IT-Sicherheit (ESC-IT)

Willkommen im WIki von ESC-IT :)

ESC-IT (gesprochen escape it oder escape IT) ist ein Kollektiv welches Inhalte für IT-Sicherheitstrainings für Aktivist*innen erstellt. Zielgruppe sind Aktivist*innen und Trainer*innen im Kontext des politischen Aktivismus.

Zur Aktualität und Qualität des Inhalts:
"Auch wir wissen natürlich nicht alles. Um Fehler in unserem Material zu vermeiden, gehen alle Inhalte vor der Veröffentlichung durch einen Review-Prozess. Für die Veröffentlichung muss mindestens eine zweite Person zustimmen.
Dennoch können Fehler passieren. Falls euch etwas auffällt, freuen wir uns über Hinweise. Am besten erstellst du hierfür einen Issue in unserem git-Repository oder schreibst uns eine Mail."

Dieses Wiki wird hier automatisch durch einen Bot eingebunden und aktuell gehalten.
Es kann nur durch den oben beschriebenen Prozess im Git-Repo bearbeitet werden.

- Anleitungen
  - Diceware
  - Signal
- Bedrohungen
  - Datenspeicherspürhunde
  - Phishing
  - Funkzellenabfrage
  - Verkehrsdatenüberwachung
  - Forensik
  - Persönliche-Überwachung
  - Public-Charger

Anleitungen

Diceware

Diceware ist ein Verfahren um mit Würfeln und einer Wortliste, Passphrases / Passwörter zu generieren. Diese enthalten echten Zufall und sind bei ausreichender Länge als sicher zu betrachten.

In diesem Tutorial wird kurz beschrieben, wie du in wenigen Schritten so ein sicheres Passwort erstellen kannst. Eine Anleitung auf Englisch findest du hier.

Tip

Wir empfehlen dir vorher die Seite zu Passwörtern durchzulesen. Dort erklären wir auch, wie lang deine Passphrase sein sollte und warum wir die Passphrase zufällig generieren. Es ist in jedem Fall nicht ausreichend, wenn du dir selbst 'zufällig' Wörter ausdenkst bzw. aus der Liste aussuchst. Außerdem empfehlen wir dir einen Passwortmanager zu benutzen damit du dir nur wenige wirklich sichere Passwörter merken musst.

Konzept

Die Idee ist, dass du für dein Passwort verschiedene Wörter aus einer Liste von ca. 7000 Wörtern auswählst. So bekommst du ein Passwort, das leicht zu merken ist und trotzdem echten Zufall enthält. Dazu brauchst du nur einen Würfel.

Schritt 1

Wähle eine Wortliste in einer Sprache aus, in der du dich wohlfühlst. Wenn deine Sprache nicht in der Liste ist, kannst du eine Wortliste finden, indem du nach "Diceware Wordlist" + "Sprache" suchst. Suche dir dabei eine Liste die für mindestens fünf Würfel ausgelegt ist, also mindestens 7776 Wörter enthält.

- Dereko Wortliste (kurze Worte) DE
- dys2p/wordlists-de DE
- EFF's Long Wordlist EN

- Website mit anderen Sprachen

Für dieses Beispiel verwenden wir die deutsche Dereko Wortliste mit kurzen Wörtern. Ihr könnt aber auch jede andere Liste welche für fünf Würfel ausgelegt ist nehmen.

Schritt 2

Würfle nun fünfmal mit dem Würfel und schreibe das Ergebnis in der Reihenfolge auf, in der du gewürfelt hast. zum Beispiel: `14314`

Nun schlage in der Wortliste nach welches Wort zu dieser Zahl passt. In diesem Fall: `batterie`

Schritt 3

Wiederhole Schritt 2 insgesamt sechs Mal. Du solltest jetzt sechs Wörter haben. Zum Beispiel:

`batterie tacker pferde wehen tresen zettel`

Herzlichen Glückwunsch zu deinem neuen Passwort!

Schritt 4

Wenn keine akute Repressionsgefahr besteht. Schreibe das Passwort auf einen Zettel und gib es ein- bis zweimal täglich ein. Nach ein bis zwei Wochen können sich die meisten Leute ihr neues Passwort gut merken. Dann vernichte den Zettel! Es ist auch ratsam, sich eine Geschichte zu den Wörtern auszudenken, um sie sich besser merken zu können.

Technische Details
Die Empfehlung sechs Wörter zu nehmen stammt aus dem offiziellen EFF Guide für Diceware

Anleitungen

Signal

Credit: Sämtliche Inhalte dieses Artikels wurden 1-zu-1 aus dem Signal Bereich des LG-Wikis übernommen.

Signal PIN einrichten

Es ist sehr wichtig, dass du in Signal eine PIN einrichtest. Diese schützt vor unberechtigter Neuregistrierung. Dein Netz-Provider muss auf richterlichen Beschluss hin SMS an die Polizei umleiten. Ohne PIN kann die Polizei Signal mitlesen - aber das merkst du, weil du dann selbst aus Signal raus fällst: es kann nur ein Handy bei Signal registriert sein.

So geht’s:

- iOS: tippe deinen Avatar an » Einstellungen » Konto
- Android: Einstellungen » Account (Konto) » Registration Lock (Registrierungssperre)

Verschwindende Nachrichten

In einzelnen Chats/Gruppen: Im Chat oben auf den Namen klicken » Disappearing Messages/Verschwindende Nachrichten

Es lässt sich auch ein default Zeitraum einstellen, dass das Feature für neue Chats automatisch aktiviert ist:

- Einstellungen » Privacy/Privatsphäre » Disappearing Messages/Verschwindende Nachrichten » Default Timer/Standardablaufzeit für neue Chats

Mehrere Signal-Accounts auf einem Gerät

Du kannst mehrere Signal-Accounts auf einem Gerät nutzen. Die Möglichkeiten sind für jedes Betriebssystem unterschiedlich, siehe die entsprechende Anleitung für dein Gerät.

Multiple Signal Accounts auf PC

Am einfachsten ist es, wenn du dir das Tool `signal-account-switcher` herunter lädst. Damit kannst du vier zusätzliche Signal-Accounts gleichzeitig nutzen. Dazu

1. auf diesen Link klicken: https://github.com/kmille/signal-account-switcher/releases/tag/v0.1.0
2. das Tool für dein entsprechendes Betriebssystem herunterladen (unten auf der Seite, `signal-account-switcher.exe` für Windows, `signal-account-switcher` für Linux, `signal-account-switcher-mac-{amd,arm}` für Mac).
3. das Tool starten (es kann sein, dass Windows erst mal meckert, weil das ja "unsicher" sei, einfach eine Datei aus dem Internet auszuführen) und einfach auf "Start Signal Account #1" klicken. Dann öffnet sich eine neue signal-desktop Instanz.

Wenn du keine Lust hast, ein extra Tool dafür zu installieren, kannst du das auch mit etwas manueller Konfiguration selbst machen:

- Anleitung für Windows: https://www.youtube.com/watch?v=TejhH80jktE
- Anleitung für Mac (dazu erst die Kommandozeile/Terminal öffnen):

```
mkdir $HOME/Library/Application/Signal-Account-1
/Applications/Signal.app/Contents/MacOS/Signal --user-data-dir="$HOME/Library/Application/Signal-Account-1"
```

Multiple Signal Accounts auf Android

Molly

Es gibt den Signal Fork Molly, der neben der normalen Signal App installiert und mit einem anderen Account eingerichtet werden kann.

1. Falls noch nicht geschehen, installiere F-Droid
   - Lade den alternativen App-Store FDroid herunter.
   - Installiere f-droid, indem du die .apk-Datei öffnest, die du heruntergeladen hast.
   - Lasse “Installation von Apps aus unbekannten Quellen” zu, wenn du danach gefragt wirst.
   - Erlaube ggf. “Apps aus dieser Quelle installieren”.
2. Füge Molly's Paketquelle zu deinem F-Droid hinzu (Anleitung)

- Gehe auf https://molly.im/download/fdroid/ und wähle Molly (wenn du gerade am Handy liest), oder scanne den QR-Code, wenn du den Artikel am PC liesst. **Wähle Molly, nicht Molly-FOSS, außer du weißt, was du tust** (zB keine Google-Play Dienste).
- Öffne F-Droid und refresh einmal (wische vom oberen Rand nach unten; damit lädst du Infos über alle verfügbaren Apps, dies kann bis zu 2 Minuten dauern.)

3. Installiere Molly über F-Droid
   - Suche in F-Droid nach Molly und installiere es. Lass dafür ggf. wieder “installieren aus dieser Quelle” für F-Droid zu.

Jetzt ist Molly bereit und du kannst die App ganz normal wie Signal einrichten.

Am Anfang wirst du jedoch gefragt, ob du eine zusätzliche *Passwortverschlüsselung* nutzen möchtest, deine Wahl kann später nicht mehr geändert werden. Für sensible Accounts (z.B. PP) ist das sinnvoll, ansonsten ist es wie bei der normalen Signal-App.

Erstelle eine Signal-PIN, die du dir wirklich sicher merken kannst, oder speichere sie in deinen sicheren Passwortmanager, aber schreib sie nicht auf einen Zettel! Dieser kann nach einer Hausdurchsuchung von der Polizei genutzt werden, um Nachrichten an dich abzufangen.

App Klone

Einige Hersteller bieten eine Dual-App-Funktion, um mehrere Accounts auf einem Handy zu betreiben. Suche im Netz, ob dein Gerät über diese Funktion verfügt. Ab Android 14 könnte diese Option standardmäßig auf vielen Geräten vorhanden sein.

Du kannst diese Funktion auch nutzen, um Signal und Molly zu klonen, so dass du dann 4 Accounts hast. Du könntest damit auch auf die Nutzung von Molly verzichten und 2x Signal nutzen, Molly ist aber sinnvoller, da Molly über eine leicht bessere Verschlüsselung und Sicherheitsmechanismen verfügt, die im Falle einer Hausdurchsuchung einen Vorteil bieten.

Du kannst die Funktion einfach in den Android-Einstellungen aktivieren:

Samsung: Einstellungen > Erweiterte Funktionen > Dual Messenger

Huawei: Einstellungen > Apps > App Twin

LG: Einstellungen > Allgemein > Dual App

Daraufhin sollte ein Menü mit allen klonbaren Apps angezeigt werden, dort kannst du Signal (und ggf. weitere zu klonende Apps) einfach auswählen und verdoppeln.

Weitere Android Profile

Android bietet die Möglichkeit, wie Linux MacOS und Windows auch, mehrere Benutzerprofile anzulegen.

Bedrohungen

Bedrohungen

Datenspeicherspürhunde

Im folgenden wird dieser Artikel unter der Creative Commons BY-NC-SA 4.0 von Netzpolitik.org wörtlich zitiert, da dieser das Thema ziemlich gut erklärt:

Der unwiderstehliche Geruch von Festplatten

Bei Hausdurchsuchungen kommen immer öfter auch „Datenspeicher-Spürhunde“ zum Einsatz. Sie können Smartphones, Festplatten und sogar SIM-Karten riechen. Bei deren Ausbildung will sich die Polizei allerdings nicht in die Karten schauen lassen.

Von Polizeihunden, die nach Rauschgift oder Sprengstoff suchen, haben alle schon gehört. Auch von Hunden, die nach Banknoten schnüffeln, auf der Suche nach Steuerflüchtlingen. Am Ende der letzten Dekade kam dann eine neue Ausbildung dazu: Hunde, die Datenträger erschnüffeln – und das Land Sachsen war Vorreiter. Im Fall des massenhaften Kindesmissbrauchs auf einem Campingplatz in Lüdge kam Deutschlands bis dahin einziger „Datenspeicher-Spürhund“ zum Einsatz. In der Folge bildete die Polizei von Nordrhein-Westfalen ebenfalls solche Hunde aus und präsentierte „Odin“, „Jupp“ und „Ali Baba“ auch in sozialen Medien.

Auf der Transparenz-Plattform FragdenStaat gibt es gleich mehrere Anfragen zu Datenspeicher-Spürhunden. Dort hätte man also mehr dazu erfahren können, wie die Polizei Hunde trainiert, damit diese CDs, Festplatten, Speicherkarten, USB-Sticks, Smartphones und SIM-Karten finden. Denn ganz offenbar haben Speichermedien einen ganz eigenen Geruch, den Hunde erkennen, wenn sie auf diesen konditioniert werden. Allerdings hat die NRW-Polizei die Ausbildung der Hunde als „Verschlusssache“ eingestuft und großflächig geschwärzt, und so muss man sich stattdessen auf Medien wie zooroyal und deren Berichterstattung über die „Fellnasen“ verlassen.

In einem Bericht der Süddeutschen Zeitung heißt es, dass die Suche nach Datenträgern viel schwieriger sei als nach Drogen, die einfach stärker riechen würden als die handelsübliche Festplatte. Auch die Polizei Sachsen-Anhalt schreibt in einer Präsentation, dass die Datenträger kaum Geruchsmoleküle freisetzten.

Der sächsische Diensthundeführer sagte der Zeitung damals, dass der Hund die Chemikalien rieche, die zur Herstellung der Speichermedien verwendet werden. Er habe sogar den Eindruck, dass sein Hund Lithium-Ionen-Akkus schneller fände als Handys mit Chrom-Nickel-Batterien und gehe davon aus, dass „Artus“ Lithium riechen könne.

Weil die gesuchten Datenträger so wenig Geruch verströmen, verlange die „Spürarbeit“ eine „hohe, ausdauernde und körperlich anstrengende Leistung“ des Diensthundes, heißt es in den Unterlagen aus Sachsen-Anhalt. Deswegen setze diese Ausbildung „ein fokussiertes, sachliches Spürverhalten des DH [Diensthundes] voraus.“

Belohnung: Beißwurst

Die Polizei NRW selbst verrät auf ihrer Webseite, wie die Suche vor sich geht: „Hört Hank [Hund] das Kommando »Spür!«, beginnt er zu suchen. Bleibt er bewegungslos stehen, weiß Peter Baumeister [Hundeführer]: Er hat etwas gefunden. Als Belohnung bekommt Hank dann sein Lieblingsspielzeug: eine Beißwurst.“

Demnach dauert die Zusatz-Ausbildung eines Spürhundes zum Datenspeicher-Spürhund 20 Tage, welche der Hund zusammen mit seinem Bezugsmenschen absolviert. Nach der Ausbildung darf sich der Mensch dann „Datenspeicherspürhundführer“ nennen. Ein Wort, wie es deutscher kaum klingen könnte.

Phishing

Das Phishing mit E-Mails oder SMS ist zwar im Allgemeinen eher im Kontext von Enkeltricks oder anderem Scam bekannt, doch auch staatliche Akteure nutzen gerne Phishing, um Zielpersonen mit Malware zu infizieren.

Hierbei sind ein paar Sachen zu bedenken. One-Click-Malware, also jene, bei der User*innen proaktiv auf einen Link klicken, oder einen Download tätigen müssen, damit das Gerät infiziert werden kann, ist um einiges günstiger zu haben, als Zero-Click-Lösungen, bei denen Geräte, ohne weiteres Zutun der Nutzenden infiziert werden können.

