DSDS - Handout

Stand: 1.4.2024 (Kreta SoSe24 im Odradek). Schreibe mir bei Fragen gern eine Nachricht via eMail oder Signal

---

Kommunikation

- Signal download
- Matrix Einrichten
  - Verzeichnis aller Clients
  - Ergänzend: Hinweise von Systemli
- Begründet paranoid: Briar

eMail

Dass Google und Microsoft emails mitlesen und zum machine learning training verwenden oder einfach persönliche Daten für personalisierte Werbung verwenden ist mittlerweile Allgemeinwissen. Was wenige wissen: ein Umzug ist einfach! Alle unten genannten Anbieter bieten einen Umzugsservice an.

Hosting

- Free: https://proton.me
- 1€/Monat: https://posteo.de/ (Barzahlung möglich)
- Custom Domain: 3€/m Mailbox.org (Barzahlung möglich) oder 4€/m Proton Plus

Clients

- Windows, macOS, Linux: thunderbird
- Android: k9-Mail
- iOS, macOS: Apple Mail (der Client, nicht iCloud!)

> ⚠ **Outlook 2024 liest mit**
>
> Das 2024 Update für Windows Mail oder Outllok liest emails mit, auch wenn diese bei einem Anbieter wie Posteo liegen. **Ich rate DRINGLICHST davon ab Outlook zu benutzen!** Auch der Bundesbeauftragte für Datenschutz und Informationsfreiheit rät offiziell davon ab.

Kollaboration

Dokumente bearbeiten (Google Docs, Microsoft Office)

- Nextcloud + OnlyOffice/Collabora
  - benötigt eigene IT Infrastruktur
  - server müssen ordentlich abgesichert sein
- Cryptpad
  - gut für kleingruppen ohne eigene IT Infrastruktur
  - kann Textdokumente, Tabellkalkulation, Präsentationen, Formulare, Diagramme

Videokonferenzen (Zoom, Webex)

- Wenige Leute, sicherer: Jitsi
- Größere Konferenzen, telefoneinwahl: Senfcall

Termine & Umfragen (Doodle, Google Forms)

- Termine und Abstimmungen: https://www.systemli.org/poll/
- Formulare: https://cryptpad.fr/form/

Hosting

- Radical Servers List
  - Aktivistische Gruppen können in der Regeln einfach bei Kollektiven anfragen
- Auf Spendenbasis: https://linxx.net/
- Selfhosting mit YunoHost
  - wichtig: Festplatte ordentlich verschlüsseln!

Persönlich

Webbrowser

Empfehlung: Firefox mit folgenden Add-Ons

- Werbeblocker: uBlock Origin
- Tracking-Blocker: Privacy Badger
- Passwordmanager: Bitwarden (siehe unten)
- Wenn viele accounts: Cookie-Containers

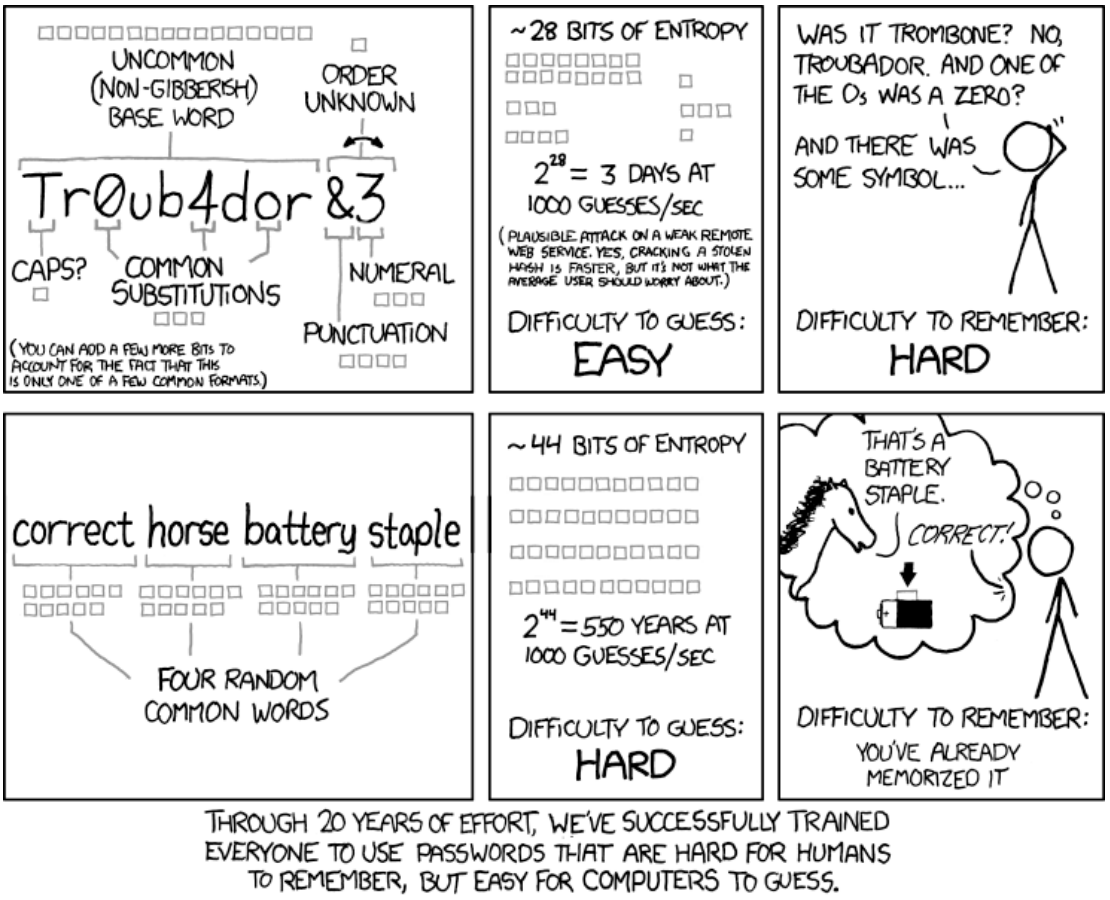
Alternativ:

