computers zuzuordnen! Auch zu Hause kann ein Angreifer, der sich in euren Router hackt, unterscheiden, welcher Rechner (z.B. in der WG) eine bestimmte Mail verschickt hat. Wir kommen gleich dazu, wie ihr euch gegen eine Identifikation per MAC-Adresse schützen könnt.

Das Tor-Prinzip (The Onion Router)

Statt in eurem Standard-Browser z.B. die Webseite `http://tagesschau.de` direkt zu besuchen und dieser beim Kontaktaufbau die IP-Adresse eures Routers mitzuteilen, geht ihr beim voreingestellten *Tor-Browser* von Tails einen Umweg über drei Zwischenstationen.

Die Datenpakete werden samt IP-Adresse des eigentlichen Empfängers wie in einer Zwiebel in verschiedenen Schichten verschlüsselt. Das wird Onion Routing genannt, daher der frühere Name The Onion Router - abgekürzt Tor. Perfect Forward Secrecy wird durch den Diffie-Hellman-Schlüsselaustausch erreicht. Die verwendeten Schlüssel existieren nur für den Zeitraum der Kommunikationsverbindung.



Um den Ursprung der Daten zu verschleiern, werden sie durch mehrere Rechner geschleust. Sie gehen zunächst an einen sogenannten Eintrittsknoten (Entry Node). Dazu baut ein Client-Rechner über ein Socks-Proxy eine Verbindung mit dem Eintrittsknoten auf. Der erstellt eine weitere Verbindung mit einer willkürlich ausgewählten Zwischenstation (Relay), die wiederum eine Verbindung mit einem sogenannten Exit Node oder Austrittsknoten herstellt. Von dort wird dann die Verbindung mit dem eigentlichen Ziel hergestellt, etwa dem Webserver jener Adresse, die der Benutzer in seinen Tor-Browser eingegeben hat. Der Webserver kennt nur die IP-Adresse des Ausgangsknotens und nicht die des ursprünglichen Absenders.

Eintrittsknoten, Zwischenstation und Austrittsserver werden alle auch Relays genannt. Dir drei Rechner werden von der Tor-Software aus weltweit (derzeit) über 6700 verfügbaren Tor-Rechnern *zufällig* ausgewählt und bei mehrfach aufgebauten TCP-Verbindungen etwa alle zehn Minuten ausgewechselt. Bei einer länger bestehenden TCP-Verbindung, etwa bei einer Unterhaltung per IRC, bleibt die Verbindung jedoch bestehen. So soll verhindert werden, dass ein Angreifer nicht nur eine, sondern mehrere Möglichkeiten hat, eine Verbindung zu entdecken.

Mit jeder Weitereichung wird eine Verschlüsselungsschicht entfernt. So kennt die Zwischenstation zwar den Eingangsknoten, aber nicht den ursprünglichen Versender der Daten. Die Zwischenstation weiß auch, an welchen Ausgangsknoten die Daten verschickt werden sollen, kennt aber nicht das eigentliche Ziel außerhalb des Tor-Netzwerks. Das kennt nur der Ausgangsknoten, der die Daten von der letzten Verschlüsselungsschicht befreit und die Daten mit seiner eigenen IP-Adresse an den Zielrechner weiterleitet.

Der Inhaber des Servers, auf dem die Zielwebseite liegt (oder ein dort mitlesender Schnüffler) erhält nicht eure IP-Adresse, sondern die vom Tor-Exit-Rechner **3** als Besucher*innen-IP. Zwar ist erkennbar, dass es sich hierbei um einen Rechner des Tor-Netzwerkes handelt (die Liste aller verfügbaren Tor-Rechner ist öffentlich einsehbar), aber eure Identität ist nicht rekonstruierbar, es sei denn, der Inhalt eurer Kommunikation mit der Zielwebseite verrät euch (persönliche Identifikation). Keiner der drei Tor-Rechner kennt den kompletten Pfad von eurem Rechner bis zum Zielserver. Nur ein Angreifer, der den Netzverkehr von Tor-Rechner **1** und **3** mitprotokolliert, kann versuchen eure IP mit dem Besuch der Ziel-Webseite in Verbindung zu bringen[19].

Umgekehrt werden die Daten vom Empfänger wieder verschlüsselt über das Tor-Netzwerk an den Sender übermittelt. Der ursprüngliche Eintrittsknoten wiederum entfernt die letzte Verschlüsselungsschicht und leitet die Daten an den Client weiter.

---

18 Bei dem neueren Internetprotokollstandard IPv6 kann die MAC-Adresse in der IP mitkodiert werden. Das würde die Verschleierung des verwendeten Rechners gefährden. Deshalb verwendet Tails diesen Protokollstandard nicht.

19 Ein Angriff über eine sogenannte Timestamp-Analyse kommt ohne Kenntnis des Datenverkehrs von Tor-Rechner 2 aus.

Standardmäßig sind es immer drei Relays. Zum einen soll damit eine einigermaßen leistungsfähige Verbindung gewährleistet werden, denn die Weitereichung und die Entschlüsselung kosten Zeit. Zum anderen gewährleisten zusätzliche Relays im Tor-Netzwerk nicht mehr Anonymität. Das mag paradox klingen, hat aber einen einfachen Grund: Je mehr Rechner in eine einzelne Verbindung miteinbezogen werden, desto größer ist die Wahrscheinlichkeit, dass einer oder sogar mehrere davon einem Angreifer gehören.

Dennoch ist das Tor-Netzwerk darauf angewiesen, auf möglichst viele Rechner zugreifen zu können. Das verringert im ganzen Netzwerk die Wahrscheinlichkeit, dass ein gekapertes Relay in die Verbindungskette gelangt.

512 Bytes

Die Verschlüsselung ist allerdings nicht der einzige Schutz, den Tor zu bieten hat. Denn die Daten werden nicht nur verschlüsselt, sondern außerdem in immer gleich große Pakete oder Zellen von 512 Bytes aufgeteilt, um Rückschlüsse auf den Inhalt zu verhindern. So können Angreifer nicht unterscheiden, ob es sich um einfache Serveranfragen oder etwa um übertragene Multimediadaten handelt.

Wo passiert die Namensauflösung?

Tor-Clients führen im Allgemeinen keine direkten DNS-Anfragen durch. Wenn eine Verbindung über das Tor-Netzwerk aufgebaut wird, werden DNS-Anfragen anstatt über das Betriebsystem über den Tor-Client (auf seinen Socks-Ports) durchgeführt. Sobald der Tor-Client eine Verbindung hergestellt hat, sendet er diesen Hostnamen an den Tor-Exit-Rechner in seiner initiallen Nachricht. Der Exit-Rechner führt dann eine DNS-Auflösung durch und öffnet eine TCP-Verbindung zum Ziel. Sobald diese Verbindung hergestellt ist, teilt er sie dem Client mit, dass die Verbindung offen ist, und teilt ihm zu Informationszwecken auch mit, auf welche Adresse der Hostname aufgelöst wurde.

> *Tor übermittelt die Zieladresse (in dem Tor-Protocol) an das Exit-Relay, welches dann den Namen zu einer IP-Adresse auflöst.*

Tor hat darüber hinaus eine Art DNS-Fernauflösungs-protokoll eingebaut[20]. Diese Unterstützung erlaubt es Clients, nach bestimmten Ressourcentypen, wie IPv4- oder IPv6-Adressen, zu fragen. Auch hier übernimmt der Ausgangsknoten das eigentliche Senden und Empfangen von DNS-Paketen und leitet nur die Antwort an den Client weiter.

Tatsächlich werden vom Client aus nie UDP-Pakete weitergeleitet.

Verschleierung der Identität bedeutet nicht automatisch Verschlüsselung

Die Verbindungen von eurem Rechner zum Tor-Rechner **1**, sowie **1—2** und **2—3** sind verschlüsselt. Damit ist der Inhalt bei einem Schnüffel-Angriff auf diese Verbindungen, bzw. auf die Tor-Rechner **1** und **2** nicht lesbar. *Die Verbindung von **3—Ziel** ist hingegen unverschlüsselt!*

Nur, wenn Ihr eine Webseite beginnend mit HTTPS besucht, wie z.B. `https://de.indymedia.org`, ist auch der Inhalt dieser letzten Verbindung verschlüsselt. Der Tor-Browser von Tails versucht immer eine HTTPS-Verbindung zum Ziel aufzubauen. Bietet der Webseitenbetreiber jedoch nur HTTP-Verbindungen an, ist eure Kommunikation mit diesem Server unverschlüsselt und kann dort bzw. auf dem Tor-Exit-Rechner **3** oder zwischen Exit-Node und Zielserver mitgelesen werden!

Verschiedene Nutzungsmodelle von Tor

Tor verschleiert eure IP-Adresse, mit der ihr zum Surfen, Mailen oder Chatten mit anderen Servern Kontakt aufnehmt. Einer der Zwecke von Tor liegt in der **Verschleierung der eigenen Identität**.

Als Besucher*in einer Webseite geht das, solange ihr dort keine Daten über euch preisgebt, oder spezifische Inhalte euch eindeutig identifizieren. Beim Mailen können euch Mail-Kontakte oder Mail-Betreffzeile leicht verraten, selbst wenn ihr peinlich genau darauf geachtet habt, dass (inklusive Account-Eröffnung) über die gesamte Historie der Account-Nutzung alles anonym ablief.

Deshalb wird vielfach behauptet, dass Tor unsinnig ist, wenn ihr euch persönlich (ohne Pseudonym) bei eurer Mail-Account einloggt oder eine Mail von einer Adresse verschickt, die mit eurer Person eindeutig in Verbindung steht. Das stimmt nur zur Hälfte. Richtig ist, dass ihr mit einem (realen) persönlichen *login* eure Identität gegen über dem Server offenbart – da hilft auch kein Tor. Aber ihr könnt auch in diesen Fällen Tor zur **Verschleierung eures Aufenthaltsortes** nutzen. Ein weiterer Anwendungsfall für Tor ist das **Erschweren von Zensur und Überwachung eurer Netzwerkaktivitäten**.

> *Wir raten euch, **immer** per Tor ins Netz zu gehen und eure Netzaktivitäten entlang verschiedener Identitäten „aufzutrennen“.*

Identitäten sauber trennen

Es ist nicht ratsam, in ein und derselben Tails-Sitzung verschiedene Aufgaben im Internet zu erledigen, die nicht miteinander in Verbindung gebracht werden sollen. Ihr müsst selbst verschiedene (kontextuelle) Identitäten sorgsam voneinander trennen!

Ein Beispiel: Es ist gefährlich, in der gleichen Sitzung per Tor (ortsverschleiernd) die persönlichen Mails abzurufen und anonym bei indymedia einen Text zu publizieren. Das heißt, ihr solltet nicht gleichzeitig *identifizierbar* und *anonym* ins Tor-Netz. Ihr solltet auch nicht gleichzeitig unter Pseudonym A

---

20 Es gibt auch einen Vorschlag, Tor mit vollwertiger DNS-Unterstützung auszustatten. Proposal 219 - Support for full DNS and DNSSEC resolution in Tor (`https://gitweb.torproject.org/torspec.git/tree/proposals/219-expanded-dns.txt`). Bislang wurde dies noch nicht umgesetzt.

21 Cookies sind kleine Dateien, die z.B. ein Webseitenbetreiber auf eurem Rechner als Webseitenbesucher zur Wiedererkennung von bestimmten Einstellungen ablegt. Tails untersagt das Speichern der meisten Cookie-Sorten. Die meisten zugelassenen Cockies werden beim Beenden des Tor-Browsers gelöscht. Andere, zugelassene Cookies verbleiben im flüchtigen Arbeitsspeicher und verschwinden bei einem Neustart.

und Pseudonym B ins Tor-Netz gehen, denn diese Pseudonyme könnten auf einem überwachten/korrumpierten Tor-Exit-Rechner 3 miteinander in Verbindung gebracht werden.

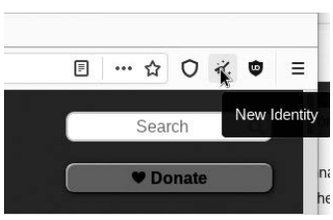
Da ihr euch nicht in allen Fällen auf die Funktion „Neue Identität“ im Tor-Browser verlassen könnt, um die verschiedenen Netzaktivitäten (durch verschiedene IP-Adressen der verschiedenen Tor-Guard-Rechner) voneinander zu separieren (siehe Abschnitt „Correlation Attack“ im Kapitel „Grenzen von Tails und Tor“), lautet die unbequeme, aber sichere Empfehlung:

> *Tails zwischen Netzaktivitäten unterschiedlicher Identität herunterfahren und neu starten!*

Sogenannte *Cookies*[21], ein Tor-Anwendungsfehler eurerseits oder eine (noch nicht bekannte oder behobene) Sicherheitslücke in einem Programm innerhalb von Tails könnten Informationen über eure Tails-Sitzung offenlegen. Diese könnten offenbaren, dass ein und dieselbe Person hinter den verschiedenen Netzaktivitäten der gleichen Tails-Sitzung (trotz wechselnder IP-Adresse des Tor-Exit-Rechners 3) steckt.

Tor Identität wechseln

Wenn ihr im Tor-Browser auf „Neue Identität“ klickt ändert Tor die letzten beiden von drei Knoten.



Unter anderem den Exit-Knoten, was sinnvoll sein kann, wenn ihr gegenüber der Webseite die ihr besucht mit unterschiedlichen Identitäten wahrgenommen werden wollt. Tor wechselt allerdings nicht den Entry-Knoten eurer Verbindung. Der bleibt gleich und hat damit die Möglichkeit euch wiederzuerkennen. Die New-Identity-Funktion tut folgendes:

- Schließen aller geöffneter Tabs
- Löschen aller Session Daten: Cache, History und Cookies
- Schließen aller Web-Verbindungen und Aufbau neuer TorCircuits (Entry-Knoten bleibt gleich)
- Löschen des Zwischenspeichers(Clipboard).

Tor kann keinen Schutz gegen einen Angreifer bieten, der den ersten und letzten Knoten kontrolliert. Mit Hilfe von Packet- und Zeitanalysen könnte ein*e Nutzer*in deanonymisiert werden. Da die Torverbindungen sehr kurzlebig sind, geht die Wahrscheinlichkeit, dass über einen längeren Zeitraum irgendwann eine Verbindung davon betroffen ist gegen 100 Prozent. Zusätzlich kann durch die Kontrolle eines mittleren Knoten auch der Aufbau einer neuen Verbindung erzwungen werden. Um die Wahrscheinlichkeit einer überwachten Verbindung mathematisch zu minimieren werden die Entry-Knoten nicht dynamisch gewählt sondern bleiben über einen längeren Zeitraum gleich. Tails wechselt den Entry-Knoten bei einem Neustart.[22]

Das Tool Onion-Circuits zeigt an welchen Tor-Circuit (Weg) eine Verbindung zu einem Server(Webseite oder anderes) nutzt. In Abbildung 2. seht ihr welche 3 Knoten die Verbindung zu tails.boum.org nutzt.

An den 2 Buchstaben in Klammern hinter der IP-Adresse seht ihr auch, dass der Exit-Node in Deutschland liegt.

relayon0328
Fingerprint: 470BC5C6A8BD1D9FDBB55689FB3030310181E
Published: 2021-01-11 05:55:45
IP: 185.220.101.207 (de)
Bandwidth: 38.48 Mb/s

Der Exit-Node ist der Knoten der dem Server, in diesem Fall tails.boum.org, bekannt ist. Manchmal kann es sinnvoll sein, dass dieser nicht in einem bestimmten Land liegt. Zum Beispiel um den leichteren Zugriff von Ermittlungsbehörden entzogen zu sein. Hierzu erklären wir euch wie ihr in Tails festlegen könnt welche Länder in den Exit-Nodes ausgeschloßen werden sollen.

Vorraussetzung: Ihr müsst ein Administrator Passwort gesetzt haben.

1. Öffnet ein Root-Terminal. Ihr müsst hier euer Administrator Kennwort eingeben.
2. Tippt dort `gedit` und drückt Enter. Damit öffnet ihr einen Texteditor als Administrator.
3. Geht nun auf Open ▶ Other Documents
4. Öffnet Filesystem ▶ etc ▶ tor ▶ torrc
5. Geht ans Ende der Datei und gebt dort folgendes ein:

   ```
   StrictNodes 1
   ExcludeExitNodes {de}
   ```

   Damit verhindert ihr, dass deutsche Exit Nodes genutzt werden. Andere Ländercodes findet ihr unter `https://b3rn3d.herokuapp.com/blog/2014/03/05/tor-country-codes/`.

   Solltet ihr mehrere Länder ausschließen wollen, muss das folgendermaßen aussehen:

   ```
   StrictNodes 1
   ExcludeExitNodes {de},{fr},{us}
   ```

   Wenn ihr generell Deutsche Knoten ausschliessen wollt, dann nutzt `ExcludeNodes` statt `ExcludeExitNodes` Dies gilt auch für den Entry-Node.
6. Nun Speichern und den Texteditor wieder schliessen.
7. Im Root-Terminal gebt ihr nun folgendes ein um Tor neu zustarten

   ```
   service tor restart
   ```

22 Vergleiche dazu: `http://www.onion-router.net/Publications/WDIAU-2000.ps.gz`, `http://freehaven.net/anonbib/cache/ccs07-doa.pdf`, `https://www.torproject.org/docs/faq`, `https://blog.torproject.org/blog/research-problem-better-guard-rotation-parameters`, `https://web.archive.org/web/20120204054921/`

23 `https://2019.www.torproject.org/docs/faq.html#ChooseEntryExit`

> *Das Tor-Projekt empfielt diese Einstellungen nur zum Testen zu verwenden und warnt das ein Überschreiben der Tor-Knoten die Anonymität beeinträchtigen kann.*

Falls ihr die Tor-Knoten Wahl trotzdem anpassen wollt solltet ihr euch auf die Ausgangsknoten beschränken.[23]

Website Fingerprinting erschweren

Wenn ihr eine Webseite über euren Browser anfordert, wird diese in kleinen Paketen, die sich durch eine bestimmte Größe und zeitliche Abfolge auszeichnen (und weiteren Charakteristiken), an euch übertragen. Auch bei der Nutzung von Tor kann die Abfolge der übertragenen Pakete analysiert und bestimmten Mustern zugeordnet werden. Die Muster können hier mit denen von überwachten Seiten aus dem Netz abgeglichen werden. Um diese Analyse-Methode zu erschweren und eure Spuren zu verschleiern, hilft folgendes: Öffnet vor dem Aufruf der gewünschten Webseite diverse andere Seiten in weiteren *Tabs* eures Browserfenster. Dadurch entsteht eine Menge von weiterem Traffic, der die Analyse eures Musters erschwert[24].

Tor Bridge Modus

Wenn *Tor* in Verbindung mit *Tails* in seiner Standardkonfiguration verwendet wird, kann jeder, der die Datenströme einer Internetverbindung überwachen kann (beispielsweise ein Internetanbieter und möglicherweise auch die Regierung sowie Strafverfolgungsbehörden) feststellen, dass jemand *Tor* benutzt.

Dies kann ein Problem sein, wenn man sich in einem Land oder einer Stadt befindet, in dem die Nutzung von *Tor* durch Zensur blockiert und deshalb nicht benutzbar ist, oder wenn die Benutzung von *Tor* als gefährlich eingestuft und damit als verdächtig erachtet wird.

Tor Entry Nodes werden in einem öffentlichen Verzeichnis gelistet, dadurch können sie aber auch relativ einfach von Regierungen oder Internetprovidern blockiert werden. *Tor* Bridges, auch Tor Bridge Relais genannt, sind alternative, nicht öffentlich aufgelistete Eingangspunkte in das Tor-Netzwerk.

Eine Nutzer*in kann einen Rechner auch als Tor-Brücke zur Verfügung stellen. Dann tritt sie als Vermittler*in zwischen dem durch Zensur blockierten Nutzer und dem Tor-Netzwerk auf. Die IP-Adresse kann die Betreiber*in einer Tor-Bridge selbst mitteilen. Es gibt aber auch anonyme Sammelstellen, die sogenannten Pools. Eine davon ist eine Webseite, die anderen beiden setzen auf eine Vermittlung per E-Mail oder Chats.

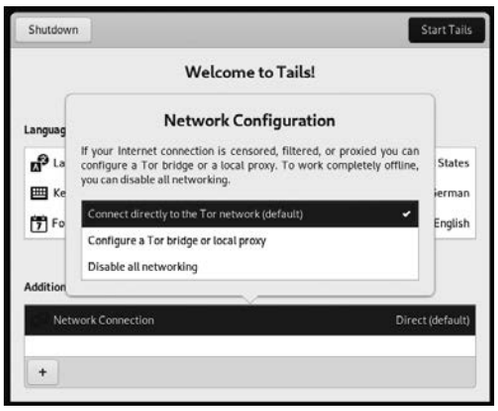
Die Nutzung einer Bridge macht es schwieriger (jedoch nicht unmöglich) für Internetprovider festzustellen, dass jemand Tor nutzt. Eine weitere Möglichkeit um die Nutzung von Tor zu verschleiern ist das benutzen von „Austauschbaren Übertragunsarten“. Mehr Informationen dazu findet ihr im TorBrowser Manual.[25]

Um *Tor* über Bridges zu benutzen, muss man im Vorfeld eine Adresse von zumindest einer Tor Bridge kennen. Das Tor-Projekt verteilt diese auf verschiedenste Art und Weise, beispielsweise auf ihrer Website als auch über E-Mail.[26]

Bridge-Benutzer sind wie normale Tor-Benutzer, mit dem Unterschied, dass Bridge-Relays sowohl als Entry-Guards (ihr erster Hop) als auch als Directory-Guards (die Quelle aller ihrer Verzeichnisinformationen) benutzen

Um euch mit Tails über eine Tor-Bridge zu verbinden müsst ihr dieses direkt im Anmeldefenster aktivieren. Besorgt euch vorher unter `https://bridges.torproject.org/options` eine Bridge Adresse

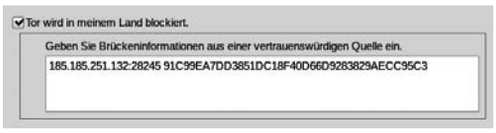
1. Im Anmeldefenster klickt `+` und dann unter „Additional Setting“ den Punkt „Network Connection“
2. Wählt hier „Configure a Tor Bridge or local Proxy“



3. Nach dem Start führt euch ein Assistent durch die Schritte um eine Bridge einzurichten.
4. Im Anfangsfenster müsst ihr `Konfigurieren` wählen.

5. Für den Bridge Mode, macht dann einen Haken bei „Tor wird in meinem Land blockiert“. Dann öffnet sich ein Feld, in dem ihr die Bridge Adresse eintragen könnt.

24 `http://arxiv.org/pdf/1512.00524v1.pdf`
25 `https://tb-manual.torproject.org/de/circumvention/`
26 `https://bridges.torproject.org/`



6. Klickt dann auf Verbinden und Tails verbindet sich mit dem Tor-Netzwerk.

Onion Services

Tor bietet in seinem Netzwerk auch die sogenannten Onion Services. Hierbei wird im Tor-Netzwerk eine Verbindung aufgebaut, bei der sowohl Sender*in als auch Empfänger*in anonym bleiben, etwa, wenn eine Aktivist*in einen Blog betreiben will, zu dem die Zensurbehörden ihres Landes keinen Zugriff haben sollen. Dafür muss etwa für einen Webserver mit vom Tor-Projekt bereitgestellter Software ein Schlüssel erstellt werden. Diese Schlüssel werden in einem Verzeichnisserver abgelegt. Dort werden auch zufällig gewählte Eintrittspunkte eingetragen, über die der Dienst später erreichbar sein soll. Erreichbar ist der versteckte Dienst dann zunächst über den Hash-Wert des öffentlichen Schlüssels, eine alphanumerische Zeichenkette, gefolgt von dem Suffix onion.

Ruft eine Nutzer*in eine Onion-Adresse in einem Tor-Browser auf, wird sie zunächst mit einem Tor-Server verbunden, der später als Rendezvous-Punkt dienen wird. Anhand der Informationen auf dem Verzeichnisserver, die mit dem Hash-Wert verknüpft sind, wird sie dann auf einen der Eintrittspunkte weitergeleitet, von dem eine Mitteilung an den Webserver verschickt wird. Antwortet dieser, werden die beiden Teilnehmer*innen am Rendezvous-Punkt verbunden, ohne dass sie sich kennen.

Onion-Services sind also Dienste/Anwendungen, die ein Server bereitstellt, auf die nur über Tor zugegriffen werden kann. Das Ausführen eines Onion Services gibt den Nutzer*innen die Sicherheit von HTTPS mit den zusätzlichen Datenschutzvorteilen des Tor-Browsers. Oft ist der Onion-Dienst eine weitere sicherere Kontaktmöglichkeit.

Die Adresse eines Onion Services ist eine aus ehemals 16 bzw. in der neuen Generation 56 zufälligen Buchstaben bestehende Zeichenkette, gefolgt von .onion. Beispielsweise lautet die Adresse des Onion Service von `riseup.net` `vww6ybal4bd7szmgncyruucpgfkqahzddi37ktceo3ah7ngmcopnpyyd.onion`. Das sieht seltsam und willkürlich aus, weil es der öffentliche Schlüssel der Identität des Onion Services ist[27]. Onion Services mit kurzen Adressen (16 Zeichen) sind kryptographisch unsicherer sowohl bezüglich der Ende-zu-Ende-Authentifizierung als auch der Ende-zu-Ende-Verschlüsselung. Des Weiteren gab es bösartige Tor-Knoten im Tor-Netzwerk, die Adressen von Onion-Diensten gesammelt haben (Stichwort: Onion Service Harvesting).

Warum Onion Services?

Onion Services bieten ihren Nutzer*innen verschiedene Datenschutz- und Sicherheitsvorteile.

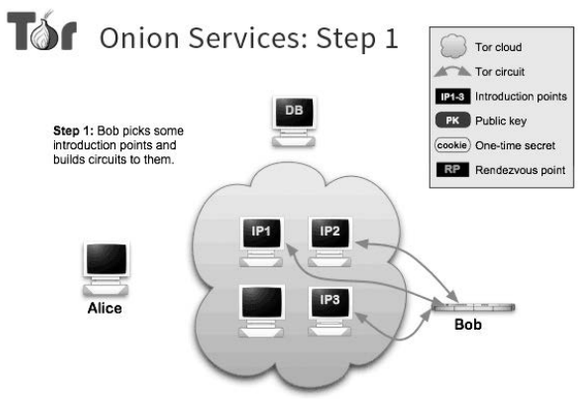
- Standort verstecken[28]: Die IP-Adresse eines Onion Services ist geschützt. Onion Services sind ein Overlay-Netzwerk über TCP/IP, so dass IP-Adressen in gewissem Sinne nicht einmal für Onion Services von Bedeutung sind: Sie werden nicht im Protokoll verwendet.
- Ende-zu-Ende-Authentifizierung: Wenn eine Nutzer*in einen bestimmte Onion Service benutzt, kann sie sicher sein, dass der Inhalt, den sie sieht, nur von diesem bestimmten Onion Service stammen kann. Eine Nachahmung ist nicht möglich, was im Allgemeinen nicht der Fall ist.
- Ende-zu-Ende-Verschlüsselung: Der Onion Services-Verkehr wird vom Client zum Onion-Host verschlüsselt.
- NAT-Punching: Falls das Netzwerk durch eine Firewall gefiltert wird und die Nutzer*in nicht die Berechtigung hat, die Firewall zu konfigurieren (was so ziemlich überall der Fall ist), dann ist es trotzdem möglich, einen Onion Service zu starten. Onion Services brauchen keine offenen eingehenden Ports - sie bauen nur ausgehende Verbindungen auf.

Das Onion Service-Protokoll

Das Protokoll des Onion Services verwendet das Tor-Netzwerk, so dass der Client (Alice) sich dem Dienst (Bob) vorstellen kann und dann einen Treffpunkt mit dem Dienst über das Tor-Netzwerk einrichten kann. Sowohl Alice als auch Bob verwenden in der Regel drei Tor-Knoten (also insgesamt 6 Relais) für ihre Verbindung zum Treffpunkt. Im Folgenden feindet ihr eine detaillierte Aufschlüsselung, wie dies geschieht[29].

1. Als ersten Schritt im Protokoll kontaktiert Bob (der Onion Service) eine Reihe von Tor-Relais und bittet sie, als seine Einführungspunkte zu fungieren, indem er langfristige Verbindungen zu ihnen aufbaut. Diese Verbindungen sind anonymisierte Verbindungen, so dass Bob seinen Einführungspunkten seine Standorte nicht verrät.

   Als Teil dieses Schrittes gibt Bob seinem Einführungspunkt einen speziellen „Authentifizierungsschlüssel“, so dass der Einführungspunkt diesen Schlüssel benutzen kann, um Clients, die später zur Einführung kommen, Bob zuzuordnen.



2. Jetzt, wo die Einführungspunkte eingerichtet sind, müssen wir einen Weg schaffen, damit die Clients sie finden können.

   Aus diesem Grund stellt Bob einen Onion Services-Deskriptor zusammen, der eine Liste seiner Einführungspunkte (und ihrer „Authentifizierungsschlüssel“) enthält, und signiert diesen Deskriptor mit seinem privaten Identitätsschlüssel. Der hier verwendete private Identitätsschlüssel ist der private Teil des öffentlichen Schlüssels, der in der Adresse des Onion Services verschlüsselt ist.

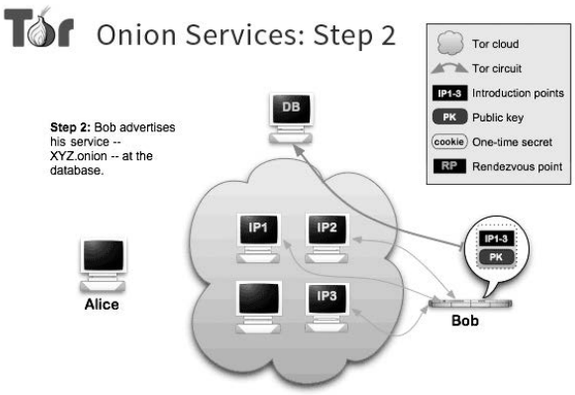
   Nun lädt Bob diesen signierten Deskriptor in eine verteilte Hash-Tabelle hoch, die Teil des Tor-Netzwerks ist,

27 Es gibt auch Dienste, bei denen es nicht ganz so willkürlich aussieht, wie beispielsweise bei `qubes-os.org`, wo die dazugehörige Onion-Adresse der Website `qubesosfasa4zl44o4tws22di6kepyzfeqv3tg4e3ztknltfxqrymdad.onion` lautet. Diese sind nicht mehr oder weniger sicher. Von den Betreiber*innen wurden lediglich viele Schlüssel erzeugt, bis endlich ein „schöner“ dabei war.

28 Aus diesem Grund wurden Onion Services initial Hidden Services genannt.

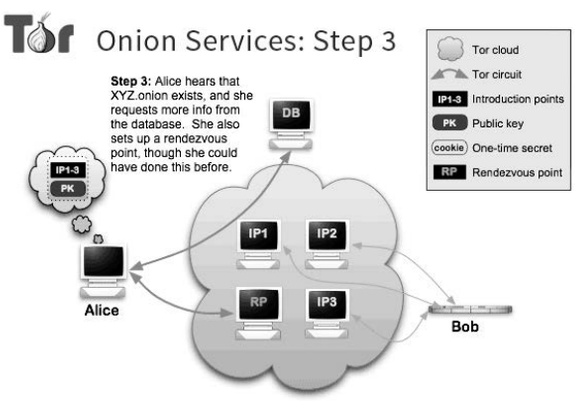
29 `https://community.torproject.org/onion-services/overview/`

so dass auch Clients ihn erhalten können. Bob benutzt eine anonymisierte Tor-Verbindung, um diesen Upload durchzuführen, so dass er seinen Standort nicht preisgibt.

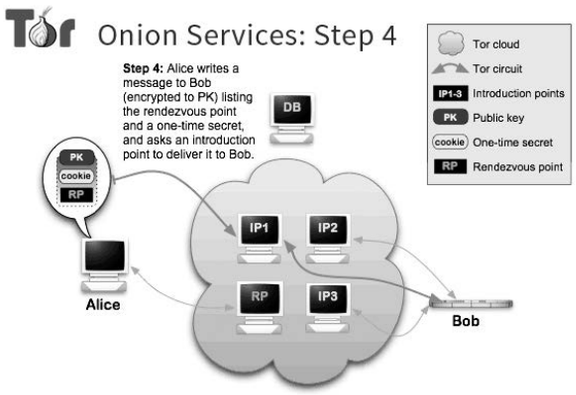


3. Kommmen wir nun zu dem Punkt, an dem ein tatsächlicher Client den Dienst besuchen möchte: In diesem Fall hat Alice (Client) die Onionadresse von Bob und sie möchte sie besuchen, also verbindet sie sich mit ihrem Tor-Browser damit. Als nächstes muss Alice die verteilte Hashtabelle aus dem obigen Schritt aufrufen und nach dem signierten Deskriptor von Bob fragen.

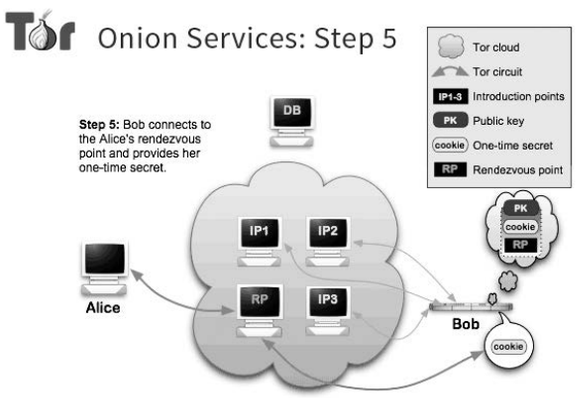
   Wenn Alice den signierten Deskriptor erhält, verifiziert sie die Signatur des Deskriptors mit Hilfe des öffentlichen Schlüssels, der in der Onionadresse verschlüsselt ist. Dies bietet die Sicherheitseigenschaft der End-to-End-Authentifizierung, da wir nun sicher sind, dass dieser Deskriptor nur von Bob und niemand anderem erstellt werden konnte. Und innerhalb des Deskriptors gibt es die Einführungspunkte, die es Alice ermöglichen, sich Bob vorzustellen.



4. Nun, bevor die Einführung stattfindet, wählt Alice ein Tor-Relais aus und stellt eine Tor-Verbindung zu diesem her. Alice bittet das Relais, ihr Rendezvouspunkt zu werden und gibt ihm ein „einmaliges Geheimnis“, das als Teil des Rendezvousverfahrens verwendet wird.



5. Nun geht Alice weiter, stellt sich an einem von Bobs Einführungspunkten und stellt sich Bob vor. Durch diese Einführung lernt Bob Alices Wahl des Treffpunkts und das „einmalige Geheimnis“ kennen.

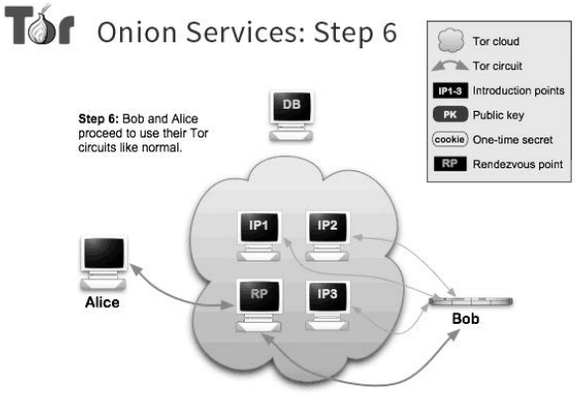


6. In diesem letzten Schritt ist dem Onion Service nun der Treffpunkt von Alice bekannt. Der Onion Service verbindet sich mit dem Rendezvouspunkt (über eine anonymisierte Verbindung) und sendet ihm das „einmalige Geheimnis“.

   Sobald der Rendezvouspunkt das „einmalige Geheimnis“ von Bob erhält, teilt er Alice mit, dass die Verbindung erfolgreich hergestellt wurde, und nun können Alice und Bob über diese Verbindung miteinander kommunizieren. Der Rendezvouspunkt leitet einfach (Ende-zu-Ende-verschlüsselte) Nachrichten vom Client zum Dienst und umgekehrt weiter.

   Im Allgemeinen besteht die vollständige Verbindung zwischen Client und Onion Service aus 6 Relais: 3 davon wurden vom Client ausgewählt, wobei das dritte der Treffpunkt

ist und die anderen 3 vom Onion Service. Dadurch wird dieser Verbindung ein versteckter Standort zugewiesen:



Es gibt noch einige Modifikationen, die wir kurz erwähnen, aber nicht in allen Details ausführen wollen.

1. Wenn es nicht wichtig ist, dass der Standort des Servers (Bob) unbekannt bleibt: Dann kann der Onion Service auch so eingestellt werden, dass seine Verbindung zum Tor-Netzwerk nicht anonymisiert wird. Dies führt zu erheblicher Performanz. Die Sicherheitseigenschaften 2-4 bleiben bestehen und eure Verbindung bleibt anonym.
2. Durch Kopieren des privaten Schlüssels des Server auf mehrere Rechner kann ein Dienst auf vielen Rechnern redundant laufen. Alle Server führen die in Punkt 1 und 2 beschriebenen Punkte unabhängig voneinander durch. Ein Client, der sich zu dem Dienst verbinden möchte, verbindet sich zufällig (und nicht kontrollierbar) zu irgendeinem der Server.

Weitere Informationen und best practices sind auf riseup.net[30] zu bekommen.