Außerdem sind Phishingangriffe auch relativ schwierig zurück zu verfolgen. Fliegt das Phishing auf, bleibt trotzdem meist unklar, von wem der Angriff stammt, was eine ziemlich sichere Angriffsposition ermöglicht. Bei einer heimlichen Wohnraumverwanzung aufzufliegen ist deutlich riskanter und alarmiert die Betroffenen. Phishing hingegen landet bei uns allen ständig im Postfach und weckt kaum Misstrauen.

Hier ist ein Beispiel für, durch geschickte Wahl von Unicodezeichen, gefälschte Links. Erkennst du einen Unterschied in den Links? Welcher Link führt auf welche Seite?

Beispiel 1

- https://codeberg.org/esc-it/esc-it.org/releases/tag/@esc-it.org
- https://codeberg.org/esc-it/esc-it.org/releases/tag/@esc-it.org

Ausnahmsweise, nur zum Lernen, kannst du jetzt auf die beiden Links klicken, um zu sehen was passiert. Hat deine Vermutung gestimmt?

Der 1. Link führt nicht auf codeberg.org sondern auf esc-it.org. Durch das @ wird der Teil davor als Nutzername verwendet. Eigentlich sollte das nicht funktionieren wenn vor dem @ ein / ist, aber im 1. Link sind Unicode Zeichen, die kein "normales" Slash sind.

Manche Browser zeigen bei dem falschen Link sogar eine Warnung an, wie hier in Firefox und dessen Fork Librewolf:
Ein Pop-Up in Firefox warnt, dass wir dabei sind uns bei einer Webseite anzumelden die keine Anme

Chromium zeigt beispielsweise keine solche Warnung.

Auffällig an den Links ist, dass am Ende eine Domain steht (...@<esc-it.org>). Aber auch das ist kein eindeutiges Zeichen für Fakes und wird mit immer neuen Top-Level-Domains zunehmend schwer zu erkennen. Hier ein Beispiel mit einer ".zip"-Endung, sodass es sowohl eine .zip-Datei als auch eine .zip-Domain sein könnte:

Achtung: Der erste Link führt auf eine Domain *(1312.zip)*, die nicht uns gehört. Das heißt wir wissen nicht was darauf geschieht. Daher besucht diesen Link bitte nicht einfach, wenn ich nicht genau wisst, was ihr tut.

Beispiel 2

- https://codeberg.org/esc-it/esc-it.org/releases/tag/@v1312.zip
- https://codeberg.org/esc-it/esc-it.org/releases/tag/v1312.zip

Auch hier führt der erste Link nicht auf eine Zip-Datei auf codeberg.org, der zweite Link aber schon. Hier erscheint auch keine Warnung, weil es die Domain bisher nicht gibt.

Fazit

- Klickt nicht auf komische Links
- Hinterfragt den Ursprung des Links. Kann das sein, dass mir diese "Adresse" genau diesen Link schickt.
  - Geht auf Nummer sicher und sucht die Seite über verifizierbare Wege. Speichert originale Links in euren Passwortmanagern, in Lesezeichen im Browser oder nutzt Suchmaschinen.
- Tippt die Links im Zweifel von Hand ab.
  - Das hilft aber nichts, wenn der Link per se ein Fake ist. [systeml1.org] wird Euch so oder so auf die falsche Fährte führen. Hierbei wieder der Verweis auf den Punkt oben drüber um die korrekte URL festzustellen.

Funkzellenabfrage

Um dieses Kapitel zu verstehen ist es notwendig die grundlegenden Konzepte von Mobilfunkzellen (im Folgenden MFZ abgekürzt), insbesondere den Verbindungs- bzw Authentifizierungsprozess zwischen Handy und Mobilfunkzelle, zu verstehen. Wir haben versucht, das im Artikel Mobilfunk verständlich zu veranschaulichen.

Die Funkzellenabfrage ist eine in § 100g Abs. 3 StPO geregelte Maßnahme, derer sich Strafverfolgungsbehörden in ihren Ermittlungen bedienen können. Dabei Fragen die Behörden bei den Betreibern der in dem Fall interessanten MFZ bestimmte Daten zu deren Nutzung ab.

Karte, die symbolisch zeigt, wie mobilfunkzellen in einer Stadt verteilt sind

Was wird bei Funkzellenabfragen abgefragt?

Bei Funkzellenabfragen werden folgende Daten im abgefragten Zeitraum und "Ort" (also ein bestimmtes Gebiet, das evtl von mehreren MFZ abgedeckt wird) erhoben:

- eingeloggte Rufnummern
- Zeitpunkte von:
  - Einwahl/Auswahl der Geräte
  - Aus- und eingehender Anrufe
  - Mailbox Gespräche
  - gesendete/empfangene SMS

Oftmals werden beispielweise bei Demos Funkzellenabfragen vor, während und nach der Demo gemacht. Dadurch kann beispielsweise ersichtlich werden, welche Geräte sich nur zum Zeitpunkt der Demo an diesem Ort aufgehalten haben und welche Geräte dort evtl "zu Hause" sind.

Welche Geräte zu Zeitpunkt X an welchem Ort, durch FZA

Außerdem können natürlich über Funkzellenabfragen auf einem größeren Gebiet Bewegungsprofile erstellt werden, in dem Ein- und Auswahlzeitpunkte einzelner Geräte bei den jeweiligen MFZ betrachtet werden:

Route von Gerät durch Stadt wird durch FZA ersichtlich

Statistiken zu Funkzellenabfragen

Verfahren in denen Funkzellenabfragen durchgeführt wurden

Die Zahlen belaufen sich auf die durchgeführten Abfragen. In einer Abfrage können durchaus mehrere Hunderttausend Geräte betroffen sein. Das geht sogar soweit, dass in Berlin im Jahr 2016 statistisch jedes einzelne Handy alle 11 Tage in einer Funkzellenabfrage landete.

Mehr Details zu dieser Statistik

Verkehrsdatenüberwachung

Überwachung von Verkehrsdaten

Das ist meistens gemeint, wenn allgemein von TKÜ gesprochen wird. Hier zwingen die Behörden die Serviceanbieter dazu, eure Anschlüsse explizit zu überwachen und den Behörden sämtliche mitgeschnittenen Verkehrsdaten zu kommen zu lassen. Dafür ist ein richterlicher Beschluss notwendig.

Das ist möglich, weil normale Telefonverbindungen, also: Festnetz, Sprachanrufe, SMS und (last but still not missing) Mailboxgespräche lediglich **transportverschlüsselt** sind.

Transportverschlüsselung

Bei der Transportverschlüsselung wird quasi jedem Teilnehmer in der Kette der gesamten Übertragung einer Nachricht das Recht gegeben die Nachricht zu öffnen und zu lesen.

Schreibt ihr beispielsweise eine normale Email, so geht die Email zunächst transportveschlüsselt an den Mailserver. Dazwischen kann niemand mitlesen. Der Mailserver jedoch kann die Mail öffnen und scannen. Das tun sie in der Regel auch, denn woher sollten eure Mailanbieter wissen was in den Spamordner gehört. Jetzt schickt euer Mailserver die Mail, wieder transportverschlüsselt, an den Mailserver des Empfängers der Mail. Auch dieser kann die Mail auspacken und scannen. Daraufhin schickt dieser Mailserver die Mail abermals transportverschlüsselt an den Empfänger.

Eine schematische Darstellung eines MITM-Angriffs durch die Polizei bei Transportverschlüsselung

Und so funktioniert das im Grunde auch mit Sprachanrufen und SMS.

Hieraus ist ersichtlich, das die Mailanbieter/Mobilfunkanbieter, die ja immer die Berechtigung haben euren Verkehr mitzulesen, der optimale Angriffspunkt für die Behörden sind. Dort können sie (mit richterlichem Beschluss) anklopfen und euren gesamten Datenverkehr verlangen.

Deshalb ist es so wichtig Ende-zu-Ende Verschlüsselung zu benutzen!

Statistiken zur TKÜ

Hier findest du eine detaillierte Erklärung zu dieser Statistik.

Forensik

Digitale Forensik

Hilfe gesucht
Wenn du dazu etwas beizutragen hast, schau gerne bei dem Issue vorbei und mach mit!

Physische Forensik

Bisher gehen wir hier nicht im Detail drauf ein. Generell sind klassische Forenskimethoden der Strafverfolgung zu beachten. Dazu gehören die Sicherstellung von:

- Faserspuren
- Schuhabdrücke
- Fingerabdrücke
- DNA
- ...

All diese Spuren können durchaus schwer zu vermeiden sein, besonders DNA und Faserspuren werden bei so ziemlich jeder Bewegung hinterlassen. Was das allerdings für das spezifische Threat Modeling bedeutet muss gesondert diskutiert werden. Die Analyse von diesen Dingen ist in aller Regel sowohl sehr Zeit als auch Kosten aufwendig. Trotzdem zeigen sich in einzelnen Fallbeispielen, dass verwirrte Cops das auch bei Bagatellen schon angeordnet haben, wie im Beispiel Adbusting Höcke

Persönliche-Überwachung

Hilfe gesucht

Zu den verschiedenen Arten von verdeckten Ermittler*innen suchen wir nach weiteren Informationen sowie nach Statistiken zu deren Einsätzen. Falls du hierzu etwas beitragen kannst, schau doch gerne mal in die verlinkten Issues rein.

In den letzten Jahren haben sich Fälle von Personen bezogener Überwachung vermehrt. Immer häufiger werden Aktivist*innen Ziele von Zielfahnder*innen, V-Leuten oder anderen Spitzeln des deutschen Repressionsapparates.

Zu den Begrifflichkeiten und Unterschieden:

- Zielfahnder: Suchen und observieren Personen
- Tatbeobachter: Das ist die klassische Demo-Zifte. Sie lungern meist in BFE-Einheiten und sind oft bei Demos dabei um Straftaten zu beobachten. Zur besseren Dokumentation machen Sie teilweise während der Demo Bilder von den Personen, deren Kleidung, Rucksäcken oder Schuhen. Sie verfolgen vermeintliche Täter*innen, deren Festnahme teils direkt nach der Demo oder nach nur wenigen Stunden erfolgt. Sie sind vergleichsweise unauffällig, haben also keinen Knopf im Ohr, oder im Ärmel. Das Äußere wird dem entsprechenden Anlass angepasst, gerne auch selbst vermummt.
- Verdeckte Ermittler*innen (VE): Oftmals wenig inhaltliche Positionierung. Haben nur Zeit bei "spannenden Sachen".
- Zivilpolizei: Mit Westen und Knopf im Ohr, erkenntlich am Rand der Demo
- Vertrauens-/V-Personen: Sie werden gezielt vom Staat aus der Szene angeworben. Sie sitzen in Plena und wissen über Aktion/Leute und beteiligen sich rege am Szene-Leben

Public-Charger

Öffentliche "Ladegeräte" finden sich beispielsweise in öffentlichen Verkehrsmitteln, Cafés, Bibliotheken, Flughäfen, Einkaufshäusern und co.

Unterschieden werden sollen hier natürlich zwischen einfache Steckdosen und USB-Ladebuchsen.

Das Schlimmste, was bei normalen Steckdosen passieren kann ist, dass dir dein eigenes Ladegerät kaputt geht. Abgesehen davon ist ja dein eigenes Ladegerät eh nur zum Aufladen gut und kann daher auch nicht wirklich mehr.

Bei USB-Ladebuchsen sieht es schon ein bisschen anders aus. Seit Jahren häufen sich Fälle von manipulierten Ladebuchsen, hinter denen sich nicht nur eine Spannungsquelle, sondern gleich ganze Mikroprozessoren verbergen, die versuchen auf das angeschlossene Gerät zuzugreifen. Dabei könnte Malware installiert werden, auf den Speicher zugegriffen werden und so weiter.

Netterweise sind mittlerweile sämtliche (mobilen) Betriebssysteme mit Schutzvorkehrungen ausgestattet und fragen die Nutzenden, ob dem angeschlossene "Gerät" Zugriff auf das Handy gegeben werden soll. Allein diese Frage sollte uns schon misstrauisch machen, denn:

Achtung

eine einfache USB-Buchse mit der klassischen 5V Spannungsversorgung wird von keinem Handy als "Gerät" erkannt, dem irgendwelche Rechte gegeben werden sollten!

Weiter kann dem vorgebeugt werden, wenn zum Aufladen nur USB-Kabel ohne "data lines" verwendet werden. Das sind solche Kabel mit denen keine Daten übertragen werden können. Das kann man in der Regel einfach am eigenen Rechner mal ausprobieren. Wenn mit dem USB Kabel nicht auf das Handy zugegriffen werden kann, dann hat dieses USB Kabel sehr wahrscheinlich nur 2 Drähte: Plus und Minus. Darüber können dann keine Daten übertragen werden.

Achtung

Besonders bei USB Ladebuchsen sei vor manipulierten Spannungsversorgungen gewarnt!

Anders als bei manipulierten Steckdosen, an denen ja noch euer eigenes Ladegerät steckt, kann hier eine manipulierte Spannungsversorgung das Gerät sehr direkt ernsthaft beschädigen.

Daher empfiehlt es sich diese Buchsen wo es auch geht zu meiden.

Falls sie doch einmal benutzt werden müssen, am besten:

- nur mit zwei-adrigen USB Kabeln benutzen
- Buchsen benutzen, bei denen ihr gesehen habt, dass schon vorher jemand ein Handy geladen hat, ohne es danach schreien von sich zu werfen.

Staatstrojaner

Quellen-TKÜ

Die Quellen-TKÜ ist quasi eine Online-Durchsuchung "light". Dabei wird zwar die selbe Software wie bei der Online-Durchsuchung eingesetzt, allerdings soll hier nur der live ein- und ausgehende Datenverkehr mitgeschnitten werden. Das Durchforsten von gespeicherten Inhalten ist hierbei nicht erlaubt und angeblich bei eingesetzter Software - durch entsprechende Modifikationen - auch nicht möglich.

Entstanden ist dieses Konstrukt, weil Online-Durchsuchungen einen sehr extremen Eingriff in die Privatsphäre sind, werden sie manchmal von Richter*innen auf Grund von "Unverhältnissmäßigkeit" nicht genehmigt. E2E-Verschlüsselung verhindert aber eine effektive TKÜ bei Serviceanbietern. Also wird diese "abgespeckte" Schadsoftware eingesetzt, da sie eher richterlich genehmigt wird. So können sämtliche Up- und Downloads (hier sind auch Chat-Nachrichten mit gemeint) jeweils vor der Verschlüsselung, oder nach der Entschlüsselung, auf den Endgeräten mitgelesen werden.

Statistiken Quellen-TKÜ

Hier findet ihr mehr Details zu der Statistik der **Quellen-TKÜ**

Online-Durchsuchung

Wenn von Staatstrojanern die Rede ist, dann ist meist die Online-Durchsuchung gemeint. Hierbei werden betroffene Geräte mit Schadsoftware infiziert, sodass die Angreifer (i.d.R. Cops) vollen Zugriff auf das Gerät haben. Das bedeutet sie können sowohl live mitverfolgen was gerade auf dem Gerät gemacht wird, Kameras und Mikro's anschalten, Standorte abrufen, als auch gespeicherte Inhalte wie Nachrichten, Bilder, Kontakte, Kalender, Notizen einsehen und ausleiten. Die Vorteile davon liegen auf der Hand. Betroffene bemerken die Maßnahmen überhaupt nicht. Geräte müssen eventuell noch nicht einmal beschlagnahmt werden und Festplattenverschlüsselung wird somit "nutzlos" gemacht.

