Security Crashkurs für PCs und Handys (2017)

Grundbegriffe

Closed Source Software (proprietäre Software)

- Quelltext nicht einsehbar
- abhängig vom Hersteller
- Sicherheitslücken werden spät/überhaupt nicht repariert
- Kommerziell entwickelt

Libre/Open Source Software

- Quelltext ist einsehbar
- Prüfung durch Experten auf Sicherheitslücken/Hintertüren möglich
- Sicherheitslücken werden schnell geschlossen
- Fast immer kostenlos
- Von der Gesellschaft entwickelt

Verschlüsselung

- Mit viel Mathematik können Nachrichten verschlüsselt werden
- „End2End“ Verschlüsselung: Nur Empfänger kann Nachricht lesen, Übertragungsweg komplett verschlüsselt
- Verschlüsselung funktioniert (siehe Expertenmeinungen, NSA/CIA-Leaks)
- Wir müssen **alles** verschlüsseln. Egal ob der Inhalt wichtig ist oder nicht:
  - Gesamtkosten für NSA und co. werden erhöht → mehr Schutz für alle

Metadaten

- Übergeordnete Daten, die nötig sind, um die eigentlichen Informationen zu transportieren (Absender, Empfänger, Zeitpunkte)
- Selbst bei perfekter Verschlüsselung fallen Metadaten an

Proxy

- Leitet Verbindungen weiter
- Empfänger sieht den Proxy-Server als Absender, nicht den eigentlichen Absender
- Geheimdienste können mit Metadaten den eigentlichen Absender aber trotzdem herausfinden

TOR

- Immer 3 zufällige Proxies hintereinander
- Schützt auch Metadaten
- Effektiv gegen Geheimdienste

Helfen lassen

Lasst euch ruhig helfen! In vielen Städten gibt es „Hackerspaces“ und „Linux User Groups“, bei denen euch gerne geholfen wird. Nehmt das Handout mit und sagt, was ihr gerne installieren oder einrichten wollt.

Computer

Betriebssystem:

- Bestehenden Windows PC weiterhin für Closed-Source Software nutzen, sofern notwendig (Microsoft Office, Netflix, Spotify, Skype, Steam, Flash Player, ...)
  - Windows PC mit Open-Source absichern (!)
    - Komplettverschlüsseln:
      - Mit Vera Crypt: https://veracrypt.codeplex.com
      - Dauert ein paar Stunden, je nach Festplattengröße
      - Macht vorher ein Backup der wichtigsten Daten!
  - Der Windows PC bleibt eine Notlösung. Desto weniger man ihn nutzt, desto besser!
- Sicheren Linux-PC aufsetzen (zB. gebrauchtes Thinkpad-Laptop mit 4 GB RAM kaufen), auf dem nur Open-Source Software verwendet wird
  - Kubuntu Linux installieren: https://kubuntu.org
    - Bei der Installation **Komplettverschlüsselung** auswählen!
- Falls ein zweiter PC nicht möglich ist:
  - Tails für sichere Kommunikation verwenden https://tails.boum.org (Betriebssystem, das man vom USB-Stick starten kann - enthält TOR und hinterlässt keine Spuren auf dem PC)

Software (sowohl für Windows, als auch für Linux):

- **Tor Browser** (Firefox mit Tor integriert) für Surfen im Internet – Grundlage für Anonymität: https://torproject.org
- **Firefox** (Linux: meist vorinstalliert, Windows: https://mozilla.org)
  - Videos anschauen, zB. YouTube (dauert mit TOR sehr lange)
  - Man ist **nicht** anonym mit Firefox
  - Cookies löschen, wenn Firefox beendet wird
  - Adblocker installieren: uBlock Origin
  - Ggf. Seiten besuchen, die Tor sperren (zB. Banken)
  - „Privates Fenster“ Funktion nutzen!

- **Passwort-Safe:** KeepassX (Linux: über Paketmanager installieren, Windows: https://keepassx.org)
  - Windows-PC: nur die für Windows relevanten Passwörter speichern (Spotify, Netflix, …)
  - Linux-PC: alle Passwörter speichern
  - (**nicht** am Handy installieren!)