.onion-Gateways

Es gibt Websites wie Tor2web, die als Proxies in das Tor-Netzwerk dienen. Sie ermöglichen den Zugriff auf Onion Services von Nicht-Tor-Browsern und für Suchmaschinen, die nicht Tor-fähig sind. Durch die Verwendung eines Gateways geben Nutzer*innen ihre eigene Anonymität auf und vertrauen darauf, dass das Gateway die richtigen Inhalte liefert. Sowohl das Gateway als auch der Onion Service können Merkmale des Browsers auslesen (fingerprinting) und auf die IP-Adressdaten der Nutzer*in zugreifen.

Wir raten von der Verwendung dieser Proxies ab und empfehlen, bei den .onion-Adressen genau hinzuschauen.

Tails als System für sensible Arbeiten

Das *Tails*-Live-System ist eine Zusammenstellung von vielen Programmen auf der Basis eines *Debian-Linux*. Alle Programme zu erläutern, erfordert viel zu viel Platz – selbst, wenn wir nur deren grundlegende Handhabung beschreiben würden. In den folgenden Kapiteln gehen wir auf unterschiedliche Aspekte des Live-Systems ein. Wir geben explizite Anleitungen für bestimmte, häufig auftretende Anwendungsfälle.

Vorinstallierte Programme

Daher hier nur die Verweise für einige vorinstallierte Programme:

Surfen: Tor-Browser
`https://tails.boum.org/doc/anonymous\_internet/Tor_Browser/index.en.html`

Mailen: Thunderbird
`https://de.wikipedia.org/wiki/Mozilla_Thunderbird`

Chatten: Pidgin + OTR
`https://tails.boum.org/doc/anonymous_internet/pidgin/index.en.html`

Office: LibreOffice
`http://wiki.ubuntuusers.de/LibreOffice`

Gemeinsames Schreiben: Gobby
`https://gobby.github.io/`

Layout+Satz: Scribus
`http://www.scribus.net/`

Videos abspielen: Totem
`http://wiki.ubuntuusers.de/Totem`

Grafikbearbeitung: Gimp
`http://wiki.ubuntuusers.de/GIMP`

Tonbearbeitung: Audacity
`http://wiki.ubuntuusers.de/Audacity`

Videobearbeitung: Pitivi
`http://wiki.ubuntuusers.de/PiTiVi`

Newsfeeds lesen: Liferea
`http://wiki.ubuntuusers.de/Liferea`

Bitcoins: Electrum
`https://tails.boum.org/doc/anonymous_internet/electrum/index.en.html`

Anonymer Datenaustausch: Onion–Share
`https://onionshare.org/`

Metadaten entfernen: MAT
`https://mat.boum.org/`

Scannen: Simple scan
`http://wiki.ubuntuusers.de/Simple_Scan`

CD/DVD brennen: Brasero
`http://wiki.ubuntuusers.de/Brasero`

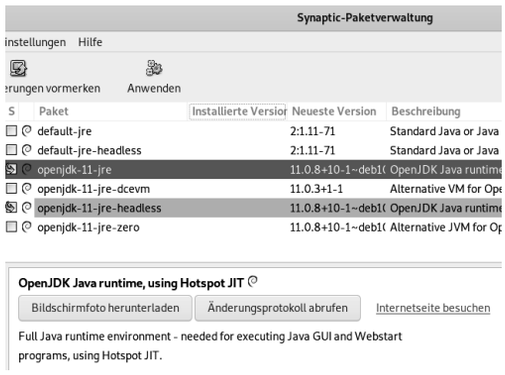
Passwortverwaltung: KeepassX
`http://wiki.ubuntuusers.de/KeePassX`

Software nachinstallieren

Tails bietet die Möglichkeit, fehlende Software nachzuinstallieren. Dieses Verfahren werden wir an einigen Stellen im Heft nochmal aufgreifen und anwenden. Wir wollen aber hier schon einmal gesondert darauf eingehen. Nehmen wir als Beispiel die Software *SearchMonkey*. Hierbei handelt es sich um eine Software zum komfortablen Durchsuchen von mehreren PDF-Dateien.

- Über das Menü Anwendungen ▶ Systemwerkzeuge ▶ Synaptic-Paketverwaltung findet ihr eine grafische Anwendung, mit der ihr Software installieren könnt (hierfür braucht ihr euer Administrationspasswort):

30 `https://riseup.net/en/security/network-security/tor/onionservices-best-practices`



- Nun sucht ihr über das **Suche-Icon** nach der Anwendung euer Wahl.
- Über die **Checkbox** merkt ihr das Programm zum Installieren vor. Dadurch werden automatisch andere Programmabhängigkeiten ausgewählt und mit dem Button **Vormerken** markiert.
- Wenn ihr mehrere Anwendungen installieren wollt, könnt ihr diesen Vorgang wiederholen.
- Die vorgemerkten Programme werden durch ein Klicken auf das **Anwenden-Icon** installiert.
- Solltet ihr eine Persistenz eingerichtet haben, so erscheint anschliessend die Frage, ob ihr die Anwendung dauerhaft installieren wollt. Wenn ja, wählt **Install Every Time**, wenn nein, wählt **Install only once**.

Online-Arbeiten

Surfen über Tor

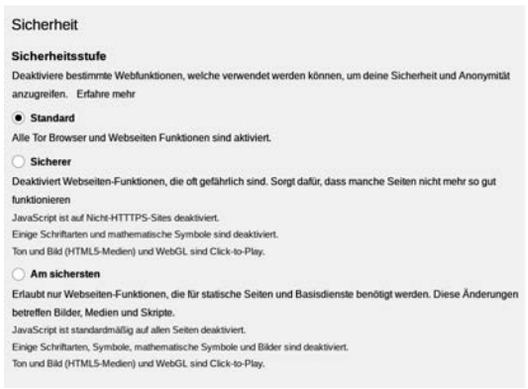
Wenn der Netzwerkmanager von *Tails* eine Netzwerkverbindung hergestellt hat, könnt ihr den *Tor*-Browser starten unter Anwendungen ▶ Internet ▶ Tor-Browser.

Skripte verbieten – NoScript

Es gibt *aktive* Inhalte auf Webseiten, die eure Anonymität gefährden können. Oft nutzen Webseiten Javascript, Java-Applets, Cookies, eingebettete Flash- oder Quicktime-Filme, PDF-Dokumente oder nachzuladende Schriften. Derartige aktive Webseiteninhalte können über einen sogenannten „Fingerprint“ viele Einstellungen und Charakteristika eures Rechners übertragen (Prozessor, Bildschirmauflösung, installierte Schriften, installierte Plugins, etc.), sodass ihr im ungünstigen Fall doch identifizierbar seid[31]. Die *Tor*-Installation von Tails kümmert sich um die Deaktivierung vieler dieser Inhalte. Wir empfehlen jedoch, gleich zu Beginn eurer Netzaktivitäten eine noch restriktivere Einstellung in eurem *Tor*-Browser vorzunehmen:

Im *Tor*-Browser könnt ihr über einen Klick auf das kleine Schild

in der Steuerleiste des Browsers das Sicherheitslevel anpassen. Hier stehen Euch drei Voreinstellungen zur Verfügung. Auf dem niedrigsten Level funktionieren auch Seiten mit aktiven Inhalten.



Der voreingestellte Standard im *Tor*-Browser von Tails ist der unsicherste und erlaubt alle *Skripte* und *Plugins* der Webseiten, die man besucht. Deshalb ist unsere Empfehlung, diese Sicherheitsstufe unbedingt zu erhöhen. Die zweite Stufe, „sicherer“, bedeutet, dass auf allen Seiten, die nicht per HTTPS besucht wurden, Javascript ausgeschaltet ist, zusätzlich sind einige mathematische Symbole und Schriftarten deaktiviert, und Videos und Audiodateien werden erst nach aktivem Anklicken abgespielt. Die dritte und sicherste Stufe lässt zusätzlich zu den Einschränkungen der zweiten Sicherheitsstufe nur statische Webseiten und Basisdienste zu, und Javascript ist auf allen Seiten deaktiviert.

> *In den Sicherheitseinstellungen solltet ihr das Sicherheitslevel auf die höchste Stufe stellen!*

Einige Seiten benöten allerdings Scripte, um zu funktionieren. Ihr könnt entweder das Sicherheitslevel anpassen oder jeweilige Scripte sukzessiv erlauben. Empfehlenswert ist es, Skripte bei den besuchten Webseiten (und ihren Unterseiten) jeweils **erst dann zuzulassen**, wenn es für eure Aktivität notwendig ist - wenn also etwas auf der jeweiligen Webseite „nicht wie gewünscht funktioniert“. Beachtet, dass ihr dadurch eure Anonymität verlieren könnt! Um Scripte für die jeweilige Webseite zu erlauben, öffnet ihr mit der rechten Maustaste ein Menü und wählt dort die Option *NoScript* aus. Es öffnet sich ein Fenster, in dem man weitere Entstellungen vornehmen kann.

Download aus dem Netz

Es ist kein Fehler, sondern Absicht, dass ihr über den *Tor*-Browser Dateien nur in das Verzeichnis Tor-Browserßpeichern dürft (im Verzeichnis *Persönlicher Ordner*). Das bewahrt euch vor unbeabsichtigtem Fehlspeichern. Falls ihr Daten auf den Desktop oder einen Datenträger speichern wollt, müsst ihr in einem zweiten Schritt die Daten an den Zielort kopieren. Dazu eignet sich der Dateimanager unter Anwendungen ▶ Zubehör ▶ Dateien.

In Ausnahmefällen ohne Tor ins Netz?

Einige öffentliche WLAN-Zugänge in Cafés, Universitäten, Büchereien, Hotels, Flughäfen, etc., leiten Webseitenanfragen auf spezielle Portale[32] um, die ein *Login* erfordern. Diese Portale sind nicht über *Tor* erreichbar. Ohne Login bleibt das Netz gesperrt und *Tor* läßt sich nicht benutzen. *Tails* bringt einen Browser mit, der eine direkte Verbindung ohne Tor erlaubt - der ist genau und ausschliesslich für diese Portale gedacht, damit ihr dort euren Netzzugang freischalten könnt.

31 https://panopticlick.eff.org/
32 engl: captive portal

Wir raten dringend von der Nutzung des Browsers ohne Tor ab!

Nur, wenn ihr auf die Verschleierung eurer Identität und auf die Verschleierung eures Standortes verzichten wollt und könnt, gibt es in Tails die Möglichkeit auch ohne *Tor* ins Netz zu gehen. Bedenkt, dass euch alles, was ihr damit „ansurft", zugeordnet werden kann. Ihr könnt den unsicheren Browser starten über: Anwendungen ► Internet ► Unsicherer Browser.

Auf keinen Fall solltet ihr diesen „nackten" Browser parallel zum anonymen Tor-Browser nutzen. Das erhöht die Angreifbarkeit und die Verwechslungsgefahr mit eventuell katastrophalen Konsequenzen!

Mailen über Tor

Im Folgenden stellen wir euch eine Methode vor, wie ihr in *Tails* mittels dem Tor Browser und einem Webmail-Interface E-Mails versenden und empfangen könnt. Wurde das Mail-Konto anonym angelegt, lässt sich darüber die eigene *Identität* verschleiern. Andernfalls könnt ihr lediglich/immerhin euren *Aufenthaltsort* verbergen.

Webmail

Die einfachste Methode, unter *Tails* E-Mails zu versenden und zu empfangen, ist der Zugriff (über *Tor*) auf ein *Webmail-Konto*.

Für alle, die **verschlüsselten Mail-Text per Webmail** verschicken wollen, stellen wir im Folgenden zwei Methoden der PGP-Verschlüsselung vor.

*Warnung: Es ist unsicher, vertraulichen Text direkt in einen Webbrowser einzugeben, da Angreifer*innen mit Javascript aus dem Browser heraus darauf zugreifen können.*
Ihr solltet euren Text daher mit dem OpenPGP Applet von Tails verschlüsseln und den verschlüsselten Text in das Browserfenster einfügen. Ihr müsst zusätzlich alle Skripte über NoScript verbieten!

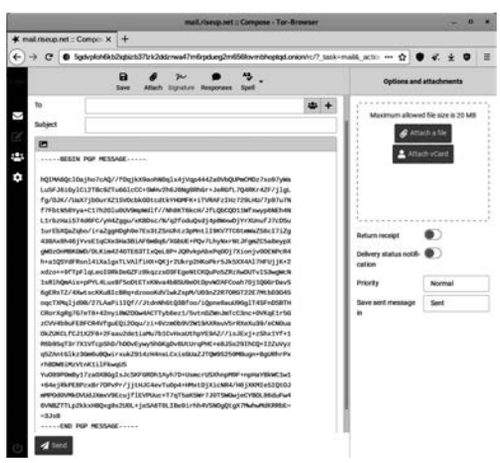
A) PGP-Verschlüsselung mit öffentlichem Schlüssel

Bei dieser Methode nutzt ihr die sehr sichere Standard-PGP-Verschlüsselung: Verschlüsseln mit den öffentlichen Schlüsseln der Empfänger*innen. Falls ihr noch nie mit PGP gearbeitet habt, könnt ihr Methode **B**) verwenden.

1. Schreibt euren Text in einen Texteditor, **nicht direkt in das Browserfenster eures Webmail-Anbieters!** Zum Beispiel könnt ihr dazu *gedit* öffnen über Anwendungen ► Zubehör ► Texteditor.
2. Markiert dort den zu verschlüsselnden oder zu signierenden Text mit der Maus. Um ihn in die Zwischenablage zu kopieren, klickt ihr mit der rechten Maustaste auf den markierten Text und wählt den Menüpunkt *Kopieren* aus. Das OpenPGP Applet zeigt durch Textzeilen an, dass die Zwischenablage *unverschlüsselten Text* enthält.
3. Klickt auf das OpenPGP Applet (in der Tails-Menüleiste oben rechts) und wählt die Option **Zwischenablage mit öffentlichem Schlüssel signieren/verschlüsseln** aus. Sollte die Fehlermeldung „Die Zwischenablage beinhaltet keine gültigen Eingabedaten" angezeigt werden, versucht erneut, den Text gemäß Schritt 2 zu kopieren.

4. Falls ihr den Text verschlüsseln wollt, wählt einen oder mehrere öffentliche Schlüssel für die Empfänger*innen des verschlüsselten Textes im „Schlüssel wählen"-Dialog aus (siehe dazu Abschnitt „PGP-Schlüssel importieren").
5. Falls ihr den Text signieren wollt, wählt den geheimen Schlüssel aus der „Nachricht signieren als"-Dropdown-Liste aus. Bedenkt, dass der Besitz dieses Schlüssels die Urheber*innenschaft der so signierten Mail schwer abstreitbar macht.
6. Klickt auf OK. Falls die Frage „Vertrauen Sie diesen Schlüsseln?" angezeigt wird, beantwortet dies entsprechend.
7. Falls ihr einen oder mehrere öffentliche Schlüssel zum Verschlüsseln des Textes ausgewählt habt, zeigt das OpenPGP Applet durch ein *Vorhängeschloss* an, dass die Zwischenablage nun verschlüsselten Text enthält.
   Habt ihr einen geheimen Schlüssel zum Signieren des Texts ausgewählt, so zeigt das Applet nun durch ein *Siegel* an, dass die Zwischenablage signierten Text enthält.

8. Um den verschlüsselten oder signierten Text in das Webmail-Fenster eures Mail-Anbieters (oder in eine andere Anwendung) einzufügen, klickt mit der *rechten Maustaste* auf das Eingabefeld, in das ihr den Text einfügen möchtet, und wählt die Option *Einfügen* aus dem Menü aus.



B) PGP-Verschlüsselung mit Passphrase

Bei dieser Methode müsst ihr eine geheime Passphrase mit den Personen teilen, die die Nachricht entschlüsseln sollen. Ihr müsst die Passphrase also zuvor über einen **sicheren** Kanal (im günstigsten Fall face-to-face) kommunizieren!

Die beiden ersten Schritte sind identisch mit **1**) und **2**) aus Methode **A**). Dann geht es weiter mit:

1. Klickt auf das OpenPGP Applet von Tails und wählt die Option „Zwischenablage mit Passwort verschlüsseln" aus. Sollte die Fehlermeldung „Die Zwischenablage beinhaltet keine gültigen Eingabedaten" angezeigt werden, versucht erneut, den Text gemäß Schritt 2 zu kopieren.
2. Gebt eine Passphrase in den Passphrase-Dialog ein. Wiederholt die gleiche Passphrase im zweiten Dialog.

3. Das OpenPGP Applet zeigt durch ein Vorhängeschloss an, dass die Zwischenablage verschlüsselten Text enthält.

4. Dieser Schritt ist identisch mit Schritt **8**) aus Methode **A**).

Entschlüsseln oder Signatur überprüfen

Die Entschlüsselung eines verschlüsselten Textes / einer verschlüsselten Mail funktioniert für *beide Verschlüsselungs-Methoden* folgendermaßen:

1. Markiert mit der Maus den verschlüsselten bzw. signierten Text (z.B. in eurem Webbrowser), den ihr entschlüsseln bzw. überprüfen möchtet. Schließt die Zeilen `---BEGIN PGP MESSAGE---` und `---END PGP MESSAGE---` mit in die Markierung ein.
2. Ist der ausgewählte Text verschlüsselt, zeigt dies das OpenPGP Applet durch ein *Vorhängeschloss* an. Ist der ausgewählte Text nur signiert, aber nicht verschlüsselt, wird dies durch ein *Siegel* angezeigt.
3. Klickt auf das OpenPGP Applet und wählt „Zwischenablage entschlüsseln/überprüfen“ aus dem Menü aus.
   - Ist der ausgewählte Text nur signiert und die Signatur gültig, erscheint direkt das GnuPG-Ergebnis-Fenster.
   - Ist der Text signiert, aber die Signatur ungültig, wird das GnuPG-Fehler-Fenster mit der Nachricht „FALSCHE Unterschrift von...“ angezeigt. Ihr könnt euch nicht sicher sein, dass der angegebene Absender auch der Tatsächliche ist.
   - Ist der Text mit einer Passphrase verschlüsselt, erscheint die Aufforderung „Geben Sie die Passphrase ein...“, danach auf `OK` klicken.
   - Ist der Text mit einem öffentlichen Schlüssel verschlüsselt worden, können zwei verschiedene Dialoge angezeigt werden:
     – Ist die Passphrase zu einem geheimen Schlüssel noch nicht zwischengespeichert, dann erscheint ein Dialog mit der Nachricht: „Sie benötigen eine Passphrase, um den geheimen Schlüssel zu entsperren“. Gebt die Passphrase für diesen geheimen Schlüssel ein, danach auf `OK` klicken.
     – Falls sich kein zum verschlüsselten Text passender geheimer Schlüssel im Schlüsselbund befindet, wird die GnuPG-Fehlermeldung „Entschlüsselung fehlgeschlagen: Geheimer Schlüssel ist nicht vorhanden“ angezeigt.
   - Ist die Passphrase falsch, so wird ein GnuPG-Fehler-Fenster mit der Meldung „Entschlüsselung fehlgeschlagen: Falscher Schlüssel“ angezeigt.
   - Ist die Passphrase korrekt oder ist die Signatur auf den Text gültig, so wird das *GnuPG-Ergebnis*-Fenster angezeigt.
   - Der entschlüsselte Text erscheint im Textfeld „Ausgabe von GnuPG“. Im Textfeld „Andere Nachrichten von GnuPG“ zeigt die Nachricht „Korrekte Unterschrift von...“ an, dass die Signatur gültig ist.

Remailer

Remailer ermöglichen das Versenden einer Mail z.B. an die Mail-Adresse einer Zeitungsredaktion, ohne (zwingend) eine eigene Mailadresse anzugeben. Nur in Verbindung mit Tails und Tor bieten Remailer eine gute Möglichkeit, anonym Mails zu versenden. Dabei entstehen teilweise beträchtliche Zeitverzögerungen, bis eine Mail die Empfänger*in erreicht.

Leider ist die Benutzung der von uns getesteten Remailer aktuell so umständlich, dass wir auf eine detaillierte Beschreibung verzichten müssen und auf die Website von `https://remailer.paranoici.org/` verweisen. Das in alten Versionen dieser Broschüre beschriebene Webinterface funktioniert derzeit nicht (mehr).

„Anonymes“ Mailen über Tor

Kommerzielle „Freemail“-Anbieter*innen[33] blockieren oft den Zugriff, falls ihr mit Tor darauf zugreifen wollt. Es gibt daher alternative Möglichkeiten, E-Mails möglichst spurenarm zu verschicken (ohne dafür eine gültige E-Mail-Adresse bei der Account-Erstellung hinterlassen zu müssen oder dabei auf die sicherste Stufe im Tor-Browser zu verzichten):

- Durch E-Mail-Anbieter*innen im Tor-Netzwerk.
- Über Onionmail[34].

In den nächsten Absätzen versuchen wir, einen Kompromiss zwischen Benutzer*innenfreundlichkeit und Sicherheit einzugehen, da alternative Möglichkeiten wie Mixmaster[35][36] uns zu kompliziert erscheinen.

> *Die hier vorgestellten Optionen zum Verschicken von E-Mails ohne Account sollten nur tempörar verwendet werden, z.B. beim Versenden einer anonymen Presseerklärung. Bedenkt, dass beim Verschicken von E-Mails über Onion Services deutsche Umlaute evtl. falsch dargestellt werden.*

E-Mail-Anbieter*innen im Tor-Netzwerk

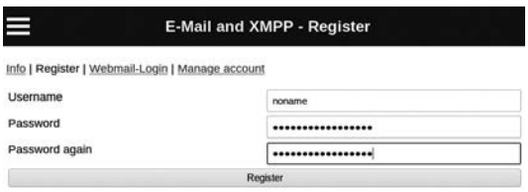
Da die Anbieter*innen dieser Dienste in der Regel nicht bekannt sind, haben wir nur Mail-Services ausgewählt, welche die folgenden Kriterien erfüllen:

- Webmailer, die mit dem Torbrowser unter dem höchsten Sicherheitslevel verwendbar sind (siehe Kapitel „Surfen über Tor“)
- E-Mail-Adressen ohne Onion-Endung (z.B. benutzerkennung@danwin1210.me).
- Anbieter*innen, die auf wenigen Blacklists stehen[37].
- Registrierung mit wenigen Daten (z.B. nur Benutzer*innenname, Passwort, ohne eine gültige E-Mail-Adresse).

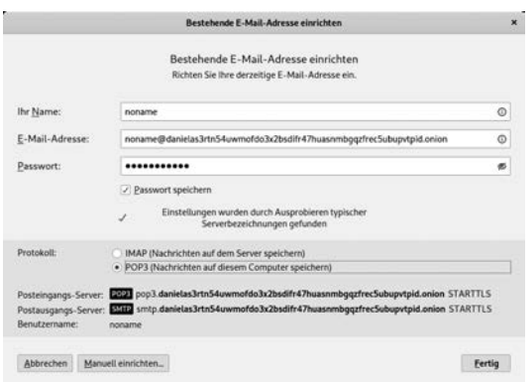
Eine Option für einen kostenlosen Webmail-Account lässt sich über die Webseite `https://danwin1210.me/mail` finden[38]. Zur Erstellung eines Zugangs sollte die Onion-Adresse

33 „Freemail“-Anbieter*innen verdienen ihr Geld mit Überwachung: Sie erstellen ein Profil über eure E-Mail-Inhalte und verkaufen dieses an die Meistbietenden.
34 https://en.onionmail.info/what.html
35 https://www.mixminion.net/
36 http://mixmaster.sourceforge.net/
37 Adressen, die auf diesen Listen stehe,n werden von den gängigen E-Mail-Providern abgewiesen.
38 Der Serverstandort befindet sich in der BRD. Der Dienst scheint authentisch zu sein, was sich u.a. über die Referenzen von diversen Github-Projekten überprüfen lässt: https://github.com/DanWin.

bevorzugt werden, da sie eine stärkere Verschlüsselung anbietet: `http://danielas3rtn54uwmofdo3x2bsdifr47huasnmbgqzfrec5ubupvtpid.onion/mail`



Über den Zugang lässt sich anschließend eine E-Mail-Adresse über ein Webinterface oder Thunderbird nutzen (siehe Kapitel „Mailen über Tor“). Nach einem erfolgreichen Verschicken einer E-Mail erscheint der Name, mit dem ihr den Account erstellt habt, automatisch in der Absende-Adresse, z.B.: noname@danwin1210.me. Falls ihr Thunderbird als Mail-Client benutzen wollt, muss auch hier die Onion-Adresse angegeben und die Server-Zertifikate akzeptiert werden: `noname@danielas3rtn54uwmofdo3x2bsdifr47huasnmbgqzfrec5ubupvtpid.onion`

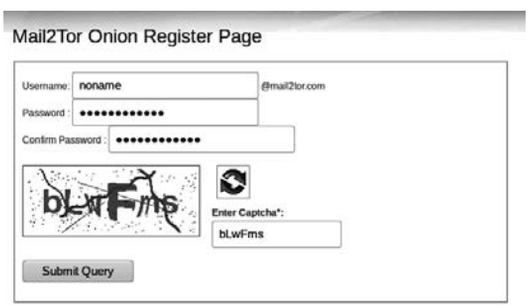


Wenn ihr die Funktionsweise der E-Mail-Verschickung überprüfen wollt, könnt ihr euch eine temporäre E-Mail-Adresse über die Anonbox des Chaos Computer Clubs erstellen[39]: `https://anonbox.net/en`

Ein weiterer Webmail-Provider aus dem Tor-Netzwerk kann unter der Webseite `https://secmail.pro` gefunden werden. Auch hier solltet ihr die Webseite über dessen Onion-Adresse beziehen: `http://secmail63sex4dfw6h2nsrbmfz2z6alwxe4e3adtkpd4pcvkhht4jdad.onion`

Über den Provider der Webseite ist nichts bekannt, außer das er kommerzielle Werbung auf seiner Webmailer-Seite einblendet. Alle E-Mails, die über diesen Dienst verschickt werden, haben die Absende-Adresse: `benutzerkennung@secmail.pro`.

Eine etwas bekannterer Anbieterin ist Mail2Tor. Aktuell ist der Mail-Dienst mit starken DDoS-Angriffen[40] konfrontiert, was sein Funktionalität stark einschränkt. Die über die Onion-Adresse erstellte E-Mail-Adresse `http://mail2tor2zyjdctd.onion/register.php` lässt sich sowohl über ein Webmail-Interface als auch über Thunderbird verwenden. Der Dienst nutzt allerdings noch Onion Services in Version 2, was eine schwächere Verschlüsselung[41] zur Folge hat. **Zudem besitzen die Services nur noch bis zum 15.10.2021 ihre Gültigkeit.** Von daher ist es wichtig, ab diesem Datum nach einer neuen Onion Service-Adresse des Projekts in Version 3 zu suchen.



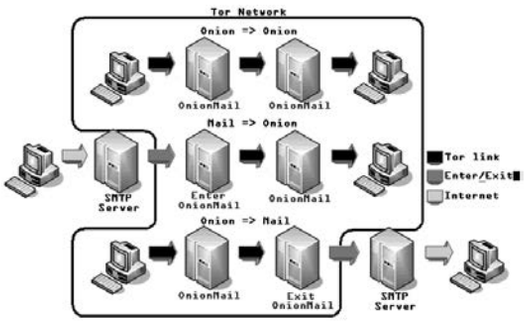
Onionmail

Onionmail ist ein Open-Source-Projekt, das nach den Snowden-Enthüllungen im Jahr 2013 entstanden ist, und sich zum Ziel gesetzt hat, einen Schutz vor den bekannt gewordenen NSA-Angriffen zu bieten[42][43]. Über den Quellcode wird ein verschlüsselter POP3/SMTP-Mail-Server generiert, der speziell auf die Funktionalität von Onion Services ausgerichtet ist[44]. Aktuell wird an einer zweiten Version des Projekts gearbeitet. Es existieren 25 öffentlich zugängliche Server, auf denen mehr als 62000 Benutzer*innen registriert sind[45]. Onionmail bietet die Möglichkeit, E-Mails an Onionmail-Adressen im Tor-Netzwerk sowie an E-Mail-Adressen im Internet zu schicken. Sämtliche Onionmail-Server sind als Onion Services in Version 2[46] konfiguriert und speichern beim Versenden von Nachrichten kei-

39 Die E-Mail-Adresse ist nur für eine kurze Zeit gültig.
40 https://de.wikipedia.org/wiki/Denial_of_Service
41 RSA 1024 Bit mit SHA-1.
42 `http://wqlc3ny6wcbxy2r7.onion/what.html`
43 `https://en.onionmail.info/manifesto_en_html.html`
44 `http://onionmail.info/paper.html`
45 Stand: Anfang Februar 2021.
46 Onion-Adressen in Version 2 verlieren ab 15.10.2021 ihre Gültigkeit.
47 Die Schlüssel liegen nicht auf dem Server selbst, sondern verteilt im Tor-Netzwerk.
48 `http://wqlc3ny6wcbxy2r7.onion/rulez.html`

ne Daten auf ihren Servern. Nur empfangene Nachrichten werden über mehrere asymmetrische Schlüssel verschlüsselt[47] und können nicht mit diesen Schlüsseln alleine geöffnet werden (dafür wird zusätzlich das Passwort der/des Benutzer*in benötigt)[48]. Zudem werden Metadaten aus den E-Mails entfernt und Nachrichten nach wenigen Tagen wieder gelöscht. Falls nur Nachrichten verschickt werden, wird der Account wegen Spam-Verdacht entfernt.

Onionmail bietet kein Webinterface an und muss daher über Thunderbird verwendet werden.



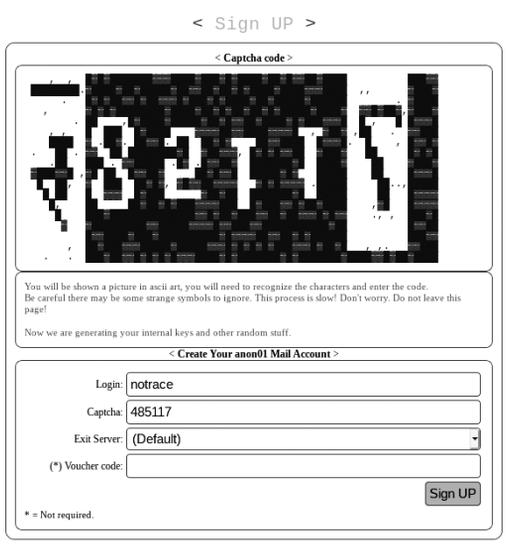
Onionmail-Account erstellen

Um einen Onionmail-Account anlegen zu können, müsst ihr euch für eine der öffentlichen Onionmail-Server entscheiden: `http://onionmail.info/directory.html`

Aus der Liste solltet ihr einen Server mit 99% Verfügbarkeit, einer niedrigen Ping-Zeit und einer Version ab 1.9.2 wählen[49]. Außerdem kann es Sinn machen, einen Server mit vielen Benutzer*innen zu wählen, z.B. anon1 oder anon2: `http://xhfheq5i37waj6qb.onion/register.html`

Das Captcha, das ihr auf der Registrierungsseite neben eurem Login[50] eingeben müsst, ist oft schwer zu lesen (spiegelverkehrte Zahlen etc.). Nach öfterer Falscheingabe habt ihr die Möglichkeit, stattdessen eine einfache Rechenaufgabe zu lösen.

Falls eine Anmeldung bei dem ausgewählten Server nicht funktioniert, wechselt zu einem anderen oder versucht es zu einem späteren Zeitpunkt noch einmal.

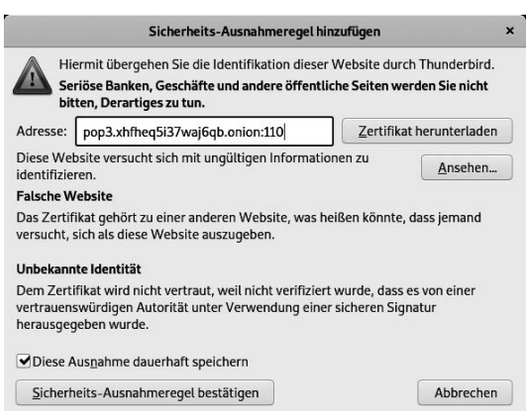


Nach dem erfolgreichen Anlegen eines Accounts erscheint eine Bestätigungsseite mit den Onionmail-Zugangsdaten. Die Passwörter für das Empfangen und Versenden von E-Mails unterscheiden sich. Im unteren Bereich der Bestätigungsseite ist unter „SSL Certificate SHA-1“ die Prüfsumme des SSL-Zertifikats abgedruckt[51], die ihr vor einem Mailen auf ihre Korrektheit überprüfen solltet. In den letzten Zeilen erfahrt ihr, wie eure E-Mail-Adresse lautet[52].

Thunderbird mit Onionmail

Um E-Mails verschicken zu können, öffnet ihr Thunderbird über das Menü Anwendungen ▶ Internet ▶ Thunderbird und gebt dort die Onion-E-Mail-Adresse und das POP3-Passwort ein. In unserem Fall ist das `notrace@xhfheq5i37waj6qb.onion`.

Nach der Prüfung der Formular-Eingaben erscheint eine Sicherheitswarnung aufgrund eines selbstsignierten Zertifikats. Über den **Button „Ansehen“** könnt ihr die SHA-1-Prüfsumme, die im Bereich „Fingerabdrücke“ abgebildet ist, mit der Prüfsumme aus der Bestätigungsseite abgleichen (bei der Prüfsumme auf der Bestätigungsseite fehlen die „:“-Zeichen).

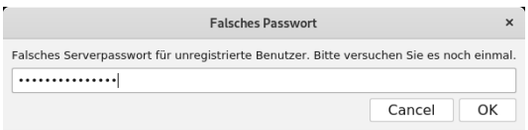


Wenn die Prüfsummen zueinander passen, bestätigt ihr die „Sicherheits-Ausnahmeregel“. Anschließend wird ein Mail-Account unter Thunderbird eingerichtet (siehe „Thunderbird - Mailen mit Persistenz“).

Eine E-Mail könnt ihr erst verschicken, nachdem ihr das Zertifikat mit jenem aus der „Signup“-Bestätigungsseite verglichen und die Ausnahmeregel akzeptiert habt (wie bereits zuvor).

49 Weil ihr sonst eine alte Version des Onionmail-Servers verwendet.
50 Der Login ist zugleich der E-Mail-Name. Z.B. wird aus noname: noname@onionmail.info.
51 Die Prüfsumme und weitere Server-Details findet ihr zusätzlich über die Webseiten der Onionmail-Server in der Kategorie „Info“. Ihr könnt auch eine E-Mail mit dem Betreff „IDENT“ an server@xhfheq5i37waj6qb.onion mailen, um detailliertere Informationen zu erhalten.
52 Was von der Domain des gesetzten Exit-Servers abhängt.
53 Nachdem ein erstes Versenden der E-Mail fehlgeschlagen ist. Das SMTP-Passwort findet ihr auf der Onionmail „Signup“-Bestätigungsseite.

Da sich das Passwort zum Versenden von E-Mails unterscheidet, muss dieses ein zweites Mal eingegeben werden[53]



Achtet beim Verfassen der E-Mail darauf, keine deutschen Umlaute einzugeben, weil diese falsch dargestellt werden. Falls eure E-Mail an eine Internet-E-Mail-Adresse adressiert war, sollte sie als Absender*in folgende Adresse enthalten: `benutzername@onionmail.info`. Wenn ihr die Funktionalität des Verschickens testen wollt, könnt ihr dies über die temporäre Erstellung einer E-Mail-Adresse auf der Webseite `https://www.anonmail.net` tun. Da die Domain onionmail.info aktuell nicht in den zentralen Blacklists eingetragen ist, sollten eure E-Mails ihre Ziel-Adresse erreichen (ohne im Spamordner zu landen).

Onionmail-Kommandos

Es besteht die Möglichkeit, über Kommandos mit dem Onion-Server zu kommunizieren (auch PGP-verschlüsselt). Z.B. könnt ihr über eine E-Mail an euren Onionmail-Server (`server@xhfheq5i37waj6qb.onion`) mit dem Betreff „SETTINGS“ Folgendes in Erfahrung bringen (ihr erhaltet eine E-Mail-Antwort mit den entsprechenden Informationen):

msgxhour: Anzahl der E-Mails, die ihr in einer Stunde verschicken könnt

exitonion: Exit Onion Server.

torvmat: E-Mails erscheinen mit einer normalen Adresse (z.B. `benutzer*innenname@onionmail.info`)

exitdomain: Domain, mit der die E-Mails verschickt werden.

Es gibt noch weitere Möglichkeiten, über Kommandos mit einem Onionmail-Server zu kommunizieren[54]. Die Optionen findet ihr unter dem Rulez-Bereich auf den Webseiten der einzelnen Oniomail-Server-Betreiber*innen.

Chatten über Tor

Pidgin ist der Name des Chatclients, der von Tails mitgeliefert wird. Im Vergleich zu einer Pidgininstallation unter einem „normalen“ Linux ist das Pidgin von Tails speziell auf Verschlüsselung abzielend vorkonfiguriert.

Es wird nur eine limitierte Auswahl an Chatprotokollen angeboten: Varianten von *XMPP* und *IRC*. Für diese beiden Protokolle stehen Verschlüsselungsmethoden bereit, die anderen Protokollen fehlen. Die Voreinstellungen, welche die Tails-Variante von Pidgin mitbringt, deaktivieren das *logging*, also das Mitprotokollieren von Sitzungen. Auch mitinstalliert ist das OTR-Plugin, welches eine Ende-zu-Ende-Verschlüsselung erlaubt[55].

Für den einmaligen Einsatz muss nichts weiter vorbereitet werden. Pidgin enthält in Tails zwei vorkonfigurierte (zufällige) Accounts, die direkt verwendet werden können. Für den regelmäßigen Einsatz (mit eigenem Account) müsstet ihr Pidgin wegen der Vergesslichkeit von Tails jedes Mal neu konfigurieren oder die privaten Schlüssel auf einem Datenträger sichern.

