>>> Einführung in die digitale Selbstverteidigung
>>> ein Vortrag der AG-Link

Nikita & Peter

16. Oktober 2024

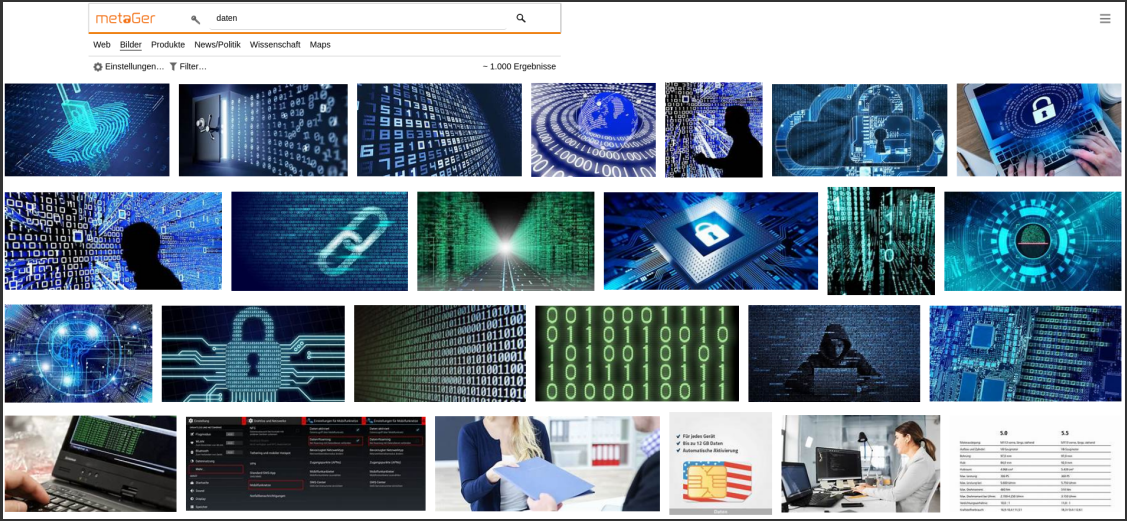
Vorstellung

>>> Vorstellung

* AG Link – AG für kritische Informatik
* seit 2018
* Website: ag-link.xyz (+ Folien)
* Email: ag-link@riseup.net
* Instagram: @ag.link_le
* Mastodon: https://systemli.social/@link

Einführung

>>> Was sind Daten?



>>> Was sind Daten?

Gebilde aus Zeichen oder kontinuierliche Funktionen, die aufgrund bekannter oder unterstellter Abmachungen Informationen darstellen, vorrangig zum Zweck der Verarbeitung und als deren Ergebnis.

[DIN 44300 Nr. 19](1985)

>>> Was sind Daten?

>>> Metadaten

Exif Tag	Value
Exif.GPSInfo.GPSLongitude	0deg 0' 0.000"
Exif.GPSInfo.GPSLongitudeRef	East
Exif.GPSInfo.GPSLatitude	0deg 0' 0.000"
Exif.GPSInfo.GPSLatitudeRef	North
Exif.GPSInfo.GPSAltitude	116.00 meter (380.48 feet)
Exif.GPSInfo.GPSAltitudeRef	Above sea level
Exif.Image.BitsPerSample	8 8 8
Exif.Image.DateTime	2021:10:10 17:04:03
Exif.Image.ExifTag	206
Exif.Image.ImageLength	3840
Exif.Image.ImageWidth	2160
Exif.Image.Make	OnePlus
Exif.Image.Model	ONEPLUS A5000
Exif.Image.Orientation	top, left
Exif.Image.ResolutionUnit	inch
Exif.Image.Software	GIMP 2.10.28
Exif.Image.XResolution	72
Exif.Image.YCbCrPositioning	Centered
Exif.Image.YResolution	72
Exif.Photo.ApertureValue	F1.7
Exif.Photo.BrightnessValue	1.74
Exif.Photo.ColorSpace	sRGB
Exif.Photo.ComponentsConfiguration	01 02 03 00
Exif.Photo.DateTimeDigitized	2021:10:10 14:48:45
Exif.Photo.DateTimeOriginal	2021:10:10 14:48:45
Exif.Photo.ExifVersion	30 32 32 30
Exif.Photo.ExposureMode	Auto
Exif.Photo.ExposureProgram	Not defined
Exif.Photo.ExposureTime	1/118 s
Exif.Photo.FNumber	F1.7
Exif.Photo.Flash	No, compulsory
Exif.Photo.FlashpixVersion	30 31 30 30
Exif.Photo.FocalLength	0.0 mm
Exif.Photo.FocalLengthIn35mmFilm	Unknown
Exif.Photo.ISOSpeedRatings	200
Exif.Photo.MeteringMode	Center weighted average
Exif.Photo.PixelXDimension	3840
Exif.Photo.PixelYDimension	2160
Exif.Photo.SceneCaptureType	Standard
Exif.Photo.SceneType	01
Exif.Photo.SensingMethod	(0)
Exif.Photo.ShutterSpeedValue	1/118 s
Exif.Photo.SubSecTime	259484
Exif.Photo.SubSecTimeDigitized	259484
Exif.Photo.SubSecTimeOriginal	259484
Exif.Photo.WhiteBalance	Auto