Statistiken Online-Durchsuchung

Statistiken Online-Durchsuchung

Hier findet ihr mehr Details zu den obigen beiden Statistiken zur **Onlinedurchsuchung**

Es ist daher mit Blick auf Online-Durchsuchung und Quellen-TKÜ zu beachten, dass die eingesetzten Softwares aus unterschiedlichen Quellen stammen. Der berühmte Staatstrojaner Pegasus der NSO-Group, oder Predator von Intellexa erfordern extrem teure Lizenzkosten.

Aus von der New York Times geleakten Predator Files ist beispielsweise zu erkennen, dass eine Lizenz zum Infizieren von 20 iOS oder Android Geräten, mit 12 monatiger Garantie, 13,6 Mio € (Euro) kosten soll. Die zu Verfügung gestellte Schadsoftware ist dabei "nur" eine 1-click-solution, bei der die Zielpersonen noch selber auf irgendeinen Link klicken müssen.

Einen Reboot von infizierten iPhones überlebt der Trojaner nicht, dafür müssen nochmal 2,4 Mio € gezahlt werden. Für Sim-Karten aus anderen Ländern, als dem agierenden, müssen 3,5 Mio € extra fließen.

Hier lässt sich also feststellen, dass eine solche Lösung sehr teuer ist. Allerdings haben deutsche (und andere) Behörden auch schon eigene Staatstrojaner gebaut, von denen aber zumindest bisher nicht bekannt wurde, dass sie remote infizieren können, sondern über Hardwarezugriff verfügen müssen.

Daher sollten Geräte auch physisch geschützt werden, denn die Behörden dürfen unter Umständen, wie bei der Wohnraumüberwachung auch, in eure Wohnung einbrechen und auf eurer Hardware heimlich Schadsoftware installieren. Um dem vorzubeugen ist es ratsam, Teile die zum Öffnen der Hardware bewegt werden müssen, so zu bearbeiten, dass ihr einen solchen Zugriff sofort bemerkt.

Quellen-TKÜ+

Die Quellen-TKÜ+ stellt lediglich weiteres ein juristisches Konstrukt dar, auf das wir aber hier nicht eingehen wollen, da es bei einem Staatstrojaner bleibt. Falls ihr mehr darüber lesen wollt, gibt es dazu eine Stellungnahme des CCC.

Zitat aus der Stellungnahme des CCC

> Die nur rechtlich definierte Trennung zwischen den „Payloads“ der heimlichen Schadsoftware, die nunmehr drei Trojaner-Varianten („Quellen-TKÜ“, „Quellen-TKÜ+“ und „Online-Durchsuchung“) hervorgebracht hat, ist technisch nicht begründbar […]
> Durch die oben skizzierten Infektionswege und den zwingend damit einhergehenden tiefen Veränderungen in den Sicherheitsmechanismen der angegriffenen Systeme wird deutlich, dass eine technische Abgrenzung zwischen dem Staatstrojaner zur Festplatten-Durchsuchung („Online- Durchsuchung“) und dem Trojaner zum Abhören der laufenden Kommunikation („Quellen-TKÜ“) sowie der mittlerweile dritten Trojaner- Variante („Quellen-TKÜ+“ oder „Kleine

Online-Durchsuchung“), die auch gespeicherte Inhalte und Umstände der Kommunikation erfassen darf, in der Praxis bei ehrlicher Betrachtung weder zuverlässig zu gewährleisten noch überhaupt klar zu umreißen ist. Die „technischen Vorkehrungen“, die alle drei Staatstrojaner-Varianten unterscheiden sollen, könnte man zwar zu implementieren versuchen, allerdings scheitert offenbar das BKA seit mehr als einem Jahrzehnt daran, Trojaner-Varianten zu entwickeln oder zu kaufen, die alle grundrechtlich gebotenen Vorgaben sicher erfüllen.

Letztlich bleibt die Unterscheidung aller drei Trojaner-Varianten eine juristische und zudem theoretische, die mit den Realitäten der Trojaner- Branche und mit den technischen Notwendigkeiten beim erfolgreichen Infizieren eines informationstechnischen Geräts nicht zusammengehen.

Hierzu gab es auch einen früheren Fall, bei dem der CCC 2011 einen Staatstrojaner zerlegt hat und dabei zeigte, dass dieser natürlich technisch alles mit dem System machen konnte. Daraufhin, hat das Bundesverfassungsgericht das Gesetz 2016 auch für teilweise Verfassungswidrig erklärt.

Bedrohungen

Video-Audio-Überwachung

Videoüberwachung - öffentlicher Orte und Plätze

Insbesondere an Anlagen und Einrichtungen der Bahn. Es besteht ein eigener Nutzungsvertrag zwischen Bahn und Bundespolizei, der festlegt, dass die Infrastruktur der Videoüberwachung durch die Deutsche Bahn betrieben wird und die Bundespolizei diese nutzen darf.

Weiter sind oft Orte betroffen, wo es "gehäuft zu Drogenhandel, Diebstahl oder Gewalt kommt"

"Intelligente Videoüberwachung"

Es gab einen Pilotversuch am Berliner Südkreuz 2019 und seit Juni 2023 in Hamburg auf dem Hansaplatz.

2023 implementiert der schweizer Bahnhof in Schaffhausen "intelligente" Kamerasysteme, um das Kaufverhalten von Kund*innen zu analysieren und Ladenmiete nach Kundenaufkommen aufzuschlüsseln.

Seit 2018 wird die Mannheimer Innenstadt mit KI-Technik vom Frauenhofer-Institut in München Überwacht. Von 68 Überwachungskameras der Polizei in Mannheim sind 10 mit "KI-Software" ausgestattet. Der Einsatz dieser Technik wurde im Dez. 2023 bis 2026 verlängert

Bisher sollen alle oben genannten Systeme keine direkte Identifikation von Individuen zulassen. Das heißt, dass die Systeme nur Situationsabhängig den gerade erkannten Personen einen *Identifier* zuweisen, der nur zur Verarbeitung der jeweiligen Videosequenz dienen soll. Personalien sollen so nicht festgestellt werden können.

In Rheinland-Pfalz gibt es seit 2023 "Handy-Blitzer", die Autofahrer*innen fotografieren und nach "Handy-am -Ohr" - Situationen analysieren.

In Frankreich werden zu Olympia 2024 massenhaft "intelligente" Verhaltensscanner eingesetzt werden.

Videoüberwachung Demonstrationen

Hilfe gesucht
Bei den Ermittlungen zu den G20 Protesten wurde Videomaterial mittels Gesichtserkennung ausgewertet. Hier könnten Details dazu eingefügt werden.

Gesichtserkennung bei G20, nicht zum Identifizieren sondern zum Verfolgen

- Polizei mit Kameras
- Kamerawagen
- Insbesondere hier Datenauswertungen

Video- Audioüberwachung - private Räume

Prinzipiell können private Räume verwanzt werden, auch wenn sich Verdächtige nur ab und zu darin aufhalten.

In der folgenden Statistik sind die Verfahren in denen Wohnraumüberwachung eingesetzt wurde aufgelistet. Die Statistik erfasst nur Verfahren, die geeignet sind den Schutzbereich des § 13 GG, die Unverletzlichkeit der Wohnung, zu berühren. Verfahren in denen andere Räume überwacht wurden sind demnach nicht erfasst.

Statistik Wohnraumüberwachung

Massenüberwachung

Chatkontrolle

Heiß diskutiert in 2023. Stand Okt. 2023 ist auch dieser Form der anlasslosen Massenüberwachung eine Absage erteilt worden. Vom Tisch ist aber auch dieses Thema nicht, da es höchstwarscheineich zu einem der großen Themen im EU-Wahlkampf Mitte 2024 wird.

Vorratsdatenspeicherung

- anlasslose, präventive Speicherung sämtlicher Verkehrsdaten (keine Inhalte)
- EUGH-Urteil (Sep. 2022): rechtswidrig

Quick-Freez

- BKA fordert "Quick-Freez"
  - "einfrieren" von Verkehrsdaten nach richterlichem Beschluss (einen Monat lang)
  - bisher politisch noch nicht umgesetzt

Imsi-Catcher

Ein IMSI-Catcher simuliert eine kommerzielle Mobilfunkzelle (MFZ), um die Clients dazu zu bewegen, mit ihnen eine Verbindung aufzubauen. Generell gilt:

- Endgeräte loggen sich bei MFZ mit stärkstem Signal ein.
- Funkzelle fordert „Identity Request“
- Endgeräte authentifizieren sich mit IMSI + IMEI (und erhalten TMSI von der MFZ).

Dabei kann im Groben zwischen passiven und aktiven IMSI-Catchern unterschieden werden:

Passive IMSI-Catcher warten nur darauf, dass Clients versuchen sich mit ihren Identifier bei der MFZ zu authentifizieren. Damit können detaillierte Informationen darüber gesammelt werden, wer, oder viele Personen sich bspw. bei einer Demo aufhalten. Den Clients fällt der Schwindel auf Grund des GSM-Protokolls nicht auf.

Aktive IMSI-Catcher warten nicht nur auf die Synchronisationsanfrage des Clients. Sie geben dem Client auch eine TMSI (kann hier mit lokaler IP verglichen werden) und bauen sogar in seinem Namen eine legitime Verbindung zu einer echten MFZ her. Damit können vollwertige 'machine-in-the-middle-attacks' realisiert werden.

Welche Sicherheitslücke wird hier ausgenutzt?

Das Problem liegt bei der Authentifizierung zwischen Telefon und der MFZ(Mobilfunkzelle). Das Telefon muss sich nämlich (wie unten dargestellt) gegenüber der MFZ mit seinen einmaligen/unverwechselbaren Identitäten (IMSI, IMEI) verifizieren, um zu beweisen, dass es das Recht hat, das Mobilfunknetz zu benutzen.

Die Funkzelle authentifiziert sich gegenüber dem Telefon jedoch **nicht**. Deshalb kann das Telefon auch nie sicher wissen, ob es gerade wirklich mit einer normalen, kommerziellen MFZ kommuniziert, oder nicht doch mit einem Klon der Behörden.

Aktiver IMSI-Catcher - Systematik

Warum ist die Kommunikation Telefon-Polizei unverschlüsselt?

Die Antwort findet sich in der oben beschriebene Schwachstelle im Kommunikationsprotokoll bei der Authentifizierung. Durch bestimmte Schritte ist es dem IMSI-Catcher möglich, das Telefon beim Authentifizierungsprozess auf einen alten Mobilfunkstandart (idR. 2G) herunter zu zwingen. Das ist allgemein möglich, um in Situationen, in denen moderne Standards (3G/4G) keinen Empfang bieten, die noch vorhandene 2G Infrastruktur nutzen zu können. Diese ist oft in der territoriale Abdeckung etwas resistenter als die moderneren. Der 2G-Standart wiederrum ist schon lange überholt und Sicherheitstechnisch in keinem Fall zu empfehlen. Von staatlichen Akteuren einmal abgesehen, ist es sogar privaten Menschen möglich, 2G-"verschlüsselte" Kommunikation sehr schnell zu entschlüsseln und mitzulesen/hören. Deshalb Kennzeichnen wir diese Kommunikation in seiner Praxis als "unverschlüsselt"

Warum ist die Kommunikation Polizei-Mobilfunkzelle wiederum verschlüsselt?

Um sogenanntem "eaves dropping" – also dem belauscht werden – entgegen zu wirken, akzeptieren die MFZ der neuen Standards nur Kommunikation, die mit ihrem jeweiligen Standard verschlüsselt wurden. Damit das Telefon also nicht merkt, das es eigentlich mit einer falschen MFZ verbunden ist, muss der IMSI-Catcher also auch eine real-funktionierende Verbindung zum Mobilfunknetz aufbauen. Dafür muss er die Verbindung zur MFZ wieder verschlüsseln.

Praktische Gefahren

Das heißt

- Handy mit privater SIM & IMEI macht identifizierbar & ortbar
- "Anonyme" SIM-Karte und Handy ist nicht gleich anonym

Es ist zu beachten, dass dadurch potentiell Gefahr besteht, wenn ein "anonymes" Handy wiederverwendet wird. In Zusammenhang mit Funkzellenabfragen lassen sich unter Umständen Bewegungsprofile dieser Geräte herstellen und kontextualisieren.

Ein potentielles Beispielszenario könnte so aussehen: Ihr benutzt euer Aktionshandy auf mehreren Aktionen/Demos, gerne auch in verschiedenen Städten/Bundesländern. Bei diesen Demos landet

ihr (eure IMSI+IMSI) mehrfach in Funkzellenabfragen. Damit kann erst einmal niemand etwas anfangen, außer zu sagen, dass dieses Gerät auf all diesen Veranstaltungen präsent war. Nun lauft ihr aber auf weiteren Demos an IMSI-Catchern vorbei und werdet ggf. dabei kontrolliert oder gefilmt. Dadurch könnte natürlich über die Zeit eine Korrelation zwischen euch und dem Gerät hergestellt werden.

Hardware für professionelle IMSI-Catcher kommt in in Deutschland und Umgebung in der Regel von Rhode&Schwarz. Deren Geräte sind global, nicht nur bei Strafverfolgungsbehörden, bekannt und beliebt. Diese State-of-the-Art Technik ist auch dementsprechend teuer, Preise bewegen sich in 4-5 stelligen Bereichen.

Es lassen sich allerdings auch mit ~25€ "teuren" SDR-Dongles (Software Defined Radios) simple passive IMSI-Catcher realisieren. Diese sind allerdings nur dazu fähig, den existierenden Verkehr mitzulesen, jedoch nicht dazu, eine fake MFZ aufzusetzen und tatsächliche MITM Attacken auszuführen.

Empfehlung

Lukas Arnold beschreibt in seinem Talk auf dem 37c3 (CCC-Congress 2023), wie es mit ihrem selbst gebauten Tool möglich sein sollte, fake base stations mit Hilfe eines iPhones zu erkennen.

Quellen

- https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks
- SnoopSnitch-Talk (gehört in Empfehlungen): https://media.ccc.de/v/ber15-5-detecting_imsi-catchers_and_other_mobile_network_attacks

Statistik zu IMSI-Catchern

IMSI-Catcher - Statista

Shoulder-Surfing

Shoulder Surfing meint, wenn dir jemand heimlich über die Schulter schaut, um zu sehen, was du so auf deinem Handy, Laptop, Din A4 Block oder was auch immer tust bzw. tippst.

Besonders beim Passwörter eintippen gilt besondere Vorsicht!

Denn das bester Passwort hilft natürlich nichts, wenn es den Behörden in die Hände fällt.

Zu aller erst sei hier auf die immer mehr werdende [Videoüberwachung](https://wiki.aktivismus.org/books/it-sicherheit-esc-it/page/video-audio-uberwachung) hingewiesen. Gib keine Passwörter unter Kameras ein!

Wenn du selber schonmal versucht hast shoulder zu surfen, wird dir aufgefallen sein, dass es Orte und Situationen gibt, die dafür besonders gut geeignet sind.

In vollen Hörsälen beispielsweise kriegt man die Bildschirme und Tastaturen von mindestens 3 seiner Vorderpersonen praktisch vor die Nase gehalten.