Pidgin findet sich unter Anwendungen ▶ Internet ▶ Pidgin Internet-Sofortnachrichtendienst.

Wenn Pidgin startet, zeigt es die sogenannte *Buddylist*, das ist so etwas wie ein Adressbuch. Nach dem ersten Start muss (mindestens) ein *Chat-Account* angelegt werden (das ist vergleichbar mit einer E-Mail-Adresse).

Im Menü Konten ▶ Konten verwalten aufrufen. Zum Anlegen eines neuen Accounts auf „Hinzufügen“ klicken. Hier die Daten des Chataccounts eintragen. Pidgin hat die Besonderheit, dass ein Chat-Account *name@jabber.server.org* getrennt eingetragen werden muss: „name“ kommt in das Feld „Benutzer“ und *jabber.server.org* in das Feld „Domain“. Der Rest kann leer gelassen werden.

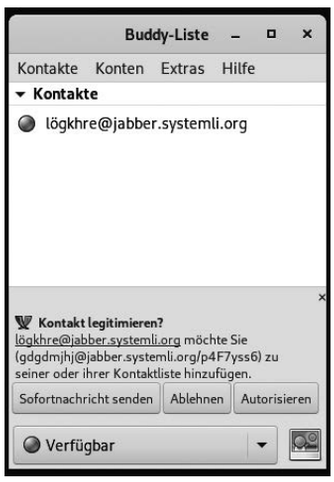
Wir empfehlen darüber hinaus die Anleitung von `systemli.org`. Sie verweist auf eine URL, wo man sich eine Jabber-Adresse von `systemli.org` anlegen kann und erklärt zusätzlich, wo man die .onion-Adresse (`x5tno6mwkncu5m3h.onion`) von `systemli.org` einträgt. Andere Abschnitte zur Einrichtung von Pidgin erübrigen sich unter Tails:
`https://wiki.systemli.org/howto/jabber`.

Kontakte hinzufügen

Um Kontakte in eure serverseitig gespeicherte Kontaktliste aufzunehmen, klickt ihr im Menu auf Kontakte ▶ Kontakte hinzufügen... und tragt dort die Jabber-Adresse eures Kontakts ein. Ihr werdet dann (sobald euer Kontakt online geht) gegenseitig gefragt, ob ihr die Aufnahme in die Kontaktliste jeweils legitimieren bzw. autorisieren wollt.

54 Z.B. könnt ihr verschlüsselte E-Mailinglisten über die Onion-Server betreiben

55 OTR: Off The Record – Ausdruck, der in Gesprächen signalisiert, dass das jetzt Gesagte nicht zitiert werden darf. Mehr zu OTR: `https://otr.cypherpunks.ca/`

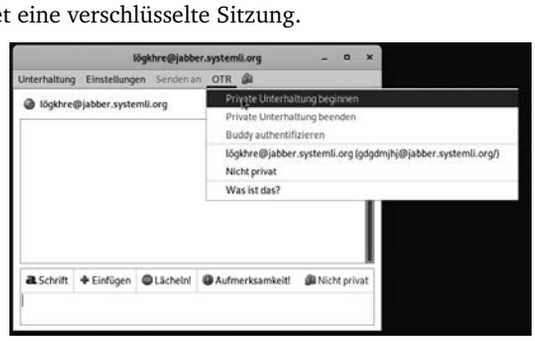


Verschlüsselte Sitzung

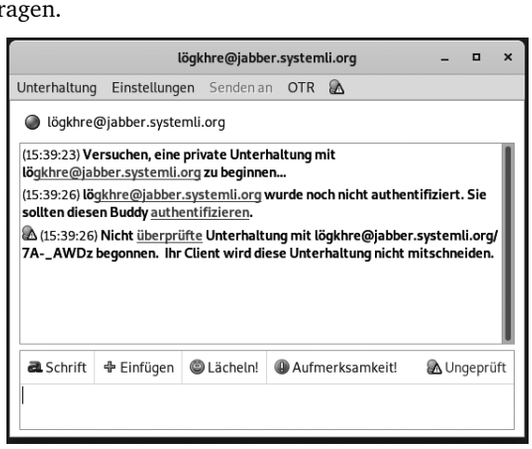
OTR verwendet das gleiche Schema wie auch PGP: Es gibt einen öffentlichen und einen privaten Schlüssel.

> *Chatsitzungen von Pidgin sind beim Start nicht verschlüsselt – das Erste, was also (für jede Chatsitzung) gemacht werden muss, ist die „Private Unterhaltung“ zu starten! Damit ist eine Ende-zu-Ende-Verschlüsselung via OTR gemeint.*

Nach der Auswahl des Menüpunktes „Private Unterhaltung“ startet eine verschlüsselte Sitzung.

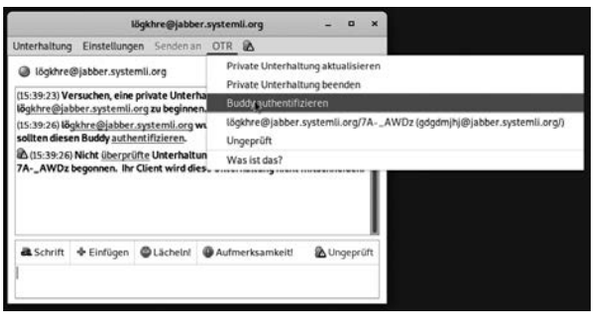


Tippt sensible Inhalte erst nach dem Erscheinen der Meldung „Unterhaltung mit ... begonnen“ ein. Erst ab dieser Stelle wird alles, was in dieser Sitzung geschrieben wird, verschlüsselt übertragen.



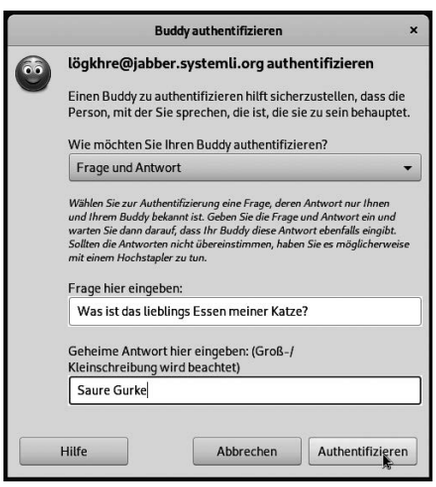
Auf dem Screenshot wird sichtbar, wenn eine Unterhaltung nicht verifiziert ist - sprich, **es ist nicht sicher, ob es sich um die Person handelt, für die sie sich ausgibt.**

Echtheit des Gegenübers verifizieren



Um Zweifel auszuschließen, enthält Pidgin mehrere Methoden, um eine Kommunikation zu verifizieren. **Es stehen drei Methoden zur Verfügung:**

Frage und Antwort: Die Idee hinter dieser Methode ist, dass euer Gegenüber die Frage nur dann richtig beantworten kann, wenn sie die richtige Person ist. Fragen wie „Wie lautet mein Nachname“ scheiden also aus, da die Antwort erraten werden kann. Vorteil dieser Methode ist, dass ihr euer Gegenüber nicht vorher getroffen haben müsst, um



ein entsprechendes Frage-/Antwort-Paar vereinbart zu haben. Nachteil ist, dass eine entsprechende Frage mit nicht oder schwer erratbarer Antwort nicht leicht zu finden ist. Auf der anderen Seite sieht es dann so aus:

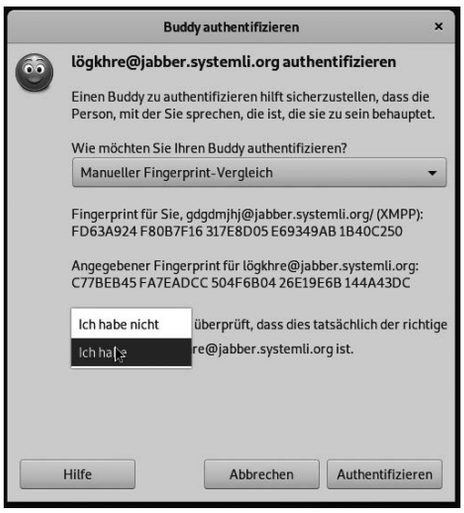
Gemeinsam bekannte Passphrase: Einfacher ist es da schon, über einen sicheren Kanal ein gemeinsames „Passwort“ oder gleich einen ganzen Satz zu vereinbaren. Dieser muss natürlich geheim bleiben.

Manueller Fingerprint-Vergleich: Mit dieser Methode werden die öffentlichen Schlüssel direkt miteinander verglichen - ihr habt den Fingerabdruck des öffentlichen Schlüssels eures Gegenübers und diese*r natürlich auch (ist ja ihr eige-

ner). Sind die Abdrücke gleich, dann sind auch die öffentlichen Schlüssel gleich. Mit der Methode lässt sich ausschließen, dass jemand in der Mitte der Verbindung sitzt und beiden Seiten vorspielt, die jeweils andere Seite zu sein.

Am sichersten, aber wohl auch am umständlichsten, ist der Fingerprint-Vergleich. Die beiden anderen Verfahren haben entweder das Problem, ein gemeinsames Geheimnis sicher auszutauschen oder aber eine nicht erratbare Antwort auf eine Frage zu entwerfen. Von der Frage-/Antwort-Variante raten wir also ab, es sei denn, diese sind über einen sicheren Kanal vereinbahrt worden.

Hier der Fingerprintvergleich als Screenshot, am Ende des Vergleichs wird das Ergebnis gespeichert, sodass der Vergleich nur einmal notwendig ist.



An dieser Stelle die Anmerkung, dass gespeicherte Fingerprints (ob überprüft oder nicht) ein Beleg für einen Kommunikationsvorgang sind und sich darüber ein Abbild eines soziales Netzes (wer kennt wen, wer kommuniziert mit wem) ansammelt. Überlegt euch, ob es das wert ist - die Alternative wäre allerdings ein erneutes Überprüfen der Fingerprints bei jeder Sitzung, und wenn ihr die Schlüssel von OTR nicht speichert, sind auch die jedes Mal neu mit entsprechend neuem Fingerprint.

Voip über Tor

Auf den nächsten Seiten erfahrt ihr, wie sich Mumble[56] für eine verschlüsselte VOIP-Kommunikation[57] unter Tails nutzen lässt.

Warum Mumble?

- Die Software eignet sich besonders durch ihre gute Audioqualität und niedrige Latenzzeit[58] für das Tor-Netzwerk.
- Das Netzwerkprotokoll UDP kann über den Steuerkanal von Mumble (TCP) getunnelt werden, was eine Voraussetzung für eine Kommunikation im Tor-Netzwerk ist[59].

Der Beitrag gliedert sich in zwei Teile:

- Mumble mit öffentlichen Servern.
- Mumble über einen lokalen Onion-Service.

Der erste Abschnitt beschreibt eine mögliche Verwendung von öffentlichen Mumble-Servern und benennt die Problematik von zentralen Server-Instanzen im Allgemeinen. Anschließend zeigen wir euch, wie sich ein Mumble-Server über Onion Services aufsetzen und für eine Peer-To-Peer[60]-Kommunikation verwenden lässt. Wer Wert auf eine sichere Kommunikation legt, sollte den zuletzt genannten Weg wählen, da er eine höhere Sicherheit als eine Kommunikation über öffentliche Server bietet:

- Ende-zu-Ende-Verschlüsselung[61] durch Tor.
- Public-Key-Authentifizierung[62][63] zur Verhinderung von Man-in-the-Middle-Angriffen[64] (sofern die Onion-Adresse auf einem sicheren Weg der Komunikationspartner*in mitgeteilt wurde).
- Temporäre Onion-Adresse, die erst einmal gefunden werden muss.

Die hier beschriebenen Nutzungsmöglichkeiten können vorübergehend oder auch längerfristig durch eine Installation im persistenten Speicher verwendet werden.

> *Falls ihr aufgrund von möglichen Sicherheitslücken in Tails befürchtet, dass euer System von Schadsoftware befallen werden kann, solltet ihr Mumble nur temporär installieren und den Absatz zum Einrichten im persistenten Speicher überspringen.*

Am Ende des jeweiligen Abschnitts zeigen wir euch, wie ihr die gemachten Einstellungen dauerhaft sichern könnt. Dafür müsst ihr euren persistenten Speicher einbinden (siehe Kapitel „Persistenz“). Ein Administrationspasswort benötigt ihr in allen Fällen.

> *Um Mumble nach einem Neustart wiederverwenden zu können, müsst ihr „Dotfiles“ über die Konfiguration im Anwendungsmenü ► Tails ► „Configure persistent volume“ zulassen (siehe Kapitel „Persistenz“).*

Mumble Client

Zum Installieren des Mumble-Clients öffnet ihr das Menü Anwendungen ► Systemwerkzeuge ► Synaptic-Paketverwaltung. Die Paketverwaltung braucht nun eine Zeit, bis sie die Quell-Informationen aus dem Internet geladen hat. Wenn hierbei Fehlermeldungen auftreten und bei der Suche nach „Mumble“ über das **Lupen-Icon** keine Ergebnisse erscheinen, könnt ihr die Quell-Informationen für Synaptic erneut über das **Neu-Laden-Icon** aktualisieren. Nachdem ihr Mumble über die Suche gefunden und die Checkbox zum Installieren ausgewählt habt, werdet ihr nach weiteren Abhängigkeiten gefragt, die ihr ebenfalls vormerkt. Anschließend müsst ihr noch auf das **Anwenden-Icon** klicken, und der Mumble-Client wird installiert.

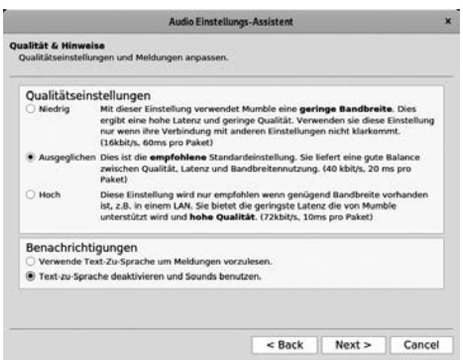
56 https://www.mumble.info
57 Sprachübertragung über das Internetprotokoll.
58 Antwortzeit.
59 Die meisten Anwendungen für Sprachübertragungen benötigen UDP als Übertragungsprotokoll, das von Tor nicht unterstützt wird.
60 Rechner-zu-Rechner-Verbindung.
61 https://de.wikipedia.org/wiki/Ende-zu-Ende-Verschl\%C3\%BCsselung
62 https://de.wikipedia.org/wiki/Public-Key-Authentifizierung
63 https://gitweb.torproject.org/torspec.git/tree/tor-spec.txt
64 https://de.wikipedia.org/wiki/Man-in-the-Middle-Angriff

Nach erfolgreicher Installation der Software erscheint eine Meldung mit der Frage, ob die Anwendung dauerhaft installiert werden soll, was ihr mit „Install Every Time“ oder „Install only once“ beantwortet.

Unter `Anwendungen ▶ Internet` solltet ihr nun einen neuen Eintrag mit dem Namen „Mumble“ finden. Nach der erstmaligen Auswahl des Eintrags wird automatisch ein Mumble Audio-Einstellungsassistent gestartet. Die Schritte zum Einrichten von Mumble sollten selbsterklärend sein[65].

Im fünften Schritt wählt ihr die Option „Push-To-Talk“ aus, klickt in das Eingabefeld und definiert durch eine frei wählbare Tastenkombination eine Funktion zum Sprechen: z.B. `Strg` + `T`.

Im sechsten Schritt wird die Qualität entsprechend eurer Internetanbindung eingestellt. Mit einer guten DSL-Anbindung könnt ihr „Ausgeglichen“ auswählen. Falls ihr euch in Regionen mit einer schlechten Internet-Anbindung befindet, solltet ihr „Niedrig“ einstellen.



Bei den Benachrichtigungen deaktiviert ihr „Text-zu-Sprache“. Im letzten Schritt deaktiviert ihr noch „Sende anonyme Statistiken an das Mumble Projekt“ und beendet mit `Finish` den Assistenten.

Nachdem der Audio-Assistent beendet wurde, öffnet sich automatisch der Zertifikats-Assistent von Mumble. Hier wählt ihr „Zertifikat automatisch erstellen“ aus und wechselt durch einen Klick auf `Weiter` in das nächste Fenster (und beendet mit `Finish` den Assistenten).

Danach schließt ihr die Server-Auswahl durch den `Cancel` Button und öffnet die Mumble-Einstellungen über das Menü `Konfiguration ▶ Einstellungen`. Nun wechselt ihr in den Bereich Netzwerk und ändert unter Proxy/Type das Drop-Down Menü auf „Socks5 Proxy“. Dann gebt ihr in das Feld Hostname `127.0.0.1` ein und fügt dem Feld Port `9150` hinzu.

Da dies der Port eures Tor-Browsers ist, könnt ihr bei einer schlechten Verbindung einen neuen Tor-Kanal auswählen (auf das Schloß in der Navigationsleiste des Tor-Browsers klicken). **Durch die Proxy-Auswahl wird Mumble automatisch in den TCP-Modus gesetzt.** Dadurch werden sämtliche Datenpakete über den Steuerkanal (TCP) mit einer stärkeren Transport-Verschlüsselung als normalerweise unter Mumble üblich übertragen[66]. Danach aktiviert ihr noch die „Checkbox“ Datenschutz und beendet mit `OK` die Konfiguration.

Mumble mit öffentlichen Servern

Um nun mit jemandem kommunizieren zu können, benötigt ihr einen öffentlichen Mumble-Server, über den ihr euch verbinden könnt. Da die Namensauflösung[67] von Mumble unter Tails nicht funktioniert, müsst ihr euch die Zugangsdaten für einen öffentlichen Server über die Webseite:
`https://www.mumble.com/serverlist` besorgen.

Besser: ihr kennt eine*n vertauenswürdige*n Betreiber*in eines Mumble-Servers und bezieht die Zugangsdaten über diese Quelle.

Umso mehr Benutzer*innen einen Server-Dienst wie Mumble verwenden, umso interessanter ist dieser auch für eine*n Angreifer*in. Von daher solltet ihr euch bei der Wahl des Mumble-Server für eine*n halbwegs vertrauenswürdige*n Betreiber*in entscheiden.

Neben diesem Aspekt könnt ihr euch als Alternative auch überlegen, welchen Server-Standort ihr wählt. In Abhängigkeit, wo ihr euch gerade befindet, gibt es z.B. einige Regionen auf der Welt, die evtl. nicht mit euren Behörden zusammen arbeiten. Wenn ihr euch in einem EU-Land aufhaltet, kann es durchaus Sinn machen, einen Mumble-Server in einem anderen Kontinent auszuwählen.

Mumble-Server-Liste[68]: `https://www.mumble.com/serverlist`.

Wenn ihr einen Server eurer Wahl gefunden habt, merkt ihr euch die IP-Adresse (das ist die Zahlenfolge bis zu dem bzw. ohne den Doppelpunkt). Falls hier nur der Domainname abgebil-

65 Mumble Handbuch: `https://wiki.natenom.de/mumble/benutzerhandbuch/mumble`
66 Ende-zu-Server-Verschlüsselung mit TLS v1.2 AES_256_GCM.
67 `https://de.wikipedia.org/wiki/Domain_Name_System#Beispiel/_Namensaufl\%C3\%B6sung`
68 Die Auflistung der Server über das Länder-Auswahlmenü funktioniert nur mit den „sicheren“ Tor-Browser-Einstellungen.

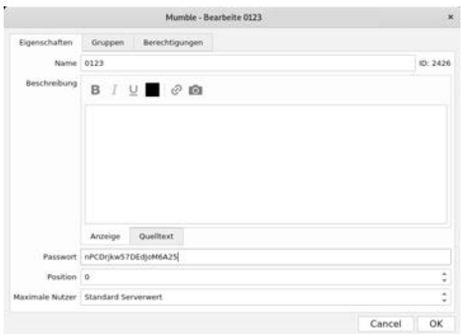
det ist, lässt sich die IP-Adresse auch über folgenden Terminal-Befehl ermitteln: (Anwendungen ▶ Systemwerkzeuge ▶ Terminal):

```
tor-resolve domain # z.B. talk.systemli.org
```

Durch die direkte Eingabe der IP-Adresse umgeht ihr eine DNS-Auflösung[69] und mögliche DNS-Leaks[70][71]. Danach öffnet ihr das Verbindungsfenster über das Menü Server ▶ Verbinden und fügt über Server hinzufügen die zuvor notierte IP-Adresse und einen evtl. abweichenden Port ein (die Zahl nach dem „:“).

Nun könnt ihr einen passwortgeschützten Kanal über ein Klicken mit der rechten Maustaste auf das Root-Verzeichnis im Mumble-Client hinzufügen.

Diesen Kanal könnt ihr nach Belieben benennen und durch ein Passwort schützen. Dafür müsst ihr mit der rechten Maustaste auf den zuvor angelegten Kanal klicken und das Menü „Bearbeiten...“ auswählen. Im unteren Bereich des Bearbeitungsfensters findet ihr eine Zeile, in der ihr ein beliebiges Passwort eingeben könnt.



Dieses und den zuvor vergebenen Kanal-Namen müsst ihr noch euren Komunikationspartner*innen mitteilen (z.B. über eine verschlüsselte E-Mail). Die Empfänger*in muss den erhalten Zugriffscode über das Mumble-Menü Server ▶ Zugriffscode hinzufügen und kann anschließend den geschützten Kanal betreten. Nun könnt ihr über die zuvor vergebene Tastenkombination Strg + T miteinander kommunizieren.

> *Manche Sonderzeichen wie das Anführungszeichen werden unter Mumble nur mit einem vorgestellten Back-Slash unterstützt. Falls ihr Probleme mit dem Kanalnamen oder eurem Passwort habt, versucht es erneut - ohne Sonderzeichen.*

Mumble-Einstellungen dauerhaft speichern

Um die Einstellungen dauerhaft zu speichern, müssen folgende Ordner über Anwendungen ▶ Systemwerkzeuge ▶ Root Terminal angelegt und kopiert werden (dafür braucht ihr euer Administrationspasswort):

```
cd /live/persistence/TailsData_unlocked
mkdir -p dotfiles/.config
mkdir -p dotfiles/.local/share
cd dotfiles
rsync -av /home/amnesia/.config/Mumble .config
rsync -av /home/amnesia/.local/share/Mumble \
 .local/share
```

Wenn ihr die Einstellungen von eurem Mumble-Client ändert, müsst ihr die letzten beiden Befehle erneut ausführen („rsync“).

Mumble über einen lokalen Onion-Service

In diesem Abschnitt zeigen wir euch, wie sich ein Mumble-Server temporär (oder auch dauerhaft) als Tor Onion Service aufsetzen[72] und für eine Peer-to-Peer-Kommunikation nutzen lässt[73]. Für die Kommunikation über Mumble muss nur eine*r von euch einen Mumble-Server installieren. **Den Mumble-Client braucht ihr auf beiden Seiten.**

> *Mumble benutzt keine Ende-zu-Ende-Verschlüsselung, sondern nur eine Ende-zu-Server-Verschlüsselung. Da ihr Mumble über eine Tor Onion-Adresse tunnelt und die Kontrolle über den Mumble-Server besitzt, findet die Kommunikation Ende-zu-Ende-verschlüsselt statt (über drei zufällig ausgewählte Onion-Server).*

Nachdem ihr euch mit einem Administrationspasswort angemeldet habt (siehe Kapitel „Tails starten“), müsst ihr das Paketverwaltungssystem Synaptic über das Menü Anwendungen ▶ Systemwerkzeuge ▶ Synaptic-Paketverwaltung starten (hierfür benötigt ihr erneut das Administrationspasswort). Um die Software über Synaptic zu installieren, könnt ihr sie über das **Lupen-Icon** suchen („mumble“) und mit dem Aktivieren der Checkbox vormerken. Ihr werdet hier nach weiteren benötigten Paketen gefragt, die ihr ebenfalls vormerkt. Auf demselben Weg wählt ihr noch sqlite3 aus (damit könnt ihr das Server-Zertifikat auslesen und überprüfen). Falls ihr die Software dauerhaft installieren wollt, beantwortet ihr die Meldung mit „Install Every Time“.

Nun müsst ihr noch auf das **Anwenden-Icon** klicken und die Software wird installiert. Anschließend müsst ihr über das Menü Anwendungen ▶ Systemwerkzeuge ▶ Root Terminal eine „Eingabeaufforderung“ öffnen und dort mit dem Befehl

```
nano /etc/tor/torrc
```

die Konfigurationsdatei von Tor bearbeiten, um einen Tor Onion Service aufzusetzen, über den ihr kommunizieren könnt. In der Konfigurationsdatei scrollt ihr über den Editor „nano“ an das Ende der Datei und fügt folgende Zeilen hinzu:

```
HiddenServiceDir /var/lib/tor/mumble
HiddenServicePort 50489 127.0.0.1:50489
```

Dann beendet ihr den Editor über die Tastenkombination Strg + X und bestätigt die Frage nach einem Speichern mit „J“ und einem anschließenden „return“, ohne den angezeigten Pfad zu ändern.

69 https://de.wikipedia.org/wiki/Domain_Name_System
70 https://tails.boum.org/contribute/design/Tor_enforcement/DNS/
71 Laut folgendem Kommentar sollten DNS-Leaks in Mumble nicht mehr möglich sein: https://github.com/unascribed/mumble/commit/e7762b58804e9bfbf8af314454c626da2e447d96
72 Siehe Kapitel „Nur über Tor ins Netz“
73 Für eine Kommunikation mit vielen Teilnehmer*innen eignet sich die Software aufgrund der geringen Latenz von Tor nur bedingt.

Über denselben Weg müsst ihr nun noch die Konfigurationsdatei von Mumble anpassen:

```
nano /etc/mumble-server.ini
```

Hierfür müsst ihr über den Editor mit Strg + W nach „;host“ suchen, das Semicolon am Anfang der Zeile entfernen und „127.0.0.1“ eingeben:

```
host=127.0.0.1
```

Drei Zeilen unter diesem Eintrag vergebt ihr noch ein sicheres Passwort (siehe Kapitel „Sichere Passwortwahl“):

```
serverpassword=rVVZHZ8LYnM4k4qguYMT
```

Nun müsst ihr Tor neu starten und solltet über den zweiten hier abgebildeten Terminal-Befehl die Tor Onion Service-Adresse des Mumble-Servers erhalten:

```
service tor restart # Tor neu Starten
cat /var/lib/tor/mumble_onion_service/hostname
```

> *Zur Erhöhung der Sicherheit kann die Onion-Adresse z.B. jede Stunde gewechselt werden. Dafür muss der Name, den ihr zuvor in der „/etc/tor/torrc“ Konfigurationsdatei eingetragen habt, geändert und Tor neu gestartet werden (auf dieselbe Weise wie bereits zuvor beschrieben).*

Die Prüfsumme des Mumble Server-Zertifikats erhaltet ihr über folgenden Befehl:

```
sqlite3 -batch \
 /var/lib/mumble-server/mumble-server.sqlite \
'select value from config where key="certificate" and \
 server_id="1"' \
| openssl x509 -fingerprint -sha256 -noout
```

Um euch nun mit dem Mumble-Server verbinden zu können, muss allen an der Gesprächsrunde Beteiligten die Onion Service-Adresse und die Prüfsumme des Server-Zertifikats über einen sicheren Weg mitgeteilt werden. Hierfür bietet sich beispielweise eine mit GPG verschlüsselte E-Mail an (siehe Kapitel „Mailen über Tor“).

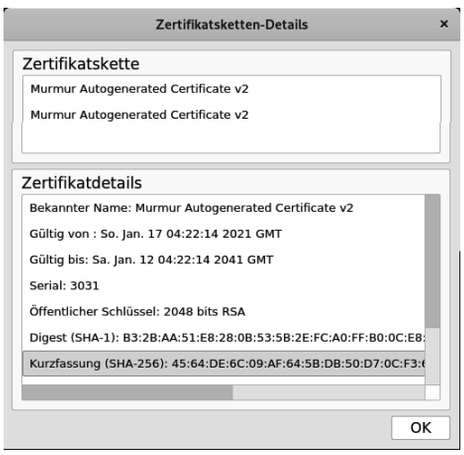
Aufgrund der schlechten Internet-Anbindung von Tor sollte sich eine Sitzung nur auf wenige Teilnehmer*innen beschränken.

Im Begrüßungsmenü von Mumble könnt ihr über Server hinzufügen die Onion-Adresse, den zuvor vergebenen Port (50489) und einen beliebigen Benutzernamen eintragen.

> *Wenn ihr den Mumble-Server dauerhaft im persistenten Speicher installiert habt, müsst ihr nach einem Neustart von Tails die Onion-Adresse erneut auslesen und verschlüsselt allen Kommunikationspartner*innen mitteilen:* ***cat /var/lib/tor/mumble_onion_service/hostname***

Nach einer erfolgreichen Verbindung werdet ihr darauf hingewiesen, dass die Überprüfung des Zertifikats gescheitert ist (was bei selbst generierten Zertifikaten normal ist).

Durch einen Klick auf Zertifikat zeigen findet ihr im unteren Bereich des Fensters die SHA-256 Prüfsumme, die ihr mit der zuvor erhaltenen Prüfsumme des Zertifikats abgleicht.



Mumble- und Onion Service-Einstellungen dauerhaft speichern

Um die Einstellungen des Mumble-Clients dauerhaft speichern zu können, öffnet ihr das Menü Anwendungen ▶ Systemwerkzeuge ▶ Root Terminal und führt folgende Befehle aus:

```
cd /live/persistence/TailsData_unlocked
mkdir -p dotfiles/.config
mkdir -p dotfiles/.local/share
cd dotfiles
rsync -av /home/amnesia/.config/Mumble .config
rsync -av /home/amnesia/.local/share/Mumble \
 .local/share
```

Danach müsst ihr noch die Konfigurationsdatei von Mumble und Tor in euren persistenten Speicher sichern:

```
cp /etc/mumble-server.ini /home/amnesia/Persistent
cp /etc/tor/torrc /home/amnesia/Persistent
```

Die abgelegten Dateien müssen nach jedem Neustart von Tails aus dem eingebundenen persistenten Speicher über ein Root-Terminal in das Konfigurationsverzeichnis „/etc“ von Tails kopiert werden:

```
cp /home/amnesia/Persistent/mumble-server.ini /etc
cp /home/amnesia/Persistent/torrc /etc/tor/torrc

systemctl restart mumble server
systemctl restart tor server
```

Nach einem erfolgreichen Restart der Dienste sollte Mumble mit den neu konfigurierten Einstellungen nutzbar sein.

Onionshare

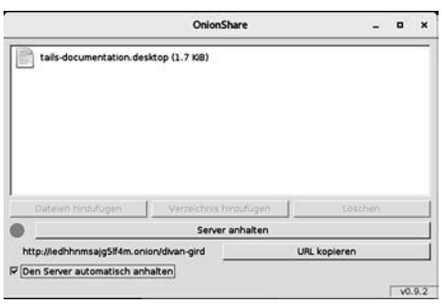
Tails erlaubt Filesharing, ohne dass es dafür einen dedizierten Server im Internet geben muss. *Onionshare* ist ein Ad Hoc Fileserver, der einen „Tor Hidden Service“ startet und darüber Dateien direkt vom Rechner herunterladbar macht. Ein Upload auf den Rechner ist nicht möglich.

Onionshare läßt sich entweder über Anwendungen ▶ Internet ▶ Onionshare starten oder über den Dateimanager.

- Öffnet den Datei-Browser, entweder über den Menüpunkt „Orte“ oder indem ihr den „Persönlichen Ordner“ auf dem Desktop öffnet.
- Klickt euch durch den Dateimanager, bis ihr zur Datei kommt, die ihr teilen wollt.
- Macht einen Rechtsklick auf eine Datei oder einen Ordner, den ihr teilen wollt.
- Wählt nun „Share via Onionshare“

- Im nun folgenden Fenster könnt ihr weitere Dateien zum Teilen hinzufügen.
- Normalerweise stoppt Onionshare den Hidden Service, nachdem die Dateien einmal heruntergeladen worden sind. Solltet ihr die Dateien zum mehrmaligen Herunterladen anbieten wollen, dann müsst ihr den Haken bei „Den Server automatisch anhalten“ entfernen.
- Klickt nun auf Server starten, und der Tor Hidden Service wird gestartet.

- Nach einer kurzen Weile startet der Server und ihr bekommt eine Adresse ähnlich dieser angezeigt: `http://bwwijokny5qplq5q.onion/assam-cover`. Diese Adresse müsst ihr weitergeben, damit andere an die Dateien kommen.
- Um diese Adresse zu verschicken, könnt ihr sie mit dem Button URL kopieren in die Zwischenablage kopieren.



Onionshare informiert euch in diesem Fenster auch, wenn die Dateien heruntergeladen werden. Sobald ihr Onionshare schliesst, die Internetverbindung kappt oder Tails herunterfahrt, kann auf die Dateien nicht mehr zugegriffen werden.

Zum Download der angebotenen Dateien muss die von Onionshare erzeugte Adresse im Tor-Browser geöffnet werden.

Offline-Arbeiten

Im Februar 2015 veröffentlichte der Antiviren-Software-Hersteller *Kaspersky*, dass die NSA in größerem Umfang die Firmware von Festplatten infiziert. Die eingeschleuste Schadsoftware überlebe eine Formatierung der Festplatte oder Neuinstallation des Betriebssystems und sei nicht zu entdecken. Gleichzeitig werde sie genutzt, um einen versteckten Bereich auf der Festplatte zu schaffen, auf dem Daten gesichert werden, um sie später abgreifen zu können. Die einzige Möglichkeit, die Schadsoftware loszuwerden, sei die physikalische Zerstörung der Festplatte.

Für ein sicheres, spurenfreies Bearbeiten von extrem sensiblen Dokumenten empfehlen wir die Arbeit an einem Rechner, der weitgehend abgeschottet ist und insbesondere keine Festplatte(n) besitzt. Da ihr teilweise Hand an euren Rechner legen müsst, um Teile auszubauen, die ihr nicht braucht, oder die euch verraten könnten, besorgt euch das Manual für eure Hardware[74].

Festplatte(n) abschalten

Zwar müsstet ihr die im Computer vorhandene Festplatte wie jeden anderen Datenträger auch in Tails erst im Menü Orte ▶ Rechner verfügbar machen, bevor ihr (versehentlich) darauf etwas speichern könnt. Aber genau solche „Versehen“ und die Möglichkeit, dass eine in der Sitzung eingeschleuste Schadsoftware doch auf die Festplatte zugreifen könnte, wollen wir vermeiden. Wir stellen euch zwei Methoden vor und empfehlen euch die Erste:

Festplatte ausbauen: In der Bedienungsanleitung *(nach User Manual im Internet suchen)* eures Rechners sind die dazu notwendigen Schritte erläutert. Als erstes müsst ihr den Akku aus eurem Laptop herausnehmen und den Netzstecker abziehen. Bei vielen Laptops müsst ihr die Schrauben auf dem Boden lösen und den Boden abnehmen. Die Festplatte ist mit dem Restgehäuse zusätzlich verschraubt. Nachdem ihr diese gelöst habt, könnt ihr die Festplatte vom Stecker abziehen.

Festplatte im BIOS deaktivieren: Wenn euch der Ausbau zu aufwändig erscheint, müsst ihr zumindest im BIOS die interne(n) Festplatte(n) eures Computers deaktivieren [75].

74 Die Manuals sind üblicherweise einfach im Internet zu finden.

75 Unmittelbar nach dem Computer-Start eine der Tasten F1, F2, DEL, ESC, F10 oder F12 gedrückt halten (auf einen Hinweis auf dem kurz erscheinenden Startbildschirm achten), um in das BIOS-Setup zu gelangen. Siehe dazu das Kapitel im Anhang: „Bootreihenfolge im Bios ändern“.

Alle kabellosen Schnittstellen abschalten

Das kabelgebundene Netz (LAN) lässt sich einfach über das Abziehen des Netzwerkkabels „deaktivieren“. Zusätzlich ist es für diese besonders sichere Betriebsart von Tails als „Quasi-Schreibmaschine“ unerlässlich, sämtliche Funkschnittstellen abzuschalten. Wir beschreiben hier vier unterschiedliche Methoden *(1 ist die sicherste, 4 die unsicherste)*:

1. **WLAN und Bluetooth ausbauen:**[76] Analog zu Schritt **1**) im Kapitel *Gefahren von kabellosen Schnittstellen*. Ihr ersetzt die ausgebaute Karte jedoch nicht.
2. Einige Laptops haben **Schalter im Gehäuse**, mit dem sich die **Funkschnittstellen deaktivieren lassen**.
3. **Alle Netzwerkadapter im BIOS deaktivieren** (leider nicht bei allen Computern möglich).
4. Ihr startet Tails neu und klickt am Startbildschirm unter „Additional Settings“ den `+`-Button. Im aufgehenden Fenster wählt ihr „Network Connection“, um dann „Disable all networking“ anzuklicken. Hiermit bleiben alle Netzwerkadapter softwareseitig beim Start deaktiviert. Dies geschieht sinnvoller Weise, *bevor* Tails seine Netzwerkfunktionalität startet. So bleiben u.a. WLAN und WWAN still und können eure Anwesenheit in Funkreichweite anderer Geräte nicht mehr preisgeben.

Mikrofon und Kamera deaktivieren

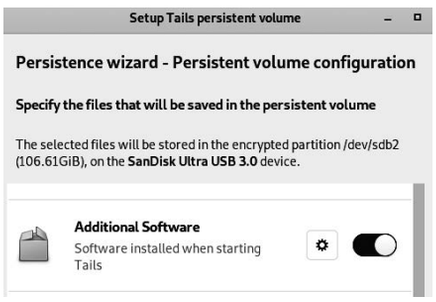
Die Kamera, die mittlerweile in den meisten Laptops fest eingebaut ist, lässt sich am einfachsten durch einen über der Linse platzierten Sticker „deaktivieren“. Für das Mikrofon müsst ihr das Laptop aufschrauben und nach Manual soweit zerlegen, dass ihr an das Mikro rankommt. Häufig ist das Mikro durch einen Stecker mit dem Mainboard verbunden. Es reicht dann, diesen abzuziehen. Ist das uneindeutig, gibt es keinen Stecker, weil das Kabel direkt verlötet ist, oder wird der Stecker noch zu anderen Zwecken benötigt, dann zerschneidet das Mikrofonkabel mit einem Seitenschneider. Die Kamera lässt sich mit der gleichen Methode dauerhaft stilllegen, wenn ihr der Stickermethode nicht traut.