>>> Metadaten

Exif Tag	Value
Exif.GPSInfo.GPSLongitude	0deg 0' 0.000"
Exif.GPSInfo.GPSLongitudeRef	East
Exif.GPSInfo.GPSLatitude	0deg 0' 0.000"
Exif.GPSInfo.GPSLatitudeRef	North
Exif.GPSInfo.GPSAltitude	116.00 meter (380.48 feet)
Exif.GPSInfo.GPSAltitudeRef	Above sea level
Exif.Image.BitsPerSample	8 8 8
Exif.Image.DateTime	2021:10:10 17:04:03
Exif.Image.ExifTag	206
Exif.Image.ImageLength	3840
Exif.Image.ImageWidth	2160
Exif.Image.Make	OnePlus
Exif.Image.Model	ONEPLUS A5000
Exif.Image.Orientation	top, left
Exif.Image.ResolutionUnit	inch
Exif.Image.Software	GIMP 2.10.28

>>> Wer verwendet meine Daten?

* ich +
  Freund*innen,
  Familie,
  Bekannte

>>> Wer verwendet meine Daten?

* ich + Freund*innen, Familie, Bekannte
* Hacker, Erpresser, etc.

Government	Agency	Year	Records	Organization type	Method	Sources
United Kingdom	Transport for London	2024	5000+ Passengers data including home addresses, bank account details, unconfirmed number of Staff data leaked too	Local Transport authority	hacked	[11]
Sydney, Australia	Western Sydney University	2024	7,500, including email accounts, SharePoint files, and the Microsoft Office 365 environment	academic	hacked	[17][18]
United Kingdom	BBC	2024	25,290 employee pension records, including name, date of birth, home address, national insurance number	public broadcasting	hacked	[20][21]
United Kingdom / Scotland	NHS Dumfries and Galloway	2024	still unknown	healthcare	cyber attack	[25][26]
England/Wales	England and Wales Cricket Board	2024	43,299	government	unknown	[48]
India	Indian Council of Medical Research	2023	815,000,000+, including Aadhaar IDs, passport details, names, phone numbers, addresses	government	hacked by pwn0001	[14]
Bangladesh	Office of the Registrar General, Birth & Death Registration	2023	50,000,000+	government	data leak due to security vulnerabilities	[19]
United Kingdom	British Library	2023	unknown	government	ransomware	[22]
United States	Consumer Financial Protection Bureau	2023	256,000	bureau	poor security	[37]
Indonesia	Directorate General of Immigration of Indonesia	2023	34,900,867	Government	hacked and published	[43]
Indonesia	Directorate General of Population and Civil Registration (Dukcapil)	2023	337.225.463	Government	leaked and published	[44]
Philippines	Various law enforcement agencies (Philippine National Police, National Bureau of Investigation, Bureau of Internal Revenue)	2023	1,279.437	government	poor security	[88]
50 companies and government institutions	Various	2022	6,400,000	various	poor security	[12][13]
Shanghai, China	Shanghai National Police Database	2022	1,000,000,000, including name, address, birthplace, national ID number, mobile number, all crime/case details	government	unsecured database	[72][73]
Russia	Roscosmos	2022	handwritten forms, PDFs, spreadsheets, descriptions of lunar missions.	aerospace	hacked by v0g3isec	[93]
Ireland	Health Service Executive	2021	unknown	healthcare	unknown	[59]

Abbildung: kürzliche Datenlecks 2024[a]

[a] https://en.wikipedia.org/wiki/List_of_data_breaches

>>> Wer verwendet meine Daten?

* ich + Freund*innen, Familie, Bekannte
* Hacker, Erpresser, etc.