Auch in öffentlichen Verkehrsmitteln sind besonders jene Sitze geeignet, die sich nicht direkt hinter der Zielperson, sondern schräg dahinter befinden. Ist der Bus extrem voll, fällt es noch nichtmal auf, wenn eine Person geradezu über deinem Handy hängt, während du tippst.

In solchen Situationen ist es wichtig sich wie im ehrlichen Thread-Modelling genau zu überlegen:
- besteht diese potentielle Gefahr wirklich, oder ist das übertrieben?
- ist es das Risiko wert, trotzdem mein Passwort einzutippen, oder kann ich warten/einen besseren Ort finden?

Bedrohungen

Stille-Sms

Die Stille SMS ist nach GSM-Spezifikation 03.40 aus dem Jahr 1996 definiert: „Ein Kurzmitteilungstyp 0 bedeutet, dass das Endgerät (ME) den Empfang der Kurzmitteilung bestätigen muss, aber ihren Inhalt verwerfen kann.“

Das bedeutet, dass diese "leere" SMS an die entsprechende SIM zugestellt wird und das Telefon sofort eine Empfangsbestätigung an den Absender zurück sendet. Da das Telefon aber von vornherein weiß: "Ah, das steht eh nix drin, weg damit", ignoriert es diese SMS einfach, ohne der Benutzer*in überhaupt den Empfang dieser Nachricht mitzuteilen.

Dadurch entsteht bei den Mobilfunkbetreibern aber zurückverfolgbarer Datenverkehr, da die SMS (und später auch ihre Empfangsbestätigung) ja bis an ihr Ziel durch sämtliche dafür nötigen Mobilfunkzellen weitergeleitet wurden. Dieser Pfad, den die SMS dabei nimmt, kann dann von den Behörden ausgewertet werden und somit Standorte mit einer Genauigkeiten von bis zu wenigen Metern bestimmt werden.

auf mittel/osteuropäischer Karte Darstellung des Versands einer stillen SMS und dem Empfang ihrer

Stille SMS - Anwendung

Stille SMS

Bemerkung: Die hier gezeigten Zahlen stammen von kleinen Anfragen der Fraktion Die Linke im Bundestag und beziehen sich dadurch auch nur auf die aufgeführten Bundesbehörden. Leider haben wir keine offiziellen Statistiken dazu aus dem Bundesjustizministerium, was auch die Landesbehörden mit einschließen würde.

Das Bundesamt für Verfassungsschutz gibt seit dem zweiten Halbjahr 2018 keine Zahlen mehr dazu raus.

Mobilfunk

Für die Bedrohungen im Bereich Mobilfunk müssen zunächst einige Grundlagen erklärt werden. In diesem Artikel dreht es sich um die Frage, wie die Kommunikation eines einzelnen Handys mit dem Mobilfunknetz, in Form der Mobilfunkzelle [ugs.: Antennenmast]. Dabei tauchen die Begriffe IMSI und IMEI (und manchmal auch TMSI) häufiger auf, die hier ebenfalls kurz erläutert werden.

Wem gehören Mobilfunkzellen?

Mobilfunkzellen (MFZ) werden von Mobilfunkanbietern betrieben. Dementsprechend kontrollieren die jeweiligen Mobilfunkanbieter auch den Datenverkehr durch diese MFZ hindurch. In dem unteren Bild symbolisieren die verschiedenen Farben, verschiedene Anbieter, wie z.B. Telekom, Vodafon, O2, etc.

Karte, die symbolisch zeigt, wie mobilfunkzellen in einer Stadt verteilt sind

IMSI: SIM-Identifier

Jede SIM-Karte besitzt eine eindeutig identifizierbare Nummer, die International Mobile Subscriber Identity, kurz IMSI. Durch die Registrierungspflicht von SIM-Karten in den meisten europäischen Ländern lässt sich die SIM-Karte eindeutig einer Identität zuordnen. Das können die Repressionsbehörden einfach bei den Mobilfunkanbietern abfragen und machen es auch sehr regelmäßig:

Welche Nummern gehören Anna und Arthur ?

Welche Nummern gehören Anna und Arthur ?

Natürlich funktioniert diese Abfrage auch in die andere Richtung, von SIM-Karte zur Identität:

Wem gehört diese Nummer ? Natürlich funktioniert diese Abfrage auch in die andere Richtung, von SIM-Karte zur Identität:

Wem gehört diese Nummer ?

Quelle: Bestandsdatenauskunft 2022: Behörden fragen sekündlich, wem eine Nummer gehört

IMEI: Geräte-Identifier

Auch Mobilfunkmodems (also der Chip im Handy der sich mit dem Mobilfunknetz verbinden kann), besitzen eine eindeutige Nummer, die International Mobile Equipment Identity, kurz IMEI. Diese IMEI sind in der Regel 15-Stellen lang und global einzigartig. Der Aufbau schaut wie folgt aus:

- die ersten 8 Ziffern sind, einfach gesagt, Typen spezifisch. Zum Beispiel haben alle Google Pixel 7a als erste 8 Stellen: 35917382
- die nächsten 8 Ziffern sind Seriennummern
- *die letzte Ziffer ist zur Fehlerkorrektur (error correction)*

picture of IMEI sets of different models from same and different vendors next to each other.

Wie wird sichergestellt, dass diese Nummern einzigartig sind?

Da viele verschiedene Firmen solche Mobilfunkmodems produzieren ist es notwendig, sich untereinander abzusprechen. Sonst würden bei den täglich abertausend produzierten Modems schnell Nummern multiple Male vergeben werden.

Darum kümmert sich die **GSMA** (Global System for Mobile Communications Association). Der Name spricht hier für sich selbst.

- Will ein Hersteller also ein neues Modell auf den Markt bringen, gehen sie zur GSMA und bitten um einen "Nummernraum", die 8 ersten Stellen. Nun dürfen sie alle produzierten Chips dieses Modells mit diesem Nummernraum benennen, also IMEIs vergeben.
- Die Seriennummern dienen zur Unterscheidung einzelner Geräte des selben Modells.
- Die Fehlerkorrektur ist ein bisschen schwarze Magie und kann hier wirklich vernachlässigt werden.

EIR: (Equipment Identity Register)

EIRs (Equipment Identity Register) sind im Grunde Datenbanken mit IMEIs. Meistens werden dort IMEIs gestohlener Handys in "blacklists" verwaltet (siehe weiter unten). Der Standard sieht aber auch "whitelists" vor. Das würde bedeuten, dass alle produzierten IMEIs erfasst werden und nur diese erfassten auch am Netzwerk teilhaben dürfen. Das wäre dann ein bedeutendes Sicherheitsrisiko, wenn ein Handy mit zurückverfolgbaren Zahlungsmethoden gekauft wird.

Beispiele für Modemhersteller: Qualcomm, Huawei, ZTE, Sierra Wireless, Netgear, Alcatel, TP-Link

Durch die IMEI ist also jedes mobilfunkfähige Gerät identifizierbar.

Wenn ein Gerät gleichzeitig mit mehreren SIM-Karten verwendet werden kann (egal ob bspw. 2 physische SIMs, oder 1 e-SIM & 1 physische SIM), hat es auch entsprechend viele IMEIs.

Warnung

Oft ist es aber ziemlich einfach eine Verbindung zwischen diesen beiden IMEIs herzustellen:

- Oft werden die Seriennummern einfach hochgezählt *(außer die error correction)*
- Wenn dauerhaft zwei IMEIs immer am selben Ort sind lässt sich das korrelieren
- Die Hersteller und Händler kennen die Korrelation der beiden IMEIs
- Sollte hier ein EIR im Spiel sein, sind diese beiden IMEIs im EIR auch miteinander verknüpft. Ist also eine der beiden IMEIs bekannt, ist aus dem EIR auch die Zweite ersichtlich.

Die IMEIs lassen sich nicht ohne Weiteres ändern. In vielen Ländern ist ihre Manipulation sogar strafbar und erfordert zudem spezielle Hardware, die am ehesten aus China bezogen werden kann.

Probleme beim Kauf von Handys

Kauft Ihr also ein Handy im Laden und bezahlt mit Karte, liegt danach dem Laden die Verknüpfung eurer Karte und der IMEI(s) eures Handys vor. Kauft Ihr ein Gerät sogar direkt bei eurem Mobilfunkanbieter, kann sogar durch die oben gezeigten Abfragen wie "Welche Nummern gehören dieser Person?" bei den Anbietern direkt auch euer genaues Gerät bestimmt werden (also inklusive Seriennummer, IMEI, etc). Kauft Ihr also ein Handy im Laden und bezahlt mit Karte, liegt danach dem Laden die Verknüpfung eurer Karte und der IMEI(s) eures Handys vor. Kauft Ihr ein Gerät sogar direkt bei eurem Mobilfunkanbieter, kann sogar durch die oben gezeigten Abfragen wie "Welche Nummern gehören dieser Person?" bei den Anbietern direkt auch euer genaues Gerät bestimmt werden (also inklusive Seriennummer, IMEI, etc).

Als Konsequenz daraus ist es Behörden möglich, durch Abfragen bei Verkäufern und Geräteherstellern, die per Werk vergebenen IMEIs zu spezifischen Geräten zurück zu verfolgen.

Und damit besteht, wenn das Handy über die eigene Identität gekauft wurde, auch diese Zuordnung.

Uns ist allerdings bisher nicht bekannt ob und wie oft Behörden diese Zuordnung abfragen.

- Identifier eines Gerätes, nicht der SIM-Karte
- weltweit einzigartig
- wird an Mobilfunkanbieter übertragen, wenn mit Mobilfunknetz verbunden (siehe [Authentifizierung](./mobilfunk.md#authentifizierung))

Authentifizierung

Schematische Darstellung des Authentifizierungsprozesses zwischen Sim und Mobilfunkzelle

- Erkennt das Handy das Signal einer MFZ, versucht es bei ihr mit einer Art "HALLO" anzuklopfen, um zu sehen, ob die MFZ überhaupt erreichbar ist und sagt ihr, das falls das der Fall ist, das es sich gerne ins Netz einloggen möchte.
- Wenn die MFZ diese Nachricht empfangen konnte, fragt sie zuerst einmal nach der Identität des Handys, um sicher zu gehen, dass es überhaupt das Recht hat, sich bei ihr einzuloggen.
- Daraufhin schickt das Handy die IMSI seiner SIM-Karte um zu beweisen, dass es das Recht hat sich zu verbinden. Gleichzeitig schickt es aber auch die IMEI seines Mobilfunkmodems (also des Handys) mit.
  - Eine Telekom MFZ würde also eine Vodafon Sim-Karte ablehnen und ihr sagen, dass sie kein Recht hat das Telekom-Netz zu benutzen.
- Damit ist die Authentifizieren quasi abgeschlossen und eine Verbindung kann aufgebaut werden. Was es mit der TMSI auf sich hat ist hier zweitrangig und deshalb übersichtshalber in den Details eingeklappt.
- Dem Standard nach können solche Verbindungen auch nur "verschlüsselt" aufgebaut werden. Warum das hier in Anführungszeichen steht, kannst du hier nachlesen.

Was ist die TMSI?

Würde nun einfach eine Verbindung aufgebaut werden, könnte jede*r in der Nähe mit geeigneter Hardware (bspw. Software Defined Radios ab 20€) sehen, welche Handys gerade mit welchen Sim-Karten im Netz eingeloggt und wie viel sie kommunizieren. Damit das nicht geschieht, geht das Prozedere noch um einen Schritt weiter: Die MFZ gibt dem Handy eine TMSI (Temporary Mobile Subscriber Identifier). Das Handy nutzt von nun an, aber auch nur in dieser Session, diese TMSI zur Identifikation. Loggt sich das Handy irgendwann aus dieser MFZ wieder aus und später wieder ein, beginnt das gesamte Prozedere von vorn und eine neue TMSI wird vergeben.

Falls du dich jetzt noch fragst, wofür das Handy sich nach der ersten Authentifizierung überhaupt noch weiter identifizieren muss: Versendete Pakete benötigen natürlich immer Empfänger (und Absender). Damit dein Handy also während einer Verbindung mit bspw. einer Webseite wieder gefunden werden kann, um dir die Inhalte zu präsentieren, muss "das Netz" natürlich wissen, welches Gerät du denn überhaupt bist.

Sowohl die IMSI als auch die IMEI werden bei der Authentifizierung mit dem Mobilfunknetz übertragen. Damit entstehen bei den Mobilfunkanbietern Tabellen (Datenbanken), die eine eindeutige Zuordnung zwischen IMSI und IMEI, also Handy und SIM-Karte, ermöglichen. Bei den Anbietern liegen diese Daten zwar nicht lange rum (zum Zeitpunkt des Schreibens dieses Artikels gibt es in Deutschland noch **keine** Vorratsdatenspeicherung). Dennoch sollte einem diese Gefahr

bewusst sein, wenn ein Handy verwendet wird welches vorher bereits mit einer anderen SIM-Karte verwendet wurde, welche wiederum Rückschlüsse auf die eigene Identität zulässt. Außerdem kann das Handy auch vorher mit einer anderen SIM in einer Funkzellenabfrage gelandet sein.

Logger

Logger bezeichnen Geräte, mit denen etwas 'geloggt', also mitgeschnitten werden kann. Für uns hier sind zwei Arten von Logger relevant: Keylogger und Screenlogger.

Keylogger

Keylogger sind Geräte, die im Grunde sämtliche Tasteneinschläge auf eurer Tastatur mitschneiden. Dafür sitzen sie zwischen Tastatur und Computer und sehen aus wie normale USB-Adapter:

Keylogger neben Tastatur

Keylogger zwischen Laptop und Tastatur

Sie können über Funk/WLAN/LTE in Echtzeit jeden einzelnen Tasteneinschlag zu einem Angreifer senden. Das Problem daran ist offensichtlich.

Diese Keylogger sind für sehr kleines Geld zu haben und einfach zu besorgen, sodass ihre Anwendung auch für Amateure sehr simpel ist!

Es gibt sogar Keylogger die wie ein ganz normales Kabel aussehen, siehe z.B. das O.MG Cable.

Fortgeschrittenere Angreifer (zB. Behörden) können auch Keylogger in den Tastaturen selbst verbauen, indem sie die Tastatur aufschrauben und eine kleine Keylogger-Platine an der Elektronik der Tastatur direkt verbauen. Oder sie tauschen die Tastatur einfach durch eine manipulierte aus. Das würde dann allein am USB-Port natürlich nicht auffallen.

Screenlogger

Screenlogger funktionieren nach dem gleichen Prinzip wie Keylogger. Ein Adapter-ähnliches Gerät wird zwischen Display und PC gesteckt (je nach verwendetem Anschluss: VGA, HDMI, DisplayPort,...) und kann dann die gesamte Bildübertragung mitschneiden und über Funk/WLAN/LTE an den Angreifer senden.

Warnung

- vor öffentlich zugänglichen PC's
- anderen PC's die nicht immer unter Beobachtung sind (das eigene Büro zB.)

Es sei noch erwähnt, dass mit "Key-" bzw. "Screenlogger" auch Software-Logger gemeint sein können. Dass sind dann aber nichts anderes als Viren und beschreiben eine völlig andere Bedrohung als diese hier.

Über-Uns

Freundinnen

Hier sind einige andere tolle Kollektive, Initiativen und Gruppen.