Ein vollständig abgeschotteter Schreib-Computer, aus dem ihr die Festplatte(n) und alle kabellosen Netzwerkadapter ausbaut, gibt euch erhöhte Sicherheit beim Erstellen und Bearbeiten von Dokumenten: Ihr seid ohne Weiteres nicht zu identifizieren und zu lokalisieren, und ihr verhindert ein „versehentliches“ Speichern auf der Festplatte!

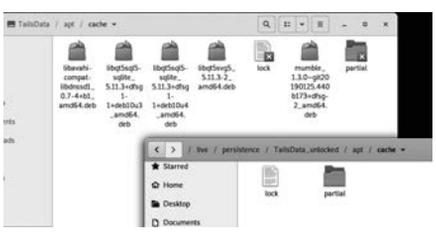
Software offline installieren

Sollte es der Fall sein, dass ihr auf einen Tails-Stick, den ihr nicht mit dem Internet verbinden wollt, Software nachinstallieren wollt, so geht das auch „offline“. Ihr braucht dafür ein zweites Tails-System (hier „Online-Tails“), mit der gleichen Version wie euer Offline-Tails.

1. Installiert zuerst die Software, die ihr benötigt, auf dem Online-Tails. Sollte auf dem System auch schon andere Software installiert sein, so achtet auf die Abhängigkeiten, die mitinstalliert werden. Merkt euch ihre Namen.
2. Startet euer Offline-Tails.
3. Geht dort auf das `Anwendungsmenü` ▶ `Tails` ▶ `Configure Persistence` und aktiviert dort den Punkt `Additional Software`.



4. Macht nun einen Neustart des Offline-Tails, damit die Änderungen wirksam werden. Wichtig: Setzt ein Administrations-Passwort bei der Anmeldung.
5. Steckt nun den Stick des Online-Tails in den Computer. Er wird nun im Ordner `Dateien` angezeigt. Mit dem Persistenz-Passwort des Online-Tails könnt ihr ihn nun einbinden. Geht dort in den Ordner `apt`.
6. Macht nun ein zweites Fenster des Dateibrowsers auf und geht zu `Computer` ▶ `live` ▶ `TailsData-unlocked` und dort in den Ordner `apt`. Hierfür müsst ihr eurer Administrator*innen-Passwort eingeben.
7. Kopiert nun den Inhalt des `apt`-Ordners vom Online-Tails in den Ordner `apt` des Offline-Tails.



8. Geht nun auf dem Offline-Tails wieder einen Ordner zurück zu `Computer` ▶ `live` ▶ `TailsData-unlocked` und öffnet dort die Datei `live-additional-software.conf` mit dem Texteditor. Hierfür braucht ihr euer Administrations-Passwort.
9. Schreibt in die Datei die Namen der Software, die ihr installieren wollt - ein Softwarepacket pro Zeile - und speichert das Ergebnis.
10. Schaltet den Rechner aus und entfernt den Online-Tailsstick. Starte nun erneut euer Offline-Tails mit der Persistenz. Die Software sollte nun installiert werden. Nach ein paar Minuten ist sie über das Anwendungsmenü zu finden.

---

76 Da die Bauart dieser Karten und die Orte, an denen sie (im Rechner) genau verbaut sind, variieren, müsst ihr in der Betriebsanleitung (User Manual) eures Computers nach einer Beschreibung zu deren Ein-und Ausbau suchen. Hier ein Abbild einer kombinierten WLAN- und Bluetooth-Karte eines Laptops.

77 `https://osmand.org/list`

Offline-Karten

In den nächsten Absätzen erfahrt ihr, wie sich Karten offline unter Tails nutzen lassen. Und das ohne ein Live-Tracking, wie es ansonsten bei den gängigen Online-Diensten der Fall ist. Wir verwenden dafür das Kartenmaterial von OsmAnd[77], das wiederum auf Openstreetmap basiert und sich nach weiteren nützlichen Infos durchsuchen läßt, sogenannten POI (Points of Interest).

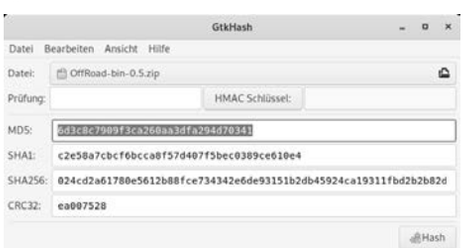
Nachdem ihr Tails gestartet habt, müsst ihr euch mit einem Administrationspasswort (siehe Kapitel „Tails starten“) und der Einbindung eures persistenten Speichers anmelden (siehe Kapitel „Persistenz“). Falls ihr Bedenken wegen möglicher Malware[78] habt und die Sicherheit beim wiederholten Betrachten des Kartenmaterials erhöhen wollt, könnt ihr die Karten auch ohne persistenten Speicher verwenden - allerdings nur temporär.

Alle hier erklärten Schritte müssen dafür jedes Mal neu ausgeführt werden (da sämtliche Installationsdateien nach einem Neustart von Tails verloren gehen).

OffRoad

Das Programm *OffRoad* besorgt ihr euch über die Webseite: `https://sourceforge.net/project/offroadosm/files/latest`.

Unter Anwendungen ► Zubehör ► GtkHash findet ihr ein Programm, mit dem ihr die Prüfsumme von OffRoad 0.5 abgleichen könnt (verwendet die Software nur, wenn dieselbe Prüfsumme wie unter „SHA256“ erscheint):



Hierfür müsst ihr das zuvor bezogene Programm *OffRoad-bin-0.5.zip*[79] im oberen Fensterbereich des Programms auswählen (neben dem Zeileneintrag „Datei:“) und anschließend den Hash-Button drücken. Um die ganze SHA-256-Prüfsumme[80] unter GtkHash erkennen zu können, muss das Programmfenster entsprechend vergrößert werden. Alternativ kann dies auch mit folgendem Befehl im Terminal überprüft werden (das Terminal findet ihr im Menü Anwendungen ► Systemwerkzeuge ► Terminal):

```
shasum -a 256 ~/Tor\ Browser/OffRoad-bin-0.5.zip
```

Die Ausgabe sollte folgende sein:

```
024cd2a61780e5612b88fce734342e6de93151b2db45924ca19-
311fbd2b2b82d
```

Wenn die Prüfsumme mit der hier Abgedruckten übereinstimmt, dann wurde die Datei nicht manipuliert.

Jetzt fehlt nur noch das gewünschte Kartenmaterial. Es ist unter `https://osmand.net/list` zu finden. Die Karten-Datei holt ihr euch am besten ein zweites Mal mit dem Tor-Browser über einen neuen Tor-Kanal (auf das graue Schloß in der Navigationsleiste klicken, um einen neuen Kanal zu wählen) und vergleicht sie anschließend mit GtkHash[81] oder über den Terminal-Befehl:

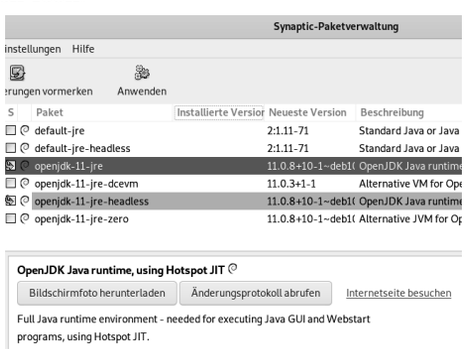
```
diff map-1.obf.zip map-2.obf.zip
```

Falls keine Warnmeldung im Terminal erscheint, handelt es sich (wie gewünscht) um dieselben Dateien.

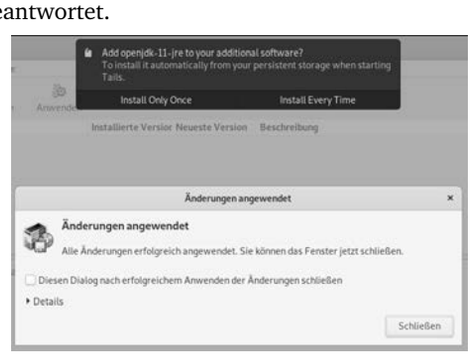
Benötigte Software

Danach müsst ihr noch eine aktuelle Java Runtime installieren, da OffRoad dies voraussetzt. Über das Menü Anwendungen ► Systemwerkzeuge ► Synaptic-Paketverwaltung findet ihr eine grafische Anwendung, mit der ihr die Java Runtime installieren könnt (hierfür braucht ihr euer Administrationspasswort):

Im nächsten Schritt müsst ihr über das **Suche-Icon** der Anwendung nach „openjdk-11-jre“ suchen und diese über die **Checkbox** zum Installieren vormerken. Dadurch werden automatisch drei weitere Programmabhängigkeiten ausgewählt, welche mit dem Vormerken-Button bestätigt werden. Anschließend installiert ihr die benötigte Java Runtime durch ein Klicken auf das **Anwenden-Icon**.



Wenn die Software erfolgreich installiert wurde, erscheint eine Meldung mit der Frage, ob die Anwendung dauerhaft installiert werden soll, was ihr mit „Install Every Time“ oder „Install only once“ beantwortet.



78 `https://de.wikipedia.org/wiki/Malware`

79 Die Datei befindet sich nach einem erfolgreichen Download im Verzeichnis `/home/amnesia/TorBrowser`.

80 Die offiziellen Prüfsummen von Sourceforge findet ihr unter folgender URL (durch einen Klick auf das I-Icon): `https://sourceforge.net/projects/offroadosm/files/OffRoad_Stable/0.5/`. Hierbei handelt es sich allerdings um SHA-1 und MD5-Prüfsummen, die als nicht mehr sicher gelten.

81 Um zu verhindern, dass euch evtl. manipuliertes Kartenmaterial untergeschoben wird.

Im persistenten Speicher

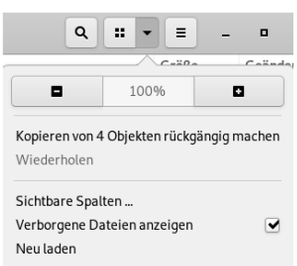
Um OsmAnd-Karten nach einem Neustart wiederverwenden zu können, müsst ihr „Dotfiles“ über die Konfiguration im Anwendungsmenü ► Tails ► Configure persistent volume zulassen (siehe Kapitel „Persistenz“).

Die zuvor bezogene Karte, welche sich nach dem Download im Ordner „Tor Browser“ befindet, verschiebt ihr in euren persistenten Speicher, nachdem ihr sie durch ein Anklicken mit der rechten Maustaste auf „Hier entpacken“ dekomprimiert habt.

Die entpackte Karte mit der Endung `.obf` muss anschließend noch in das Verzeichnis `/live/persistence/TailsData_unlocked/dotfiles/.OffRoad/maps` kopiert werden. Dafür muss das unsichbare Verzeichnis `.OffRoad` mit dem Unterverzeichnis `.OffRoad/maps` in dem zuvor genannten Dotfiles-Verzeichnis angelegt werden. Entweder mit folgenden Befehl im Terminal (OffRoad mit großem „R“):

```
cd /live/persistence/TailsData_unlocked
mkdir -p dotfiles/.OffRoad/maps
cd dotfiles/.OffRoad/maps
rsync -av /home/amnesia/Tor\ \
 Browser/Germany\_berlin\_europe.obf .
```

oder über den Dateibrowser von Tails (Andere Orte ► Rechner ► /live/persistence/TailsData_unlocked/dotfiles/.OffRoad/maps), nachdem ihr die Verzeichnisse `.OffRoad/maps` im Dotfiles-Ordner angelegt habt[82].



Das Programm OffRoad verschiebt ihr in euren persistenten Speicher, nachdem ihr es dekomprimiert habt (siehe Kapitel „Persistenz“). Damit die Karten über das Dotfiles-Verzeichnis erkannt werden, müsst ihr Tails neu starten und den persistenten Speicher durch Eingabe eures Passworts im Startmenü einbinden. Nun müsst ihr noch abwarten, bis die für OffRoad benötigte Software erneut installiert wurde (bis zur Meldung „Additional Software install succesfully“).

Die zuvor beschriebenen Installationsschritte bewirken, dass bei jedem Neustart von Tails die benötigten Programme für OffRoad neu installiert werden. Dasselbe trifft auch auf das Dotfiles-Verzeichnis zu. Alles, was ihr dort hinterlegt, wird nach einem Neustart erneut in das Verzeichnis kopiert.
Ihr hinterlasst daher keine Spuren wie Kartenmarkierungen oder eine Bewegunghistorie (außer den Karten selbst).

Wir empfehlen euch trotzdem, die Karten nach der zuvor beschriebenen Installation ausschließlich offline zu nutzen.

Ohne persistenten Speicher

Nachdem ihr die Karte durch ein Anklicken mit der rechten Maustaste auf `Hier entpacken` dekomprimiert habt, müsst ihr sie in euer Benutzer*innenverzeichnis in den Ordner `/home/amnesia/.OffRoad/maps` verschieben.

Das Verzeichnis `/home/amnesia/.OffRoad/maps` könnt ihr über das Menü Orte ► Dateien mit der rechten Maustaste auf `Neuer Ordner`) anlegen. Im Drop-Down-Menü des Datei-Fensters findet ihr die Option `Verborgene Dateien anzeigen`, mit der das Verzeichnis sichtbar wird. Alternativ kann die Karte auch über Systemwerkzeuge ► Terminal dort hinbewegt werden:

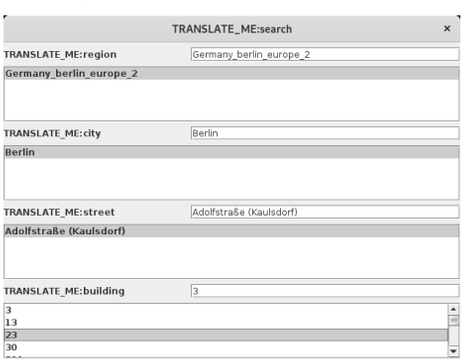
```
mkdir -p /home/amnesia/.OffRoad/maps
rsync -av /home/amnesia/Tor\ Browser/map_berlin.obf \
 /home/amnesia/.OffRoad/maps
```

Wir empfehlen euch, die Karten nach einer erfolgreichen Installation ausschließlich offline zu nutzen und auf sämtliche Netzwerkaktivitäten zu verzichten.

Zum Starten von OffRoad muss folgender Befehl im Terminal eingegeben werden (mit einem Leerzeichen hinter `-jar`):

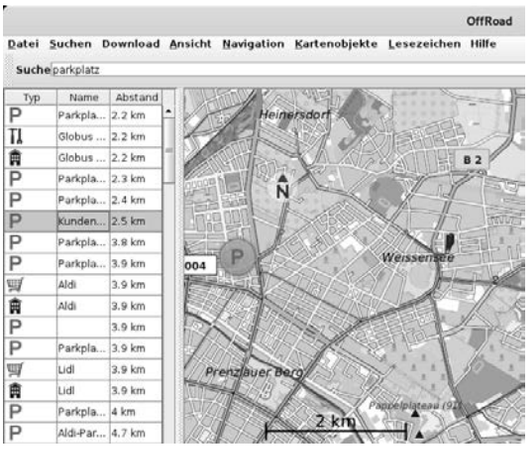
```
java -jar [OffRoad.jar ins Terminal ziehen + Return]
```

Nach dem Start des Programms werdet ihr nach einem Download einer Übersichtskarte der Welt gefragt, was ihr ablehnt. Um die zuvor kopierte Karte sehen zu können, müsst ihr das Programm-Fenster vergrößern und über das Menü Suchen ► Finden nach einer beliebigen Strasse suchen (Doppelklick auf die Hausnummer)[83].



Dadurch sollte die Karte sichtbar werden. Mit der Tastenkombination Strg + + oder Strg + - kann der Kartenbereich vergrößert oder verkleinert werden. Über das Eingabefeld im oberen Bereich des Programms kann die Karte nach unzähligen dort eingetragenen Metadaten durchsucht werden, die bei erfolgreicher Suche auf der linken Seite aufgelistet werden. Durch einen Doppelklick auf eines der gelisteten Ergebnisse wechselt die Karte in diesen Bereich.

82 Um unsichtbare Verzeichnisse einzublenden, muss „Verborgene Dateien anzeigen“ im Drop-Down-Menü des Datei-Fensters ausgewählt werden.
83 Falls ihr mehrere Karten in den Dotfiles-Ordner kopiert habt, müsst ihr die gewünschte Karte und Stadt für die Suche davor auswählen.



Aktionsfotos bearbeiten mit Gimp

Bild öffnen

Ihr startet das Grafik-Programm *Gimp* unter Anwendungen ▶ Grafik ▶ GNU Image Manipulation Program und wählt euer Bild unter Datei ▶ Öffnen aus.

Bild skalieren

Heutige Digital-Kameras machen Fotos mit weit über zehn Megapixel Bildauflösung. Das kann für Plakate und Broschüren sinnvoll sein, ist aber für eine digitale Veröffentlichung z.B. bei *indymedia* oder eine Verschickung per Mail unnötig groß. Um die Dateigröße des Bildes zu reduzieren, wählt ihr in Gimp die Funktion Bild ▶ Bild skalieren. Der Dialog zur Einstellung einer neuen Breite und Höhe ist selbsterklärend. Wenn ihr Breite und Höhe „verkettet“, ändert sich das Seitenverhältnis des Bildes nicht. Eine Breite von z.B. 800 Pixel für ein Bild im Querformat ist für die meisten Internetzwecke ausreichend. Ihr beendet den Dialog mit dem Button Skalieren.

Bild-Bereiche unkenntlich machen

Ihr wählt im „Werkzeugkasten“ das Werkzeug „Rechteckige Auswahl“ und markiert einen Bereich, den ihr unkenntlich machen wollt. Der Bereich ist nun von einer laufenden gestrichelten Linie gerahmt. Ihr wählt Filter ▶ Weichzeichnen ▶ Verpixeln als eine Möglichkeit, den Informationsgehalt dieses Bildbereichs tatsächlich zu reduzieren. In der Vorschau seht ihr das verpixelte Ergebnis.

Ihr könnt die Pixelgröße einstellen und danach mit OK bestätigen. Mit der Wiederholung dieser Prozedur könnt ihr viele Bereiche (in denen z.B. Gesichter oder andere identifizierende Merkmale wie z.B. Tattoos oder Schuhe zu sehen sind) unkenntlich machen.

Wenn ihr mit manchen Resultaten nicht zufrieden seid, lassen sich die Operationen Schritt für Schritt rückgängig machen mit der Funktion Bearbeiten ▶ Rückgängig.

Bild speichern

Dazu wählt ihr in Gimp die Funktion Datei ▶ Exportieren und gebt einen Namen für das zu speichernde Bild an (zum Beispiel *1.jpg*). Abhängig vom so gewählten Dateiformat (hier jpg) könnt ihr in diesem Dialogfenster noch die Qualität des zu speichernden Bildes beeinflussen (100 bedeutet keine Kompression, also hohe Detailgenauigkeit, aber auch größere Datei). Zum Abschluss klickt ihr auf Exportieren.

Beachtet, dass das bearbeitete Bild wie im Kapitel „Metadaten entfernen“ beschrieben bereinigt werden muss, um Metadaten wie z.B. die Kamera-Seriennummer und unverpixelte Vorschaubildchen zu entfernen!

Drucken

Zum Drucken den Drucker per USB-Kabel anschließen, anschalten und danach den Druckmanager unter Anwendungen ▶ Systemwerkzeuge ▶ Einstellungen ▶ Drucker starten. Dort + bzw. „Neuen Drucker hinzufügen“ auswählen und den (hoffentlich erkannten) Druckernamen mit „Hinzufügen“ bestätigen.

Nun müsst ihr in der (lokal vorhandenen) Datenbank einen Druckertreiber finden. Dazu wählt ihr zunächst den Druckerhersteller und dann ein Modell, was eurem möglichst ähnlich ist. Häufig ist es ausreichend, das nächstältere Modell samt dem vom Manager empfohlenen Treiber auszuwählen, falls ihr euer Druckermodell nicht findet. Ihr bestätigt die Wahl abschließend mit „Anwenden“ und könnt eine „Testseite drucken“.

Hinweis: Ein eventuell schon vor der Druckerinstallation geöffnetes Programm (z.B. LibreOffice) muss erneut gestartet werden, um den „neuen“ Drucker zu erkennen und für den Druck anzubieten.

Wer mehrfach den gleichen Drucker benutzt, kann sich die Installation am Anfang einer jeden Tails-Sitzung erleichtern, in dem er im Netz nach einem passenden Linux-Druckertreiber sucht. Die so heruntergeladene *.ppd-Datei* kann auf einem Datenstick dauerhaft gespeichert und anstelle der Suche in der lokalen Treiber-Datenbank angegeben werden.

Beachtet, dass ein Ausdruck über das spezifische Druckbild bei einer forensischen Untersuchung eindeutig einem einzelnen Drucker (nicht nur einem Druckertyp!) zugeordnet werden kann. Manche Farblaserdrucker hinterlassen zur Identifikation eine Kennung aus Einzelpunkten, die mit dem Auge nicht zu identifizieren ist[84]. Es handelt sich hierbei um unsichtbare Wasserzeichen, die einen Drucker eindeutig identifizieren können *(machine identification code (mic))*.

Das bedeutet für eine sensible Print-Veröffentlichung, dass ihr preiswerte „Wegwerf“-Schwarzweiß-Drucker benutzen müsst. Wer durch anschließendes mehrfaches Kopieren (mit unterschiedlichen Kontraststufen) das Druckbild des Druckers verschleiern will, sollte beachten, dass fast alle Copy-Shops digitale Kopierer einsetzen, die mit einer großen Festplattenkapazität auch noch nach Wochen auf die einzelnen Druckaufträge inklusive exaktem Datum zugreifen können.

84 https://eff.org/issues/printers
85 Siehe Kapitel „Aktionsfotos bearbeiten“

Scannen

Zum Scannen den Scanner per USB-Kabel anschließen, anschalten und danach das Programm *Simple Scan* unter Anwendungen ▶ Grafik ▶ Simple Scan starten. Einfache (einseitige) Scanner funktionieren oft erst dann korrekt, wenn ihr im Programm unter Dokument die Einstellungen ▶ Scan Side auf „Front“ setzt. Falls gewünscht, könnt ihr die Scan-Auflösung für Fotos bzw. Text verändern. Dann könnt ihr die Einstellungen „schließen“. Achtet auch hier auf die Zuordenbarkeit zwischen Scan und Scanner.

Jetzt könnt ihr im Programm Dokument ▶ Scannen ▶ Text/Foto auswählen, um anschließend mit dem Button Scannen eine Seite zu scannen. Falls die Einstellung „Text“ zu keinem Ergebnis führt, schaltet auf die Einstellung „Foto“ um. Ihr könnt die Seite(n) noch drehen oder auf einen bestimmten Bereich zuschneiden, bevor ihr das Dokument mit „Speichern“ sichert.

Für eine weiterführende Nachbearbeitung des abgespeicherten Scans empfehlen wir das eben erwähnte Programm *Gimp*[85].

Beamer benutzen

Wenn ihr in eurer Gruppe beispielsweise Dokumente gemeinsam diskutieren wollt, kann ein Beamer helfen. Falls euer Computer den Beamer nicht automatisch erkennt, müsst ihr in folgender Reihenfolge vorgehen: Den Beamer mit dem Computer verbinden, z.B. via VGA-Kabel  oder HDMI-Kabel  , einschalten und dann in Tails unter Anwendungen ▶ Systemwerkzeuge ▶ Einstellungen ▶ Bildschirme die Option „Gleiches Bild auf allen Bildschirmen“ auswählen und bestätigen.

Falls euer Rechner den Beamer immer noch nicht als externen „Bildschirm“ erkennt, könnt ihr euren Rechner mit einer der Funktionstasten[86] dazu bringen, das Bild auch an den VGA-Ausgang zu schicken. Mehrmaliges Drücken dieser Funktionstaste schaltet bei vielen Modellen zwischen den drei Einstellungen „nur Laptop-Bildschirm“, „nur Beamer“ oder „beide“ um.

Daten und Metadaten löschen

Es ist leider sehr kompliziert, einmal erzeugte Daten „sicher“ loszuwerden. Alle wissen vermutlich, dass es mit dem normalen Löschen einer Datei nicht getan ist – die Datei bleibt vollständig erhalten, ihr Name wird lediglich aus der Liste verfügbarer Dateien auf diesem Datenträger ausgetragen. Der belegte Platz wird freigegeben, aber nicht überschrieben.

Leider führen auch Software-Techniken, die einzelne Bereiche eines Datenträgers mit verschiedenen Datenmustern mehrfach überschreiben, zum Beispiel bei USB-Sticks nicht zum gewünschten Ergebnis!

Für Ungeduldige auch hier gleich das Ergebnis unserer Ausführungen vorweg:

Die sicherste Variante ist, Daten nur (temporär) im Arbeitsspeicher zu halten!
Wenn Daten dauerhaft gesichert werden müssen, dann muss es ***a****) ein externer Datenträger sein, und dieser muss* ***b****) komplett verschlüsselt sein. Ein sicher verschlüsselter Datenträger ist der beste Schutz gegen (lesbare) Überreste.*
Löschprogramme wie z.B. wipe oder srm funktionieren auf Flash-Medien (USB-Sticks, SD-Karten, SSD, etc.) prinzipbedingt nicht zuverlässig. Selbst, wenn das Medium als Ganzes überschrieben wird, können Reste zurückbleiben. Deshalb ***c****) zerstören wir Medien mit hochsensiblen Inhalten zusätzlich.*

Probleme beim Überschreiben von Datenträgern

Physikalische Eigenschaften der Datenträger erlauben es, den ehemaligen Inhalt einer überschriebenen Speicherstelle zu rekonstruieren. Wir ersparen euch hier Details und erläutern lieber, warum es dabei weniger um die Anzahl der Überschreibvorgänge geht!

Bei magnetischen Festplatten gibt es das Problem, dass defekte Sektoren (Speicherbereiche) von der Festplattensteuerung aussortiert und ehemals dort gespeicherte Daten umkopiert werden. Ein Überschreib-Programm zum „sicheren“ Löschen hat dann auch keinen Zugriff mehr auf diese defekten Sektoren. Im Forensik-Labor hingegen lassen sich diese Bereiche auslesen – mit unter Umständen fatalen Folgen für euch.

Bei sogenannten Flash-Speichermedien wie z.B. USB-Sticks, SD-Karten, CompactFlash-Karten und die neueren SSD-Festplatten (Solid-State-Disks) ist dieses Problem des internen Umkopierens (außerhalb der Kontrolle der Anwender*in) wegen der besonders hohen Fehleranfälligkeit des Speichers kein Ausnahmefall, sondern die Regel[87]. Eine Überschreibeprozedur zum „sicheren“ *Löschen einzelner Dateien* „erwischt“ dann nur eine von mehreren Kopien. Eine Forschungsarbeit aus dem Jahr 2011 bescheinigt sämtlichen Software-Löschtechniken, dass sie angewendet auf Flash-Speicher selbst beim Überschreiben des gesamten Speichermediums nur unzuverlässig funktionieren[88]. Das sichere Löschen von einzelnen Dateien hingegen gelang mit keinem der getesteten Programme! Die Situation ist seitdem unverändert.

Mit diesen Einschränkungen (als dringliche Warnung) zeigen wir euch, wie ihr bei Tails die Löschroutine *wipe* **zum Überschreiben des gesamten Datenträgers** nutzen könnt:

1. Datenträger im Dateimanager auswählen: Orte ▶ (Name des Datenträgers)
2. Im Dateimanager bei Ansicht ▶ Verborgene Dateien anzeigen ein Häkchen setzen
3. Alle Ordner und Dateien markieren
4. (rechter Mausklick) ▶ Sicher löschen (Die Dateien sind für euch unwiderruflich weg!)

---

86 Welche Funktionstaste zum externen Bild umschaltet, hängt leider vom Rechner-Hersteller ab, ist aber als Symbol auf der Tastatur erkennbar.

87 Zur ausgewogenen Belastung der Speicherstellen werden Bereiche ständig umkopiert. Mehr als zehn versteckte Kopien einer Datei sind keine Seltenheit bei Flash-Speichern.

88 Michael Weie et. al.: „Reliably Erasing Data From Flash-Based Solid State Drives“ 9th USENIX Conference on File and Storage Technologies. „For sanitizing entire disks, built-in sanitize commands are effective when implemented correctly, and software techniques work most, but not all, of the time. We found that none of the available software techniques for sanitizing individual files were effective.“ https://www.usenix.org/legacy/events/fast11/tech/full_papers/Wei.pdf

89 Wenn ihr in ein *Terminal* den Befehl sync eingebt und mit der Enter-Taste bestätigt, dann werden alle zu schreibenden Daten weggeschrieben. Wenn das sync-Programm endet, ist der Überschreibvorgang abgeschlossen.

5. Im (danach leeren) Feld dieses Datenträgers: (rechter Mausklick) ► Sicheres Löschen des verfügbaren Fesplattenspeichers
6. Drei Durchläufe bei zweifachem Überschreiben (also sechsfach) genügen bei neueren Datenträgern.
7. Warten – je nach Größe des Datenträgers einige Minuten bis viele Stunden[89].

Datenträger vernichten

Gerade wegen der Unzulänglichkeit vieler Software-Löschtechniken und der weitgehenden Möglichkeiten von forensischer Daten-Wiederherstellung solltet ihr sensible Datenträger lieber zusätzlich zerstören. Auch das ist leider problematischer als gedacht - optische Medien sind am einfachsten zu zerstören.

Magnetische Festplatten sind sehr schwer zu zerstören. Ihr könnt sie nicht einfach ins Feuer werfen. Die Temperaturen, die ihr damit an den datentragenden Scheiben (Aluminium mit einem Schmelzpunkt von 660°C oder Glas bei >1000°C) erreicht, ermöglichen gerade mal eine leichte Verformung. Ein Aufschrauben des Gehäuses und der Ausbau der Scheiben ist mindestens notwendig, um mit einem Lötbrenner an der Scheibe selbst höhere Temperaturen zu erzeugen. Ein Campinggas-Lötbrenner reicht dazu jedoch nicht aus. Ihr benötigt hierfür *Thermit*, ein Pulver, das in einer aus Ziegelsteinen improvisierten „Brennkammer“ 2300°C heiß brennt und die Scheiben verflüssigt. Die Handhabung erfordert allerdings einige Vorsichtsmaßnahmen![90]. Als eine Alternative könnt ihr auch Schmiedeöfen verwenden, die eine Temperatur von bis zu 1250°C erreichen. Wem/welcher das zu viel Aufwand ist, der sollte zumindest die ausgebauten Scheiben der Festplatte in kleine Stücke brechen und an mehreren Orten verteilt entsorgen (Achtung - Splittergefahr!). Wegen der hohen Datendichte könnten Forensiker*innen darauf jedoch noch reichlich Datenfragmente finden! Alternativ könnt ihr die Oberfläche der einzelnen Scheiben mit einer Bohrmaschine und Drahtbürstenaufsatz abschleifen.

Flash-Speicher (USB-Sticks, SSD, SD-Karten, ...) lassen sich ebenfalls nur unvollständig zerstören. Mit zwei Zangen könnt ihr die Platine aus dem Gehäuse herausbrechen, um dann die Speicherchips samt Platine einzeln in Stücke zu brechen und in die Flamme eines Campinggas-Lötbrenners zu halten. Ihr erreicht auch hierbei nur eine partielle Zersetzung des Transistor-Materials. Vorsicht – Atemschutz oder Abstand! Die Dämpfe sind ungesund.

Optische Medien (CD, DVD, BlueRay) lassen sich mit genügend großer Hitze vollständig und unwiderruflich zerstören. Das Trägermaterial Polycarbonat schmilzt bei 230°C (Deformation). Die Zersetzung gelingt bei 400°C und bei 520°C brennt es. Ein Campinggas-Lötbrenner reicht aus, um die Scheiben aus Polycarbonat, einer dünnen Aluminiumschicht und einer Lackschicht zu Klump zu schmelzen oder gar zu verbrennen. Vorsicht – Atemschutz oder Abstand! Die Dämpfe sind ungesund. Eine Alternative ist die Zerstörung des Datenträgers in der Mikrowelle (wenige Sekunden auf höchster Stufe).

Metadaten entfernen

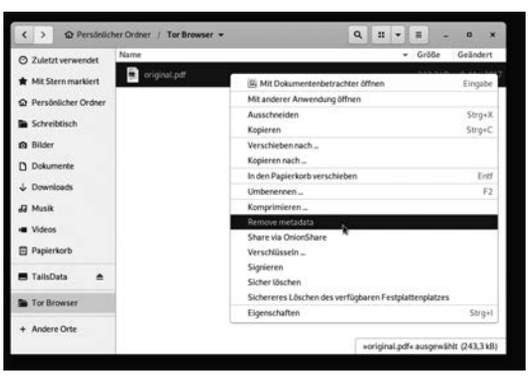
Die meisten von euch kennen das Problem bei Fotos von Aktionen. Bevor diese veröffentlicht werden können, müssen nicht nur Gesichter unkenntlich gemacht werden (hierzu könnt ihr in Tails das Programm gimp verwenden), sondern auch die sogenannten Metadaten entfernt werden, die im Bild mit abgelegt sind und die Kamera, mit der das Bild aufgenommen wurde, eindeutig identifizieren. Neben der Uhrzeit und der Seriennummer sind bei einigen neueren Kameras (insbesondere Smartphones) sogar die GPS-Koordinaten in diesen sogenannten *EXIF*-Daten abgespeichert. Ein sogenanntes *Thumbnail* (Vorschau-Foto im Kleinformat) kann Bilddetails preisgeben, die ihr im eigentlichen Bild verpixelt oder anderweitig unkenntlich gemacht habt. Diese Metadaten müssen entfernt werden! Das gelingt bei Fotos und Grafiken sehr gut.

Leider tragen z.B. auch LibreOffice- bzw. Word-Dokumente und PDF-Dateien Metadaten in sich. Anwender*innenname, Computer, Schriftarten, Namen und Verzeichnisorte eingebundener Bilder usw. lassen Rückschlüsse auf euch bzw. euren Rechner zu. Bei diesen „Container-Formaten“ (möglicherweise sind in einer PDF-Datei weitere PDFs oder Bild- und Video-Dateien verschachtelt, oder sogenannte „Wasserzeichen“ enthalten) ist ein vollständiges Entfernen ALLER Metadaten schwierig. Grundsätzlich gilt:

Je größer das Sicherheitsbedürfnis, desto simpler sollte das Datenformat sein, das ihr für die Übermittlung wählt. Reines Textformat verrät am wenigsten über den Rechner, an dem der Text erstellt wurde.

Das Metadata Anonymisation Toolkit (MAT2) kann mit der zuvor genannten Einschränkung folgende Datentypen säubern: GIF-, PNG-, TIFF- und JPEG-Bilder, HTML-Dateien, LibreOffice- und Microsoft Office-Dokumente, MPEG (MP2/MP3/MP4), FLAC und OGG (Audio-) als auch MP4-, WMV- und AVI-(Video-)Dateien, ZIP- und TAR-Archivdateien, sowie EPUB- und torrent-Dateien.

MAT2 ist mittlerweile in den Dateimanager integriert. Die im Dateimanager angewählten Dateien lassen sich per Rechtsklick und der Auswahl „Metadaten entfernen“ bzw. „remove metadata“ bereinigen. Die gesäuberte Datei wird unter dem Namen der Originaldatei mit dem Zusatz „.cleaned“ abgelegt. Über das Terminal könnt ihr dieses Werkzeug auch auf ganze Ordner anwenden. Bedenkt, dass die ursprüngliche Originaldatei auch nach dem Löschen auf diesem Datenträger immer noch rekonstruierbar ist!



Hinweis: Um Metadaten aus PDF-Dateien so zuverlässig wie möglich zu entfernen, verwandelt MAT2 seit neuem komplexere PDF-Dateien in ein PDF, bei dem alle einzelnen Seiten auf Bildpunktdateien (Pixel-Bilder) reduziert werden. Der Vorteil ist: So lassen sich die meisten versteckten Metadaten sicher entfernen. Der Nachteil ist: Die Datei wird in der Regel viermal

90 http://frank.geekheim.de/?p=2423

so groß und Text lässt sich nicht mehr markieren und weiterverarbeiten. Die so gesäuberte Datei ist unter Umständen zu groß für einen Mail-Anhang oder die Veröffentlichung auf manchen Plattformen. Nur wer hier weniger Sicherheit verantworten kann, hat die Möglichkeit, MAT2 über ein Terminal mit dem Zusatz „-L“ aufzurufen:

```
mat2 -L dateiname.pdf
```

Die daraufhin im gleichen Ordner erzeugte Datei „dateiname.cleaned.pdf“ ist ähnlich groß wie die ungesäuberte Originaldatei und der Text lässt sich weiterhin anwählen; aber mitunter sind nicht alle Metadaten entfernt worden!

Daten verschlüsselt aufbewahren

In diesem Kapitel werden wir erläutern, wie ihr verschlüsselte Partitionen auf Datenträgern anlegen und bei Tails einbinden könnt. Dabei gehen wir sowohl auf die linuxübliche Variante mit *dmcrypt* als auch auf *Truecrypt* und *Veracrypt* ein. Es gibt bei der Nutzung von Tails auf einem USB-Stick die Möglichkeit, ein sogenanntes „Persistent Volume“ zu verwenden. Gemeint ist damit ein verschlüsselter Speicherbereich auf dem Tails-Stick. Im Kapitel „Persistenz“ gehen wir gesondert darauf ein.