Abbildung: Rekonstruktion von privaten Informationen aus „KI" Modellen[a]

[a] J. Geiping, H. Bauermeister, H. Dröge, and M. Moeller, "Inverting Gradients -- How easy is it to break privacy in federated learning?," 2020, doi: 10.48550/ARXIV.2003.14053.

>>> Wer verwendet meine Daten?

* ich + Freund*innen, Familie, Bekannte
* Hacker, Erpresser, etc.
* Firmen

Report: Facebook helped advertisers target teens who feel “worthless” [Updated]

Leaked 2017 document reveals FB Australia's intent to exploit teens' words, images.

SAM MACHKOVECH - 5/1/2017, 9:00 AM

Abbildung: Profitoptimierung mit microtargeting[a]

[a] https://arstechnica.com/information-technology/2017/05/facebook-helped-advertisers-target-teens-who-feel-worthless/

>>> Wer verwendet meine Daten?

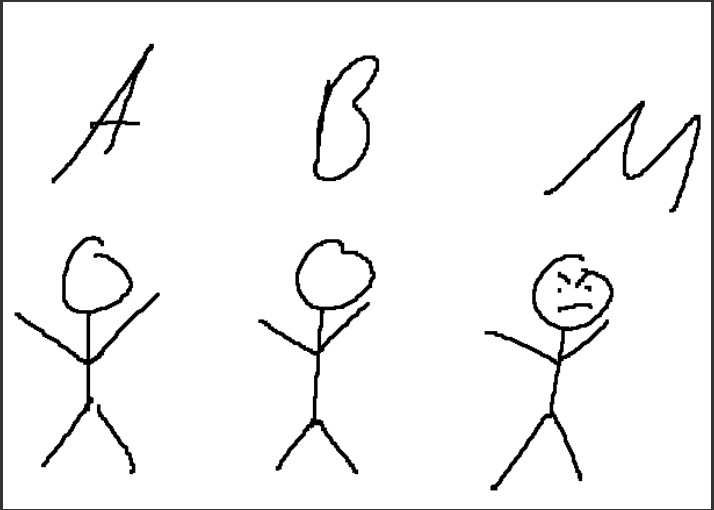
* ich + Freund*innen, Familie, Bekannte
* Hacker, Erpresser, etc.
* Firmen
* **Behörden**

Abbildung: Behörden fragen Daten von Telegram an[a]

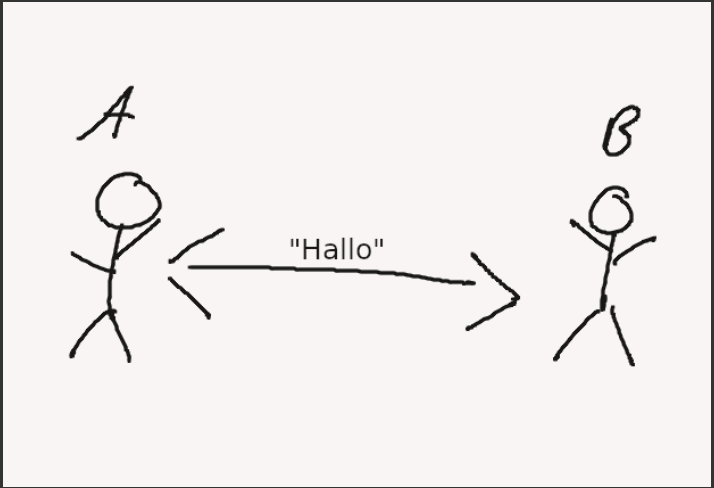
[a] https://www.handelsblatt.com/dpa/extremismus-telegram-uebermittelte-daten-an-deutsche-sicherheitsbehoerden/28666622.html

Gefahren bei der Datenübertragung

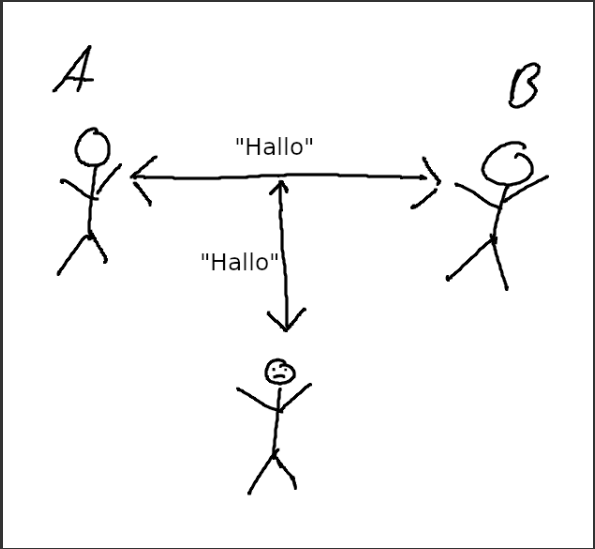
>>> Datenübertragungen



>>> Was bedeutet Datenübertragung?