E-Mails:

- Selbst Experten kriegen das nicht sicher, also: **Vermeiden, wo nur möglich!**
- Statt E-Mails besser Crypto-Messenger nutzen (siehe weiter unten)
- Falls nicht vermeidbar:
  - E-Mails nur über Tor-Browser registrieren/abrufen/senden
  - Pro Zweck eine eigene E-Mail Addresse (bzw. „ein Alias“)
  - Wichtige E-Mails abspeichern
  - E-Mails löschen nach Senden bzw. Lesen
  - Keine Namen oder sonstige Informationen senden, die irgendwen identifizierbar machen
  - Sinnvolle E-Mail-Server wählen
    - Registrierungen für Apps/Webseiten:
      - Anonyme E-Mail Adresse nutzen
        - http://mail2tor2zyjdctd.onion
        - http://sigaintevyh2rzvw.onion
        - https://bitmessage.ch
      - Ggf. „Wegwerf“ E-Mail Adressen nutzen (oft gesperrt):
        - https://mailinator.com
    - Arbeit (zB. Bewerbungen):
      - Kleine E-Mail Anbieter nehmen, zB. Von Bürgernetzen
      - Weniger wahrscheinlich, dass die überwacht werden
- Falls ihr wirklich verschlüsselte E-Mails braucht, lasst euch das von Experten und mit Tor zusammen (!!!) einrichten, fragt nach!

Crypto-Messenger

	Wire	**Signal**	**Telegram**
Homepage	https://wire.com	https://whispersystems.org	https://telegram.org
Betriebssysteme			
- Handy	Android, iOS, Windows Phone	Android, iOS	Android, iOS, Windows Phone
- PC	Linux, Windows, Mac	-	Linux, Windows, Mac
Funktionen			

- Telefonie	ja	ja	ja
- Gruppenchats	ja	ja	ja
- Dateien senden	ja	ja	ja
- Bilder senden	ja	ja	ja
- Kann Standard-SMS-Programm ersetzen	nein	ja	nein

	Wire	**Signal**	**Telegram**
<u>Sicherheit</u>			
- Open Source	ja	ja	ja
- Sicheres Protokoll	ja	ja	unbekannt
- Normale Chats verschlüsselt	ja	ja	muss pro Chat aktiviert werden
- Gruppenchats verschlüsselt	ja	ja	nicht möglich
- Dezentral	nein	nein	nein
- Registrierung ohne Telefonnr.	ist möglich	nicht möglich	nicht möglich
- Automatische Updates	Handy: ja PC: nein	ja	ja
<u>Fazit</u>	Sehr gut für verschlüsselt Chatten, Telefonieren, Dateien senden. Kann auch komplett ohne Handy am PC genutzt werden! Gruppenchats über Wire machen, da guter Kompromiss aus Sicherheit und vielen Plattformen.	Sehr gut für verschlüsselt Chatten, Telefonieren, Dateien senden. Als Standard-SMS Programm sehr leicht nutzbar: Wenn man eine SMS an einen Kontakt schreiben will, der auch bei Signal ist, wird automatisch veschlüsselt. Könnt ihr so bei euren Eltern und Großeltern installieren.	Notlösung für normale Chats, falls der Gegenüber keinen anderen Messenger hat. Man muss immer daran denken, verschlüsselte Chats auswählen!