Datenträger werden nicht automatisch „geöffnet“

Anders, als ihr es gewohnt seid, wird ein eingelegter/eingesteckter externer Datenträger nicht automatisch geöffnet und damit verfügbar gemacht. Ihr sollt damit *absichtlich* die Kontrolle über alle Datenorte behalten, um nicht aus Versehen doch etwas auf die Festplatte zu speichern!

> *Datenträger werden erst über das aktive Anwählen (linker Mausklick) unter* Orte ► Rechner *in das System eingebunden. Vorher können von/auf ihm keine Daten gelesen/gespeichert werden.*
> *Bevor ihr den Datenträger nach fertiger Arbeit abziehen könnt, müsst ihr ihn unter* Orte ► Rechner *mit der rechten Maustaste anklicken und dann „Laufwerk sicher entfernen“ wählen!*

Wie bereits erwähnt, speichert *Tails* nichts auf eurer Festplatte, es sei denn, ihr verlangt dies explizit durch die Auswahl der Festplatte im Menü Orte ► [Name der Festplatte]. Nach dem Ausschalten des Rechners gehen alle Daten verloren. Ihr solltet daher einen **Daten-USB-Stick** zur Aufbewahrung eurer Daten nutzen. Aus Sicherheitsgründen sollte dieser *nicht identisch mit dem* (möglichst schreibgeschützten) *Tails-Betriebssystem-Stick* sein! Tails ermöglicht es euch, eine persistente Partition anzulegen, die sich auch dafür eignen würde.

> *Wir empfehlen, dort nur die Softwarekonfigurationen abzulegen (E-Mail-Accounts, Cryptokeys, etc.) und die Recherchearbeit (oder was auch immer) davon getrennt zu halten.*

Da es empfehlenswert ist, alle Daten verschlüsselt aufzubewahren, legen wir auf einem neuen Daten-USB-Stick eine *verschlüsselte Partition* an. Tails nutzt die Linux-Verschlüsselungssoftware *dm-crypt*. Ihr könnt die Daten dann auf allen Linux-Betriebssystemen entschlüsseln. **Ein Datenaustausch mit Windows- oder MacOSX Betriebssystemen ist damit allerdings nicht möglich!**

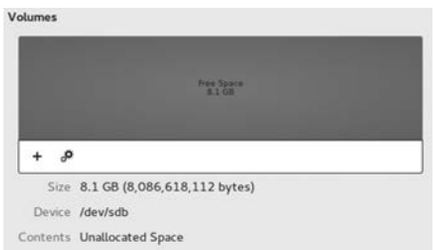
Verschlüsselte Partition auf einem Datenträger anlegen

Laufwerksverwaltung starten Anwendungen ► Hilfsprogramme ► Laufwerke Die Laufwerksverwaltung listet alle derzeit verfügbaren Laufwerke und Datenträger auf.

Daten-USB-Stick identifizieren Wenn ihr den neu zu verschlüsselnden USB-Stick jetzt einsteckt, sollte ein neues „Gerät“ in der Liste auftauchen. Wenn ihr draufklickt, seht ihr die Details des Datenträgers. Überprüft genau, ob ihr den richtigen Datenträger ausgewählt habt (blau hinterlegt) - ob also die Beschreibung (Marke, Name, Größe) mit eurem Gerät übereinstimmt! Eine Verwechslung mit einem anderen Datenträger wird die Daten auf diesem löschen.

Platz schaffen Nach dem Auswählen des USB-Sticks erscheint auf der rechten Seite eine Darstellung der Partitionen. Wenn dort kein „Freier Platz“ mehr angezeigt wird, müsst ihr bestehende Partitionen löschen. Dazu wählt ihr die betroffene Partition aus, klickt auf den „Minus“-Button und bestätigt das Löschen. Wir empfehlen, alle Partitionen zu löschen und keinen Mischbetrieb von verschlüsselten und unverschlüsselten Daten auf dem gleichen Stick zu versuchen, um Verwechslungen zu vermeiden.

Eine verschlüsselte Partition erzeugen Jetzt zeigt das Fenster einen leeren Datenträger.



Klickt nun auf `+`, um eine neue Partition zu erstellen. Es erscheint ein Dialogfenster „Partition erstellen“, in dem ihr die neue Partition konfigurieren könnt.

Größe: Das ist der Schieberegler ganz oben, sowie die Texteingabefelder darunter. Anfangs ist die Größe gleich der Größe des freien Platzes. Ihr könnt die Größe der zu verschlüsselnden Partition auch verkleinern, damit noch andere Partitionen auf dem USB-Stick Platz finden. Wir raten euch jedoch, sensible Datenprojekte nicht mit anderen Daten auf dem gleichen Stick zu speichern.

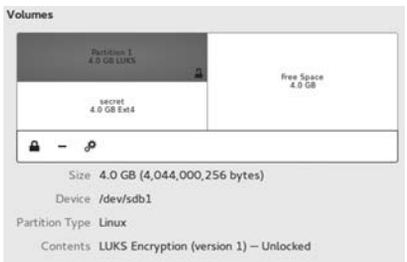
Löschen: Bevor die neue Partition im freien Platz angelegt wird, kann dieser überschrieben werden. Das solltet ihr unbedingt machen, aber im Hinterkopf behalten, dass dieses Überschreiben sehr wahrscheinlich nicht vollständig ist (siehe Kapitel „Daten löschen“). Wenn ihr sicher gehen wollt, verwendet einen unbenutzten Stick.

Typ: Hier wählt ihr „Verschlüsselt, kompatibel mit Linux-Systemen (LUKS+Ext4)“.

[91] Hinweise zu einem sicheren Passwort im Anhang.

Name: Hier könnt ihr einen Namen für den Datenträger wählen, um ihn später identifizieren zu können. Beachtet: Dieser Name ist für alle lesbar!

Kennwort: Wählt ein starkes Passwort. Das Passwort[91] sollte komplex genug sein, damit es nicht geknackt werden kann. Aber ihr müsst es euch auch merken können! Dann auf Erstellen klicken. Dieser Prozess kann eine Weile dauern. Wenn die Fortschrittsanzeige erlischt (das Rädchen sich nicht mehr dreht), seid ihr fertig.



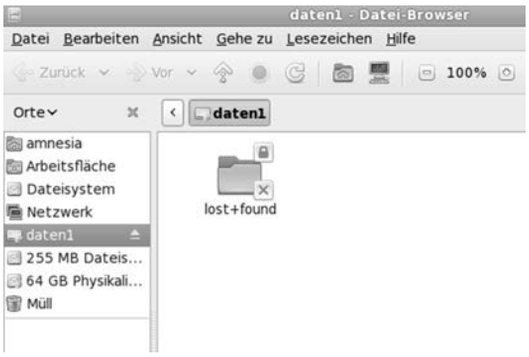
Weiterführende Informationen sind auf der Webseite vom Tailsprojekt zu finden: `https://tails.boum.org/doc/encryption_and_privacy/encrypted_volumes/index.en.html`

Verschlüsselte Partition öffnen

Wenn ihr einen verschlüsselten USB-Stick einsteckt, wird er (wie alle Datenträger) in Tails *nicht automatisch* geöffnet, sondern erst, wenn ihr ihn im Menü *Orte* anwählt.

Ihr werdet aufgefordert, das Passwort einzugeben:

Wenn es das richtige Passwort ist, dann wird die Partition im Datei-Manager wie ein Datenträger mit dem von euch gewählten Namen angezeigt. Ihr könnt nun Dateien hinein kopieren oder sonstige Dateioperationen durchführen.



Bevor ihr den Datenträger nach fertiger Arbeit abziehen könnt, müsst ihr ihn unter Orte ▶ Rechner mit der *rechten Maustaste* anklicken und dann *Auswerfen* wählen!

Bedenken gegen TrueCrypt

TrueCrypt ist eine Software, die verschlüsselte Partitionen ermöglicht und auf Windows, MacOSX und Linux läuft, was den Datenaustausch sehr vereinfacht. Die Arbeit an TrueCrypt ist aber eingestellt worden. Die im Mai 2014 erschienene letzte *TrueCrypt*-Version wird von den Entwickler*innen selbst als **nicht sicher(!)** eingestuft und erlaubt nur noch das Entschlüsseln bereits vorhandener *TrueCrypt*-Container.

Um nicht in die missliche Lage zu kommen, irgendwann die alten Datenträger nicht mehr entschlüsseln zu können, raten wir, zu sichernde TrueCrypt-verschlüsselte Inhalte zu entschlüsseln und umzukopieren auf dm-crypt-verschlüsselte Datenträger (erster Abschnitt dieses Kapitels).

Veracrypt ist eine Weiterentwicklung von TrueCrypt und hatte anfangs von dort ein paar Sicherheitsprobleme geerbt. Inzwischen sind aber alle bekannten Probleme behoben. Veracrypt ist noch nicht Bestandteil von *Tails*, wir erwähnen es, weil es das einzige uns bekannte Tool ist, das betriebssystemübergreifend einsetzbar ist. Mit Tails ist das Arbeiten mit von Veracrypt erzeugten Containern und verschlüsselten Laufwerken aber möglich (siehe nächstes Kapitel).

TrueCrypt entschlüsseln

Solltet ihr trotz der zuvor dargelegten Bedenken TrueCrypt-Partitionen (Volumes) oder -Dateien (Container) zum betriebssystemübergreifenden Datenaustausch verwenden, bietet dm-crypt nur noch die Möglichkeit zum **Lesen** der Partition bzw. des Datei-Containers. Dazu gibt es jedoch kein Programm mit einer grafischen Oberfläche. Ihr müsst ein sogenanntes *Root-Terminal* über Anwendungen ▶ Systemwerkzeuge ▶ Root-Terminal öffnen (dazu müsst ihr beim Tails-Startbildschirm ein Passwort festlegen) und dann einige Linux-Kommandos eingeben.

Identifikation von externen Datenträgern

Jeder externe Datenträger *(Festplatte oder USB-Stick)* wird von der Laufwerksverwaltung des Betriebssystems (Linux, Windows und auch MacOSX) identifiziert und registriert. Die Nutzung eines solchen Datenträgers unter Tails hinterlässt KEINE Spuren, da alle Protokoll-Dateien beim Ausschalten des Rechners aus dem (flüchtigen) Arbeitsspeicher verschwinden und dieser zusätzlich mit Zufallszahlen überschrieben wird. Aber:

92 Umgekehrt gilt das nicht: Ein (nicht manipulierter) USB-Stick merkt sich nicht, in welche Rechner er gesteckt wurde.

> *Wenn ihr einen Datenträger (auch) an einem Rechner OHNE Tails benutzt, dann besteht die Gefahr, dass sich dieser Rechner über eine eindeutige Identifikationsnummer an diesen Datenträger „erinnert“.*

Bei einer Beschlagnahmung des Rechners bzw. einer feindlichen Übernahme lässt sich damit nachvollziehen, dass und wann z.B. ein bestimmter USB-Stick zum Einsatz kam[92]. Die eindeutig identifizierbaren Spuren in den System-Protokolldateien „verbinden“ also euren USB-Stick mit allen Rechnern, in denen er jemals gesteckt hat. Wir erzählen das, weil wir damit deutlich machen möchten:

> *Datenträger, die zum Speichern eines sensiblen Dokuments benutzt wurden, müssen (z.B. nach dessen Veröffentlichung) vollständig gelöscht und vernichtet werden.*

Wie das geht, erfahrt ihr im Kapitel „Daten und Metadaten löschen“.

VeraCrypt

Seit der Tailsversion 3.9. bietet Tails die Möglichkeit, *VeraCrypt*-Container und Laufwerke zu entschlüsseln. Neue Container anlegen oder Laufwerke initial zu verschlüsseln geht mit Tails **nicht**.

VeraCrypt ist der Nachfolger von TrueCrypt. Es erlaubt das Erstellen und Nutzen von verschlüsselten Containern und Laufwerken sowohl mit MacOS, Windows, als auch Linux. Es eignet sich damit also zum verschlüsselten Transport von Daten zwischen unterschiedlichen Betriebssystemen.

Container und Laufwerke

VeraCrypt erlaubt das Speichern von Daten in Containern oder auf Laufwerken. Ein Container ist eine große Datei, in der ihr mehrere Dateien verschlüsselt speichern könnt. Ein Laufwerk ist z.B. ein USB-Stick mit einer durchgehenden Partition. Wir behandeln hier nur das Benutzen von Containern. Für alles Weitere empfehlen wir die Dokumentation des Tails Projekt (allerdings auf Englisch)[93].

Voraussetzungen:

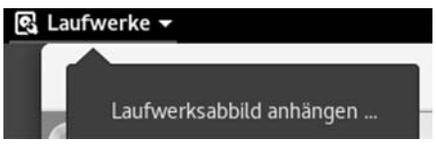
Zum Entschlüsseln eines VeraCrypt-Containers braucht ihr natürlich die nötigen Daten. Ein Container kann entweder mit einem Passwort oder aber auch (zusätzlich oder alleine) mit einem „Keyfile“ entschlüsselt werden. Ein Keyfile ist eine bestimmte Datei (z.B. Musik oder Bild), die zum Entschlüsseln benötigt wird.

Entschlüsseln eines Containers ohne Keyfile

1. Wählt Anwendungen ▶ Hilfsprogramme ▶ VeraCrypt-Container entsperren.
2. Klickt `Add` und wählt die Datei des Containers aus.
3. Gebt die Passphrase und andere Parameter ein.
4. VeraCrypt-Container entsperren - entsperrt nun euren Container.
5. Klickt nun `Öffnen`, um den Container im Dateibrowser zu öffnen.

Mit Keyfile

1. Geht zu Anwendungen ▶ Hilfsprogramme ▶ Laufwerke.
2. Wählt nun „Laufwerksabbild anhängen“.



3. Es erscheint der Dialog „Laufwerksabbild zum Einbinden auswählen“. Ihr müsst nun:
   - Unten links in der Checkbox „Schreibgeschütztes Loop-Gerät einrichten“ das Häckchen entfernen.
   - Wählt „Alle Dateien“ im Dateiformat „Filter Dialog“ in der rechten unteren Ecke.
   - Wählt nun die Datei des VeraCrypt-Containers aus und klickt `Einbinden` oben rechts.
4. Im linken Teil des Fensters könnt ihr jetzt das neue „Loop-Device“ auswählen, welches zu eurem Container gehört. Achtet dabei auf die kursiv geschriebene Beschreibung der Laufwerke. Euer Laufwerk sollte als „verschlüsselt“ markiert sein.
5. Klickt auf das Schloss-Symbol im rechten Teil des Fensters.
6. Gebt nun eure Parameter für das Entsperren des Containers ein. Hier wählt ihr auch das Key-File. Klickt nun `Entsperren`.
7. Klickt das Play-Symbol, um euren Container einzuhängen.

File Container schließen

Um einen File Container zu schließen, reicht es, ihn im Dateibrowser auszuwerfen. Hierzu klickt ihr auf den Pfeil neben dem Laufwerksnamen.

Persistenz

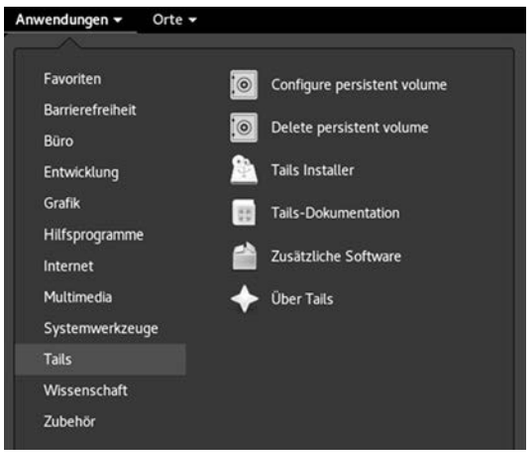
Daten und Einstellungen bleiben auf dem Tails-USB-Stick erhalten.

Bei normaler Benutzung werden alle Daten und alle Einstellungsänderungen (gespeicherte Texte, Bilder, Verschlüsselungskeys, Programmkonfigurationen, etc.) mit dem Runterfahren des Rechners verworfen. Das hat den Vorteil, dass keine individuellen Spuren auf dem Stick verbleiben, schränkt aber die Benutzbarkeit für einige Anwendungen ein. Um dem zu begegnen, gibt es bei der Nutzung von Tails auf einem USB-Stick die Möglichkeit, ein sogenanntes „Persistent Volume“ zu verwenden. Gemeint ist damit ein Speicherbereich auf dem Tails-Stick, welcher eben nicht vergesslich ist. Dieser Speicherbereich wird von dem Platz auf dem USB-Stick abgezweigt, der nicht von der Tails-Installation (etwa 4,3 GB) belegt wird. Je mehr Kapazität also der USB-Stick hat, um so größer fällt das „Persistent Volume“ aus. Achtet darauf, dass der Stick nicht schreibgeschützt ist, solange ihr den persistenten Speicher bearbeitet.

93 https://tails.boum.org/doc/encryption_and_privacy/veracrypt/index.en.html
94 Advanced Encryption Standard

Das „Persistent Volume“ ist verschüsselt und mit einem Passwort abgesichert. Verschlüsselt wird mit dem linuxeigenen Verfahren *dm-crypt*, welches AES[94] verwendet.

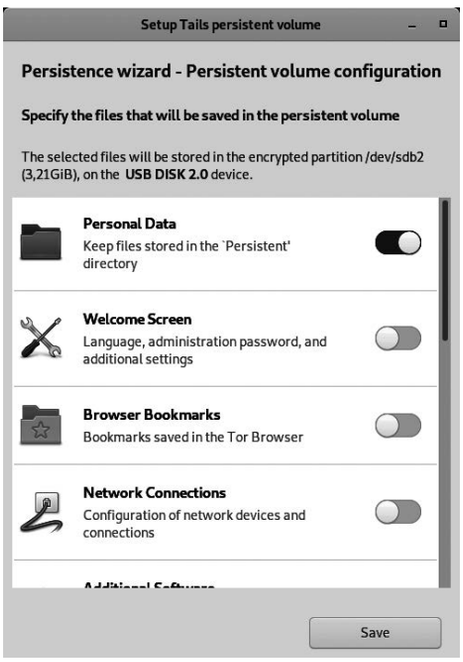
Den Konfigurationsdialog zur Erzeugung eines „Persistent Volume“ findet ihr unter Anwendungen ▶ TailsConfigure persistent volume.



Es erscheint ein Dialog mit Hinweisen und der Abfrage des Passworts. Bitte beachtet die Hinweise in dieser Broschüre zur Auswahl eines starken Passworts.

Nach Eingabe des Passworts wird der persistente Speicher erzeugt, was einen Moment dauern kann. Ist dieser Vorgang abgeschlossen, folgt der Dialog zur Konfiguration desselbigen. Ihr könnt übrigens

diese Konfiguration zu jedem späteren Zeitpunkt anpassen. Eine Erklärung des Konfigurationsdialogs:



Persönliche Daten: In eurem Home-Verzeichnis wird ein Ordner „Persistent“ erzeugt. Dokumente (Bilder, Texte, etc.), die in diesem Ordner liegen, „überleben“ einen Reboot von Tails und sind in der nächsten Sitzung immer noch vorhanden.

GnuPG: Öffentliche und private GPG/PGP-Schlüssel bleiben erhalten.

SSH-Programm: Benutzt man diese Funktion, bleibt Schlüsselmaterial des SSH-Programms erhalten.

Pidgin: Auch das Chat-Programm Pidgin verwendet Schlüssel, um eine sichere Kommunikation zu erlauben. Sollen diese Schlüssel erhalten bleiben, dann aktiviert diesen Punkt. Mehr dazu im Kapitel „Chatten über Tor“.

Thunderbird: Tails bringt ein E-Mailprogramm mit, dessen Einstellungen (Mailserver, Accountdaten, etc.), erhalten bleiben genauso wie heruntergeladene Mails, wenn dieser Punkt aktiviert ist. Mehr dazu im Abschnitt „Mailen mit Persistenz“.

Gnome Schlüsselbund: Tails benutzt einen Keymanager, der dafür sorgt, dass Passwörter, die ihr für einen Dienst eingebt, nicht nochmal eingegeben werden müssen, wenn ihr diesen Dienst ein zweites Mal verwendet – das GPG-Passwort ist ein Beispiel dafür: Einmal eingegeben wird es bei der nächsten verschlüsselten Mail wieder verwendet. Aktiviert ihr diesen Punkt, dann bleiben diese Passwörter auf dem Stick gespeichert. **Wir raten von der Benutzung ausdrücklich ab!**

Netzwerkverbindungen: Habt ihr spezielle Netzwerkkonfigurationen (z.B. UMTS-Sticks), ohne die ihr nicht ins Internet kommt, dann könnt ihr sie durch Aktivierung dieses Punktes haltbar machen.

Browser-Lesezeichen Aktiviert ihr diesen Punkt, dann bleiben die Bookmarks erhalten.

Drucker: Eure Druckerkonfiguration bleibt erhalten.

APT-Pakete: Habt ihr auf dem Tails-Stick eigene Software installiert, so ist diese normalerweise nach einem Reboot verschwunden. Aktiviert ihr diesen Punkt, bleibt sie erhalten.

APT-Listen: APT ist eine oder besser „die“ Softwareverwaltung von Debian, aus welchem Tails besteht. APT pflegt Listen

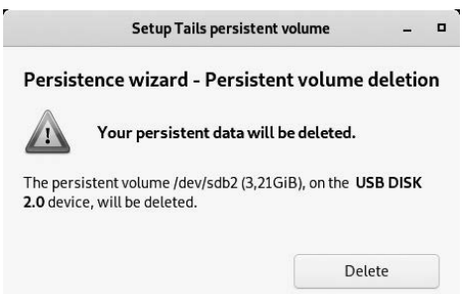
von Softwarepaketen, die installierbar sind, inklusive der Versionsnummern, sodass veraltete Pakete erkannt werden. Wenn ihr eigene Software installiert, dann aktiviert auch diesen Punkt.

Punktdateien: Tails bringt eine Menge Programme mit. Passt ihr deren Konfiguration an, dann werden diese in sogenannten Punktdateien (Dot-Files) gespeichert. Aktiviert diesen Punkt, wenn ihr eure individuellen Anpassungen behalten wollt, und diese nicht durch die oben genannten Punkte bereits abgedeckt sind.

Anpassen und Löschen des Persistent Volume

Solltet ihr euer Persistent Volume löschen wollen, dann wählt Anwendungen ▶ Tails ▶ Delete persistent volume.

Wenn ihr jetzt auf Löschen klickt, sind die Daten in dem Persistent Volume unwiederbringlich weg! Ihr könnt zu einem späteren Zeitpunkt die ganze Prozedur wiederholen, um ein neues Persistent Volume zu erzeugen.



Benutzung des Persistent Volume

Damit ihr das Persistent Volume benutzen könnt, müsst ihr rebooten. Im Anfangsdialog werdet ihr gefragt, ob ihr das Persistent Volume benutzen wollt. Bejaht das, gebt das Passwort ein und klickt Unlock. Anschließend könnt ihr Daten im Verzeichnis „Persistent (Persönlicher Ordner)“ dauerhaft speichern. Fertig.

Schlüssellängen, die noch vor zehn Jahren als sicher galten, werden heute nicht mehr empfohlen. Diese technischen Entwicklungen können tatsächlich handfeste Konsequenzen für die Sicherheit wirklich sensibler Daten haben, die ihr z.B. auf einem verschlüsselten USB-Stick abgelegt habt. Sind diese Daten auch in fünf Jahren noch vor unerwünschtem Zugriff sicher? Stellt euch vor, jemand hat vor einiger Zeit eine Kopie eures verschlüsselten Datenträgers gemacht. Diese Daten wären dann trotz Verschlüsselung rückwirkend lesbar.

Es ist wichtig, sich zu überlegen, welche Daten trotz Verschlüsselung überhaupt auf der Festplatte, im Mailprogramm, auf dem Smartphone oder in einer Cloud gespeichert werden müssen. Im Zweifel ist sicheres Löschen die bessere Wahl!

Daten von Hand vom Persistent Volume auf ein anderes Speichermedium kopieren

Falls ein Upgrade auf eine neue Tails-Version Probleme bereitet und ihr manuell einen neuen (anderen) Tails-Stick erzeugt, dann müssen eure Einstellungsdateien und eure Daten auf den persistenten Speicherbereich des neuen Sticks kopiert werden. Wir beschreiben hier, wie das geht:

Sichern der Dateien vom alten Tails-Medium:

1. Meldet euch im Startmenü von Tails mit einem Administrationspasswort an.
2. Schließt das alte Tails-Medium an (von welchem ihr eure Daten sichern möchtet).
3. Wählt Anwendungen ▶ Hilfsprogramme ▶ Laufwerke.
4. Wählt im linken Fensterbereich das Medium aus, welches dem alten Tails-Medium entspricht.
5. Wählt im rechten Fensterbereich die Partition mit dem Typ LUKS aus.
6. Klickt auf die Schaltfläche „Entsperren“ (Schlosssymbol), um das alte Persistent Volume zu entsperren. Gebt die Passphrase des alten Volumes ein und klickt auf Entsperren.
7. Wählt die Partition *TailsData* aus, die unter der LUKS-Partition erscheint.
8. Klickt auf die Schaltfläche *Einhängen* (▶). Das alte Persistent Volume ist nun unter `/media/amnesia/TailsData` eingehängt.

Kopieren der alten Dateien in das neue Persistent Volume:

1. Wählt Anwendungen ▶ Systemwerkzeuge ▶ Root Terminal aus, um ein Terminal mit Administrationsrechten zu öffnen.
2. Gebt den Befehl `nautilus` ein, um den Dateimanager mit Administrationsrechten auszuführen.
3. Navigiert im Dateimanager zu `/media/amnesia/TailsData`, um das alte Persistent Volume zu öffnen.
4. Wählt in der Titelleiste Menü ▶ Neuer Reiter aus (in dem ihr mit der rechten Maustaste in den Reiter klickt), und navigiert in diesem neuen Reiter zu dem Ordner `/live/persistence/TailsData_unlocked`.
5. Wählt den *TailsData-Reiter* aus.
6. Um einen Ordner, der persistente Daten enthält, vom alten Persistent Volume in das Neue zu kopieren, zieht diesen Ordner aus dem Reiter *TailsData* und lasst ihn über dem Reiter *TailsData_unlocked* los.

   Wählt beim Kopieren von Ordnern die Option „Diese Aktion auf alle Dateien anwenden“ und klickt auf „Zusammenführen“, um es auf alle Unterordner anzuwenden. Anschließend könnte es notwendig sein, die Option „Aktion auf alle Dateien anwenden“ auszuwählen und auf „Ersetzen“ zu klicken, um sie auf alle Dateien anzuwenden.

   Kopiert am besten nur die Ordner von den Funktionen, die ihr beim Anlegen des alten Persistent Volumes aktiviert hattet:

   - Der *apt-Ordner* entspricht der APT-Pakete- und APT-Listen-Funktion des beständigen Speicherbereichs. Aber sie benötigt Administrationsrechte, um importiert zu werden und dies sprengt den Rahmen dieser Dokumentation. Dieser Ordner enthält keine persönlichen Daten.
   - Der *bookmarks*-Ordner enthält die Lesezeichen des Browsers.
   - Der *cups-configuration*-Ordner enthält eure persönlichen Drucker-Einstellungen.
   - Der *dotfiles*-Ordner (Punktdateien) beinhaltet versteckte System-Konfigurationsdateien.
   - Der *electrum*-Ordner enthält die Bitcoin-Einstellungen.
   - Der *gnome-keyring*-Ordner und der *gnupg*-Ordner enthalten die pgp-Schlüssel.

- Der *thunderbird*-Ordner enthält die Mail-Einstellungen sämtlicher Mail-Konten, die ihr mit Thunderbird verwaltet.
- Der *nm-connections*-Ordner enthält die gemachten Netzwerk-Einstellungen.
- Der *openssh-client*-Ordner enthält SSH-Schlüssel.
- Der *Persistent-Ordner* entspricht der „Persönliche Dateien"-Funktion des beständigen Speicherbereichs. **Den benötigt ihr in jedem Fall!**

7. Schließt nach dem Durchführen der Kopie den Dateimanager.

Backup vom Persistent Volume:

Es gibt verschiedene Möglichkeiten, ein Backup von eurem persistenten Speicher in Tails zu machen. Wir wollen euch eine Variante zeigen, bei der ihr, als Backup, einen Tails-Stick erhaltet, den ihr direkt nutzen könnt. Das Ganze umfasst 2 Schritte:

1. Einen neuen Tails-Stick mit Persistenz anlegen (siehe entsprechende Anleitung hier im Heft).
   - Stellt sicher, dass euer Backupstick genauso groß oder größer ist als euer originaler Tails-Stick.
   - Ihr müßt, nach dem Erstellen des persistenten Speichers, keine Einstellungen vornehmen. Diese werden beim Backup überschrieben.
2. Euer Backup machen oder updaten.

Zur Klarheit benutzen wir folgende Bezeichnungen: Tails-Orig ist euer Tails Original. Tails-Back ist euer neuer Backup Stick mit Tails und persistentem Storage.

1. Startet eurer aktuelles Tails-Orig (ihr benötigt später Administrator*innen-Rechte, also wählt ein Administrator*innen-Passwort beim Start. Außerdem müsst ihr eure Persistenz einbinden.)
2. Wählt Anwendungen ▶ Zubehör ▶ Dateien, um den Datei-Browser zu öffnen.
3. Steckt nun den Tails-Back-Stick in den Rechner.
4. Sollte euer Tails-Back-Stick eine ältere Tails-Version haben als Tails-Orig, solltet ihr ihn updaten (siehe Anleitung im Heft).
5. Ein neues, verschlüsseltes Laufwerk erscheint in eurem Datei-Browser. Klickt darauf und gebt eurer Passwort der Persistenz von Tails-Back ein.
6. Öffnet nun ein Root-Terminal. Ihr findet es in Anwendungen ▶ SystemProgramme ▶ Root-Terminal.
7. Führt im Root-Terminal folgendes Programm aus:

```
rsync -PaSHAXv --del \
 /live/persistence/TailsData_unlocked/ \
 /media/amnesia/TailsData
```

   WARNUNG: Ihr müsst diesen Befehl von eurem Tail-Orig ausführen und NICHT von Tails-Back, da ihr sonst euren persistenten Speicher löscht! Vergewissert euch nochmal, dass ihr den richtigen Tails-Stick gestartet habt. Wenn das Programm fertig ist, erhaltet ihr eine Zusammenfassung darüber, wieviele Daten kopiert wurden. Wenn ihr den Befehl von Tails-Back aus eingebt, dann muss der Befehl anders lauten, da Quelle und Ziel vertauscht sind.
8. Ihr könnt jetzt das Laufwerk TailsData im Datei-Browser auswerfen und den Tails-Back-Stick abziehen.

Thunderbird - Mailen mit Persistenz

Tails enthält das Mailprogramm *Mozilla Thunderbird*. Seit Version 4.13 integriert Tails den E-Mail-Client mit der Version 78, mit dem sich einige grundlegende Änderungen in der Anwendung ergeben, auf die wir im folgenden Abschnitt auch eingehen.

> *Vorweg: Wir halten einige Änderungen, die die neue Thunderbird-Version mit sich bringt, aus sicherheitstechnischen Gründen für katastrophal. Leider ist dies das einzige Mailprogramm, das momentan in Tails integriert ist, und wir sehen ein, dass es deshalb notwendig ist, die Benutzung zu erläutern und gleichzeitig einen möglichst sicheren Umgang damit nahezulegen, auch wenn wir am liebsten von der Benutzung abraten würden. Achtet bitte in der Anleitung auf die Hinweise, die in Bezug auf Thunderbird 78 gegeben werden!*

Mit Thunderbird und der Persistenz von Tails könnt ihr Mails verschlüsseln und eure Nachrichten, Schlüssel und Einstellungen verschlüsselt auf dem Tails-Stick speichern. Somit könnt ihr auf diese auch nach einem Neustart zugreifen. Voraussetzung dafür ist, dass ihr beim Erstellen in der Konfiguration des persistenten Speichers GnuPG und Thunderbird aktiviert habt.

Thunderbird startet ihr entweder über das Icon links in der Toolbar oder unter Anwendungen ▶ Internet ▶ Thunderbird Email und Nachrichten.

Einrichten

Beim ersten Start führt euch ein Setup-Assistent durch die Konfiguration eures Mail-Postfachs. Es müssen zuerst der Name und die Emailadresse eingegeben werden.

Sollen die E-Mails aus dem Postfach auch von anderen Menschen mit anderen Computern abgerufen werden können, muss als Protokoll IMAP ausgewählt werden, ansonsten empfehlen wir das Protokoll POP3, bei dem die Mails vom Server heruntergeladen werden und danach nur lokal vorhanden sind. Auf dem Server werden die Daten gelöscht. Sie sind allerdings manuell wiederherstellbar, sofern sie nicht überschrieben wurden. Aber **Achtung**: Solltet ihr POP3 auswählen und die Mails nicht im persistenten Speicher oder woanders verschlüsselt speichern, so sind die Mails auch für euch nach einem Neustart von Tails gelöscht.

Ihr habt die Wahl zwischen den Buttons Weiter und Manuell einrichten... . Weiter startet die Autokonfiguration von

Thunderbird, das heißt, Thunderbird probiert übliche Servernamen basierend auf der E-Mail-Adresse aus und versucht, dort laufende Dienste probeweise anzusprechen, z.B. den IMAP-Dienst. Wenn ihr das nicht wollt, weil ihr diesen Netzwerktraffic vermeiden wollt oder bereits wisst, dass der Automatismus fehlschlagen wird, weil die Servernamen nicht mit der Domain in der E-Mail-Adresse übereinstimmen, dann klickt gleich Manuell einrichten... .

Wisst ihr die Werte für den Posteingangs- und -Ausgangserver, Port und Benutzer*innenname für eure E-Mail-Adresse nicht auswendig, könnt ihr entweder in eurem bisherigen Mail-Programm wie Thunderbird oder auf der Internetseite eures Mailanbieters diese Einstellungen nachschauen. Wichtig ist, dass bei *SSL* entweder *SSL/TLS* oder *STARTTLS* ausgewählt wird. SSL-Traffic geht bei Tails auch über Tor. Die *Authentifizierungsmethode* könnt ihr meist einfach auf *Passwort, normal* belassen. Beide Angaben könnt ihr aber ebenfalls in eurem bisherigen Mail-Programm oder auf der Internetseite eures Mailanbieters nachschauen. Mit einem Klick auf Fertig wird der Einrichtungsprozess abgeschlossen.

Einige Mailanbieter haben auch eine .onion-Adresse für ihre Dienste. Diese könnt ihr auch als Server eintragen.

Finetuning

Wählt im Menü die Punkt „Konteneinstellung“ und öffnet die Einstellungen für euren Account durch Klick auf das > .

Unter den Menüpunkten *Kopien & Ordner*, *Verfassen & Adressieren*, *Junk-Filter* und *Speicherplatz* müssen keine Änderungen vorgenommen werden.

Wählt nun den Menüpunkt *Ende-zu-Ende-Verschlüsselung*. Bei Schlüssel hinzufügen kann man den eigenen privaten Schlüssel einem Account zuordnen, sofern dies nicht schon durch eine Migration passiert ist, oder aber einen Neuen erzeugen (siehe unten). Dann sollte an dieser Stelle die ID des benutzten Schlüssels angezeigt werden. An dieser Stelle ist es wichtig, dass hier überprüft wird, ob E-Mails standardmäßig verschlüsselt werden. Man kann das auch in jeder einzelnen Mail einstellen, sicherer ist es aber, es einmal global festzulegen.

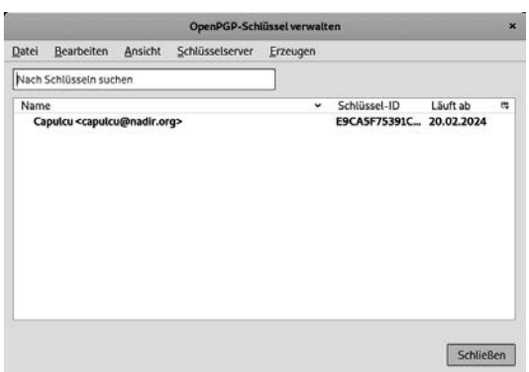
Die Standardeinstellungen sind bereits auf „Verschlüsselung aktivieren“ und „Automatische Auswahl der Verschlüsselungstechnologie“ gesetzt. Unter „Add my digital signature by default“ könnt ihr die Voreinstellung für das Signieren eurer ausgehenden Mails setzen. Auch hier gilt, dass diese Einstellung auch individuell bei jeder E-Mail geändert werden kann.

Warnung: Thunderbird 78 öffnet die Passphrases beim Importieren aller privaten Keys und dabei bleibt es auch, man wird danach nicht mehr gefragt, auch über das Schließen des Programms hinaus! Eine minimale, aber trotzdem sinnvolle Absicherung, die wir allerdings für absolut unzureichend halten, ist das Setzen eines einzigen Masterpassworts für alle Passwörter, die Thunderbird kennt (dies findet ihr unter Einstellungen ► Privacy & Security „Use a Master Password“). Man wird darauf weder beim Accountanlegen oder Keys importieren hingewiesen, noch ist das Passwort de facto verschlüsselt auf der Platte hinterlegt.

Unter den Menüpunkten *Empfangsbestätigungen, S/MIME-Sicherheit* und in den Unterpunkten des *Lokalen Ordners* müsst ihr keine Anpassungen vornehmen.

GPG/PGP Verschlüsselung

Die Schlüsselverwaltung wird in Thunderbird 78 nicht mehr mit dem Plugin *Enigmail* durchgeführt! Um neue Schlüssel hinzuzufügen, geht ihr rechts im Anwendungsmenü von Thunderbird auf Extras ► OpenPGP-Schlüssel verwalten.