IT-Sicherheit für Aktivisti

Diese Gruppen geben Workshops zu IT-Sicherheit für Aktivisti oder bieten offene Sprechstunden an. Einige davon bieten auch Workshops zu anderen Themen an.

- Skills for Utopia
- resist.berlin
- Datenschutzgruppe der Roten Hilfe
- Zucker im Tank
- Cryptosprechstunde Berlin
- ignite! Kollektiv

Andere politische Workshops

Diese Gruppen bieten zu anderen politischen Themen Workshops an.

- stuhlkreis_revolte
- skills for action
- aufbegehren
- fem*ergenz
- Gegen_Gewalt
- kikk-Kollektiv
- Kipp.Punkt Kollektiv
- Educat Kollektiv
- Organisiert euch!
- Netzwerk Selbsthilfe
- Wort.Wechsel

- Kurve Wustrow
- Werkstatt für gewaltfreie Aktion Baden
- Attac

Mitwirkende

Hier eine Liste von Menschen, welche dabei geholfen haben diese Inhalte zu verbessern. Vielen Dank an sie! Wenn du das Gefühl hast auf der Liste zu fehlen, füge dich gerne in einem Pull Request hinzu.

Lizenz

CC0 Public Domain

Kontakt

E-Mail: esc-it@systemli.org (PGP-Key)

Fingerprint: `0BDB 1EB8 2477 0874 9876 DAE0 B923 BEA9 EAAF 0B15`

Social Media

Alle unsere Profile sind hier verlinkt, was nicht hier steht gehört auch nicht zu uns. Aktuell sind wir ausschließlich auf Mastodon aktiv.

Mastodon / Fediverse: @esc_it@systemli.social

Uns abmahnen?

Sie haben eine Rechtsverletzung auf dieser Seite festgestellt? Dann wären wir für einen Hinweis dankbar und beseitigen die Ursache umgehend. Bei den verwendeten Bilder haben wir stets die Quelle verlinkt. Sollten Sie doch gleich Ihren Anwalt auf uns hetzen oder selbst ein zweifelhafter Abmahnanwalt sein, stellen Sie sich auf ein langes Verfahren bis zur letzten Instanz ein.

Haftungsausschluss

Trotz sorgfältiger inhaltlicher Kontrolle übernehmen wir keine Haftung für die Ziele externer Links. Für den Inhalt der verlinkten Seiten sind ausschließlich deren Betreibende verantwortlich. Wir übernehmen keinerlei Gewähr für die Aktualität, Vollständigkeit und Richtigkeit der dort bereitgestellten Informationen.

Werden uns Rechtsverletzungen bekannt, werden die externen Links durch uns unverzüglich entfernt.

Weiteres-Material

Hier sind einige weitere Materialien zum Thema verlinkt, welche wir teilweise auch als Quelle verwendet haben. Vielen Dank an die Ersteller*innen.

Einige der Quellen enthalten teilweise veraltete oder unvollständige Informationen. Bitte bedenkt das, schaut euch mehrere Quellen an, recherchiert selbst und fragt im zweifel bei den Gruppen oder uns nach.

Deutsch

- beschlagnahmt.org
- Datenschutzgruppe der Roten Hilfe
- esc-ctrl
- Sicherheitsratgeber vom ABC Dresden
- prism break
- systemli Wiki

Englisch

- No Trace Project
- The Hitchhiker’s Guide to Online Anonymity
- OpSec von Riot Medicine
- Privacy Handbuch
- Digital First Aid
- Surveillance Self-Defense von der EFF
- security in-a-box
- Tactical Tech
- riseup.net

Esc-It

esc-it logo

esc-it (gesprochen escape it oder escape IT) ist ein Kollektiv welches Inhalte für IT-Sicherheitstrainings für Aktivist*innen erstellt. Zielgruppe sind Aktivist*innen und Trainer*innen im Kontext des politischen Aktivismus.

Warum es uns gibt

In der linken Szene in Deutschland gibt es ein Bedürfnis sich vor der zunehmenden staatlichen Überwachung und digitalen Formen der Repression zu schützen. Dies führt teilweise zu Unsicherheit und Paranoia aber auch zu Resignation. Aufklärung und Bildung kann dem entgegen wirken und Menschen ermächtigen selbstbestimmt und informiert zu entscheiden, wie Sie mit digitaler Überwachung umgehen wollen.

Da es nur wenige Gruppen gibt welche IT-Sicherheitstraining mit spezieller Ausrichtung auf Aktivist*innen anbieten hat sich esc-it gegründet. Bei der Suche nach Material ist aufgefallen, dass es für Trainings zu IT-Sicherheit nur wenig öffentlich zugängliches Material gibt, welches auf politisch aktive Menschen und den deutschsprachigen Raum ausgerichtet ist. Die Materialien die es gibt sind teilweise auf spezielle Problemstellungen fokussiert und lassen sich daher nicht in ein zusammenhängendes Konzept eingliedern, sind nicht didaktisch aufbereitet, veraltet oder auf andere Regionen / Gesetzgebung ausgerichtet.

Deshalb haben wir begonnen eigene Materialien zu erstellt. Hiermit wollen wir nicht den Eindruck erwecken, dass alle anderen Materialien nicht zu gebrauchen sind. Wir haben uns lediglich Gedanken gemacht was uns für die Materialien wichtig ist und versuchen dies hier umzusetzen.

Menschen abholen

Wir möchten Menschen dort abholen, wo sie sind und sie dabei Unterstützen für sich passende Schutzmaßnahmen umzusetzen. Dem in der Technik- und Datenschutzszene so verbreitete Muster, andere Menschen für Ihren Technikkonsum zu verurteilen und für die eigenen Verhaltensweisen zu missionieren wollen wir nicht folgen. Kommunikation auf Augenhöhe ist uns wichtig.

Konkret heißt das beispielsweise, dass wir Aktivist*innen gerne auch dabei helfen ihre Computer mit Windows oder macOS abzusichern und nicht etwa grundsätzlich versuchen, sie davon zu überzeugen Linux zu verwenden. Aus Sicht des Datenschutzes mag Linux zu bevorzugen sein, aber

nicht unbedingt aus Sicht der Sicherheit. Klar ist auch, dass Menschen das Betriebssystem am besten sicher verwenden können, mit dem sie sich auskennen. Der Umstieg auf Linux ist damit für viele eine zusätzliche Hürde und senkt damit die Wahrscheinlichkeit, dass diese Veränderung angenommen wird. Und wenn es nicht angenommen wird, hilft es am Ende auch nicht.

Zudem ist es einfach scheiß tech bro Verhalten.

Selbstverständlich heißt das nicht, dass wir zu sicherheitsrelevanten Themen keine entsprechenden Empfehlungen aussprechen. Beispielsweise ist ein Ende-zu-Ende verschlüsselter Messenger einem vorzuziehen, der nicht Ende-zu-Ende Verschlüsselt ist. Das Ziel einer solchen Empfehlung ist jedoch zu informieren, sodass eine selbstbestimmte Entscheidung getroffen werden kann.

Fokus auf Selbstermächtigung

Unser Anspruch ist es, Aktivist*innen so zu bilden, dass sie selbstständig entscheiden können in welcher Situation sie sich wie vor digitaler Überwachung schützen wollen. Deshalb priorisieren wir ein grundsätzliches Verständnis über konkrete Handlungsempfehlungen.

Dafür gibt es mehrere Gründe. Es beginnt damit, dass wir für passende Empfehlungen wissen müssten was ihr macht. Das wollen wir allerdings gar nicht wissen. Zudem können sich Verhältnisse ändern, und damit auch Empfehlungen. Eine konkrete Software mag heute noch zu empfehlen sein, vielleicht wird sie aber bald grundsätzlich verändert, verkauft oder sie wird schlicht von neue staatliche Überwachungsmöglichkeiten eingeholt.

Ihr selbst könnt am besten Einschätzen, welche Gegenmaßnahmen die richtigen für euch sind. Daher sehen wir die Methode der Bedrohungsmodellierung als Grundlage an. Um diese Anwenden zu können müsst ihr jedoch auch wissen welche Bedrohungen und Gegenmaßnahmen es gibt. Daher versuchen wir diese aufzulisten und zu erklären.

Realistisches Bedrohungsbild

Zudem müsst ihr für die Bedrohungsmodellierung wissen, wie wahrscheinlich das Eintreten einer Bedrohung ist. Dies ist für staatliche Überwachungsmaßnahmen nicht genau zu beziffern. Dennoch versuchen wir beispielsweise durch Statistiken und Fallbeispiele eine faktenbasierte Einschätzung zu ermöglichen.

Didaktisch aufbereitet

Unser Ziel ist es Wissen zu vermitteln. Daher bemühen wir uns Inhalte so aufzubereiten, dass sie auch für Laien möglichst verständlich sind. Fremd- und Fachwörter versuchen wir zu vermeiden oder sie verständlich zu erklären.

Wir möchten Themen nicht nur sachlich erklären, sondern auch didaktisch aufbereiten. Beispielsweise durch Grafiken, Präsentationen oder interaktive Elemente wie Aufgaben oder Spiele.

Alle Materialien sollen sich zu einem ganzheitlichen Konzept zusammenfügen.

Aktuell und geprüft

Auch wir wissen natürlich nicht alles. Um Fehler in unserem Material zu vermeiden, gehen alle Inhalte vor der Veröffentlichung durch einen Review-Prozess. Für die Veröffentlichung muss mindestens eine zweite Person zustimmen.

Dennoch können Fehler passieren. Falls euch etwas auffällt, freuen wir uns über Hinweise. Am besten erstellst du hierfür einen Issue in unserem git-Repository oder schreibst uns eine Mail.

Damit das Material inhaltlich korrekt bleibt, haben wir auch den Anspruch es aktuell zu halten. Wie gut das funktionieren wird muss sich noch herausstellen.

Offene Lizenz

Alle Materialien, welche wir selbst erstellen, stehen unter einer freien Lizenz. Wenn wir externe Inhalte verwenden, versuchen wir auch hierbei möglichst Inhalte unter freien Lizenzen zu verwenden.

Damit wollen wir sicherstellen, dass Alle unser Material verwenden und verändern können. Das hilft auch dabei das Material aktuell zu halten, denn falls wir das nicht mehr tun könnte das so von anderen übernommen werden.

IT-Sicherheit als Form von Anti-Repression und Solidarität

Wir möchten vermitteln, dass IT-Sicherheit in politischen Kontexten meistens nicht nur dich selbst betrifft. Auch andere kann es betreffen, wenn du mit Informationen nicht verantwortungsvoll umgehst.

Entsprechend betreffen die Entscheidungen die du hierzu triffst nicht nur dich. Daher solltest du dir überlegen, ob du Betroffene in diese Entscheidungen einbeziehst. Beispielsweise bietet es sich für Gruppen an, sich gemeinsam Gedanken über ein standardisiertes Sicherheitslevel und Maßnahmen zu machen.

Mit IT-Sicherheit schützt du dich und andere. Daher ist es Bestandteil von Anti-Repression.

Empfehlungen

Overprovisioning-Deletion

Unter Besonderheiten in der Datenhygiene habt ihr schon gesehen, dass zum sicheren Löschen von Daten auf SSD's auch die Reserveblöcke gelöscht werden müssen, die aber für herkömmliche Software nicht zu erreichen sind.
Die meisten Hersteller liefern verschiedene Tools aus, mit denen das umgesetzt werden kann. Hier sind die gängigsten aufgelistet. Falls ihr Ergänzungen habt, schreibt uns gerne!

- Samsung
- Kingston
- Seagate
- Sk hynix
- Western Digital
- Crucial
- Sabrent
- Adata

Passwort-Manager

KeePassXC und Bitwarden sind beide Open-Source und haben Anwendungen für alle üblichen Betriebssysteme / Browser.

KeePassXC funktioniert Offline, Bitwarden online. Aber auch KeePassXC lässt sich mittels externer Dienste über mehrere Geräte synchronisieren.

Praktikable Passwortmanager für PCs:

- KeePassXC: Linux, Windows, MacOS
- Bitwarden: Linux, Windows, MacOS

Empfehlung aus KeePassXC docs für Handys:

- Android: keepassDX, Keepass2Android
- iOS: Strongbox, KeePassium

Die in Browser und Betriebssysteme eingebaute Passwortmanager sind nicht unbedingt zu empfehlen, da diese oftmals proprietär und überwiegend auf Komfort ausgelegt sind, was regelmäßig zu Sicherheitslücken führt. Besonders Browser sind stets im Fokus von Angreifer*innen und bieten viele Angriffsvektoren.

Note: Wir schreiben hier konsistent von KeePassXC. Es soll nicht unerwähnt bleiben, dass KeePassXC ein Fork von KeePassX, dies wiederum ein Fork von KeePass, ist. Da KeePassXC am aktivsten maintained wird, empfehlen wir hier diesen Fork.

Messenger

Um verschlüsselt zu kommunizieren, eignen sich neben verschlüsselten Mails einige Messenger. Vorteilhaft gegenüber Mails sind (gute) Messenger, weil bei ihnen Verschlüsselung und sichere Kommunikation von vornherein mit gedacht wurden. Dafür sind sie, vor allem die besseren, aber weniger verbreitet.

Kriterien, was einen guten Messenger auszeichnet, finden sich z.B. bei Digitalcourage. Für Aktivist*innen ist (je nach Threat Model) vor allem eine möglichst sichere, Daten-sparsame und anonyme Kommunikation wichtig.

Hierfür soll auf zwei in Aktivismuskreisen recht weit verbreitete Messenger, die mit Einschränkungen zu empfehlen sind, eingegangen werden: Signal und Matrix.

Signal

Signal wurde von dem Anarchisten Moxie Marlinspike entwickelt und ist eine der bekanntesten Alternativen zum Monopolisten WhatsApp.

Vorteile von Signal

- **Einfache Nutzung**: Signal ist simpel zu installieren und "funktioniert einfach". Mensch kann nicht viel falsch machen, was die Sicherheit gefährden würde.
- **Weite Verbreitung**: 2022 hatte Signal 40 Millionen aktive Nutzer*innen. Damit liegt es zwar noch immer weit hinter den 2 Milliarden Nutzer*innen von WhatsApp, ist aber dennoch weit verbreitet.
- **Sichere Verschlüsselung**: Signal hat ein eigens Kommunikationsprotokoll, das quell-offen ist und regelmäßig geprüft wird. Einige andere Messenger, wie WhatsApp haben das Protokoll ebenfalls übernommen, sodass sich das Protokoll durch die Nutzung von Milliarden von Menschen bewährt. Die Kommunikation in Signal ist demnach sicher Ende-zu-Ende-verschlüsselt.
- **Daten-Sparsamkeit**: Signal speichert möglichst wenig über die Nutzer*innen und kann demnach auch nur wenige Informationen preisgeben. Die einzigen Daten, die Signal in vergangenen Gerichtsprozessen raus *konnte*, waren das Erstellungsdatum des Accounts

und das Datum, als der Account zuletzt genutzt wurde.
- **Möglichkeit der automatischen Löschung**: Chats können so eingestellt werden, dass sich die Nachrichten automatisch nach einer bestimmten Zeit löschen. So sind sie selbst dann sicher, wenn Cops (nach dieser Zeit) Zugriff auf das Gerät erhalten.