- Safari (Closed Source)

- Brave (zugemüllt mit Cryptobro-krams)

Passwörter + 2FA

Ein erste wichtige schritt, ist das verwenden von Passphrasen, statt wild ausgedachten Passwörtern. Die Begründung wurde im XKCD#936 einfach dargestellt und für die interessierten gibts auch eine technische Erläuterung warum diese Methode wirklich sicherer ist:



Wichtig: sie müssen wirklich zufällig generiert sein! Sonderzeichen/zahlen sowie Großkleinschreibung sind optional. Das generieren geht einfach online oder direkt im Passwortmanager und sieht etwa so aus:

Ein **Passwortmanager** ist nicht nur sicherer, sondern auch was für faule. Ein letztes mal eine sichere Passphrase merken, dann alles andere darin ablegen und nie wieder das "passwort vergessen" spiel spielen. Firmen spielen auch gerne das "ändere dein Passwort aller XYZ Tage" Spiel, was durch einen Passwortmanager sehr entspannt wird.

- Bitwarden Video Tutorial (4 min)
  - Download
  - Hilfe: Import you Data (en)
- Proton Pass Hilfeseite
  - Download

> ⚠ **Passwörter nicht im Browser speichern!**
>
> In der Vergangenheit gab es bereits Sicherheitlücken in diesen verfahren, lange konnte google sogar Passwörter mitlesen -> Verwende ein der oben verlinkten apps

Zwei-faktor-authentifikation (2FA) wird häufig mit Google Authenticator verbunden, aber ist ein offener standard, den viele Apps können. Dafür muss eine lange kombination in die 2FA app gespeichert werden, entweder mit copy/paste oder über einen QR code.

- Crossplattform: Standardnotes + 2FA Extension (Guide: SN Extensions Installieren)
- Crossplattform: Authy
- Android: Aegis
- iOS: Sentiel

Passkeys

Passkeys sind recht neu und vereinen die Idee von Passwörtern und 2FA. Die Technologie wird stark von großen Firmen (Google, Microsoft, Apple) gepusht.

> ⚠ **Passkeys nicht auf dem Gerät oder im Browser speichern!**
>
> Wenn die Passkeys lokal auf einem Gerät gespeichert werden, sind die weg wenn es davon kein Backup gibt! Wenn Passkeys nicht ende-zu-ende verschlüsselt in google oder apple-IDs gespeichert werden, ist viel Sicherheit dahin!

Darum ist es sinnvoll Passkeys mit Bitwarden oder ProtonPass zu verwalten:

- Bitwarden Infoseite
- Proton Pass Infoseite

Für 2024 empfehle ich bei Passwörtern + 2FA zu bleiben, 2025 ist die Sache sicher ausgereifter. An sich aber ein sehr sinnvoller Schritt zu einfacherer IT Sicherheit.

Notizen & Secrets

Wer einfach Notizen schreiben möchte und sich keinen Kopf um Verschlüsselung machen will, sollte Standard Notes ausprobieren. Wer viel schreibt, viele miteinander verbundene Gedanken und Aufgaben hat, sollte Obsidian ausprobieren. Ein Backup von Secrets (wie recovery keys von Filevault oder Bitlocker) ist auch in Standard Notes gut aufgehoben.