Habt ihr bereits ein Schlüsselpaar, das ihr weiterverwenden wollt, oder möchtet ihr öffentliche Schlüssel von Freund*innen hinzufügen, dann habt ihr zwei Möglichkeiten. Entweder kopiert ihr die Schlüssel in einem anderen Programm wie zum Beispiel einem Texteditor in die Zwischenablage, dann könnt ihr sie mit Bearbeiten ► Aus Zwischenablage einfügen hinzufügen. Die zweite Möglichkeit ist, die Schlüsseldatei mit Datei ► Importieren hinzuzufügen. Dabei müsst ihr unter Umständen in dem *Datei Öffnen*-Dialog rechts unten *Alle Dateien* zum Anzeigen auswählen, da sonst nur Dateien mit der Endung *.gpg* angezeigt werden.

Habt ihr noch kein eigenes Schlüsselpaar, könnt ihr dieses unter Erzeugen ► Neues Schlüsselpaar nun erstellen:

Wählt den Mailaccount aus, für den ihr den neuen Schlüssel erstelllen wollt. Geht dort in die Kontoeinstellungen in den Unterpunkt „Ende-zu-Ende-Verschlüsselung“. Klickt dort auf Schlüssel hinzufügen , in dem aufgehenden Fenster wählt ihr „Neuen OpenPGP-Schlüssel erzeugen“ und klickt Weiter .

Ein nächstes Fenster geht auf. Überprüft kurz die angegebene „Identität“, das sollte die Mailadresse sein, für die ihr den Schlüssel erstellen wollt. Als nächstes wählt das Ablaufdatum - die Voreinstellung von 3 Jahren ist schon ziemlich gut, ändert

die nur, wenn ihr einen Grund habt. Das Ablaufdatum lässt sich übrigens jederzeit verlängern, ohne dass der Schlüssel ungültig wird.

In den „Erweiterten Einstellungen“ wählt als Schlüsseltyp RSA und ändert die Schlüsselgröße auf 4096. Dann klickt ihr auf Schüssel erzeugen und im folgenden Fenster auf Bestätigen. Ist die Erzeugung abgeschlossen, schließt sich das Fenster und im Hauptfenster ist jetzt ein grüner Kasten mit der Nachricht „OpenPGP-Schlüssel erfolgreich erstellt“ erschienen. Weiter unter seht ihr auch, dass der neue Schlüssel für diesen Account ausgewählt ist.

Falls ihr euch wundert, dass ihr an keiner Stelle nach eine Passphrase für den neuen Schlüssel gefragt wurdet: Thunderbird hat eine zufällige Passphrase erzeugt, die im Passwortmanager hinterlegt ist. Habt ihr kein Masterpasswort gesetzt, dann ist der neue Schlüssel ungeschützt.

Wenn ihr weiter unten auf OpenPGP-Schlüssel verwalten klickt, öffnet sich die Schlüsselverwaltung. Wählt euren Schlüssel per Doppelklick aus und ihr könnt die Eigenschaften eures neuen Schlüssels nachprüfen - unter anderem wird euch dort der Fingerprint (hier „Fingerabdruck“) eures Schlüssel angezeigt. Dort findet ihr übrigens auch die Möglichkeit, das Ablaufdatum des Schlüssels zu ändern.

Nun seht ihr in der Schlüsselübersicht neben den Schlüsseln von Tails die von euch hinzugefügten oder erstellten Schlüssel. Einzelne Schlüssel könnt ihr mit der rechten Maustaste ▶ In Datei Exportieren in einer Datei speichern. Achtet darauf, dass ihr nur den öffentlichen (nicht den privaten) Schlüssel exportiert, wenn ihr diesen weitergeben wollt.

Wenn ihr das *OpenPGP-Schlüsselverwaltung*-Fenster nun schließt, könnt ihr mit einem Klick auf *Verfassen* eine neue E-Mail verfassen.

Wichtig beim Verfassen einer Mail ist, dass in dem Reiter neben dem Menüpunkt „Sicherheit“ das Feld „Nur mit Verschlüsselung senden“ ausgewählt ist. Wollt ihr die Nachricht zusätzlich signieren, könnt ihr das mit einem Klick auf das Feld „Nachricht unterschreiben“ im gleichen Menüpunkt machen. Wollt ihr euren öffentlichen Schlüssel an die Mail hängen, sodass die Empfänger*in euch auch wieder verschlüsselt zurück schreiben kann, könnt ihr auch dies an dieser Stelle im Feld „Meinen öffentlichen Schlüssel anhängen“ tun. Sendet ihr die Mail und habt *Signieren* ausgewählt, müsst ihr seit der neuesten Thunderbird-Version nicht mehr eure Passphrase eingeben, sondern nur noch euer E-Mail-Passwort.

> *Achtung: Wenn ihr eine verschlüsselte Mail über einen Verteiler senden und gleichzeitig die Mail signieren müsst, weil der Verteiler es so voraussetzt, achtet darauf, dass ihr nicht automatisch euren eigenen PGP-Key mitschickt! Setzt man nämlich das Häkchen unter „Signieren“, so wird automatisch das Häkchen „Meinen öffentlichen Schlüssel anhängen“ mit gesetzt. Dies kann man einzeln wieder ausschalten. Besonders wichtig ist dies, wenn ihr mit einer Gruppen-Emailadresse an eine listenfremde Person schreiben wollt, sonst würde anhand des angehängten Keys die Emailadresse, von der die Mail verfasst wurde, sichtbar.*

Beim Abrufen der Mails müsst ihr zuerst auch euer E-Mail-Passwort eingeben, falls ihr verschlüsselte Mails bekommen habt, werdet ihr nicht mehr nach der GPG/PGP-Passphrase gefragt. Beim Betrachten von eingegangenen Mails symbolisiert ein geschlossenes Schloss am oberen Rand der Nachricht, dass die Nachricht verschlüsselt ist und ein Siegel, dass diese signiert ist.

Hack: Benutzen des externen GnuPG

Über eine Einstellung im Konfigurationseditor lässt sich Thunderbird dazu überreden, *GnuPG* zur Verwaltung des privaten Schlüssels zu verwenden. Diese Funktionalität ist erhalten geblieben, weil *GnuPG* in der Lage ist, mit privaten Schlüsseln auf einer SmartCard zu arbeiten. Auch diese Funktionalität soll zukünftig in Thunderbird integriert werden. Das Verfahren, welches wir hier beschreiben, wird also nur eine begrenzte Zeit funktionieren.

Die Einstellung zur Benutzung des externen *GnuPG* findet ihr im Konfigurationseditor. Dort müsst ihr im Menü *Preferences* auswählen, in dem sich öffnenden Fenster den Punkt *General* auswählen und dann ganz nach unten scrollen: *Config Editor*

Es erscheint ein Fenster mit einer Warnmeldung, dort einfach weiterklicken. Der Eintrag, den ihr braucht, lautet **mail.opengpg.allow_external_gnupg** .

Am leichtesten findet ihr den, wenn ihr oben in den Suchschlitz *gnupg* eingebt. Ein Doppelklick auf *mail.opengpg.allow_external_gnupg* wechselt den Wert von *false* auf *true* (und auch wieder zurück). Stellt den Wert auf *true*. Danach wird euch in eurem Account unter *Ende-zu-Ende-Verschlüsselung* bei Schlüssel hinzufügen jetzt auch das externe *GnuPG* angeboten.

Wenn ihr dort euren bisherigen privaten Schlüssel verwenden wollt, müsst ihr euch vorher die *ID* des Keys besorgen - in einer Konsole:

```
gpg --list-secret-keys
```

Dieser Befehl gibt euch eine Liste aller privaten Schlüssel aus. Kopiert euch die ID des Schlüssels, den ihr verwenden wollt, und *pastet* den in Thunderbird in die entsprechende Eingabe.

Der Vorteil der Nutzung des externen *GnuPG* ist, dass euer privater Key nach wie vor durch eure Passphrase verschlüsselt ist. Andernfalls wird er effektiv nur durch das Masterpasswort von Thunderbird geschützt. Das Benutzen des externen *GnuPG* betrifft allerdings **nicht** eure öffentlichen Schlüssel! Die werden in der Version 78 von Thunderbird verwaltet.

Hack: Mitsenden des eigenen öffentlichen Schlüssels unterbinden

Thunderbird 78 hängt euren öffentlichen Schlüssel an Mails, die ihr signiert habt (siehe oben). Das lässt sich unterbinden, indem ihr im Konfigurationseditor den Wert von

mail.identity.default.attachPgpKey

auf *false* setzt. Für den Fall, dass ihr mehrere Accounts in Thunderbird benutzt, gibt es pro Account jeweils einen persönlichen Eintrag der Form

mail.identity.id1.attachPgpKey,

id1 betrifft den ersten Account, *id2* den zweiten und so fort.

Offline

Wenn ihr mehrere E-Mail-Konten in Thunderbird eingepflegt habt, solltet ihr in Erwägung ziehen, Thunderbird im Offline-Modus starten zu lassen, um so mehr Kontrolle zu haben, welche eurer Adressen wann abgerufen werden sollen. Ansonsten wird diejenige automatisch abgerufen, die ihr zuletzt vor dem Beenden von Thunderbird offen gelassen habt. Auch wenn ihr nur ein E-Mail-Konto habt, möchtet ihr ja vielleicht zuerst Mails im Offline-Modus verfassen, ohne dass sie automatisch (je nach Einstellungen) mit eurem Entwürfe-Ordner eures Mailproviders synchronisiert wird.

Die Offline-Einstellungen könnt ihr unter Einstellungen ▶ Allgemein ▶ Netzwerk ▶ Speicherplatz ▶ Offline ▶ Offline… finden. Dort könnt ihr euch dann für „Immer offline starten“ entscheiden. Weitere Einstellungen, wie zum Beispiel, ob beim Wechsel in den Offline-Modus vorher noch alle Nachrichten herunterladen werden sollen, sind auch noch möglich. Ganz einfach an- und ausschalten lässt sich der Modus durch Klicken auf das Funk-Symbol links unten im offenen Thunderbird.

E-Mailen mit Mutt

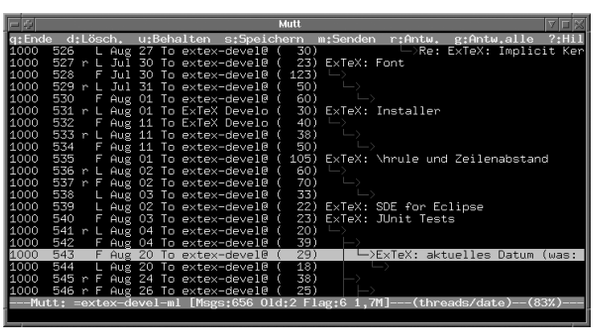
„All mail clients suck. This one just sucks less.“ (Auf deutsch: „Alle Mailprogramme nerven. Dieses hier nervt einfach ein bisschen weniger.“) So steht es auf der Website des schlanken, textbasierten, aber trotzdem mächtigen E-Mail-Clients für Unix und unixartige Betriebssysteme. Ob dieser E-Mail-Client etwas für euch ist, müsst ihr selbst entscheiden.

E-Mail ist Text. E-Mails in HTML zu schreiben und HTML-Mails automatisiert vom E-Mail-Client oder auch Anhänge (wie Bilder) gleich im Body einer E-Mail anzuzeigen, ist eine schlechte Idee und birgt eine prinzipielle Gefahr. Ein Teil des E-Fails-Angriffs[95] 2019 basierte beispielsweise auf Interpretation von HTML in E-Mails und ermöglichte so die Extraktion des Textes in einer E-Mail, nachdem diese entschlüsselt wurde. Mutt war gegen diesen Angriff sicher. Denn HTML in E-Mails wird in Mutt nicht interpretiert. Statt dessen wird der HTML-Sourcecode angezeigt. Es ist allerdings möglich, den HTML-Body an ein externes Programm zu übergeben und damit darzustellen. Davon raten wir allerdings ab. Durch aufmerksames Lesen des HTML-Codes als auch des E-Mail-Headers (in dem die wesentlichen Informationen zur Zustellung der E-Mail stehen und der durch einen simplen Tastendruck einblendbar ist) sind Phishing-Angriffe leicht zu erkennen.

Des Weiteren ist Komplexität fast immer etwas, was es zu minimieren gilt. In der Software-Technik ist eine Daumenregel, dass ein Bug (der nicht unbedingt von einem Exploit ausnutzbar ist) auf etwa 1000 Zeilen Programmcode vorkommt. Die Codebasis zu reduzieren ist sinnvoll. Sicherheit auf dieses Argument zu reduzieren ist allerdings unzureichend.

Mutt arbeitet im Textmodus und ist damit im Terminal einsetzbar. Andere Medien und Formate als Text werden durch einfache Aufrufbarkeit unabhängiger Programme zu deren spezieller Verarbeitung unterstützt.

Die Benutzung ist ausschließlich tastaturgesteuert, daher für an grafische Oberflächen gewöhnte Benutzer*innen eher gewöhnungsbedürftig. Mutt ist flexibel konfigurierbar und sehr gut dokumentiert[96]. Dank Funktionen wie Sortierung nach Ursprungs-/Antwort-E-Mail (Threading) oder regelbasierte Wertkennzeichnung (Scoring) ist es für große Mengen von E-Mails besonders geeignet. GnuPG (für PGP/MIME als auch Inline-PGP, wobei wir von Inline-PGP abraten[97]) und OpenSSL (für S/MIME) zum Verschlüsseln und Signieren von E-Mails kann von Mutt eingebunden werden. Entsprechende Konfigurationsoptionen, Ausgaben und Tastaturkürzel sind integriert.



Installation

Mutt ist nicht in Tails enthalten und muss daher mit root-Rechten installiert werden:

```
apt-get install mutt
```

Konfiguration

Die Konfiguration von Mutt erfolgt über Textdateien.

Basiskonfiguration

Um euch den Einstieg so leicht wie möglich zu machen, haben wir euch eine Konfigurationsdatei erstellt, die ihr verwenden könnt. IMAP und GPG sind vorkonfiguriert. Ihr findet die Datei unter: `https://capulcu.blackblogs.org/muttrc/`.

Beim Starten von Mutt sucht das Programm unter dem Pfad `/home/amnesia/.mutt/` im Dateisystem nach der Konfigurationsdatei `muttrc`. Der Ort, an dem die E-Mails gespeichert werden, ist frei konfigurierbar. In unserer Datei ist der Ordner `/home/amnesia/.cache/mutt` vorkonfiguriert.

1. `muttrc` runterladen und in `muttrc` umbenennen.

95 `https://de.wikipedia.org/wiki/Efail`

96 `http://mutt.org/#doc` und `https://wiki.archlinux.org/index.php/Mutt`

97 Ein paar Gründe dafür finden sich z.B. unter `https://dkg.fifthhorseman.net/notes/inline-pgp-harmful/`

2. Prüfsumme berechnen:

```
sha256sum muttrc
```

   Die Ausgabe sollte folgende sein:

```
f66e3d7000ca77f21c3c93d6610826ace134947fd68c84537a3-
9bb686617949a
```

   Wenn die Prüfsumme mit der hier Abgedruckten übereinstimmt, dann wurde die Datei nicht manipuliert.

3. Verschiebe die Datei nach `/home/amnesia/.mutt/`:

```
mv muttrc /home/amnesia/.mutt/
```

Account-Konfiguration

1. Lege die Datei `/home/amnesia/.mutt/account` mit folgendem Inhalt an:

```
set realname= "a"
set my_account = "b"
set my_domain = "c"
set my_onion = "d"
set my_keyid = "e"
```

   Schreibe zwischen die Anführungszeichen bei a deinen Namen, der Leuten angezeigt werden soll, bei b deinen Account-Namen (das, was vor dem @ steht), bei c deinen Provider, z.B. riseup.net, bei d, wenn es den gibt und du den verwenden willst, den Onion Service, z.B. `vww6ybal4bd7szmg ncyruucpgfkqahzddi37ktceo3ah7ngmcopnpyyd.onion` und bei e den Fingerprint deines Private Keys. Nur d ist optional. Die `muttrc` ist so konfiguriert, dass sie den Onion Service verwendet. Wenn du das nicht willst, dann musst du 4 Zeilen (`setsmtp\_url=smtps://...` und `setfolder=imaps://...`) in der `muttrc` anpassen.

2. Wenn ihr nicht mit dem Text-Editor *vim* eure E-Mails schreiben wollt, dann solltet ihr in `muttrc` einen anderen Editor eintragen.

Verschlüsselte Kommunikation

GnuPG und OpenSSL (für S/MIME) zum Verschlüsseln und Signieren von E-Mails kann von Mutt eingebunden werden. Entsprechende Konfigurationsoptionen, Ausgaben und Tastaturkürzel sind integriert.

Verschlüsselte Mailinglisten vom Typ *Schleuder* verhalten sich wie normale E-Mail-Adressen.

Verschlüsselte E-Maillisten, bei denen zu jeder Empfänger*in separat verschlüsselt wird, sind etwas komplizierter. In Thunderbird gibt es die Empfänger*innenregeln. In Mutt heißt das Konzept crypt-hook. Pro E-Mailadresse gibt es auf der Liste einen Hook:

```
crypt-hook supergeheimeliste@example.org \
 A490D0F4D311A4153E2BB7CADBB802B258ACD84F
crypt-hook supergeheimeliste@example.org \
 AF5208547EF1711AF25057CBD0D0A3C5DF309590
```

Dabei ist supergeheimeliste@example.org eure Mailingliste und dahinter jeweils der Fingerprint des Public-Keys, mit dem verschlüsselt werden soll.

Selbstverständlich können so auch mehrere Mailinglisten konfiguriert werden.

Persistenz

Du kannst das Verzeichnis `.mutt` auch so konfigurieren, dass es im persistenten Speicher abgelegt wird. Dotfiles müssen aktiviert sein, dann wird es entsprechend eingebunden.

98 `https://tails.boum.org/doc/about/warning/index.de.html`

Mutt starten

Das Programm startet ihr wie gewohnt, z.B. unter Applications ► Internet ► mutt.

Bedienung

Es folgen einige Tasten mit denen ihr das Programm bedient.

Hauptmenu (in dem E-Mails aufgelistet werden):

- m: mail; startet das E-Mail-Schreiben-Menü
- r: reply; startet das Auf-E-Mail-Anworten-Menü zu der aktuell ausgewählte Nachricht.
- g: group reply; startet das auf E-Mail-Anworten-Menü (an alle antworten) zu der aktuell ausgewählte Nachricht.
- f: forward; startet das Auf-E-Mail-Anworten-Menü (an alle antworten) zu der aktuell ausgewählte Nachricht.
- c: change directory; startet das Navigations-Menü. Weitere Infos findet ihr unten.
- d: delete; löscht die ausgewählte Nachricht.
- u: undo; macht Löschen rückgängig
- s: save; Speichern der Nachricht in einem anderen Verzeichnis. Die Eingabe ? start das Navigations-Menü.
- Pfeiltasten und Enter: Mit hoch und runter könnt ihr Nachrichten auswählen. Enter bestätigt die Auswahl.
- ?: help; öffnet die Hilfe.
- q: quit; beendet das Programm.

Selbstverständlich gibt es auch die Möglichkeit, mehrere Nachrichten auszuwählen (zu taggen) und dann beispielsweise zu verschieben oder zu löschen. Tastenkombinationen: t zum Taggen; strg+; zum Auswahl bestätigen. Dann z.B. s oder d zum Verschieben/Löschen.

Jedes Menu/Submenü kann mit strg+c und anschliessend mit der Auswahl no abgebrochen werden.

Navigationsmenu (Ordner auswählen):

- Mit den Pfeiltasten und Enter navigiert ihr in der Verzeichnisstruktur.
- In diesem Menü können auch neue Verzeichnisse angelegt werden (Taste C).

E-Mail-Menü (nachdem ihr die E-Mail verfasst habt):

- y: yes; senden
- q: quit; abbrechen
- t/c/b/s: to/cc/bcc/Betreff anpassen
- a: attachment; Anhang hinzufügen
- p: pgp; öffnet das pgp-Submenü.
  - e: encrypt
  - s: sign
  - a: sign as
  - b: both, sign and encrypt
  - i: inline encrypt
  - c: clear; unverschlüsselt und nicht signiert.

Grenzen von Tails und Tor

In diesem Kapitel stellen wir einige Angriffe auf Tails und Tor sowie Warnungen zu deren Nutzung zusammen. Die Informationen könnt ihr in die Bewertung eurer Sicherheit und zur Überprüfung, in welchem Umfang Tails für eure spezifischen

Anforderungen geeignet ist[98], einfließen lassen. Grundsätzlich macht es Sinn, sich eigene potenzielle Bedrohungen zu verdeutlichen, Risiken und strukturelle Schwachstellen oder das Fehlen geeigneter Schutzmaßnahmen zu identifizieren und systematisch Gegenmaßnahmen aufzubauen. Eine systematische Bedrohungsmodellierung beantwortet Fragen wie „Wo bin ich am anfälligsten für Angriffe?“, „Welche Angriffsvektoren kommen für mich in Frage?“, „Was sind die wichtigsten/wahrscheinlichsten Bedrohungen?“, also „Wer sind die möglichen Angreifer*innen und welche Möglichkeiten haben sie?“ und „Was muss ich tun, um mich vor diesen Bedrohungen zu schützen?“. Cops haben zum Beispiel andere Möglichkeiten als Geheimdienste. Gehe ich von einem „Live“-Angriff aus, oder will ich meine Daten im Falle einer Hausdurchsuchung sicher wissen? Wenn ihr euch diese Fragen beantwortet, sollte ihr mit Hilfe der unterschiedlichen Anleitungen konkrete Anhaltspunkte haben, um eine eigene Risikoanalyse vorzunehmen und einige Sicherheitsvorkehrungen zu treffen.

Aber Tails ist kein Wunderheilmittel für Computer-Nicht-Expert*innen. Tails verschlüsselt nicht automatisch eure Dokumente, löscht nicht automatisch die Metadaten aus euren Dokumenten und verschlüsselt auch keine Mail-Header eurer verschlüsselten Mails! Tails nimmt euch auch nicht die Arbeit ab, eure Netzaktivitäten (entlang tätigkeitsbezogener Identitäten) aufzutrennen, und Tails macht schwache Passwörter[99] nicht sicherer. Ihr müsst also grob verstehen, was ihr (mit Hilfe von Tails) macht und ihr müsst euer Netzverhalten neu entwerfen[100].

Tails gibt es mittlerweile seit einigen Jahren, und Tor sogar noch länger. Mit der Zeit sind einige Sicherheitslücken entdeckt und auch wieder behoben worden. Einige mögliche Angriffe liegen aber auch in der Funktionsweise von Tails und Tor begründet. Des Weiteren gibt es immer wieder Gerüchte, dass man Tor nicht vertrauen könne. Beispielsweise, weil es angeblich von der US-Marine (Navy) programmiert wurde, weil es zum Teil mit projektgebundenen Forschungsgeldern finanziert wird oder, dass die NSA & Co. die Hälfte der Relays betreibe, um Nutzer*innen so zu de-anonymisieren. Um diese Gerüchte zu entkräften und euch eine eigene Sicherheitseinschätzung zu ermöglichen, haben wir uns deshalb entschlossen, dieses Kapitel zu Angriffen und Grenzen der Software mit in die Broschüre zu nehmen.

Kompromittierte Hard- oder Firmware

Tails bietet keinen Schutz vor kompromittierter Hard- oder Firmware. Wir raten grundsätzlich:

> *Wenn ihr der Hardware nicht trauen könnt, benutzt sie nicht für sensible Arbeit!*

Aber wie ist das einzuschätzen und was sind mögliche Maßnahmen?

- Tails läuft unabhängig von dem auf dem Computer installierten Betriebssystem. Wenn der Computer also nur durch Software kompromittiert wurde, die innerhalb des regulären Betriebssystems läuft (Virus, Trojaner, etc.), dann ist es sicher, Tails zu verwenden. Dies gilt, solange Tails selbst über ein vertrauenswürdiges System installiert wurde.
- Wenn ihr einen nicht vertrauenswürdigen Computer verwendet, z.B. einen öffentlich zugänglichen in einer Bibliothek, dann kann potentiell alles, was ihr über die Tastatur eingebt, von einem *Hardware Keylogger* aufgezeichnet werden. Außerdem gehört das Fernauslesen des Bildschirminhalts nachweislich zu den Angriffsmethoden der Geheimdienste.

  Um die Eingabe von Passwörtern oder sensiblen Texten vor einem Keylogger zu schützen, könnt ihr die *Bildschirmtastatur* verwenden. Um die Bildschirmtastatur anzuzeigen, klickt ihr auf das Tastatursymbol in der Kontrollleiste oben. Jeder Klick auf dieser *virtuellen* Tastatur ersetzt dann einen *realen* Tastaturanschlag.
- Wenn ihr einen Computer mit Tails startet, kann es nicht durch einen Virus, der in dem eigentlichen Betriebssystem ist, kompromittiert werden. Aber Tails-Systeme können kompromittiert werden und den Schutz, den Tails bietet, verlieren, wenn sie in nicht vertrauenswürdigen Systemen installiert oder dort USB-Sicks eingesteckt werden. Folich sollte erstens Tails ausschließlich von einem System, dem vertraut werden kann, installiert werden. Zweitens: Benutzt den USB-Stick mit Tails nur dazu, um Tails zu starten.
- Es ist auch unmöglich für Tails, vor Angriffen zu schützen, die durch das BIOS oder andere in den Computer eingebettete Firmware durchgeführt werden. Diese werden nicht direkt durch das Betriebssystem verwaltet oder bereitgestellt, und kein Betriebssystem kann vor solchen Angriffen schützen.

Coldboot-Angriffe

Bei der Benutzung eines Computers werden alle bearbeiteten Daten temporär im Arbeitsspeicher zwischengespeichert - auch Passwörter und PGP-Schlüssel!

Nachdem ihr den Computer ausschaltet, geht der Inhalt des Arbeitsspeichers nicht sofort, sondern (je nach Temperatur[101]) *erst nach einigen Minuten* verloren. Angreifer*innen können diese Zeit zum Auslesen des Arbeitsspeichers nutzen, benötigen dazu jedoch physischen Zugang zum Rechner.

Tails überschreibt deswegen beim Herunterfahren bzw. Ausschalten des Rechners (per Power-Off) Teile des Arbeitsspeichers mit Zufallszahlen. Das klappt jedoch nicht bei allen Computern: Wenn sich euer Rechner beim Herunterfahren oder beim „Ausschalten“ nach zwei Minuten nicht selbstständig ausschaltet, dann gibt es keine Garantie dafür, dass das Überschreiben (vollständig) funktioniert hat.

> *Im Fall einer überraschenden Beschlagnahmung eures Rechners sofort den Tails Stick aus dem Rechner ziehen oder den Ausschalter drücken! Es ist ratsam, den Rechner herunterzufahren, auch wenn er nur kurze Zeit unbeaufsichtigt ist.*

VRAM Analyse

Bei einer nicht weiter bekannten Anzahl von verbreiteten Grafikkarten kann ein*e Angreifer*in die im Arbeitsspeicher der Grafikkarte (VRAM) hinterlegten Bildschirmdaten wiederher-

99 siehe dazu den Abschnitt „Sichere Passwortwahl“

100 siehe Kapitel „Nur über Tor ins Netz“

101 Je kälter, desto länger „hält sich“ der Speicherinhalt. Daher benutzen Forensiker*innen zur Datenwiederherstellung beschlagnahmter Geräte Kältemittel zur kurzfristigen „Daten-Konservierung“.

102 `https://hsmr.cc/palinopsia/`

stellen. Tails bietet aktuell (in Version 4.8) keine Möglichkeit, dies zu unterbinden. Die Wiederherstellung von Bildschirmdaten, die unter dem Namen „Palinopsie Bug“ bekannt wurde, betrifft auch virtuelle Umgebungen wie Virtualbox. Davon betroffen sind mehrere ATI- und NVIDIA-Grafikkarten[102].

Ihr könnt nicht verschleiern, dass ihr Tor und Tails verwendet

Tor-Nutzer*innen sind als solche erkennbar – folglich auch die Nutzer*innen von Tails, denn Tails schickt automatisch alle Verbindungen über das Tor-Netzwerk. Der Zielserver (z.B. die Webseite, die ihr besucht) kann leicht feststellen, dass ihr Tor nutzt, da die Liste der Tor-Exit-Rechner (siehe Kapitel „Nur über Tor ins Netz“) für alle einsehbar ist.

Tor Bridges sind ein guter Weg, die Verwendung von Tor gegenüber einem lokalen Beobachter wie beispielsweise einem Internetanbieter oder einer lokalen Netzwerkadministrator*in zu verbergen.

Tails versucht, es so schwierig wie möglich zu machen, Tails-Nutzer*innen von *anderen* Tor-Nutzer*innen abzugrenzen, insbesondere von Nutzer*innen des Tor Browser Bundles.

Manche Webseiten fragen viele Informationen über die Browser der Besucher*innen ab. Zu den gesammelten Informationen können unter anderem Name und Version des Browsers, die Fenstergröße, eine Liste mit den verfügbaren Erweiterungen und Schriftarten sowie die Zeitzone gehören. Einige dieser Merkmale können z.B. über die Nutzung von *NoScript*[103] im Tor-Browser unterdrückt werden. Andere, wie z.B. die Bildschirmauflösung und die Farbtiefe, können unseres Wissens nach nicht unterdrückt werden. Diese Kennungen können eine Identifikation des Rechners erleichtern, bzw. eine Zuordnung eures Aufrufes einer Webseite zu anderen bereits besuchten Webseiten ermöglichen[104].

Ein Tails-System erzeugt fast ausschließlich Aktivität im Tor-Netz. Nutzende des Tor Browser auf anderen Betriebssystemen verursachen aber üblicherweise auch Aktivität außerhalb des Tor-Netzwerks, beispielsweise durch einen anderen Browser oder andere Internetanwendungen. Deshalb kann der proportionale Anteil der Tor-Aktivität ein Indikator dafür sein, ob jemand bei der Verwendung vom Tor Browser Tails verwendet oder nicht. Teilen sich mehrere Anwender*innen einen Internetanschluss, ist es für den Internetdienstanbieter schwieriger zu ermitteln, ob eine einzelne Anwenderin überwiegend Tor-Verkehr verursacht und daher wahrscheinlich Tails verwendet.

Tails verwendet nicht den Entry-Guards-Mechanismus von Tor. Mit dem Entry-Guards-Mechanismus verwendet ein*e Tor-Benutzer*in immer die gleichen wenigen Relays als erste Hops. Da Tails keine Tor-Informationen zwischen den einzelnen Arbeitssitzungen speichert, speichert es auch keine Entry-Guards-Informationen. Dieses Verhalten könnte genutzt werden, um Tails-Benutzer*innen über mehrere Arbeitssitzungen hinweg zu unterscheiden.

Beim Start synchronisiert Tails die Systemuhr, um sicherzustellen, dass sie richtig geht. Falls die Systemzeit zu weit in der Vergangenheit oder in der Zukunft liegt, wird Tor automatisch beendet und neu gestartet. Dieses Verhalten kann zur Unterscheidung von Tails-Nutzenden verwendet werden, vor allem, da dies bei jedem Neustart von Tails auftritt.

Benutzung von Tails in einer Virtuellen Maschine

Aus Sicherheitsgründen raten wir und andere von der Benutzung von Tails in einer Virtuellen Maschine ab. Interessierte Leser*innen verweisen wir an folgende Websites[105].

Auch Tails ist angreifbar

2020 wurde bekannt, dass Facebook 2017/2018 eine externe IT-Sicherheitsfirma beauftragte, um einen sogenannten Exploit zu entwickeln, der auf Tails zugeschnitten ist[106]. Die Firma lieferte - für eine sechsstellige Summe. Ihr Code war in der Lage, eine bis dahin öffentlich und auch den Entwickler*innen von Tails nicht bekannte Sicherheitslücke im Betriebssystem auszunutzen, die dessen Anonymisierungsfunktionen aushebelt. Zero-day-Exploit wird so etwas genannt.

Diesen Exploit ließ Facebook dann über Dritte dem FBI zukommen. Laut *Vice* ist unklar, ob das FBI wusste, woher der Exploit stammt. Aber die Behörde nahm ihn dankend an. So konnte das FBI mit Hilfe eines Opfers einen Sexualstraftäter, der auf Facebook agierte, mit einer Schadsoftware infizieren. Die Behörde schickte ihm eine präparierte Videodatei, in der sich der Exploit verbarg, an eine Dropbox-Adresse. Als das Video (vermutlich mit dem installierten Media Player GNOME Videos) geöffnet wurde, nutzte der Schadcode die unbekannte Sicherheitslücke aus und offenbarte dem FBI seine wahre IP-Adresse. So steht es in Gerichtsdokumenten.

Man-in-the-Middle-Angriffe

Bei einer solchen Attacke greift ein *Man-in-the-Middle* aktiv in die Verbindung von eurem Rechner zu einem Zielserver ein: Ihr denkt, dass ihr direkt mit dem Server eures Mail-Anbieters oder mit der Eingabemaske z.B. des Nachrichten-Portals de.indymedia.org verbunden seid, tatsächlich sprecht ihr mit der Angreifer*in, die das eigentliche Ziel imitiert[107].

Auch bei der Benutzung von Tor sind derartige Angriffe möglich - sogar Tor-Exit-Rechner können solche Angreifer sein[108]. Eine verschlüsselte Verbindung (SSL-Verschlüsselung im Browser am https://... erkennbar) ist hilfreich, aber nur dann, wenn ihr die **Echtheit des Zertifikats einer solchen Verbindung überprüfen** könnt.

---

103 Siehe dazu das Kapitel „Surfen über Tor“

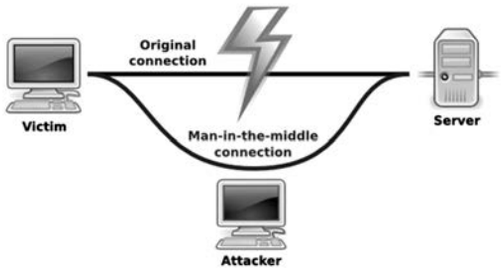
104 `http://heise.de/-1982976`

105 `https://github.com/Qubes-Community/Contents/blob/master/docs/privacy/tails.md` und `https://tails.boum.org/doc/advanced_topics/virtualization/`

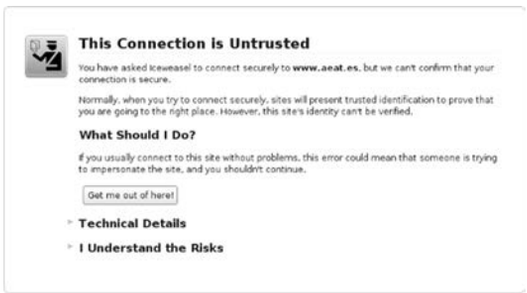
106 `https://www.vice.com/en_us/article/dyz3jy/privacy-focused-os-tails-wants-to-know-how-facebook-and-the-fbi-hacked-it`

107 Die NSA geht hier noch einen Schritt weiter und erweitert Man-in-the-Middle-Angriffe durch Man-on-the-Side-Angriffe: Diese Variante hat den „Vorteil“, dass keine Verzögerungen im Datenverkehr wahrgenommen werden. Siehe dazu: `https://en.wikipedia.org/wiki/Man-on-the-side_attack`

108 Man-in-the-Middle Angriffe von Tor-Exit-Rechnern ausgeführt: `https://www.heise.de/security/meldung/Anonymisierungsnetz-Tor-abgephisht-Teil-2-197888.html`



Wir gehen hier nicht tiefer auf Zertifizierungsmethoden und deren Verlässlichkeit ein, wollen euch aber zumindest die Basis für ein gesundes Misstrauen mitgeben:



Wenn euch dieser Bildschirm beim Verbindungsaufbau angezeigt wird, dann konnte die *Echtheit eures Zielservers* (in unserem Beispiel der Mailanbieter oder indymedia) nicht garantiert werden. Damit ist allerdings nicht gesagt, dass an der Verbindung wirklich etwas „faul“ ist.

Wenn ihr jedoch die Möglichkeit habt, den unter „Technical Details“ angezeigten (vorgeblichen) *Fingerprint* eures Zielservers zu überprüfen (besucht die Seite von einem anderen Rechner aus, oder verwendet andere Quellen), dann solltet ihr das tun!

Das wehrt nicht alle Arten von Man-in-the-Middle-Attacken ab, erledigt aber einen großen Anteil.

> *Tails unterstützt euch mit dem Tor Browser Plugin HTTPS-Everywhere dabei, (wo möglich) SSL-verschlüsselte Verbindungen aufzubauen. Wenn ihr die Möglichkeit habt, die Echtheit dieser Verbindung über den Fingerprint zu überprüfen, solltet ihr das unbedingt tun.*

Ist Tor noch sicher?

Diese Frage scheint einfach, ist aber schwierig zu beantworten, weil sie eine Angreifer*in mit einbezieht - wem gegenüber ist Tor sicher? Eure Arbeitgeber*in wird Tor vermutlich nicht knacken können, das Gleiche gilt wahrscheinlich auch für lokale und nationale Polizeibehörden. Bei Geheimdiensten sind wir mit Aussagen über die Sicherheit vorsichtiger.

Es ist bekannt, dass Geheimdienste Tor attackieren, um die Anonymität der Nutzer*innen aufzuheben. Die bislang veröffentlichten „Ermittlungserfolge“ bei der Deanonymisierung beruhten auf Sicherheitslücken der verwendeten Browser oder auf Anwendungsfehlern, die es ermöglichten, unterschiedliche Identitäten zu verknüpfen. Es sind auch Sicherheitslücken im Tor-Protokoll gefunden und behoben worden - allerdings ist nicht bekannt, ob diese Lücken zur Enttarnung einer User*in beigetragen haben. Es sei nochmal betont, dass Tor nur einen Teil des Datentransportes übernimmt und dass im konkreten Anwendungsfall immer noch weitere Software nötig ist - zum Beispiel der Webbrowser oder aber auch das Betriebssystem - und dass es für eine Angreifer*in einfacher sein kann, diese Software anzugreifen, als Tor zu knacken.