Nachteile von Signal

- **Anonymität**: Signal wurde nicht entwickelt um anonym zu sein, sondern um sichere Verschlüsselung anzubieten. Stand heute (Januar 2024) ist eine Telefonnummer notwendig, um sich zu registrieren; diese muss (rein rechtlich) auf eine real existierende Person registriert sein. Die Telefonnummer ist sichtbar für alle, mit denen mensch kommuniziert. Die konkrete Gefahr ist hier, dass entweder ein Cop in einem sensiblen Chat ist und mensch so identifiziert wird, oder dass ein Handy mit Zugriff auf sensible Chats konfisziert wird.
- **Sitz in den USA**: Die Signal Foundation hat ihren Sitz in den USA und kann demnach gezwungen werden, Daten an Geheimdienste weiter zu geben.
- **Zentralität**: Signal läuft nur über die eigene Infrastruktur (die bei Amazon, Microsoft, Google und Cloudflare liegt) und lässt sich nicht selber hosten. Somit muss mensch Signal ein Stück weit vertrauen, dass sie ihren Job gut machen. Außerdem gibt es somit eine zentrale Stelle, die angegriffen werden kann.

Matrix

Matrix ist ein Kommunikationsprotokoll (ähnlich wie Mail, bzw. genauer so was wie IMAP, eines ist). Für dieses Protokoll gibt es diverse Clients, der bekannteste ist Element. Vor allem in letzter Zeit findet Matrix mehr Verbreitung in Aktivismus- und Hackerkreisen.

Funktionsweise

Der wichtigste Unterschied von Matrix im Vergleich zu anderen Messengern, wie z.B. Signal, ist die Dezentralität, bzw. *Föderation*. Ähnlich wie bei Mails gibt es viele verschiedene Server ("*Homeserver*") (wie z.B. *matrix.org* oder *matrix.systemli.org*). Kommuniziert ein Aktivisti mit einem Matrix-Account bei matrix.org mit einem Aktivisti mit einem Matrix-Account bei matrix.systemli.org, so müssen die (verschlüsselten) Nachrichten zwischen den beiden Servern synchronisiert werden.

Matrix Föderation Funktionsweise

Vorteile von Matrix

- **Sichere Verschlüsselung**: Matrix nutzt eine eigene Implementation des Signal-Protokolls. Es hat Nachteile im Vergleich zum Signal-Protokoll, ist aber dennoch ähnlich sicher.
- **Dezentralität**: Matrix ist föderiert und damit dezentral. Es gibt viele verschiedene Server, die miteinander kommunizieren; somit gibt es viele Stellen, die angegriffen werden müssten, um ganz Matrix lahm zu legen.
- **Anonymität**: Bei einigen Servern werden keine persönlichen Informationen zur Erstellung eines Accounts benötigt. Somit ist es prinzipiell möglich, Matrix anonym zu nutzen.
- **Offenheit**: Der Quelltext von Matrix, sowie von Element ist quelloffen und kann (und wird) regelmäßig überprüft.

Nachteile von Matrix

- **Komplizierte Nutzung**: Zuweilen ist es kompliziert, Matrix zu nutzen. Das Prinzip der Föderiertheit ist unintuitiv, es gibt viele sehr verschiedene Clients und vieles funktioniert nicht einfach.
- **Noch nicht weit verbreitet**: Menschen müssen häufig erst mal dazu überredet werden, sich einen Matrix-Account einzurichten.
- **Mangelnde Daten-Sparsamkeit**: Weil Matrix föderiert ist, müssen alle Daten auf allen föderierten Servern synchronisiert werden. Das bedeutet auch, dass es praktisch unmöglich ist, Daten wieder zu löschen. Auf allen Servern werden standardmäßig für immer die Matrix ID persönliche Informationen, Nutzungsdaten, IP-Adressen, Geräteinformationen, andere Server mit denen kommuniziert wird und Raum-IDs gespeichert. (Die Quelle bezieht sich auf eine ältere Matrix-Version. Inwiefern die standardmäßig gespeicherte Datenmenge und das Löschverhalten auf aktuelle Versionen übertragbar sind, ist unklar.)

Resümee

Für den aktivistischen Alltag, in dem mensch nicht anonym sein möchte, eignet sich Signal sehr gut. Insbesondere im Vergleich zu kommerziellen Alternativen ist es Privatsphäre-freundlich und sicher. Sollte aber doch mal Anonymität (und gleichzeitig eine sichere Verschlüsselung) in der digitalen Kommunikation wichtig sein, eignet sich Matrix besser. Hier sollte dann aber darauf geachtet werden, dass keine persönlichen Informationen (wie die IP-Adresse) preis gegeben werden, da diese auf den Servern liegen bleiben.

Graphene-Os

GrapheneOS ist ein alternatives Android Betriebssystem. Es wird stark empfohlen, nicht unbedingt weil es komplett ohne Google-Services genutzt werden kann, sondern weil GrapheneOS in Kombination mit den von ihnen unterstützten Geräten, hochmoderne Sicherheitsfeatures mit sich bringt.

Einstellungs Empfehlungen

Datenschutz & Sicherheit

Exploit protection

- auto reboot: so niedrig wie möglich, aber für die Anwendenden noch komfortabel! (nach Reboot kommen ohne erstmaliges Entsperren z.B keine Signalnachrichten/anrufe mehr an)
- USB - C Port: hier sollte mindestens "Charging only" gewählt werden. "Charging only when locked" ist nochmal eine Stufe strenger (potentiell besser), führt aber dazu, dass das Handy nicht mehr geladen werden kann, wenn es gleichzeitig benutzt werden muss.
  - Hier könnte es sich empfehlen standardmäßgig "Charging only when locked" auszuwählen und im Zweifel direkt zu wissen, wie die Einstellung auf "Charging only" geändert werden kann, wenn dies nötig ist.
- WiFi & Bluetooth automatisch ausschalten: Hier sollte bei Beiden eine noch komfortable Zeitspanne gewählt werden.
- Geräteentsperrung

Geräteentsperrung

- Duress Passwort: Dieses Passwort sorgt dafür, dass wenn es eingegeben wird, das Handy komplett auf Werkseinstellungen zurückgesetzt wird. Das ist sehr praktisch, solltet ihr einmal gegängelt/gezwungen o.ä. werden euer Handy zu entsperren. Das funktioniert übrigens auch, falls ein Angreifer versucht euer Passwort per Brute-Force zu erraten. Voraussetzung ist natürlich, dass auf dem Gerät keine lebensnotwendigen Daten sind, von denen ihr keine Backups habt. Wählt für das Duress Passwort also am besten eins:
  - an das ihr euch im Zweifel sofort erinnert!
  - das die Polizei z.B erraten würde

    - oder: eins, dass ihr für euer richtiges Passwort niemals wählen würdet.

WiFi

Für sämtliche WiFis, über die nicht ihr selber die volle Kontrolle habt:

- In die Einstellung der jeweiligen Verbindung (Zahnrad bei WiFi-Name): nicht persistente MAC-Adress-Generierung für diese Verbindung aktivieren.

2FA für Fingerprint

Seit kurzer Zeit gibt es die Möglichkeit einen zweiten Faktor für die Entsperrung per Fingerprint zu nutzen. Das bringt einen enormen Fortschritt im Spannungsfeld zwischen Usability und Security mit sich!

Wo war bisher das Problem?

Im Normalfall ist es ja so, dass biometrische Entsperrmethoden mit äußerster Vorsicht zu genießen sind, aus dem einfachen Grund, dass sie von euch erzwingbar sind. Die Polizei kann im Zweifel euren Finger mit Gewalt auf euer Handy legen und es entsperren.

Das heißt bisher ging die Nutzung der biometrischen Entsperrung immer einher mit der Gefahr überrumpelt und zum Entsperren gezwungen zu werden, bevor das Handy ausgeschaltet werden kann.

Wie schaut die Lösung aus?

Die 2FA Option bietet die Möglichkeit einen mindestens 4-stelligen (empfohlen werden 6Stellen) Zahlen PIN einzurichten, der jedes mal nach dem Fingerprint zusätzlich einzutippen ist, um das Handy zu entsperren.

Dann muss zwar trotzdem noch etwas getippt werden, aber einen z.B 6-stelligen PIN auf dem großen Zahlen-Pad ist viel einfacher und schneller getippt, als eine 7 Wörter lange Passphrase auf der kleinen Tastatur. Außerdem lässt sich der PIN viel entspannter ändern (wenn es sein muss), da man keine große Sorge davor haben muss, jetzt ein neues langes Passwort lernen zu müssen.

Das bedeutet das Handy kann mit einem sehr starken Passwort verschlüsselt werden, ohne dass man nun dieses elendig lange Passwort etliche Male am Tag eintippen muss.

Kann der PIN nicht gebrute-forced werden?

Nur sehr eingeschränkt:

- Die gesamte Fingerprint-Methode ist nur 48h nach der letzten Eingabe des primären (langen) Passworts.

- Es sind maximal 4 * 5 Fehlversuche erlaubt. Zwischen jedem 5. Fehlversuch gibt es eine 30 sekündige Auszeit. Es gibt also maximal 20 Fehlversuche. [1]

PIN Scrambling

PIN scrambling ist ziemlich nerdig, hat aber durchaus seine Anwendungsfälle:

Anstatt dass die Ziffern immer in numerischer Reihenfolge auf dem Bildschirm angezeigt werden, werden die Ziffern bei der PIN-Eingabe an zufälligen Stellen auf dem Bildschirm angezeigt. Wenn euch also ein Angreifer aus kleiner Entfernung dabei beobachtet hat, wie ihr euren PIN eingegeben habt, in der er nur z.B. die Richtung des Daumens auf dem Bildschirm erkennen konnte, ist der PIN für ihn nicht rekonstruierbar.

PIN scrambling ist auch für die 2FA beim Fingerprint verfügbar.

Module

Module

Rollenspiel-Netzwerkverkehr

Dieses Spiel soll versuchen Menschen den Ablauf, nicht aber die Funktionsweise von Netzwerkkommunikation am Beispiel von E-Mails ohne Verschlüsselung, mit Transportverschlüsselung und mit Ende-zu-Ende (und Transportverschlüsselung) zu veranschaulichen. Dabei ist es weniger wirklich ein Spiel, dass Spaß machen soll, sondern dient als eher Mittel dazu das Thema nicht nur mit einem Netzwerkdiagramm erklären zu müssen und somit für nicht-Nerds zugänglicher zu machen.

Rollen

- 2x Server (systemli.org & gmail.com)
- 2x Kommunikationsparteien (Alice & Bob)
- 1x (oder mehr) Polizei (Eve)
- 3x Internet [Optional]

Material

- 1x Blatt für Text
- 1x Blatt mit E-Mail Metadaten
- 3x Blatt mit IP-Metadaten für die Strecken zwischen den Knoten
- 2x Schild mit Namen der Server
- 2x Schild mit E-Mail und IP-Adresse der Kommunikationsparteien
- 1x kleine Kiste, welche mit Vorhängeschloss verschlossen werden kann (in welche das Blatt mit dem Text passt)
- 3x große Kiste mit Deckel (in welche die andere Kiste passt)
- 2x Vorhängeschloss
- 3x Stuhl
- Stifte

Im Idealfall werden die Blätter laminiert und mit Whiteboardmarker beschrieben. Dann können sie auch wiederverwendet werden.

Ablauf

Zur Vorbereitung wird auf jede der großen Kisten einer der Internet Metadaten geklebt.

Dann werden die Rollen verteilt. Die Rolle der Polizei sollte am besten ein Mensch ohne großes technisches Wissen übernehmen, sodass für die Angriffe Kreativität gefragt ist. Die restliche Menschen schauen zu.

Die 2 Server und 2 Kommunikationsparteien stellen sich in einem Viereck auf. Die Server und Kommunikationsparteien bekommen die Schilder mit ihren Informationen umgehängt.

Zwischen die 4 Menschen wird jeweils 1 Stuhl gestellt auf den sich jeweils eine Person die das Internet spielt setzt. Zudem bekommen sie die Kiste mit den passenden Internet Metadaten.

Alice schreibt auf das Blatt für den Text eine Nachricht an Bob und auf das Blatt mit den Metadaten die nicht bereits ausgefüllten Metadaten.

Nun werden die verschiedenen Szenarien durchgespielt. Jedes Szenario wird einmal ohne MITM, einmal mit MITM (in unserem Fall durch die Polizei) gezeigt. Dabei ist die Rolle der Polizei angehalten, sich selbst auszudenken wie sie das Szenario angreifen kann. Ausgenommen werden lediglich Angriffe auf Alice und Bob welche nicht Ziel dieses Spiels sind. Zudem wird nicht behandelt inwiefern die Angriffe rechtlich möglich sind oder die Parteien die Daten an Behörden herausgeben würden, alle technisch möglichen Angriffe können behandelt werden. Die Polizei kann nur beim Internet und bei den Servern angreifen.

Wenn der Polizei selbst keine Angriffsmöglichkeit einfällt können die Zuschauenden aushelfen. Wenn auch diese keine Idee haben, kann die Moderation aushelfen.

Anschließend sollen die Zuschauenden erklären was passiert ist, ob der Angriff so funktioniert und welche Daten die Polizei bekommen hat.

Unverschlüsselt

Anna gibt Internet die Blätter mit dem Text und den E-Mail Metadaten, gibt sie dem ersten Server, welcher sie wieder an das Internet gibt, der es zum zweiten Server bringt, der sie erneut dem Internet gibt welches die Blätter schließlich zu Bob bringt. Bei jedem Knoten werden die Blätter in die Kiste mit den entsprechenden IP Metadaten gelegt.

Unverschlüsselt – MITM

Mögliche Angriffsziele sind:

- Das Internet
- Die Server

Bei beiden können alle Daten abgegriffen werden.

Transportverschlüsselt

Diesmal werden die Kisten mit dem Deckel "verschlossen". Diese Kiste wird in dem Spiel zwar nicht verschlossen, jedoch wird darauf hingewiesen, dass sie trotzdem als sicher zu betrachten ist. Sie schützen allerdings nur auf dem Transportweg, die Knoten müssen die entsprechenden Kisten ja öffnen können.

Ansonsten läuft es wie beim unverschlüsselten Szenario. Es ist darauf zu achten, dass an jedem Knoten beide Blätter aus der Kiste geholt und anschließend in die passende andere Kiste hinein gepackt werden. Dies ist notwendig, da die Server ja die Metadaten brauchen um zu wissen, wohin sie die Mail weiterleiten müssen.

Transportverschlüsselt – MITM

Mögliche Angriffsziele sind:

- Die Server

Dort können alle Daten abgegriffen werden.

Ende-zu-Ende-Verschlüsselung

Zuerst wird erklärt, dass es bei Ende-zu-Ende Verschlüsselung einen öffentlichen und einen privaten Schlüssel gibt. Wir stellen denn öffentlichen Schlüssel als vorhängeschloss und den privaten als Schlüssel für das Schloss dar. Es wird kurz darauf hingewiesen, dass dieser öffentliche Schlüssel so ausgetauscht werden muss, dass sicher ist, das dieser auch zu der Person gehört. Für dieses Szenario machen wir das so, dass Bob persönlich zu Alice geht und ihr das Vorhängeschloss gibt.

Nun packt Alice den Zettel mit dem Text in die kleine Kiste, verschließt diese mit dem Vorhängeschloss und packt diese Kiste zusammen mit dem Blatt mit den Metadaten in die große Kiste. und übergibt diese an das Internet. Danach ist der Ablauf wie vorher, die große Kiste wird an jedem Knoten wieder ein und ausgepackt, bei Bob wird schließlich auch die kleine Kiste geöffnet.