- Simple Notizen: Standard Notes
  - Tipp: Student Discount oder einfach Fragen
  - Umzug: official importers oder community importers
- Persönliches Wiki: Obsidian oder logseq
  - Beide sind ohne sync & backup kostenlos
  - Tipp: Obsidian student discount
  - Umzug: Obsidian importer plugin

> ⓘ **Verschlüsseltes synchronisieren aktivieren!**
>
> Bei Obsidian sync muss ein e2ee Passwort gesetzt werden. Logseq kann momentan nur sicher über iCloud mit aktivierter advanced data protection synchronisiert werden.

Kontakte & Kalender Sync

- Android, Apple, Linux, Windows: Etesync
- Apple: iCloud Advanced Data Protection
- Android, Apple, Linux, Windows: Posteo

Daten Verschlüsseln

(Cloud) Speicher

Unsicherer Cloudspeicher – Cryptomator

- verschlüsselt Dateien und Verzeichnisstruktur in synchronisierbare Teile zerlegt
- gut für Speicher wie OneDrive, Google Drive, Dropbox, etc

Sicherer Cloudspeicher – Filen

- sichere Architektur und privat im Design
- alternative zu OneDrive, Google Drive, Dropbox

USB Stickes & Festplatten – Veracrypt

- erstellt einen großen Verschlüsselten Container/Block, der an einem beliebigen Ort gespeichert werden kann
- gut für tragbare Speicher oder ganze Windows/Linux Computer
- ermöglicht glaubhafte Abstreitbarkeit in dem Fall, dass ein Passwort herausgegeben werden muss, zum Beispiel unter Androhung von Gewalt

Endgeräte

> ⚠ **Geräte verschlüsseln ist ein muss!**
>
> Alle bisherige Schritte schützen vor Online-Überwachung oder Online-Datenlecks. Für einen wirksamen Schutz der Daten im Falle eines Diebstahls oder einer Repressionsmaßnahme *muss* auch das lokale Endgerät verschlüsselt sein!

- Windows – Bitlocker (4min)
  - wichtig: startup pin einrichten!
- Linux – Cryptsetup (6min) oder Linux + TPM (sehr sicher) (40min)
  - wichtig: argon2 verwenden!
- macOS – FileVault2 (4min)

> ⓘ **Geräte herunterfahren, nicht nur zuklappen**
>
> Bei allen Varianten gilt: das Gerät muss wirklich runterfahren werden, damit die Verschlüsselung in voller stärke greift. Zuklappen oder Ruhemodus lassen häufig eine Seitenkanalatacke offen.

Metadaten löschen

- Mobil/Desktop: Signal (zB an Note to Self) löscht Metadaten aus Bildern
- Desktop: mat2 läuft offline und kann viel mehr Datentypen (PDF, Video und mehr)
- metadata.systemli.org ist die onlineversion von mat2, kann auch alles

Daten schreddern

Festplatten müssen lediglich mehrmals überschrieben werden, bei SSDs bzw Flashspeicher wie USB Sticks hilft das wenig, hier muss von Anfang an Verschlüsselung her (zB mit Veracrypt, siehe oben) oder der Speicher muss physisch zersetzt/geschreddert/mit einem Hammer malträtiert werden.

- HDDs: Windows, Linux und macOS
- SSDs: hier verschiedene Methoden zur Zerstörung

Tracking und Logging deaktivieren

- Android Privacy Dashboard
  - Google Location History
- iOS Datenschutzeinstellungen
- Windows Telemetrie deaktivieren
  - leider keine offizielle Doku, weil Microsoft schlimmer als google ist
- Firefox Telemetrie deaktivieren

Weiterführendes

...einfach einmal in die Suchmaschine des Vertrauens eingeben

- Android Open Source Project. 2021. Organizational and Operational Security. Juni 18.
- Buermeyer, Ulf, und Andre Meister. 2018. *Funkzellenabfrage: Die alltägliche Rasterfahndung unserer Handydaten*.
- Leith, Douglas J. 2021. Web Browser Privacy: What Do Browsers Say When They Phone Home? *IEEE Access* 9: 15. https://doi.org/10.1109/ACCESS.2021.3065243.
- Microsoft. 2020. How OneDrive safeguards your data in the cloud.
- Seitenkanalattacke. 2022. *Wikipedia*.
- Telegram.org. 2016. End-to-End Encryption, Secret Chats.
- Telegram.org. 2017. Mobile Protocol: Detailed Description.

Talks

- Böcker, Stefan. *Digitale Selbstverteidigung – Wie schütze ich mich vor Überwachung?*
- Fischer, Josephine, und Tobias Naumann. *Demokratie auf Sächsisch*.
- Kleemann, Uli. *Ich habe doch nichts zu verbergen*.
- Melzer, Marius. *Datenschutz für Aktivist*innen*.