> *Geheimdienste und Polizeibehörden weltweit attackieren das Tor-Netzwerk, um die Anonymität der Tor-Nutzer*innen zu brechen. Wir können die Effektivität von Tor nicht garantieren!*

Wir wissen, dass es seit vielen Jahren massive Anstrengungen von sehr starken Angreifer*innen (NSA, GCHQ, BND, FSB, ECCC, FBI) gibt, Tor-Nutzer*innen und Tor Onion Services zu „deanonymisieren“.

Eine ganze Reihe an Forscher*innen hat anhand von praktischen Angriffen demonstriert, dass durch Zählen der übertragenen Pakete[109], über die Analyse von Zeitfenstern[110] oder durch einen Bruchteil des Verkehrs[111] Nutzer*innen im Tor-Netzwerk identifiziert werden können. Diese Forschung ist öffentlich einsehbar und auch das Tor-Team warnt immer wieder davor, sich nur auf Tor zu verlassen. Tor sei lediglich eines von vielen Werkzeugen, die erst in der Kombination effektiv vor der Enttarnung schützen könnten. Außerdem könnten Fehlkonfigurationen oder andere Unvorsichtigkeiten dazu führen, dass Dritte die anonymen Surfer*innen identifizieren könnten. Die Geheimdienste beobachten diese Forschung, nutzen sie für eigene Zwecke und nutzen theoretische Schwachstellen in ihrer praktischen Überwachung aus. Der BND stützte sich 2009 beispielsweise bei einem Angriff auf eine Studie einer amerikanischen Universität[112]. Zur Umsetzung betrieb der BND wahrscheinlich eigene Server im Tor-Netzwerk.

Absolute Sicherheit gibt es nicht und Tor ist zur Zeit das Beste, was es gibt, um die eigene Identität zu schützen. Tor wird ständig weiterentwickelt, um bekannt gewordene Schwächen zu beseitigen. Daher:

> *Benutzt auf jeden Fall immer die neueste Tails-Version!*

Das Ergebnis bleibt leider unbefriedigend: Erst bei Kenntnis des Versagens des Tor-Netzwerks sind wir in der Lage, eine klare (negative) Aussage zu treffen - das heißt, erst wenn das Kind in den Brunnen gefallen ist, können wir mit Sicherheit sagen, dass es so ist. Das bedeutet, ihr müsst bei der Bewertung etwaiger Konsequenzen von der *Möglichkeit* ausgehen, dass eure IP-Adresse einer Recherche oder einer Veröffentlichung zugeordnet werden *könnte*. Der Ort des Routers wäre in einem solchen Fall enttarnt. Die durch Tails veränderte MAC-Adresse hilft euch zumindest zu verschleiern, welcher Rechner an dem dann enttarnten Router für diese Netzaktivität verantwortlich sein soll *(siehe Abschnitt „Tails ändert eure MAC-Adresse(n)“)*.

Da niemand kategorisch ausschließen kann, dass auch diese zusätzliche Ebene der Verschleierung technisch durchbrochen werden *könnte*, solltet ihr *zusätzlich* auf für euch kontrollierbare Sicherungsmethoden zurückgreifen. Zu zwei dieser Methoden raten wir bei besonders sensiblen Aktivitäten im Internet:

109 https://www.freehaven.net/anonbib/cache/SS03.ps
110 https://www.freehaven.net/anonbib/cache/timing-fc2004.pdf
111 https://www.freehaven.net/anonbib/cache/murdoch-pet2007.pdf
112 https://netzpolitik.org/2017/geheime-dokumente-der-bnd-hat-das-anonymisierungs-netzwerk-tor-angegriffen-und-warnt-vor-dessen-nutzung/

Geht nicht von einem für euch gewohnten Ort ins Netz und nutzt keinen Rechner, der euch zugeordnet werden kann (d.h. nicht übers Internet, sondern so anonym wie möglich *offline* besorgt).

Damit ergeben sich dann folgende Sicherungsebenen zur Anonymisierung besonders sensibler Netzaktivitäten:

1. *Sichere Konfiguration der jeweiligen Anwendungsprogramme (in dieser Anleitung)*
2. *Verschleierung der IP-Adresse per Tor*
3. *Verschleierung der MAC-Adresse per Tails*
4. *Netzzutritt an einem für euch ungewöhnlichen Ort ohne Kameras, ohne euer Handy, ohne andere WLAN- oder Bluetooth-Geräte*
5. *Anonymer Kauf und versteckte Lagerung eines „Recherche-Computers“*

Tor schützt nicht vor globalen Angreifer*innen

Wie sicher ist die Verschleierung der IP-Adresse bei Benutzung des Tor-Netzwerks? Ergänzend zum Abschnitt „Ist Tor noch sicher?“ in der Einführung hier noch einige Anmerkungen.

Ihr könnt in jedem Fall enttarnt werden, wenn ihr es mit *globalen Angreifer*innen* zu tun habt, das heißt, wenn jemand alle Rechner des Tor-Netzwerks korrumpiert hat, bzw. den Datenverkehr zwischen allen Tor-Rechnern in Echtzeit mitprotokolliert. Eine*r solchen Angreifer*in ist es möglich, über die Analyse von Zeitstempeln und Größe der ausgetauschten (verschlüsselten) Datenpakete einzelne Tor-Nutzer*innen den jeweiligen Zielservern zuzuordnen – also die Anonymität aufzuheben![113].

Jeder Mensch weltweit mit einem Netzanschluss genügend großer Bandbreite kann ihren/seinen Rechner dem Tor-Netzwerk zur Verfügung stellen – auch Behörden und andere verdeckte Angreifer*innen. Verteilt über die ganze Welt beteiligen sich derzeit über 6700 Rechner von verschiedenen Institutionen und Privatmenschen am Tor-Netzwerk.

Eine im Oktober 2013 veröffentlichte Studie von Wissenschaftler*innen[114] befasste sich mit dem bereits bekannten Problem der ausgedehnten Protokollierung des Tor-Netzwerkverkehrs. Ziel war es, die Wahrscheinlichkeit und den Zeitraum einschätzen zu können, der benötigt wird, um genügend Daten (über Alltagsroutinen im Netz) für eine Zerstörung der Anonymität zu sammeln. Nach dem dort untersuchten Modell könnte in sechs Monaten durch den Betrieb eines einzigen Tor-Rechners die Anonymität von 80% der verfolgten Benutzer*innen durch gezielte Suche nach wiederkehrenden Traffic-Mustern gebrochen werden.

Die Praxis schien zumindest *zum Zeitpunkt der von Snowden kopierten Geheimdokumente* (im Frühjahr 2013) etwas komplizierter als derartige Modelle. Ein Artikel der britischen Zeitung *The Guardian* berichtete im Herbst 2013 von geringen Erfolgen, welche die NSA beim Versuch verbuchte, Tor-Benutzer*innen zu identifizieren. Zugrunde lagen dem Artikel die Snowden-Dokumente über *Prism*. „Wir werden niemals alle Tor-Nutzer identifizieren können“, zitierte der Guardian aus einer Top-Secret-Präsentation mit dem Titel „Tor stinks“. Mit manueller Analyse sei man *(damals)* lediglich in der Lage (gewesen), einen sehr kleinen Anteil der Tor-Nutzer*innen zu identifizieren. Insbesondere habe die Agency bislang keinen Erfolg damit gehabt, Anwender*innen auf konkrete Anfragen hin gezielt zu deanonymisieren.

Die bislang veröffentlichten „Enttarnungserfolge“ beruhten auf (noch nicht geschlossenen) Sicherheitslücken und insbesondere der installierten Browser-Plugins(!), auf Anwendungsfehlern oder auf immer gleichen Mustern der Nutzer*innen.

Attacken auf Tor-Server

Es kommt immer wieder vor, dass Tor-Server, insbesondere Exit-Nodes und Directory-Authorities, welche die Liste von Tor-Servern verwalten, angegriffen werden. Auf der technischen Seite gab und gibt es sowohl DDoS-Attacken auf Tor-Server als auch automatisierte und manuelle Versuche, in diese einzudringen. Auf der administrativen Seite kommt es vor, dass Exit-Knoten der Serverplatz im Rechenzentrum gekündigt oder ausgesetzt wird, oder diese beschlagnahmt werden.

Blacklisting

Das Problem bei den Entry- und Exit-Nodes ist, dass sie in einer öffentlichen Liste verzeichnet sind. Zensurbehörden und Systemadministrator*innen können daher die dort verzeichneten Server blockieren.

Weltweit kommt es vor, dass Serveranfragen von diesen Servern blockiert werden. Meistens werden aber nicht alle blockiert, sodass ein neuer Circuit die Kommunikation ermöglicht.

Anders sieht es bei den Entry-Nodes aus: In China ist es beispielsweise bereits seit mehreren Jahren der Fall, dass alle Entry-Nodes blockiert werden. Tor-Bridges helfen, diese Zensur zu umgehen. Allerdings haben vor allem die chinesischen Zensurbehörden bereits auch hier wirksame Maßnahmen gefunden, um Tor-Brücken zu enttarnen. Das liegt auch an deren stets geringer Anzahl. Anderswo ist die Situation nicht unbedingt besser. Wir verweisen für weitere Informationen hierzu auf das OONI-Projekt.

Attacken von Tor-Servern

Es stimmt nicht, dass die NSA & Co. die Hälfte der Relays betreibt, um Nutzer*innen so zu deanonymisieren. Zwar haben die Snowden-Dokumente belegt, dass Geheimdienste einen Teil der Relays betreiben – aber nicht genug, um Tor aushebeln zu können. Dingeldine (Tor-Begründer) äußerte 2017 bei der Hacker-Konferenz DefCon[115], dass er zwei Drittel aller Betreiber*innen der insgesamt 6700 Relays persönlich kennt und daher ausschließen könne, dass Strafverfolger und Geheimdienste die Tor-Infrastruktur unterwandert haben. Allerdings kommt es immer wieder vor, dass Tor-Server selbst bösartig agieren. An entsprechenden Gegenmaßnahmen wird entsprechend immer gearbeitet.

Exit-Nodes können die Kommunikation abhören und manipulieren

Der letzte Punkt im Tor-Netzwerk ist der Exit-Node. Dort wird die letzte Verschlüsselungsschicht entfernt und die Daten werden an den Zielrechner außerhalb des Anonymisierungsnetzwerks unverschlüsselt weitergegeben. Für den Server, der die Daten empfangen soll, stammen diese augenscheinlich zwar

---

113 Wer mehr über die Zielsetzung und das Bauprinzip von Tor erfahren will: Tor Project: The Second-Generation Onion Router (Kapitel 3, Design goals and assumptions) `https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf`

114 `http://www.ohmygodel.com/publications/usersrouted-ccs13.pdf`

115 `https://www.heise.de/security/meldung/Tor-Mitgruender-Dingledine-Das-Darknet-spielt-keine-Rolle-3786550.html`

vom Ausgangsknoten und nicht vom ursprünglichen Client-Rechner, die Verschlüsselung des Tor-Netzwerks greift hier aber nicht mehr.

Spätestens auf dem Ausgangsknoten können die Daten eingesehen werden, wenn sie nicht auf dem Ursprungsrechner zusätzlich verschlüsselt wurden, etwa über eine HTTPS-Verbindung. Tor dient also nicht zur Ende-zu-Ende-Verschlüsselung, sondern lediglich dazu, den Ursprung der Daten zu verschleiern.

Sowohl der Betreiber des Ausgangsknotens als auch des Zielservers kann natürlich anhand der gesendeten Daten Rückschlüsse auf den ursprünglichen Client-Rechner ziehen, etwa durch Browser-Fingerprinting oder versehentlich übermittelte persönliche Daten oder IP-Adressen.

Angreifer*innen, die sich für den Datenverkehr im Tor-Netzwerk interessieren, könnten ebenfalls einen Ausgangsknoten betreiben und dort in dem Datenverkehr schnüffeln.

Beispielsweise hat ein Sicherheitsforscher im Jahr 2007 weltweit tausende private E-Mails zwischen ausländischen Botschaften und Menschenrechtsgruppen abgehört, indem er die aus von ihm betriebenen Ausgangsrelais ausgehenden Verbindungen überwacht hat[116].

Selbstverständlich haben auch Geheimdienste ein Interesse daran, Exit-Nodes zu betreiben. Allerdings wollen sie dort nicht nur Daten abgreifen, sondern sie zur Deanonymisierung verwenden. Denn es gibt inzwischen über 1.000 Ausgangsknoten. Da sie immer zufällig ausgewählt werden, ist die Wahrscheinlichkeit, die Daten genau einer Zielperson zu finden, sehr gering. Gerät zudem ein Exit Node in Verdacht, kann er vom Tor-Netzwerk ausgeschlossen werden.

Die Exit-Nodes stehen dadurch im Visier von Überwachunsaktionen. Da das Tor-Netz von Freiwilligen betrieben wird, kann jede Person oder Institution weitere Stationen bzw. Knoten dem Tor-Netzwerk hinzufügen. Dies gilt auch für Exit-Nodes. Daher muss sich nicht die Mühe gemacht werden, Exit-Nodes zu infiltrieren, sondern man kann stattdessen eigene betreiben.

Es ist möglich, viele eigene Exit-Nodes zu betreiben und so die Chancen zu erhöhen, dass eine Kommunikation gezielt abgehört werden kann. Ebenso ist dies ein Geschäftsmodell fragwürdiger Dienstleister*innen, die Exit-Nodes betreiben, um möglichst viele Daten zu sammeln. Wird keine Ende-zu-Ende-Verschlüsseltung eingesetzt, werden die Daten im Klartext diesen präparierten Exit-Nodes bereitgestellt. Die abgefangenen Informationen werden nach eindeutigen Daten wie E-Mails oder Logins durchsucht. Anschließend werden diese verwendet, um sie mit öffentlich zugänglichen oder bereits erfassten Daten abzugleichen. Wenn dies erfolgreich ist, kann eine Deanonymisierung durchgeführt werden. Bösartige Tor-Exit-Rechner können auch Man-in-the-Middle-Attacken durchführen, um ggfls. eine SSL-Verbindung aufzubrechen[117].

Um sich vor solchen Angriffen zu schützen, sollte immer eine Ende-zu-Ende-Verschlüsselung verwendet und die Verbindung geprüft werden.

Correlation Attack

Vor allem über die Korrelation zwischen eingehenden und ausgehenden Daten lässt sich zumindest festzustellen, welche Rechner eine Zielperson kontaktiert. Dabei muss ein*e Angreifer*in die Kontrolle über einen Eingangsknoten und Ausgangsknoten haben. Über den Ausgangsknoten kann sie/er feststellen, wohin die Daten gehen. Vergleicht man die zeitliche Abfolge und Anzahl der versendeten Daten zwischen Ausgangsknoten und Zielrechner mit den Daten, die beim Eingangsknoten eingehen, kann man daraus schließen, von welchem Client aus sie verschickt worden sind.

Je länger eine Verbindung steht und je öfter ein*e Nutzer*in die gleichen Ziele ansteuert, desto größer ist die Wahrscheinlichkeit, dass diese Korrelation zur Deanonymisierung führt. Untersuchungen gehen davon aus, dass es durchschnittlich mehr als ein halbes Jahr dauern würde, um eine einzige Person zu enttarnen.

2014 gelang es einem Forscherteam aufgrund eines inzwischen reparierten Fehlers in der Tor-Software, eigene Pakete in den Datenverkehr einzuschleusen, die dann an beiden Enden der Verbindung registriert werden konnten[118].

Es gab bereits Versuche, so viele Relays wie möglich einzusetzen, um solche Korrelationen schnellstmöglich zu entlarven. Sie wurde aber bald von den Betreiber*innen des Tor-Netzwerks entdeckt. Obwohl auch GCHQ und NSA diese Möglichkeiten bereits in Erwägung gezogen haben[119], gibt es keine Hinweise darauf, dass sie tatsächlich großflächig eingesetzt werden. Die Chancen für eine Deanonymisierung dieser Art steigen allerdings, wenn sowohl der Eingangsknoten als auch der Ausgangsknoten im Netz des gleichen Internet Service Providers sind. Um diese Wahrscheinlichkeit dennoch weiterhin möglichst gering zu halten, nutzt Tor sogenannte Entry Guards.

Aus einer Liste aller verfügbaren Server wird nur eine kleine Anzahl an Eingangsknoten gewählt, die die Nutzer*in über einen Zeitraum von mehreren Wochen nutzt. Wenn diedrei standardmäßig ausgewählten Eingangsknoten nicht von Angreifer*innen kontrolliert werden, ist die Nutzer*in ohnehin sicher. Sollte jedoch ein Relay überwacht werden, können Angreifer*innen zwar einen Teil der versendeten Daten sehen, die Wahrscheinlichkeit, alle Daten zu überwachen, ist jedoch deutlich geringer als die bei willkürlich ausgewählten Eingangsknoten.

Tails verwendet allerdings nicht den Entry-Guards-Mechanismus von Tor. Mit dem Entry-Guards-Mechanismus verwendet ein*e Tor-Benutzer*in immer die gleichen wenigen Relays als erste Hops. Da Tails keine Tor-Informationen zwischen den einzelnen Arbeitssitzungen speichert, speichert es auch keine Entry-Guards-Informationen. Dieses Verhalten könnte genutzt werden, um Tails-Benutzer*innen über mehrere Arbeitssitzungen hinweg zu unterscheiden.

Onion-Harvesting

Die alte Generation von Onion Services hatte die Schwachstelle, dass durch Bereitstellen eines Tor-Servers die Möglichkeit bestand, Onion-Adressen zu sammeln (sogenanntes Onion-Harvesting) und zu analysieren[120]. Durch die neue Generation von Onion Services ist das Problem behoben.

116 http://archive.wired.com/politics/security/news/2007/09/embassy_hacks

117 Man-in-the-Middle-Angriffe von Tor-Exit-Rechnern ausgeführt: https://www.heise.de/security/meldung/Anonymisierungsnetz-Tor-abgephisht-Teil-2-197888.html

118 https://www.golem.de/news/hidden-services-die-deanonymiserung-des-tor-netzwerks-1501-111747.html

119 http://www.spiegel.de/media/media-35543.pdf

120 https://www.golem.de/news/hidden-services-die-deanonymiserung-des-tor-netzwerks-1501-111747.html

Angriffe auf Hidden Services

Zuletzt wollen wir noch zwei Angriffe auf Hidden Services eingehen.

Operation Onymous gegen Silk Road 2

Bei der Operation Onymous im Herbst 2014 gelang es der USA-Bundespolizei und anderen Strafverfolgungsbehörden nach eigenen Angaben, die Betreiber*innen der als Onion Service erreichbaren Handelsplattform Silk Road 2 und weiteren illegalen Onlinehändlern im Tor-Netzwerk zu identifizieren[121][122]. Wie, wollte das FBI zunächst nicht verraten. Erst als behauptet wurde, dass das FBI die Daten ungesetzlich von der NSA erhalten habe, dementierte die Bundespolizei und erklärte, sie habe die Daten von einem fehlkonfigurierten Login des Rechners ermittelt. Es waren also Benutzer*innenfehler, über die die US-Bundespolizei die IP-Adresse des mutmaßlichen Betreibers entdeckte.

Die im Zuge des Gerichtsprozesses in Seattle veröffentlichten Unterlagen geben weitere Details preis. In dem Schreiben des Richters Richard Jones heißt es: "Die IP-Adresse des Angeklagten wurde vom Software Engineering Institute (SEI) der Carnegie Mellon University (CMU) identifiziert, als das SEI wissenschaftliche Forschungsarbeiten im Tor-Netzwerk durchführte, die vom Pentagon (Verteidigungsministerium) finanziert wurden."[123]

Über einen Zeitraum von sechs Monaten hatten zwei Forscher der CMU damals das Tor-Netzwerk unterwandert und einen Weg gefunden, dessen Nutzer*innen massenhaft zu deanonymisieren. Der Text der (zurückgezogenen) Einreichung bei der Black Hat Conference 2014 besagt Folgendes: „we demonstrate how the distributed nature, combined with newly discovered shortcomings in design and implementation of the Tor network, can be abused to break Tor anonymity. In our analysis, we've discovered that a persistent adversary with a handful of powerful servers and a couple gigabit links can de-anonymize hundreds of thousands Tor clients and thousands of hidden services within a couple of months. The total investment cost? Just under $3,000. During this talk, we will quickly cover the nature, feasibility, and limitations of possible attacks, and then dive into dozens of successful real-world de-anonymization case studies, ranging from attribution of botnet command and control servers, to drug-trading sites, to users of kiddie porn places.“[124]

Ed Felten hat folgende Zeitleiste rekonstruiert (alle Daten im Jahr 2014)[125]:

- 30. Januar: 115 neue Maschinen schließen sich dem Tor-Netzwerk als Relais an und führen einen fortlaufenden, neuartigen Identifizierungsangriff gegen die versteckten Dienste von Tor durch.
- 18. Februar - 4. April: Forscher des CERT (Teil des Software Engineering Institute an der Carnegie Mellon University) reichen einen Präsentationsvorschlag bei der Black Hat ein, in dem sie einen neuen Identifikationsangriff auf Tor diskutieren wollen.
- Irgendwann März - Mai: Das Tor-Projekt erfährt von der Forschung und bittet um Informationen von den Forschern, die sich weigern, Details zu nennen.
- Anfang Juni: Black Hat akzeptiert die Präsentation und veröffentlicht eine Zusammenfassung der Forschung, die sich auf die Sicherheitslücke bezieht und sagt, dass die Forscher den Angriff in freier Wildbahn durchgeführt haben.
- Ende Juni: Die Forscher geben dem Tor-Projekt ein paar Hinweise auf den Angriff, verraten aber keine Details.
- 4. Juli: Das Tor-Projekt entdeckt den laufenden Angriff, wirft die angreifenden Relays aus dem Tor-Netzwerk und beginnt mit der Entwicklung eines Software-Fixes, um den Angriff zu verhindern. Die Entdeckung wurde durch einige Hinweise begünstigt, die das Tor-Team von den Forschern erhalten konnte.
- 21. Juli: Black Hat kündigt die Absage der geplanten Präsentation an, mit der Begründung, dass "die Materialien, über die er sprechen würde, noch nicht von CMU/SEI zur Veröffentlichung freigegeben sind."
- 30. Juli: Das Tor Project veröffentlicht ein Software-Update, um die Sicherheitslücke zu beheben, zusammen mit einer detaillierten technischen Diskussion des Angriffs. Der Tor Project ist sich immer noch nicht sicher, ob die Angriffe, die sie gesehen haben, von den CERT-Forschern durchgeführt wurden, obwohl dies angesichts der Ähnlichkeiten zwischen den Angriffen und dem Abstract der Präsentation der Forscher wahrscheinlich scheint.

Nach der CMU-Attacke sahen sich die Entwickler*innen gezwungen, verstärkt auf ungewöhnliche Aktivitäten im Netzwerk zu achten und diese im Zweifel schnell zu unterbinden. Auf auf die Gefahr hin, wertvolle Forschungsarbeit dadurch im Keim zu ersticken, wie Tor-Chefarchitekt Nick Mathewson sagte[126].

Operation Pacifier gegen Playpen: Deanonymisierung durch einen Honeypot und Schadsoftware

Im Jahr 2015 setzte das FBI in der „Operation Pacifier“ einen Honeypot und Schadsoftware gegen Nutzer der Kinderpornografie-Plattform Playpen weltweit ein, um die Nutzer dieses Onion-Services zu deanonymisieren[127]. Mit dieser Aktion schaltet das FBI nicht nur die Seite Playpen ab, die zu diesem Zeitpunkt rund 150.000 Nutzer verzeichnet, die Ermittler starten so auch eine Hacking-Kampagne von bis dahin unbekanntem Ausmaß. Über 800 Computer in mehr als 120 Ländern wurden aufgrund eines einzelnen richterlichen Beschlusses mit Schadsoftware infiziert, um so möglichst viele Nutzer der Seite zu identifizieren.

FBI-Ermittler*innen hatten bereits am 19. Februar den damals 56-jährigen Administrator von Playpen verhaftet, doch die Aktion wurde streng geheim gehalten. Die Nutzer von Playpen sollten nichts mitbekommen. Die Ermittler*innen verschafften sich dank der Festnahme Zugang zu den Servern, täuschten eine Wartungspause der Server vor und stellten die Plattform als sogenannten Honeypot am 20. Februar wieder online. Dank des Honeypots konnte das FBI jeden Schritt aller User, die sich mit dem Tor-Browser auf Playpen anmeldeten, nachverfolgen.

Doch der Honeypot ist nur der eine Teil, der Operation Pacifier so effizient machte. Denn die Ermittler*innen wurden für die Operation auch zu Hacker*innen, indem sie die Rechner

121 https://www.golem.de/news/hidden-services-die-deanonymiserung-des-tor-netzwerks-1501-111747.html
122 https://www.zeit.de/digital/datenschutz/2016-02/darknet-pentagon-bezahlt-forscher-angriff-auf-tor
123 https://www.documentcloud.org/documents/2719591-Farrell-Weds.html
124 https://web.archive.org/web/20140705114447/http://blackhat.com/us-14/briefings.html\#you-dont-have-to-be-the-nsa-to-break-tor-deanonymizing-users-on-a-budget
125 https://freedom-to-tinker.com/blog/felten/why-were-cert-researchers-attacking-tor/
126 https://blog.torproject.org/did-fbi-pay-university-attack-tor-users
127 https://www.vice.com/de/article/59qpwz/das-fbi-hat-hunderte-deutsche-tor-nutzer-gehackt

der Verdächtigen mit Schadsoftware infizierten, die ihnen die IP-Adressen der User verriet, welche normalerweise durch die Nutzung von Tor verschleiert gewesen wären.

Der Durchsuchungsbeschluss, den die Richterin Theresa C. Buchanan aus dem Bundesstaat Virginia unterschrieben hatte, erlaubt es den Ermittler*innen, die Computer von Playpen-Nutzern mit einem sogenannten „Network Investigation Tool" (NIT) anzugreifen. NIT ist der FBI-Begriff für Hacking-Werkzeug – bei Operation Pacifier war es eine Schadsoftware, die die Computer der Verdächtigen infizierte.

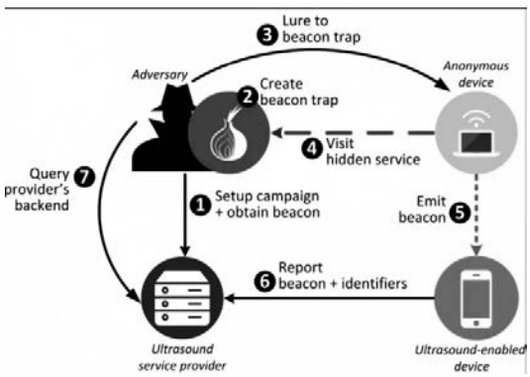
Was die Ermittler*innen durch das NIT über die Verdächtigen herausbekommen konnten, verrät der Durchsuchungsbeschluss im Fall Playpen: Das NIT schickte heimlich die IP-Adresse, das Betriebssystem, den Namen des Nutzers des Betriebssystems und die MAC-Adresse eines Computers an das FBI. Außerdem vergab das NIT eine einmalige Identifikationsnummer für jeden Verdächtigen und fragte ab, ob das NIT schon einmal auf dem Computer eingesetzt wurde. Die Schadsoftware wurde so programmiert, dass Nutzer erst dann angegriffen wurden, wenn sie sich tatsächlich auf Playpen einloggten oder einen neuen Nutzeraccount erstellen wollten.

Weitere technische Details sind über das Tool nicht bekannt. Das FBI hält geheim, wie es die Computer der Verdächtigen gehackt hat. Als ein Richter in einem Verfahren gegen einen Playpen-Nutzer später anordnet, dass die US-Behörden zumindest einen Teil des Codes öffentlich machen müssen, lässt das US-Justizministerium die Anklage fallen. Auch, ob die NIT eine bekannte Sicherheitslücke oder einen Zero-Day-Exploit ausnutzt, bleibt unbekannt.

Cross-Device-Tracking

Dass Marketingunternehmen für Menschen unhörbare Ultraschallsignale benutzen, um ihre Werbebotschaften über Geräte hinweg gezielt platzieren zu können, ist seit einigen Jahren bekannt[128] und im Alltag schon verbreitet. Dabei emittiert eine auf einem Gerät angezeigte Werbung, also zum Beispiel ein Werbebanner auf einer Webseite, ein Audiosignal im Ultraschallbereich zwischen 18 und 20 kHz. Diese Frequenzen sind nicht für das menschliche Ohr hörbar. Aber sie können von präparierten Apps auf den anderen Geräten der Nutzer*in, etwa Smartphones oder Tablets, empfangen werden. Firmen wie das US-Marketingunternehmen Silverpush bieten seit 2014 eigene SDKs (Software Development Kits) an, die Entwickler*innen in ihre werbefinanzierten Apps einbauen können[129]. Unterstützt ein solches SDK dieses sogenannte Ultraschall-Cross-Device-Tracking (uXDT), dann kann es über das eingebaute Mikrofon Ultraschallsignale anderer Geräte empfangen. Laut Angaben haben die Signale eine Reichweite von bis zu sieben Metern, können physische Hindernisse wie Wände aber nicht durchdringen.

uXDT lässt sich aber auch dazu gebrauchen, Tor-Nutzer*innen zuverlässig zu identifizieren[130]. Wenn eine Tor-Nutzer*in beispielsweise ein Smartphone oder Tablet, auf dem ein solches Werbe-SDK installiert ist, in der Nähe hat, dann empfängt dieses die Ultraschallsignale und sendet entsprechende Inhalte an die im Werbe-SDK gespeicherten Server. Das SDK kann auch nicht wissentlich installiert sein, denn es könnte unbemerkt, eingebettet in kostenlose Apps, auf das Smartphone oder Tablet installiert worden sein.



In ihren Tests gelang es einem Forscher*innen-Team, an Informationen wie E-Mail- und IP-Adresse, Telefonnummer, IMEI und Geolokalisationsdaten der Geräte zu gelangen und damit eine vormals anonyme Tor-Nutzer*in in Echtzeit einem identifizierbaren Smartphone zuzuordnen.

Zwar hat der Tor-Browser standardmäßig die Browsererweiterung NoScript aktiviert, allerdings ist Javascript standardmäßig aktiviert (über die Sicherheitseinstellungen anzupassen). Webseiten könnten Audiosignale aber auch über die HTML5-Audio-API abspielen, ohne dass die Nutzer*in davon etwas merkt.

> *Wir empfehlen bei sensiblen Arbeiten das Smartphone entweder auszuschalten oder besser erst garnicht dabei zu haben.*

Gefahren von kabellosen Schnittstellen

Netzwerkverbindung herstellen

Tails sucht nach dem Start selbständig nach verfügbaren Netzwerkverbindungen. Wenn ihr beim Start von Tails ein Netzwerkkabel eingesteckt habt und euer LAN-Zugang nicht passwortgeschützt ist, dann startet Tor automatisch. Der Aufbau eines Tor-Netzwerks mit der dazu notwendigen Synchronisation der Systemzeit dauert eine Weile – bei Erfolg erscheint die Meldung, „Tor ist bereit. Sie haben jetzt Zugriff auf das Internet". Ab jetzt werden alle Surf-, Chat- und Mail-Verbindungen durch das Tor-Netz geleitet.

Für eine (in der Regel passwortgesicherte) WLAN-Verbindung könnt ihr den Netzwerkmanager in der oberen Kontrollleiste anklicken oder über das Menü `Anwendungen ► Systemwerkzeuge ► Einstellungen ► Netzwerk` auswählen und dann das Passwort eingeben.

WLAN ständig auf der Suche nach verfügbaren Netzen

Wenn ihr mit angeschaltetem Laptop, Tablet oder Smartphone bei aktiviertem WLAN[131] durch die Stadt geht, dann versucht eure WLAN-Karte bei allen WLAN-Routern in Funkreichweite eine Verbindung aufzubauen. Und das, ohne dass ihr im Netzwerk-Manager eine solche Verbindung aktiv auswählt und herstellt! Die Router aller dort gelisteten WLAN-Netze der Umgebung haben euren Computer bereits über dessen WLAN-

128 `http://arstechnica.com/tech-policy/2015/11/beware-of-ads-that-use-inaudible-sound-to-link-your-phone-tv-tablet-and-pc/`

129 `https://www.golem.de/news/anonymitaet-ultraschall-tracking-kann-tor-nutzer-deanonymisieren-1701-125434.html`

130 `https://media.ccc.de/v/33c3-8336-talking_behind_your_back`

131 Das WLAN lässt sich bei *Tails* wie bei allen Betriebssystemen über den Netzwerk-Manager an- und abschalten, sofern ihr es nicht im BIOS deaktiviert habt.

MAC-Adresse bei einer *initialen* Begrüßung identifiziert![132] Ihr hinterlasst also eine zurückverfolgbare Spur[133], falls diese flüchtigen „Begrüßungen“ aufgezeichnet werden[134].

Im Falle eines Anwendungsfehlers oder sonstigen Tor-Problems könnte ein*e Angreifer*in euren Rechner anhand der aufgezeichneten MAC-Adresse des WLANs identifizieren, sofern sie/er sich Zugang zum Router verschafft, über den ihr ins Netz gegangen seid.

Tails ändert eure MAC-Adresse(n)

Zur zusätzlichen Sicherheit ersetzt Tails vor der ersten Netzeinwahl (beim Start von Tails) die MAC-Adresse(n) aller im BIOS aktivierten Netzwerkadapter eures Rechners durch zufällige Adressen, und behält diese bis zum nächsten Reboot.

Es gibt allerdings Situationen, in denen das nicht funktioniert: Manche Netzwerke erlauben nur einer beschränkten Liste von voreingestellten MAC-Adressen den Zugang. Nur, wenn ihr glaubt, auf diese zusätzliche Sicherheit verzichten zu können, könnt ihr *Tails* neu starten und beim *Tails*-Begrüßungsfenster „+“ (bei Additional Settings) anklicken, und dann die (standardmäßig gesetzte) Option „Alle MAC-Adressen manipulieren“ abwählen. **Wir raten jedoch zugunsten eurer Anonymität davon ab!**

Vorsicht beim UMTS-Stick

Auch ein UMTS-Stick ist ein eigenständiger Netzwerkadapter, der somit auch eine eigene MAC-Adresse besitzt. Auch diese wird von *Tails* beim Start mit einer Zufallsadresse überschrieben. Dennoch muss man hier auf die zusätzliche Sicherheit einer veränderten MAC-Adresse verzichten, da auch die eindeutige Identifikationsnummer eurer SIM-Karte (**IMSI**) und die eindeutige Seriennummer eures Sticks (**IMEI**) *bei jeder Netzeinwahl an den Mobilfunkanbieter übertragen* werden und eine Identifikation sowie eine geografische Lokalisierung ermöglichen. Der UMTS-Stick funktioniert wie ein Mobiltelefon!

Wer nicht möchte, dass verschiedene Recherche-Sitzungen miteinander in Verbindung gebracht werden können, darf weder den UMTS-Stick noch die SIM-Karte mehrmals benutzen![135]

Für sensible Recherchen oder Veröffentlichungen sind sowohl der UMTS-Stick als auch die SIM-Karte zu entsorgen.

Andernfalls wären verschiedene Recherchen über die gemeinsame IMEI oder die gemeinsame IMSI miteinander verknüpft. *Der Austausch der SIM-Karte allein genügt ausdrücklich nicht!*

Wir legen euch einige weitere Anmerkungen zu den Grenzen von *Tails* (im Anhang) ans Herz!

Bluetooth

Beim Start von Tails werden die kabellosen Schnittstellen WLAN, WWAN, WIMAX - sofern in eurem Computer vorhanden - (mit geänderter MAC-Adresse) aktiviert.

Beim **WLAN** reicht die Manipulation der MAC-Adresse aus, um von anderen Geräten in Reichweite *falsch* identifiziert zu werden.

Daher ist es für eine sichere Betriebsart von Tails unerlässlich, sämtliche nicht benötigten Funkschnittstellen abzuschalten. Wir beschreiben hier drei unterschiedliche Methoden. Wir halten Variante 1 für die Sicherste:

1. **Bluetooth**[136] **ausbauen**. In vielen neueren Laptops findet sich eine Karte, die sowohl das WLAN, als auch das Bluetooth-Modul beinhaltet (siehe Abbildung oben). Nach Lösen aller Schrauben des Laptop-Bodens und dem Abnehmen des Bodendeckels könnt ihr die beiden Antennenanschlüsse abziehen und die Karte(n) herausnehmen. Im Falle einer kombinierten Bluetooth/WLAN-Karte[137] müsst ihr diese durch eine WLAN-Karte ersetzen.
2. **Bluetooth, WWAN und WIMAX im BIOS deaktivieren:** Dies ist leider nicht bei allen Computern möglich.
3. **Softwareseitig abschalten:** Solange Tails in seinem Startbildschirm *nicht* die Option anbietet, WWAN und andere Funkschnittstellen vor Systemstart zu deaktivieren, müsst ihr einen umständlichen *Workaround* nutzen: An einem für euch untypischen Ort Tails starten, dann alle Geräte in Tails manuell deaktivieren und danach einen **Ortswechsel** vornehmen, um woanders mit der Arbeit zu beginnen. Dazu müsst ihr:
   - Beim Startbildschirm „Additional Settings“ wählen und ein *Administrations-Passwort* eingeben[138]
   - Nach dem Start `Anwendungen ▶ Systemwerkzeuge ▶ Root Terminal` anklicken. Jetzt werdet ihr nach dem zuvor eingegebenen Administrations-Passwort gefragt. Bei richtiger Eingabe öffnet sich ein sogenanntes Terminal, in dem ihr folgende Befehlssequenz eintippt und mit der *Eingabe*-Taste abschickt:

     ```
     rfkill block all
     rfkill unblock wlan
     ```

     mit rfkill block wwan bzw. rfkill block wlan lassen sich die Schnittstellen auch einzeln abschalten, falls ihr die jeweils andere benötigt.