Ende-zu-Ende-Verschlüsselung – MITM

Mögliche Angriffsziele sind:

- Die Server

Dort können nun nur die Metadaten abgegriffen werden.

Ende-zu-Ende-Verschlüsselung mit TOFU

Diesmal wird der öffentliche Schlüssel, wie so üblich per E-Mail ausgetauscht ohne das dieser überprüft wird.

1. Alice schreibt Bob "gib mal Key"
2. Bob schickt Key
3. Alice schreibt Ende-zu-Ende verschlüsselt wie oben

Ende-zu-Ende-Verschlüsselung mit TOFU – MITM

Mögliche Angriffsziele sind:

- Die Server

Dort können alle Daten abgegriffen werden.

Der Angriff läuft wie folgt ab:

1. Alice schreibt Bob "gib mal key"
2. Bob schickt Alice Key
3. Polizei greift den Key ab, ersetzt ihn durch eigenen.
4. Alice verschlüsselt Nachricht mit Key der Polizei
5. Polizei fängt die Nachricht ab und liest sie.
6. Polizei verschlüsselt Nachricht neu mit eigentlichem Schlüssel von Bob und sendet sie weiter

So bekommen weder Alice noch Bob etwas von dem Angriff mit die Polizei kann jedoch alles mitlesen. Durch den Austausch des Keys durch die Polizei wird hier ein zweites Vorhängeschloss benötigt.

Fallbeispiele

Gegenmassnahmen

Passwörter

Wovor schützen gute Passwörter ? Und wovor nicht ?

Prinzipiell sind gute Passwörter natürlich unvermeidbar. Was ein gutes Passwort ist, behandeln wir weiter unten. Es soll aber schon darauf hingewiesen sein: Passwörter hindern Behörden fast nie davor, in ungesicherte Social-Media Accounts wie Instagram, Twitter, Reddit, Tiktok und so weiter, hinein zu kommen. Dafür reicht ihnen ein richterlicher Beschluss, denn dort liegen eure Daten unverschlüsselt und deshalb brauchen sie dafür euer Passwort nicht.

Generell gilt

- Passwörter nicht wiederverwenden
- Starke Passwörter verwenden
- Einen Passwort Manager benutzen
- 2-Faktor-Authentifizierung

Passwortmanager

Ein Passwortmanager speichert alle Passwörter in einer, mit einem Hauptpasswort, verschlüsselten Datenbank. Dadurch liegen eure Passwörter nicht einfach in Klartext auf eurem System und ihr müsst sie euch nicht alle selbst merken.

Da ihr euch Passwörter nicht mehr selbst merken müsst, ist es kein Problem und auch empfohlen, dass ihr für jeden Account ein eigenes, starkes Passwort generiert, was mit dem Passwortmanager selbst sehr einfach zu machen ist.

Der Passwortmanager speichert dann auch die Zuordnung zu Webseiten & Apps, für die ihr das jeweilige Passwort generiert habt. Das erschwert so auch Phishing, weil das Passwort auf einer falschen URL nicht als Vorschlag angezeigt wird.

Wie oben schon erwähnt ist der Passwortmanager selbst durch ein starkes Hauptpasswort, und/oder andere Faktoren geschützt (s. unten 2-Faktor-Authentifizierung). Dies ist damit das

einzige Passwort, das ihr euch wirklich merken müsst und kann dementsprechend auch etwas komplexer sein, denn es gilt: lieber ein starkes Passwort merken, als viele unsichere (und wahrscheinlich sehr ähnliche) Passwörter.

Starke Passwörter

Okay, aber zumindest ein starkes Passwort für den Passwortmanager braucht ihr ja trotzdem...

Tip

Wie du ein starkes Passwort mithilfe von Diceware einfach erstellen kannst erklären wir dir übrigens hier.

Wann ist ein Passwort denn stark? Eine Wichtige Grundvoraussetzung ist, dass das Passwort zufällig generiert ist. Alles was du dir ausdenkst, egal wie clever dein System sein mag, ist als unsicher zu betrachten. Deine Passwörter sollten also zufällig generiert sein. Eine Möglichkeit dazu ist ein Passwortmanager, eine weitere ist Diceware zeigen wir weiter unten.

Um zu klären wie ein sicheres Passwort aussehen muss, wenn es zufällig generiert wurde, schauen wir uns an wie lange es dauert ein Passwort zu cracken.

Zeit zum cracken eines Passworts

Tatsächlich kommt es sehr auf die genauen Umstände an. Die Berechnungen hier nehmen ein konkretes Szenario an. Das hier gezeigte Szenario geht von relativ guten Konditionen für die Angreifer aus. Das heißt, in der Praxis dauert es eher noch länger.

Technische Details

Wir gehen von einem MD5 gehashten Passwort aus und davon, dass die Angreifer die Hardware zur Verfügung haben die für das Training von ChatGPT verwendet wurde: 10000 NVIDIA A100 GPUs.

Kaufpreis: ca. 9000€ pro Stück für die günstigere Variante mit 40GB Speicher. Insgesamt also 90 Mio. Euro. Auch zur Miete ist diese Masse an Hardware auf Dauer nicht günstiger. Weitere details zum Szenario gibt es bei hive-systems welche die Berechnungen durchgeführt haben.

Zudem ist bei den Zeiten zu bedenken, dass diese für *ein* Passwort von *einer* Person sind. Die komplette Hardware ist damit beschäftigt, es kann währenddessen kein anderes Passwort gecrackt werden.

Wichtige Voraussetzung: Das Passwort muss zufällig generiert worden sein! Das heißt hier geht es um reines Character-Bruteforcing, also ohne auf die Zielperson optimierte Wortlisten.

a table shows the amount of time to password-cracking, according to above described scenario

Zeit zum cracken einer Passphrase

Ein zufälliges, ausreichend langes Passwort aus Buchstaben, Zahlen und Sonderzeichen ist jedoch für Menschen schwer zu merken. Deshalb empfehlen wir für die Passwörter die ihr euch merken müsst, beispielsweise das für für den Passwortmanager, Passphrasen zu verwenden. Diese bestehen aus Wörtern statt aus einzelnen Buchstaben. Damit können Menschen deutlich besser umgehen, sie sind aber nicht weniger sicher Passwörter. Siehe auch: xkcd 936

Technische Details

In der Informationstheorie muss zur Bewertung der Sicherheit immer angenommen werden, dass der Angreifer weiß nach welchem Verfahren wir das Passwort gebildet haben. Daher verwendet der Angreifer hier eine Wordlist-Attack. Ansonsten bleibt alles gleich.

Diceware: Das Erstellen zufälliger Passphrasen kann, wie schon erwähnt, mit Passwortmanagern geschehen, oder ganz analog mit Würfeln und einer möglichst großen Wortliste.

Info

Die Passphrase muss zufällig generiert worden sein. Beispielsweise mit Würfeln und Wortliste (Diceware), oder der jeweiligen Funktion des Passwortmanagers.

a table shows the amount of time to passphrase-cracking, according to above described scenario

2-Faktor Authentifizierung

2FA sorgt dafür, dass das bloße eingeben eines Passworts, nicht als vollständige Autorisierung genügt, da davon ausgegangen wird, das Passwörter eventuell korrumpiert sind. Deshalb wird eine zweite Instanz zur vollständigen Autorisierung angefordert. Das kann auf verschiedenen Kategorien beruhen:

- Wissen: Der alte Klassiker in Form eines Passworts oder Sicherheitsfragen wie "Wie lautet ihr Geburtsort?"
- Besitz: Ihr benötigt ein spezielles Ding, dass euch entweder eine Nummer anzeigt, oder was per USB in den Rechner gesteckt werden muss. Besitzt der/die Angreifer*in dieses "Ding" nicht, erfolgt auch keine Autorisierung. (Hardware-Token, *2FA-Apps*, *SMS*)

- Sein: Einzigartige biometrische Eigenschaften müssen verifiziert werden. (Biometrie)

Im Folgenden werden verschiedene Technologien aufgelistet, die für 2-Faktor Authentifizierung (2FA), aber auch als einfache 1-Faktor-Authentifizierung, genutzt werden können:

- Hardware-Token mit USB: Sie sehen aus wie normale USB-Sicks. Soll ein damit konfigurierter Service/Festplatte o.ä. entsperrt werden, muss auch dieser Stick in das genutzte Gerät gesteckt werden. Oftmals sind diese Token wiederum mit einem PIN geschützt, sodass es nicht reicht diesen zu klauen. Die PIN-Eingabe ist dabei oftmals auf x versuche limitiert. Da dies alles auf Hardware-Ebene umgesetzt und geschützt wird, ist es eine relativ sichere Möglichkeit der Authentifizierung. Der relevante Standards für Securitytoken dieser Art heißt FIDO2, der alte Standard U2F.
- Hardware-Token mit Screen: Diese USB-Stick großen Geräte haben einen kleinen Bildschirm, auf ein x-stelliger Code angezeigt wird (meist 4-6 stellig). Sie können mit bestimmten services verknüpft werden. Diese Services verlangen dann bei jeder Anmeldung (neben dem Passwort) auch den code, der gerade in diesem Moment auf dem Token angezeigt wird. Die Standard für Token dieser Art sind nicht Open-Source, weshalb wir dazu raten diese nicht zu verwenden.
- TOTP (2FA) Apps: Diese Apps können ebenfalls mit verschiedenen Services verknüpft werden und generieren dann für jeden Service jeweils alternierende Security-Codes.
- Biometrie: Schon lange berühmt in Hollywood. Soll der entsprechende Service entsperrt werden, fordert er eine Biometrische Verifizierung der Nutzenden (Fingerabdruck, Gesichtserkennung, Iris-Scan, Handabdruck, Stimmerkennung etc)
- SMS: Die wohl bekannteste Methode sind 2FA SMS. Zur Verifizierung der Identität der Nutzenden sendet der jeweilige Service eine SMS an die mit dem Account registrierte Telefonnummer. Da das Mobilfunknetz nicht als sicher zu betrachten ist, raten wir hiervon ab.

Biometrie

Biometrie wie Fingerabdrücke oder Gesichtserkennung sind nachweislich fälschbar. Wie einfach das geht hat Starbug vom CCC, bereits für Fingerabdruck-, Gesichts-, Iris- und Venenerkennung gezeigt.

Abgesehen davon können Behörden oder Cops euch zwingen Dinge mit Biometrie zu entsperren. Zur Herausgabe von Passwörtern dürfen sie das nicht.

Der wichtigste Punkt hierbei ist aber wohl, das ihr eure biometrischen Merkmal nie wieder ändern könnt. Ein korrumpiertes Passwort kann zurück gesetzt werden. Ein Fingerabdruck, oder das Gesicht jedoch nicht.

Fazit
Daher bietet Authentifizierung mit Biometrie keinen guten Schutz gegen Sicherheitsbehörden.

Datenhygiene

Egal ob bei TKÜ, digitaler Forensik oder Hausdurchsuchungen: Es geht immer um Daten, aus denen euch potentiell ein Strick gedreht werden soll. Deshalb gehört es dazu, sich die Frage, welche Daten wirklich notwendig sind, regelmäßig zu stellen.
Natürlich bereitet das ein bisschen mehr Aufwand, Daten tatsächlich zu vernichten und erfordert vor allem Disziplin.

- Brauchen wir für dieses Treffen ein Protokoll?
- Muss das Handy mit auf die Aktion?/Habe ich vor das Handy für irgendwas zu benutzen?
- Muss ich Freund*innen schreiben, welche coole Aktion ich gerade gemacht habe?
  - Selbstdarstellung ist schon vielen zum Verhängnis geworden
- Wenn alle beim Treffen waren, braucht es für manches vielleicht kein Protokoll

Wenn es keine Daten gibt, kommt auch niemand dran. Allerdings kann die Einschätzung einiger weniger, dass die Recherche-Unterlagen jetzt veraltet sind und vernichtet werden können, ein paar Jahre später schwer bereut werden. Der berühmte Aktenordner unter dem Bett wäre aber vielleicht zu riskant gewesen. Wie also Daten sicher aufbewahren? Auf Papier auf jeden Fall nur in den wenigsten Fällen!

Was aber, wenn "euch selbst belastendes Material" entstanden ist? Weg mit dem Mist. Den meisten dürfte jedoch bekannt sein, dass das einfache Löschen von Dateien keineswegs heißt, dass Daten unwiderruflich verschwunden sind. Noch nicht einmal wenn Windows euch warnt, dass mit dem leeren des Papierkorbs aber nun wirklich alles für immer in einem schwarzen Loch verschwindet.

Daten sicher löschen

Um zu veranschaulichen was passiert, wenn Dateien "normal" gelöscht werden gibt es eine Metapher:

Info

Das folgende Szenario gilt aus technischer Perspektive nur bedingt für gängige Arten von Speichern, bspw. für klassische HDD-Festplatten! Bei Flashspeichern wie bspw. SD-Karten, USB Sticks oder SSD's gibt es noch zusätzliche Dinge zu beachten. Mehr dazu unter

"Besonderheiten" weiter unten.

Anna & Arthur's WG

Anna & Arthur wohnen in einer WG. Ihre Namen und Adresse stehen im Adressbuch (anders als beim Telefonbuch ist hier alles nach Adresse geordnet).
Die Wohnung ist das Speichermedium/Datenträger (Festplatte, USB Stick, SD-Karte, etc) und Anna & Arthur sind die Daten auf dem Datenträger. Das Adressbuch ist die Adressverwaltung des Datenträgers.
Wollt ihr euch nun Arthur auf eurem Bildschirm anzeigen lassen, gebt ihr dem PC die Adresse von Arthur. Dieser geht für euch zu besagter Adresse, holt Arthur aus seiner Wohnung und präsentiert ihn auf dem Bildschirm.
Soweit der Normalbetrieb, wenn Daten im Speicher liegen und benutzt werden.

Leider ist Arthur aber bei der letzten Aktion der Schlauchschal unter die Nase gerutscht, er wurde erkannt und muss nun schnell weg. -> Daten müssen gelöscht werden.

Klickt ihr nun auf "löschen" wandert diese Datei in den Papierkorb. Im Papierkorb ist gar nichts gelöscht; seht das einfach als einen "Noch zu löschende Dateien"-Ordner.
Also leert ihr auch den Papierkorb. Was ist nun passiert? Ist Arthur verschwunden?

Nein, ihr habt lediglich Arthurs Namen aus dem Adressbuch gelöscht. Arthur selbst sitzt noch immer auf seiner Couch und wartet, dass etwas passiert. -> Die Daten liegen physisch noch immer auf dem Datenträger. Sie sind bloß nicht mehr im Adressverzeichnis des Speichers indexiert.

Schauen die Cops nun ins Adressbuch, werden sie Arthurs Namen nicht mehr finden. Doch wenn sie einfach Straße für Straße, Haustür für Haustür absuchen, stoßen sie irgendwann auf Anna & Arthurs WG, in der Arthur immer noch sitzt.

Das führt uns zum Überschreiben mit zufälligen Bits: Anna & Arthur brauchen random Nachmieter*innen. Denn wenn ihre Genoss*innen einziehen, oder eben alles nur mit Nullen überschrieben wird, könnte das Spuren hinterlassen.