Handys

- Alle Handys haben Closed-Source Komponenten und dadurch an mit Sicherheit grenzender Wahrscheinlichkeit Hintertüren (Treiber, Modem hat Zugriff auf RAM, …). Situation generell viel schlimmer als bei Computern.
- Android ist das einzige massentaugliche Open-Source Handy Betriebssystem
- **Updates**:
  - **Immer Updates machen, wenn sie herauskommen. Alle Updates nachholen, die ihr versäumt habt!** >90% aller Android Handys sind verwundbar für Angriffe, weil Updates nicht gemacht wurden oder nicht bereitgestellt werden vom Hersteller. Praktisch heißt das: Jemand (Geheimdienst, Krimineller oder gleangweilter Jugendlicher) schickt dir eine MMS und kontrolliert alles auf deinem Handy: Mikrofon, Kamera, Standort, alle Nachrichten, Dateien, Browserverlauf. Er kann die Daten einsehen und verändern (jemandem etwas unterschieben). Ihr bekommt den ganzen Angriff nicht mal mit. Das Gilt für alle Handy-Betriebssysteme, wenn ihr keine Updates macht!
  - Wenn ihr **nicht zumindest monatliche Updates** für euer Handy bekommt, dann braucht ihr leider **ein neues Handy**
    - Nur Android: Alternativ kann man evtl. die nicht-kommerzielle Android-Version **LineageOS** (nachfolger von *CyanogenMod*) installieren, die dann auch Sicherheitsupdates liefert und komplett frei von Werbung und Google-Abhängigkeiten funktioniert. Unterstützte Geräte: http://wiki.lineageos.org/devices.html
      - Lasst euch bei der Installation helfen (siehe „Helfen lassen“ auf S. 2)
  - Neues Android Handy: Zb. ein gebrauchtes Nexus 4 für ~100€, und dort das sichere LineageOS installieren. (Google Handys Nexus bzw. Pixel werden derzeit am besten unterstützt von LineageOS, weil der Entwicklungsaufwand dafür geringer ist)
- Handy **verschlüsseln**:
  - Geht bei allen neuen Android/iOS Versionen (schaut in den Einstellungen)
  - Neues Handys teilweise schon von Haus aus verschlüsselt
  - Bringt nur etwas, wenn das Handy aus ist
  - Passwort für die Verschlüsselung setzen!

- Sichere Android Apps
  - F-Droid: „App Shop“, in dem es nur Open-Source Programme gibt (natürlich alle kostenlos). Download: https://f-droid.org
  - In den Einstellungen die „Guardian Project Repositories“ aktivieren (nötig für Orfox, Orbot, Notecipher, siehe unten)
  - Empfohlene Programme:
    - Tor-Browser: *Orfox* (*Orbot* (Tor für Android) braucht man dafür auch)
    - Dateimanager: *Amaze*
    - Kalender: *Etar* und *Offline Calendar*
    - Navigation: *OsmAnd~*
    - Media Player: *VLC*
    - Bahn/Bus: *Transportr*
    - Verschlüsselte Notizen: *NoteCipher*
  - Hinweis: E-Mail am besten überhaupt nicht am Handy!

Allgemeine Tipps

- Immer Updates machen
- Suchvervollständigungen ausschalten
- Regelmäßig verschlüsselte Backups machen
- Fast alle **Anti-Viren-Programme** sind Closed-Source und **stellen selbst Sicherheitslücken dar** (wurde erst wieder im CIA-Leak bestätigt). Besser: Vorsichtig sein bei dem, was ihr installiert (nur Open-Source, aktuelle Software)
- Nicht auf verdächtige Links klicken, egal wer sie euch schickt.
- Installiert nur das, was ihr braucht.
- Funktionen (GPS, WLAN) bzw. ganze Geräte ausschalten, wenn ihr sie längere Zeit nicht braucht
- Immer HTTPS nutzen!
- Daten sicher austauschen: ohne Handy, 2 Linux PCs, verschlüsselte SD-Karten
- Daran denken, Metadaten zu löschen, bevor ihr etwas hochladet (zB. Bilder)!
- Datenkraken wie Facebook, WhatsApp, Google, YouTube, … verlassen. Falls nötig, neues Profil mit so wenig preisgegebenen Daten, wie möglich erstellen.
- Kein Telefon nutzen, wenn es sich vermeiden lässt (Handy und Festnetz)
- Fingerabdruckscanner nur in Kombination mit einem Passwort nutzen
- Modebegriffe für Überwachung: Big Data, Cloud, Internet of Things, Künstliche Intelligenz (KI) bzw. Artificial Intelligence (AI)
- Meinungen von Experten einholen
- **Technik im Zweifelsfall nicht vertrauen!**