---

132 Aktuellere Versionen eures Betriebssystems verwenden initial eine zufällige Zahl als WLAN-MAC-Adresse, wechseln aber im Laufe eines Verbindungsaufbaus zur „Echten“

133 Siehe dazu den folgenden Abschnitt „WLAN-Adapter als digitaler Fußabdruck“.

134 In der Standard-Einstellung der Router werden solche Ereignisse nicht mitprotokolliert. Werbeanbieter*innen nutzen allerdings genau diese Möglichkeit, um potentielle Kund*innen vor dem Schaufenster oder im Laden zu identifizieren und ihre Verweildauer zu messen – mit ganz normaler Hardware!

135 Das gilt auch bei anonymem Erwerb von UMTS-Stick und SIM-Karte und deren anonymer Freischaltung.

136 Da die Bauart dieser Karten und die Orte, wo (im Rechner) genau sie verbaut sind, variieren, müsst ihr in der Betriebsanleitung (User Manual) eures Computers nach einer Beschreibung zu deren Ein- und Ausbau suchen.

137 Siehe dazu das Kapitel „Tails als Quasi-Schreibmaschine“.

138 Siehe dazu das Kapitel „Tails starten“.

Fertig - jetzt könnt ihr an den *Ort wechseln*, an dem ihr per WLAN ins Netz gehen wollt. **Achtet darauf, dass der Rechner während des Ortswechsels nicht ausgeht!** Ein Neustart bedeutet, dass ihr die Prozedur von vorne beginnen müsst.

Bei der (unsichersten) Variante 3 habt ihr das Problem jedoch lediglich software-technisch auf Betriebssystem-Ebene gelöst. Eine eventuell während der Sitzung eingeschleuste Schadsoftware kann eben diese Deaktivierung aller Funkschnittstellen mit einem weiteren Kommando genauso einfach rückgängig machen.

WLAN-Adapter als digitaler Fußabdruck

Im September 2019 veröffentlichten wir ein kurzes Statement („Sicherheitswarnung MAC-Changer“)[139], in dem wir vor einer möglichen **Deanonymisierung durch die Nutzung von WLAN-Adaptern** warnen. Wir versuchen hier, einen tieferen Einblick in die Problematik von kabellosen WLAN-Schnittstellen zu geben (ergänzend zum vorherigen Kapitel „Gefahren von kabellosen Schnittstellen“).

Einführung

Nach einer Anmeldung über das Tails-Begrüßungsfenster scannt das darunterliegende Betriebssystem (Debian Linux) bzw. die Firmware automatisch nach vorhandenen Access Points, indem es in regelmäßigen Abständen ein Funksignal (Probe Request) an alle in der Nähe erreichbaren Access Points schickt. Die Funksignale werden entweder über die WLAN-Karte (welche fest in eurem Laptop verbaut ist) oder über einen externen WLAN-Adapter verschickt.

Falls sich Access Points in der Nähe befinden, antworten sie ebenfalls mit einem Funksignal (Probe Response), in dem Informationen zum Netzwerknamen (SSID), Authentifizierung und Verschlüsselung enthalten sind. In den Funksignalen wird auf beiden Seiten die MAC-Adresse als Information eingebunden. Tails schützt euch hier, indem es gefälschte MAC-Adressen von kabellosen Schnittstellen, wie eurer WLAN-Karte, generiert (siehe Kapitel „Gefahren von kabellosen Schnittstellen“).

Durch die in den Funksignalen enthaltenen Informationen ist es möglich, sich mit einem Access Point zu verbinden. Neben diesen Informationen enthalten die Funksignale auch noch weitere Informationen, über die ihr mit hoher Wahrscheinlichkeit identifizierbar seit (auch, wenn eure MAC-Adresse gefälscht wurde).

Das ergeben zumindest verschiedene Untersuchungen aus den Jahren 2016-2019, deren Ergebnisse in diversen Veröffentlichungen festgehalten sind.

Das Papier „Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms[140]“ zeigt die Möglichkeit einer Identifizierung anhand von Funksignalen (Probe Requests) durch den einheitlichen WLAN-Standard 802.11[141], der auch von Tails verwendet wird. Hierbei werden die (gefälschten) MAC-Adressen nicht weiter beachtet und es findet eine Deanonymisierung über die von WLAN-Adaptern gesendeten Funksignale statt (über ein sogenanntes „Probe Request Fingerprinting“). Das Papier bezieht sich auf Test-Daten aus der realen Welt[142] und zeigt, dass WLAN-Funksignale genug Informationen enthalten, um deren spezifische Muster eindeutig zu identifizieren. Das Papier behandelt zudem verschiedene Angriffsmöglichkeiten zur Deanonymisierung, auf die wir hier nicht weiter eingehen.

Der Beitrag „A Study of MAC Address Randomization in Mobile Devices and When it Fails[143]“ nimmt die vorherige Studie als Ausgangspunkt und erweitert sie mit einer Reihe von neuen Möglichkeiten zur Identifikation von Endgeräten mit gefälschten MAC-Adressen. Die Untersuchung kommt zur Schlussfolgerung, dass eine Fälschung von MAC-Adressen über die von ihr dargestellten Angriffe aufgehoben werden kann und für eine Anonymisierung nicht ausreicht.

Es schlägt vor, die gesamte MAC-Adresse zu fälschen und nicht nur die Stellen nach dem OUI[144], wie dies bei Tails der Fall ist[145][146]. Zudem sollte laut dem Papier für jeden Probe Request eine zufällige MAC-Adresse verwendet werden.

Ein weiterer Beitrag mit dem Titel „Defeating MAC Address Randomization Through Timing Attacks“[147] befasst sich mit Probe Requests und der Erkennung von Geräten, die ihre MAC-Adressen in periodischen Zeitabständen fälschen (was unter Tails nicht passiert und laut dem Papier fatal ist). In der Zusammenfassung kommen die Autor*innen des Beitrag zu dem Ergebnis, dass der von ihnen verwendete Angriff einen Großteil der Geräte deanonymisieren kann (bis zu 77%), auch wenn bei den Funksignalen keine Daten übertragen werden.

Weitere Veröffentlichungen zu möglichen Angriffsvektoren auf den IEEE Standard 802.11 findet ihr hier (die nicht explizit das Linux-Betriebssystem mit einschließen):

- „Know Thy Quality: Assessment of Device Detection by WiFi Signals“[148]
- „Accurate and Efficient Wireless Device Fingerprinting Using Channel State Information“[149]
- „Fingerprinting 802.11 Implementations via Statistical Analysis of the Duration Field“[150]
- „Device Fingerprinting in Wireless Networks: Challenges and Opportunities“[151]

Probe Request Fingerprinting

WLAN-Adapter verschicken in kurzen zeitlichen Abständen Probe Requests, um die Gegend nach vorhandenen Access Points zu durchsuchen. Im sogenannten „Frame Body“ der Funksignale ist ein „Management Frame“ enthalten, das wiederum WLAN-Adapter-spezifische „Information Elements (IEs)“ enthält. Die

139 https://capulcu.blackblogs.org
140 https://papers.mathyvanhoef.com/asiaccs2016.pdf
141 https://de.wikipedia.org/wiki/IEEE_802.11
142 Acht Millionen Probe Requests, die zum größten Teil an einem belebten Platz in Rom und an einem Bahnof in Lyon gesammelt wurden.
143 https://arxiv.org/pdf/1703.02874
144 https://de.wikipedia.org/wiki/MAC-Adresse
145 https://tails.boum.org/contribute/design/MAC_address/#active-probe-fingerprinting
146 Laut den Tails-Entwickler*innen fallen ungewöhnliche Mac-Adressen auch auf und werden daher nicht von Tails verwendet.
147 http://papers.mathyvanhoef.com/wisec2016.pdf
148 http://sig-iss.work/percomworkshops2019/papers/p639-rutermann.pdf
149 https://www.cs.ucr.edu/~zhiyunq/pub/infocom18_wireless_fingerprinting.pdf
150 http://www.uninformed.org/?v=5&a=1&t=pdf
151 https://arxiv.org/pdf/1501.01367v1.pdf
152 http://download.aircrack-ng.org/wiki-files/other/managementframes.pdf
153 https://de.wikipedia.org/wiki/ProprietÃd're_Software

Werte der IEs[152] sind zum Teil herstellerspezifisch (was den Inhalt und ihre Reihenfolge betrifft). Dadurch eignen sie sich besonders für ein Fingerprinting, dass auch in den zuvor erwähnten Beiträgen zum Einsatz kam. Das Problem ist, dass es unter den verschiedenen Implementierungen von proprietärer WLAN-Firmware[153] so viele divergierende Möglichkeiten und Anordnungsreihenfolgen gibt, dass ein Tracking erfolgreich sein kann. Daneben kann oft auch anhand der Sequenznummer[154], der Daten-Durchsatzrate und weiteren funksignalspezifischen Parametern[155] eine Unterscheidung getroffen werden (vgl. die genannten Untersuchungen in der Einführung).

Den digitalen Fußabdruck reduzieren

Die Paket-Größen von Probe Requests unterscheiden sich nach den darin enthaltenen Informationen. In den meisten Fällen hängt dies stark von den Firmware-Implementierungen der Hersteller*innen ab. Es gibt allerdings auch freie WLAN-Adapter, die ohne proprietäre Firmware auskommen und über das Betriebssystem gesteuert werden können[156].

> ath9k is a Linux kernel driver supporting Atheros 802.11n PCI/PCI-E chips, introduced at Linux 2.6.27. It does not require a binary HAL (hardware abstraction layer) and no firmware is required to be loaded from userspace.[157]

Dadurch erhaltet ihr die Kontrolle über euren WLAN-Adapter und reduziert bereits euren digitalen Fußabdruck (z.B. enthalten Ath9k WLAN-Adapter keine „Vendor specific Tags“). Dies macht sich auch in der Paketgröße der Probe Requests bemerkbar[158]: z.B. 91 Bytes (bei Ath9k WLAN-Adapter) zu Größen von bis zu 182 Bytes (bei WLAN-Adaptern mit herstellerspezifischer Firmware). Auf der folgenden Seite findet ihr neben den Ath9k WLAN-Adaptern auch noch andere Hardware, die ohne herstellerspezifische Firmware auskommt[159]: `https://en.wikipedia.org/wiki/Comparison_of_open_source_wireless_drivers`

Über folgenden Terminal-Befehl könnt ihr euch die geladenen Treiber anzeigen lassen:

```
lspci -k
```

Nach unserer Warnung im Sommer 2019 gab es Überlegungen unsererseits, wie wir sinnvoll mit der Problematik von Probe Requests und möglichen Angriffen auf das 802.11-Protokoll umgehen können. Eine Richtung, die uns immer noch beschäftigt, ist das Vermeiden von Probe Requests und die Ermittlung von vorhandenen Access Points über ein passives Lauschen nach Funksignalen (Probe Responses). Die Überlegungen dazu sind in einem Tails-Ticket zusammengefasst: `https://gitlab.tails.boum.org/tails/tails/-/issues/17831`.

Darin schlagen wir vor, Netzwerk-Software[160] unter Debian durch neuere Anwendungen, in denen sich das periodische Scannen nach Access Points deaktivieren lässt, zu ersetzen. In unseren Tests war es darüber möglich, passiv Access Points zu finden und eine Verbindung ohne Probe Requests aufzubauen. Das Ganze ist bisher nur oberflächlich getestet, aber zumindest eine möglich Option. Leider wurden die Überlegungen aus dem Tails-Ticket erst einmal von den Entwickler*innen abgelehnt[161], da eine von uns verwendete Software (iwd) in ihren Augen noch zu instabil ist.

> *Bis es eine Lösung für das in den letzten Absätzen beschriebene Problem gibt, solltet ihr für sensible Veröffentlichungen billige WLAN-Adapter verwenden und sie nach dem Gebrauch entsorgen. Zudem raten wir euch, WLAN-Adapter zu verwenden, die ohne herstellerspezifische Firmware über das Tails-Betriebssystem gesteuert werden können.*

Sicherere Passwortwahl

Es ist immer noch so, dass starke Verschlüsselungstechniken (bei ausreichender Schlüssellänge) „nicht knackbar“ sind, bzw. der Rechenaufwand für Geheimdienste zu hoch ist.

Hauptangriffspunkt, um an verschlüsselte Daten zu kommen, ist daher meist das verwendete Passwort, mit dem z.B. ein Schlüssel gesichert ist. Mit bereits im Einzelhandel erhältlichen Computern, die leistungsfähige Grafikchips für einfache Rechenoperationen nutzen, ist das Knacken von Passwörtern für Angreifer*innen immer einfacher geworden. Eine Mischung aus simpler Rechenleistung, riesigen Tabellen bereits geknackter Passwörter und clever programmierter Software macht das Passwort-Knacken erschreckend effizient. Daher kommt der richtigen Passwortwahl eine wichtige Bedeutung zu.

ERSTENS: Je „unmenschlicher“, desto besser

Rein mathematisch sieht die Lage für uns Passwort-Nutzer*innen gar nicht schlecht aus. Die Zahl aller möglichen Passwörter wächst exponentiell mit deren Länge und der Größe des verwendeten Zeichenraums. Diese muss ein*e Angreifer*in im Prinzip durchprobieren (*Brute Force-Methode*), oder aber die Verschlüsselung zur Ablage der Schlüssel auf dem Computer knacken.

> *Fast alle Angriffe basieren mittlerweile auf Wörterbüchern und Namenslisten, erweitert um riesige, gehackte Datenbanken mit mehreren 100 Millionen Passwörtern.*

Die Programme zum Knacken von Passwörtern nutzen darüber hinaus zusätzliche „Regeln“ zur Modifizierung solcher Wörter und orientieren sich dabei an „menschlichen“ Mustern der Veränderung. Die Kombination von Wörtern sowie das Anhängen von Ziffern und insbesondere die *Ersetzung einzelner Buchstaben*, wie das übliche „3“ statt „E“ oder „1“ statt „i“ oder „l“ stellen für diese Programme kein Problem dar. Darüber werden selbst sicher aussehende Passwörter wie „polU09l1nk3d1n“ geknackt.

---

154 Tails ändert nicht die MAC-Adresse nach einer zufälligen Anzahl von Probe Requests und setzt auch nicht die Sequenznummer der übertragenen Pakete zurück, was ein zusätzliches Tracking ermöglicht.

155 HT Capabilities, Supported Rates, Extended Supported Rates, Extended Capabilities, VHT Capabilities, Vendor Specific, ...

156 Genauer: über den Kernel.

157 `https://wiki.debian.org/ath9k`

158 Umso kleiner die Paketgröße, desto weniger Spuren fallen auch an

159 Zu erkennen an den grünen Feldern in der Spalte „Non-free firmware required.“

160 Wie den wpa_supplicant und den Networkmanager.

161 `https://gitlab.tails.boum.org/tails/tails/-/issues/6453`

ZWEITENS: Kein Wort für viele Zwecke

Neben der Komplexität des verwendeten Passworts entscheidet die Art, wie es auf eurem Rechner, beim Mail-Provider oder Online-Shops abgelegt ist, über dessen Sicherheit.

Kein System sollte Nutzer*innen-Passwörter im Klartext speichern. Aber die Verschlüsselungsmethoden für die Ablage von Passwörtern sind unterschiedlich gut. Beim eigenen Rechner haben wir bedingt Einfluss darauf, wie leicht unsere Passwörter zu rekonstruieren sind. Bei irgendwelchen Diensten im Internet müssen wir (häufig zu Unrecht) darauf vertrauen, dass damit sorgsam umgegangen wird. Millionen geklauter Kund*innendaten inklusive Passwörter von unterschiedlichen Service-Anbieter*innen sind eindeutiger und dringender Appell, das dort verwendete Passwort nicht identisch für andere, sensiblere Zwecke zu nutzen!

> *Vollständig zufällige Passwörter mit mehr als 16 Zeichen gelten auf absehbare Zeit als sicher. Sogar bei Verwendung von Supercomputern – aber sie sind auch sehr schwer zu merken. Daher verwenden viele vermeintlich individuelle Kombinationen, Abkürzungen und Veränderungen existierender Worte. Das macht Passwörter angreifbar.*

Nun habt ihr wahrscheinlich das Problem, möglichst lange und komplexe Passwörter für jeden genutzten Dienst erzeugt zu haben, aber merken könnt ihr euch davon bestenfalls drei oder vier. Die Einen nutzen daher spezielle Programme wie *KeePassX* (in Tails), die Passwörter in einer sicheren Datei abspeichern und müssen sich daher nur ein *Master-Passwort* merken. Andere nutzen lieber mehrere Basis-Passwörter, aus denen sie dann verschiedene Varianten generieren. Welche Methode ist sicherer? An der Frage scheiden sich die Geister. Wir wollen euch beide Möglichkeiten vorstellen, entscheiden müsst ihr.

Methode I: Verschlüsselte Passwort-Datei

Alle verwendeten Passwörter werden in einer zentralen, *verschlüsselten Datei* gespeichert. Dies hat den Vorteil, sich nur ein Passwort merken zu müssen. So können für alle anderen genutzten Dienste oder Programme auch möglichst sichere und unabhängig voneinander generierte Passwörter genutzt werden. Aber diese Variante hat auch klare Nachteile. Zum Einen seid ihr von der einen Datei oder dem einen Programm abhängig. Geht diese verloren oder ihr vergesst das Passwort, verliert ihr damit im Zweifel auch den Zugriff auf alle damit gesicherten Dienste. Das andere große Problem bei dieser Variante ist, wenn jemand an dieses eine **Master-Passwort** herankommt, z.B. über einen eingeschleusten *Keylogger*[162], hat die Person gleichzeitig **Zugriff auf alle anderen Passwörter** anstatt nur auf die Eingetippten, seit der Keylogger installiert wurde.

Um KeePassX zu starten, wählt ihr: `Anwendungen ▶ Zubehör ▶ KeePassX`.

Um eine neue Passwortdatenbank zu erstellen, wählt ihr `Datenbank ▶ Neue Datenbank`. Die Passwortdatenbank ist verschlüsselt und durch eine Passphrase geschützt. Dazu gebt ihr eine Passphrase eurer Wahl in das Textfeld „Passwort“ ein (*mindestens 16 Zeichen!*) und klickt anschließend auf `OK`. Wiederholt die gleiche Passphrase im nächsten Dialog und klickt dann auf OK. Das Programm bietet euch ebenfalls an, starke Passwörter (über einen Zufallszahlengenerator) zu erstellen. Zusätzlich bietet KeyPassX an, eine *Schlüsseldatei* auszuwählen, ohne die sich die Datenbank nicht verwenden lässt (was wir euch bei einer Verwendung von KeepassX empfehlen). Um die Passwortdatenbank für die zukünftige Verwendung auf einem Datenträger zu speichern, klickt ihr auf `Datenbank ▶ Datenbank speichern`.

Methode II: Individuelle Gedächtnisstütze

Ihr merkt euch eine zufällig gewählte Seite eines euch bekannten Buches und denkt euch daraus eine *fiktive Schablone* aus, die verschiedene Buchstaben eines Satzes oder eine Abschnitts auf dieser Seite markiert. Verändert dann das so entstehende Wort durch das Einfügen von Ziffern und Sonderzeichen und das Anhängen weiterer Worte.

Ein praktisches Beispiel: Ich merke mir den Namen eines mir in Erinnerung bleibenden Buches und die Seite 373. Auf dieser Seite finde ich den Satz „Er wollte sich mir nicht anvertrauen – und jetzt ist es zu spät.“. Daraus bastle ich die Basis meines Passworts aus den Anfangsbuchstaben **Ewsmna-Ujiezs**. Dieses **Basis-Passwort** verwende ich nirgendwo. Ich nutze lediglich *zwei verschiedene Ableitungen* davon für unterschiedliche Zwecke. **Variante eins** (die Ziffern der Seitenzahl an ihrer jeweiligen Positionen eingefügt) für den Zugang zu meinem privaten pgp-key: **Ews3mna7-Uji3ezs** sowie i**Variante zwei** (373 → §/§ auf einer deutschen Tastatur) für das Entschlüsseln meiner Festplatte: **Ew§/§smna-Ujiezs_against_the_empire**.

Dies ist u.a. vor dem Hintergrund der gesetzlich gedeckten Praxis zur Herausgabe von Passwörtern an Sicherheitsbehörden durch Diensteanbieter absolut notwendig!

> *Verwendet ein solches Basispasswort zum „Erzeugen“ weiterer Passwörter nur für die gleiche „Klasse“ von Passwörtern. Also Passwörter für pgp und Datenträgerverschlüsselung nicht mischen mit solchen wie für Ebay usw.*

Diese Methode hat jedoch den Nachteil, dass sich über die selbst ausgedachten Varianten des Basis-Passworts zwangsläufig menschliche „Muster“ einschleichen, die es eigentlich zu vermeiden gilt.

Überschätzt euch nicht bei der Wahl eines zu komplexen Passworts. Gelingt euch die Rekonstruktion des Passwort über die Gedächtnisstütze nicht, bleiben die Daten für immer unzugänglich.

Es gibt keine 100%ige Sicherheit bei der Auswahl des „richtigen“ Passworts. Und es wird, wie ihr in der Ergänzung im nächsten Abschnitt lesen könnt, noch komplizierter, wenn ihr den technischen Fortschritt mitzuberücksichtigen versucht. Letztendlich müsst ihr **zwischen Sicherheit und Nutzbarkeit abwägen** und selbständig entscheiden, was ihr euch zutraut und euren Bedürfnissen nach Sicherheit im Alltagsgebrauch am Nächsten kommt.

Hier nochmal kurz das Wichtigste zusammengefasst:

- Verwendet auf keinen Fall dieselben Passwörter für mehrere Zugänge. Also nicht für euer Mail-Postfach oder euer Ebay-Konto dasselbe Passwort verwenden wie für den Zugang zu eurem Rechner.
- Hängt nicht einfach eine Zahlenkombination an ein existierendes Wort.
- Verwendet keine einfachen Buchstabenersetzungen wie m!s3r4b3l (MISERABEL).

[162] Ein Keylogger zeichnet jeden Tastenanschlag der Tastatur auf und kann somit auch eure Passwörter mitprotokollieren. Ein Keylogger kann eingeschleuste Schadsoftware oder aber auch ein nachträglich in die Tastatur oder am Verbindungskabel eingebauter Chip sein. Gegen letztere Varianten schützt Tails nicht!

- Auch keine einfache Zusammensetzung von (leicht veränderten) Wörtern.
- Entscheidet euch für eine der beiden Varianten: Merken oder verschlüsseltes Speichern eurer Passwörter. Notizen auf Zettel sind dabei eine sehr schlechte Alternative.
- Eine sogenannte **Passphrase** (komplexeres Passwort) für die Nutzung eures privaten *PGP-Schlüssels* oder die Datenträgerverschlüsselung sollte tatsächlich länger und komplexer sein als ein (einfaches) Passwort für euren Mail-Account. Um auch zukünftig noch auf der sicheren Seite zu stehen, sollte sie **mindestens 16 Zeichen lang** sein.
- Wechselt eure Passwörter hin und wieder, insbesondere, wenn ihr den Verdacht habt, dass das Passwort bekannt geworden ist (z.B. durch einen Bedienfehler, copy&paste ins falsche Fenster, u.ä.).

DRITTENS: In Zukunft unsicher

Sich auf die Ebene der Analyse kryptografischer Methoden verschiedener Verschlüsselungsalgorithmen zu begeben, würde an dieser Stelle den Rahmen sprengen. Vereinfacht gesagt basiert die Sicherheit wichtiger aktueller Verschlüsselungsverfahren wie GPG auf mathematischen Problemen in Kombination mit sehr großen Zahlen. Während das Überprüfen, ob ein privater und ein öffentlicher Schlüssel zusammenpassen, kein Problem darstellt, ist das Auffinden eines zum öffentlichen Schlüssel passenden privaten Schlüssels eine extrem rechenintensive Aufgabe. Klassische Computer müssen schlicht alle möglichen Paare von Primfaktoren durchprobieren. Der Aufwand, eine solche Verschlüsselung mit klassischen Computern zu knacken, wächst exponentiell mit der Schlüssellänge. In Zahlen bedeutet dies, dass ein*e Angreifer*in bei einer Brute-Force-Attacke bei einer Schlüssellänge von 1024 Bit eine Anzahl von $2^{1024} - 1$ Zahlen nach Primzahlen durchsuchen und diese ausprobieren müsste, um den richtigen Schlüssel zu finden. Dies würde mit heutzutage zur Verfügung stehenden Rechenleistungen wahrscheinlich mehr als eine Lebensspanne dauern. Die Rechenleistung von Computerchips verbessert sich zur Zeit allerdings immer noch fortwährend aufgrund der weiter voran schreitenden Miniaturisierung der Schaltkreise und die Parallelisierung der Chips - zumindest solange, bis diese Entwicklung an ihre physikalischen Grenzen stoßen wird. Deshalb empfehlen wir keine Schlüssellängen von 1024 Bit, sondern 4096 Bit.

Quantencomputer

Vor über 25 Jahren (im Jahr 1994) entwickelte Peter Shor einen Algorithmus, dessen Rechenaufwand nicht exponentiell mit der Schlüssellänge wächst, sondern wesentlich kleiner ist (polynomiell zur Schlüssellänge). Allerdings erfordert dieser Algorithmus einen leistungsstarken universellen Quantencomputer mit hohen Kapazitäten. Zwar arbeiten seit den 1980ern Wissenschaftler*innen und Ingenieur*innen an ihrer Umsetzung und es ist längst kein rein akademisches Thema mehr. Ihre Umsetzung ist bislang aufgrund der äußerst schwierigen physikalischen Bedingungen noch nicht gelungen.

D-Wave war weltweit das erste Unternehmen, dass (spezielle) Quantencomputer kommerziell entwickelte. Die Größkonzerne IBM, Intel und Google entwickelten universelle Quantencomputer und erhielten dafür große Aufmerksamkeit und immense Forschungsgelder. Bisher sind die Kapazitäten viel zu gering (50, 49, 72 Quantenbits), um heute verwendete Schlüssel zu brechen. Krypto-Expert*innen erwarten eine solche Realisierung auch nicht so bald.

Aber insbesondere Staaten legen sich Quantencomputer zu. So auch die deutsche staatliche „Hackerbehörde“ ZITiS. Sie schafft sich gerade einen Quantenrechner an (zusammen mit der Bundeswehr-Universität in Neubiberg).

Um der Gefahr entgegenzuwirken, wird intensiv nach neuen Verschlüsselungsalgorithmen geforscht, die „quantenresistent“ sind[163]. Denn sollte eines Tages die Hardware für Quantencomputer mit ausreichend vielen Quantenbits entwickelt worden sein, dann wären asymmetrische Verschlüsselungsverfahren wie die, die GPG benutzt, nicht mehr sicher, unabhängig von der Schlüssellänge. Solange gilt jedoch: Je länger die Schlüssellänge, umso sicherer der Schlüssel vor Angreifer*innen.

Coreboot

Ein „Basic Input Output System“[164] wird gestartet, wenn ihr euren Rechner einschaltet. Der „Prozess“ initialisiert verschiedene Hardware-Komponenten eines Computers und startet anschließend den Bootvorgang des Betriebssystems. Im Kern ist es ein eigenständiges Betriebssystem, das auf nicht veröffentlichtem Quellcode der Herstellerfirmen basiert. Daher lässt sich der Quellcode auch nicht auf Schwachstellen untersuchen. UEFI, die Nachfolge für das bisherige BIOS, ist weitaus komplexer und noch weniger zu empfehlen[165]. Im Vergleich zu einer alternativen BIOS-Firmware wie Coreboot[166] besitzt es die hundertfache Menge an Quellcode und vergrößert bereits dadurch die mögliche Angriffsfläche. Sowohl das BIOS als auch der Nachfolger UEFI befinden sich auf sogenannten „BIOS Chips (SOIC-8)“ (die als wiederbeschreibbarer Speicher auf der Hauptplatine eines Rechners angebracht sind).

Da die Anwendungssoftware eines Betriebssystems auf diesen Bereich keinen Zugriff hat, bietet er sich zum Platzieren von Überwachungssoftware an (so können z.B. zum Aufspüren der Schadsoftware auch keine Antiviren-Programme oder ein IDS/HIDS[167] verwendet werden). **Eine erfolgreich dort platzierte Malware überlebt Neuinstallationen[168] und kann auch bei der Nutzung von Tails den Arbeitsspeicher auslesen** (z.B., um die Eingabe von Passwörtern mitzuprotokollieren, private Schlüssel zu speichern oder Screenshots anzufertigen und die „gewonnenen“ Daten anschließend zu verschicken[169].

---

163 Diese Verschlüsselungsalgorithmen werden als Post-Quantum-Kryptographie bezeichnet.

164 https://de.wikipedia.org/wiki/BIOS#Kritik

165 https://de.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface#Kritik

166 https://www.coreboot.org/

167 https://de.wikipedia.org/wiki/Intrusion_Detection_System

168 Auf diese Weise hat z.B. Lenovo 2015 sein eigenes BIOS manipuliert, um Benutzer*innenverhalten überwachen zu können. Die dafür verwendete Software überlebte auch Neuinstallationen des Windows-Betriebssystems oder einen Wechsel der Festplatte: https://gadgets.ndtv.com/laptops/news/lenovo-in-the-news-again-for-installing-spyware-on-its-machines-743952

169 Vorausgesetzt, eine Internetverbindung ist vorhanden. Daten können auch in geschützten Bereichen auf der Festplatte abgelegt werden: https://www.wired.com/2015/02/nsa-firmware-hacking/

170 http://legbacore.com/Research_files/HowManyMillionBIOSWouldYouLikeToInfect_Full2.pdf

Der Beitrag „How Many Million BIOSes Would you Like to Infect?“[170] stellt eindrucksvoll dar, wie einfach es ist, Malware im BIOS oder innerhalb des UEFI zu hinterlegen. Laut den Autor*innen waren für die Entwicklung eines BIOS-Trojaners nur wenige Tage nötig und es ließen sich 80 Prozent aller getesteten Rechner „infizieren“. Zum Auffinden der Schwachstellen wurde ein automatisiertes Skript verwendet, welches die vorhandenen Angriffspunkte so einfach fand, dass die Autoren aufgehört haben, mögliche „Verwundbarkeiten“ zu zählen. Da so gut wie niemand sein/ihr BIOS aktualisiert, ist eine große Anzahl der Schwachstellen auch weiterhin ausnutzbar (zum Teil stellen die Herstellerfirmen nach Bekanntwerden von Sicherheitslücken auch keine „Patches“ bereit).

Das BIOS konnte laut genanntem Beitrag über einen einfachen Phishing-Angriff[171] durch eine Software manipuliert werden. Voraussetzung hierfür war ein gestartetes Windows 10 Betriebssystem und die Ausnutzung einer Schwachstelle im „System Management Mode (SMM)“[172]. Es existieren noch diverse weitere BIOS-Trojaner, die sich bei veralteten Betriebssystemen und BIOS-Versionen durch die Ausnutzung von Schwachstellen remote installieren lassen (Speedracer, Thunderstrike, LightEater, . . .)[173]. Eine weitere Möglichkeit zum Platzieren der Schnüffelsoftware ist das „Flashen“ der entsprechenden Chips auf der Hauptplatine (Mainboard) durch einen physikalischen Zugriff (z.B. mit einem „Hardware Flasher“ wie dem *ch341a*, siehe Abschnitt „Benötigte Hardware zum Flashen der BIOS Chips, ebenfalls in der 6. Auflage der Tails-Broschüre“). Sollte ein Rechner auf einem dieser Wege manipuliert worden sein, ist es möglich, Passwörter und private Schlüssel auszulesen (und alles, was sich sonst noch im Arbeitsspeicher befindet). **Auch, wenn ihr Tails oder ein anderes Live-Betriebssystem benutzt.** Der Angriff funktioniert so einfach, weil Firmware nie mit dem Fokus auf „Sicherheit“ entwickelt wurde. Die Anleitung zur Anpassung eures BIOS im Kapitel „Wie bekomme ich Tails“ reicht leider nicht aus, um euch vor möglichen Angriffen wie den zuvor Beschriebenen zu schützen.

Und wäre das bisher Erwähnte nicht schon genug, existiert ein noch weitaus gefährlicheres und in sich geschlossenes Betriebssystem, das sich in fast allen Intel-Chipsätzen seit 2008 befindet: **die Intel Management Engine.** Sie ermöglicht folgende Optionen:

- Fernzugriff über das Internet
- Zugriff auf den Arbeitsspeicher und das Netzwerk[174]
- **Unsichtbarkeit gegenüber dem Betriebssystem (Antivirus, Firewall, . . .)**
- **Funktioniert mit jeder Stromquelle (AC, Batterie, Netzwerkkabel) - auch, wenn das Betriebssystem ausgeschaltet ist.**
- Nicht öffentlicher, undokumentierter Quellcode
- Kann nicht komplett entfernt werden, ohne den Rechner zu zerstören
- Besitzt Schwachstellen, die von Angreifer*innen ausgenutzt werden können (Behörden, Grenzübertritte, . . .)

In einer der nächsten Tails-Ausgaben wird es einen neu überarbeiteten Beitrag zum Schutz vor möglichen Firmware-Manipulationen geben. Und zwar über einen alternativen Weg, der ohne ein Zerlegen des Laptops auskommt und euer BIOS durch die alternative Firmware Coreboot[175] ersetzt. Wir orientieren uns dabei an einer Anleitung aus der Dokumentation von Coreboot, die eine UEFI-Sicherheitslücke ausnutzt und es so möglich macht, das BIOS ohne einen Hardware-Flash auf Ivy-Brigde basierende Thinkpads zu spielen. Aktuell arbeiten die Entwickler*innen von Coreboot zudem an einer Möglichkeit, die Intel Management Engine über Coreboot zu deaktivieren, was evtl. ein Flashen des zweiten BIOS-Chips erspart[176].

Alternativ besteht auch die Möglichkeit, euch von kommerziellen Anbieter*innen euer BIOS durch Coreboot ersetzen und die Intel Management Engine soweit wie möglich entfernen zu lassen. Es gibt mittlerweile auch Linux-Laptop-Hersteller*innen, die Coreboot bereits in ihrem BIOS integriert und die Intel Management Engine deaktiviert haben.

Den alten Beitrag zum Flashen der BIOS Chips findet ihr unter `https://capulcu.blackblogs.org/wp-content/uploads/sites/54/2019/01/Tails2019-01-27-A4.pdf`

171 `https://de.wikipedia.org/wiki/Phishing`

172 `https://de.wikipedia.org/wiki/System_Management_Mode`

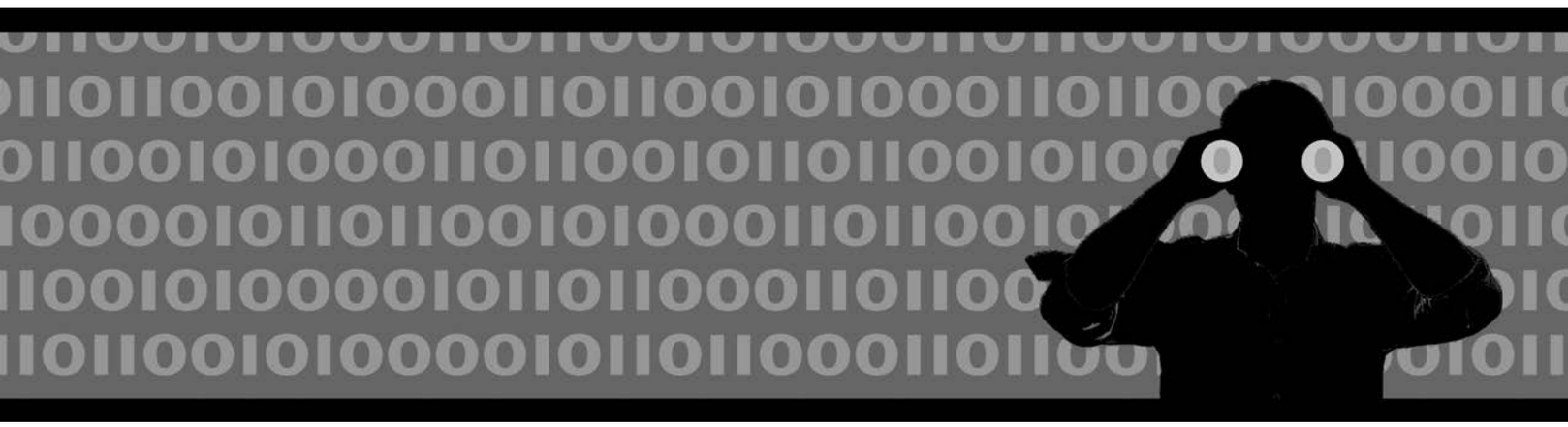
173 Ein erster Schutz dagegen sind regelmäßige Aktualisierungen des Betriebssystems/BIOS (siehe Abschnitt BIOS Upgrade (Lenovo) in Auflage 6 unserer Tails-Broschüre)

174 Auch, wenn der Rechner ausgeschaltet ist, lässt sich z.B. sämtlicher Netzwerk-Traffic mitprotokollieren.

175 `https://www.coreboot.org`

176 `https://review.coreboot.org/c/coreboot/+/37115`

Index



Hefte zur Förderung des Widerstands gegen den technologischen Angriff
Band 1: Tails - The amnesic incognito live system

Anleitung zur Nutzung des Tails-Live-Betriebssystems für sichere Kommunikation, Recherche, Bearbeitung und Veröffentlichung sensibler Dokumente

7. Auflage