Zusammengefasst: Daten sind erst richtig gelöscht, wenn die Adressen im Speicher, auf dem sie lagen, durch andere zufällige Daten überschrieben wurden. Dieser Vorgang ist jedoch in keinem gängigen Betriebssystem (egal ob PC oder Handy) Standard, denn diese löschen nur die Adresseinträge zu den Dateien. Das erfordert also extra Aktionen.

Besonderheiten

- **Adressierung:** Bei Flashspeichern wie SD-Karten, USB Sticks oder SSDs weiß das Betriebssystem nicht genau, auf welchen exakten Bits die Daten eigentlich liegen. Eine

eindeutige Verbindung zwischen physischen Bits und von außen adressierbaren Sektoradressen existiert so nicht. Deshalb können diese Bits auch nicht einfach überschrieben werden, weil gar nicht klar ist, welche denn überschrieben werden sollen.
- **Overprovisioning:** Noch dazu blockieren diese Arten von Speicher bestimmte Adressblöcke vor externem Schreibzugriff, sogenannte "Reserveblöcke". Dieses Overprovisioning hat drei Hauptfunktionen: Fehlerkorrektur, Optimierung von Schreibgeschwindigkeit und schont die Lebensdauer des Speichermediums.

Technical Details - Overprovisioning

- Fehlerkorrektur: Wenn einzelne Speicherzellen fehlerhaft werden (zum bsp. durch Verschleiß), kann der Controller auf diese Reserve zurückgreifen, um zu vermeiden, dass die Daten "kaputt" abgelegt werden.
- Schreibgeschwindigkeit: Da die Reserveblöcke bereits "leer" zur Verfügung stehen, müssen nicht immer erst Zellen gelöscht werden, um sie neu zu beschreiben. Der Controller kann so direkt auf leere Zellen zurückgreifen und sie sofort beschreiben.
- Lebensdauer: Overprovisioning vermeidet durch Rotieren der Daten auf den Speicherzellen, dass einzelne Zellen über eine sehr lange Zeit im immer gleichen Zustand bleiben. Das führt klassischerweise dazu, dass diese Zellen bezüglich ihres "an"- und "aus"-Zustandes asymmetrisch werden. Sie tendieren also eher in die eine, oder die andere Richtung zu kippen. Bei Schreibvorgängen kommt es dann zu Fehlern, weil einem Transistor, der bspw. über Jahre "an" war, nun mit einem extrem kurzen Impuls gesagt wird, dass er nun mal "aus" werden soll. Das passiert aber eventuell nicht, weil er sich schon so lange an "an" gewöhnt hat.

Deshalb reicht es hier nicht aus, mit gängigen Methoden Speicherzellen mit random Bits zu überschreiben. Damit bleiben die Reserveblöcke unangetastet, aus denen aber im Zweifel alte Daten rekonstruiert werden können. Die ATA Spezifikation bietet dafür zwei Befehle: `SECURITY ERASE UNIT` und `ENHANCED SECURITY ERASE UNIT`. Ersteres überschreibt nur mit Nullen, zweiteres mit random Bytes. Werden diese Befehle auf eine SSD angewandt, werden auch besagte Reserveblöcke überschrieben. Sowohl unter Linux als auch unter Windows finden sich dafür Kommandozeilen-Tools, die jedoch etwas *hacky* sein können. Die meisten SSD Hersteller wie Samsung, Kingston, Western Digital und Co. liefern extra dafür eigene Tools mit, derer sich bedient werden kann.

Diese Tools machen im Prinzip nichts anderes als diese Befehle auf SSDs mit ihrer eigenen (proprietären) Firmware anzuwenden.

Verschlüsselte Daten löschen

Eine effizientere Methode ist die Verschlüsselung. Das folgende gilt für sowohl für rotierende Platten (HDDs) als auch für SSDs:

Wird der Datenträger verschlüsselt, wird ein Key generiert, der im Header (~Kopfzeile) des Speichers abgelegt wird. Dabei werdet ihr aufgefordert ein Passwort für die Verschlüsselung festzulegen. Mit diesem Passwort wiederum wird der im Header liegende Key verschlüsselt - nicht die Daten selbst.

Jede Datenlese- oder Schreiboperation der Daten wird symmetrisch mit dem Key ent-, oder verschlüsselt.

Die Bit-Zustände auf dem physischen Datenträger können auf Grund der mathematischen Eigenschaften moderner Verschlüsselungsalgorithmen nicht von random Bits unterschieden werden. Ein verschlüsselter Datenträger sieht also forensisch genau so aus wie ein zufällig beschriebener.

Um diese Daten nun wieder sicher zu löschen, muss daher nur der Key im Header des Datenträgers gelöscht und überschrieben werden. Das spart nicht nur enorm viel Zeit (dauert nur ein paar Minuten), das schont auch die Lebensdauer des Datenträgers. Ein vollständiges Überschreiben von einer 1TB HDD kann gut und gerne mal mehr als 5 Stunden dauern.

Detailliertere Infos findet ihr beispielsweise hier.

Kurzfassung

- Daten auf unverschlüsseltem Datenträger: gelöschte Daten lassen Spuren zurück, die wiederhergestellt werden können. Deshalb müssen Daten beim Löschen mit zufälligen (random) Bits überschrieben werden (am besten mehrfach).
- Daten auf verschlüsseltem Datenträger: Diese sind höchstens durch den Key in ihrem Header entschlüsselbar. Dieser Key ist mit einem Passwort gesichert. Wird nur dieser Key gelöscht und überschrieben, können Daten nicht mehr hergestellt werden.

Kommunikations-Verschlüsselung

Die Verschlüsselung jeglicher Kommunikation spielt in unseren Anwendungsfällen eine essentielle Rolle. In diesem Artikel wollen wir erklären, was mit Kommunikationsverschlüsselung gemeint ist, welche Arten es davon gibt und welche Vor- bzw. Nachteile sie haben.

Wir unterscheiden hier zwischen Transportverschlüsselung und Ende-zu-Ende-Verschlüsselung (E2EE: End-To-End-Encryption). Vorwegnehmend lässt sich schonmal sagen, dass Transportverschlüsselung nice-to-have ist, für uns aber in keiner Weise ausreicht und wir deshalb immer E2EE wollen.

Transportverschlüsselung

Transportverschlüsselung wird allgemein mit SSL bzw. TLS realisiert. Das kennt ihr zum Beispiel aus eurem Browser, wenn neben der URL ein Vorhängeschloss erscheint und vor der URI `https` steht. Kommt das nicht zum Einsatz, steht dor nur `http` (und meistens erscheint eine Warnung, dass die Verbindung nicht gesichert ist).

Um die Transportverschlüsselung zu erklären, nutzen wir unten stehende Grafik. Anna will Arthur eine Nachricht übermitteln, bspw. per Email. Das Beispiel funktioniert auch mit anderen Diensten ohne E2EE, wie: Telegram, Discord, oder Chats in Spielen. Dabei gäbe es aber nur einen anstatt zwei Servern.

Hier also das Beispiel mit Email.

Anna hat eine Email-Adresse bei dem gelben Server, hier `systemli.org`. Ihre Mail lautet also `anna@systemli.org`

Arthur hat eine Email-Adresse beim roten Server, hier `riseup.net`. Seine Mail lautet also `arthur@riseup.net`

Weil wir ja von Transportverschlüsselung reden, benutzen beide keine E2EE. Das heißt, weder hat Anna einen PGP-Key von Arthur, noch anders herum!

Die Schlüssel und Schlösser symbolisieren sogenannte **Zertifikate** (Vorhängeschlösser). Jeder Server hat sein eigenes Zertifikat, mit dem die Kommunikation mit ihm verschlüsselt (also

eingeschlossen) werden kann. Nur der Server im Besitz des Zertifikats, hat auch den zugehörigen Schlüssel.

Wenn Anna jetzt eine Mail schreiben will, holt sie sich das Zertifikat von Systemli (gelbes Schloss) und verschlüsselt damit ihre Mail. Völlig unabhängig davon, an wen die Mail am Ende gehen wird! Arthurs Empfangsadresse steht dann draußen auf dem Umschlag, wie bei normaler Post auch. Diese Mail (gelber, verschlossener Umschlag mit Schloss) geht dann zum Systemli-Mailserver (gelber Kasten).

Der Systemli-Mailserver schließt nun, die mit seinem eigenen Zertifikat verschlüsselte Mail auf und scant sie z.B. nach Spam. Vor allem schaut er sich die Empfangsadresse auf dem Umschlag an: `arthur@riseup.net`. An der Stelle hinter dem `@` erkennt der Server, an welchen Mailserver er diese Mail nun weiterleiten muss: `riseup.net` (roter Kasten). Also geht er kurz rüber zu Riseup, schnappt sich eine Kopie des ihres Zertifikats und verschlüsselt damit Annas Email wieder und schickt sie so (roter, verschlossener Umschlag mit Schloss) an den Riseup-Mailserver.

Ab hier wiederholt sich dieser Vorgang so lange, bis die Mail Arthur erreicht. Der Riseup-Server packt die Mail aus und wieder ein und schickt sie schließlich an Arthur.

Grafik Ende-zu-Ende Verschlüsselung

Problem

Hier der Verweis auf die Bedrohung Verkehrsdatenüberwachung/TKÜ.

Das Problem hierbei ist offensichtlich. Jede*r Teilnehmer*in in der Kommunikationskette kann die Mail einfach öffnen und lesen. Zusätzlich bleiben bei vielen Anwendungen (wie oben aufgezählt) die Nachrichten auf den (Mail)-Severn als Kopie liegen.

Ende-zu-Ende Verschlüsselung

Wenn ihr die Bedrohung durch Transportverschlüsselung verstanden habt, ergibt sich die Ende-zu-Ende-Verschlüsselung schon fast von selbst.

1. & 2.) Anna besorgt sich das Schloss (public-key) von Arthur. Dieser Punkt ist sehr wichtig, beachtet dazu den Absatz [TOFU]!

3.) Anna verschlüsselt ihre Nachricht mit Arthurs public-key

4.) Die Nachricht bleibt in allen Teilschritten von 4 (a-e) verschlüsselt. Lediglich die Metadaten (bspw. Absende-/Empfangsadresse) darauf sind (an allen möglichen Stellen, also auch beim Transport!) sichtbar und werden von den Servern gelesen, um die Mail weiter zu leiten.

5.) Arthur empfängt seine Nachricht. Weil die Nachricht mit seinem Vorhängeschloss verschlüsselt wurde und er gut auf seinen Schlüssel (private-key) aufgepasst hat, kann nur er die Nachricht mit seinem Schlüssel wieder entschlüsseln.

Grafik Ende-zu-Ende Verschlüsselung

TOFU ist böse

Trust On First Use

Schlüssel muss "out of band" verifiziert werden. Eine unverschlüsselte (also transportverschlüsselte) Mail ermöglicht das Austauschen der öffentlichen Keys.

Grafik machine-in-the-middle attack

Zu den Gefahren von Transportverschlüsselung siehe Verkehrsdatenüberwachung.

Wifi-Sd_Cards

Besonders Fotograf*innen stehen öfter vor dem Problem, dass ihr frisch aufgenommenes Bildmaterial unverschlüsselt auf den SD-Karten ihrer Kameras liegen, bis sie, wieder zurück am Laptop, dieses auf verschlüsselte Festplatten verschieben können.

Hinzu kommt das Problem, dass sich Speichermedien wie SD-Karten, USB Sticks und SSDs nur sehr unzuverlässig bis gar nicht sicher löschen lassen, wenn die Daten darauf unverschlüsselt waren.

Dem können sogenannte Wifi SD-Karten Abhilfe schaffen. Sie werden wie normale SD-Karten auch, einfach in den dafür vorgesehenen Slot der Kamera gesteckt. Sie speichern allerdings keine Bilder, sondern lassen sich über Wifi(-direct) mit einer App auf dem Handy verbinden und schickt jede gemachte Aufnahme sofort an das Handy, wo die Daten dann zumindest schonmal durch das Handypasswort geschützt sind.

Backups

Es sind schon viele Zeilen darüber geschrieben worden, warum Backups so enorm wichtig sind und über die Kuriosität, dass das allseits bekannt ist und sie scheinbar trotzdem niemand macht, sind schon bessere und schlechtere Witze gemacht worden.

Fakt ist
Wir brauchen Backups!

Backups vs. Datenhygiene

Das größte Problem liegt oft darin, dass wir uns gar nicht so bewusst darüber sind, was wir über die Jahre so alles an Daten ansammeln und wie wichtig diese noch für uns sind. Im Artikel zur Datenhygiene beschwören wir das Credo, so wenig Daten wie möglich anzusammeln. Doch das gilt natürlich vor allem für Daten, die nur von temporärem Nutzen sind und die sonst in irgendwelchen Ecken vergessen werden würden, bis sie bei einer Hausdurchsuchung wiedergefunden werden.

So wichtig es ist, mit kompromittierenden Daten so sparsam wie möglich umzugehen, sind wir doch alle Menschen, die in irgendeiner Weise vom Staat und seinen Institutionen abhängig sind:

Amtliche Dokumente, Krankenversicherung, Bankunterlagen, Arbeitsverträge, Zeugnisse und so weiter, sind alles Dinge, die wir im Zweifel immer mal wieder brauchen, um nicht in völliger Armut zu versinken.

Ideell aber noch viel wichtiger sind vielleicht Fotos von unseren Genoss*innen und Weggefährt*innen, Briefe von ihnen, Tagebücher, Geschenke, Erinnerungsstücke. All das sind Dinge, die unendlich schmerzen könnten, wären sie auf einmal nicht mehr da.

Nicht alles von dem oben Aufgezählten kann einfach digitalisiert werden, doch das meiste davon schon.

Nun laden wir alle dazu ein, sich vorzustellen, dass sämtliche Endgeräte, auf denen all eure Passwörter, Zugänge und Ähnliches gespeichert waren, jetzt kaputt oder weg sind. Könntet ihr das verkraften?

Datenhygiene & Backup Hand in Hand

Im oberen Abschnitt haben wir die Datenhygiene dem Backup gegenübergestellt. Hier möchten wir dafür plädieren, beide Konzepte zusammen zu denken, damit das eine vom andern profitiert.

Besonders langjährig genutzte Geräte und Accounts wie iCloud, Google Drive, WhatsApp, Dropbox usw. quellen oft über vor uralten Datenleichen, von deren Existenz niemand mehr weiß.

Wie viele Daten habt ihr so auf euren Geräten, die ihr mal nicht gelöscht habt, weil ihr dachtet: "Ganz vielleicht brauche ich das doch nochmal"?

Und so haben sich über die Jahre Dutzende, wenn nicht Hunderte GB an Daten angesammelt, die viel zu umfangreich sind, als dass ihr sie mal schnell sichten und aufräumen würdet.

Hättet ihr jedoch ein verschlüsseltes Backup all eurer Dateien, könntet ihr eure täglich genutzten Geräte viel entspannter aufräumen. Dann würdet ihr nur das Nötigste mit euch herumtragen.

Success

Es geht also auch darum, Mut zu Datenhygiene zu bekommen, indem gute Backups gemacht werden.

How To Backup?

Wir arbeiten gerade noch an einem Leitfaden für Backups für die Kategorie "Anleitungen", den wir aber auch hier unten verlinken werden.