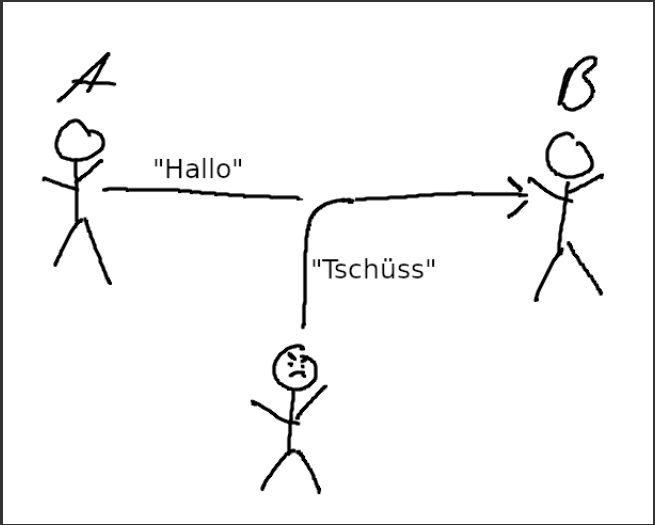


>>> Was sind Gefahren bei der Datenübertragung?



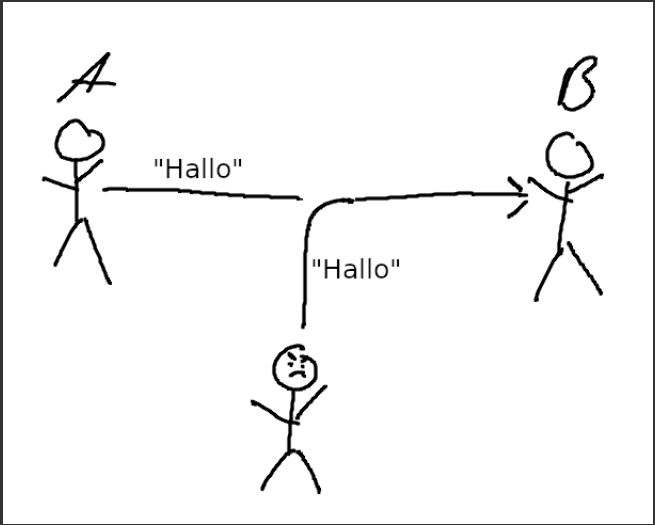
Gefahr: Lauschangriff

>>> Was sind Gefahren bei der Datenübertragung?



Gefahr: Manipulation

>>> Was sind Gefahren bei der Datenübertragung?



Gefahr: Authentizität

Was tun?

>>> Verschlüsseln!

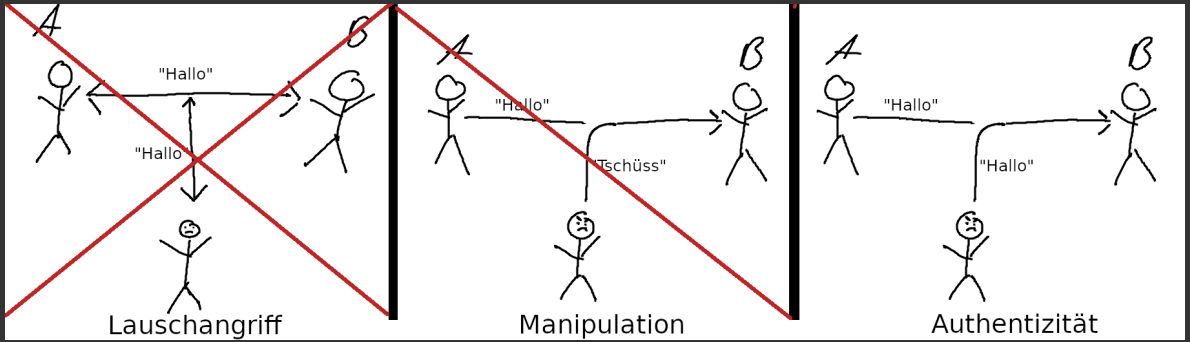


Abbildung: Probleme gelöst durch Verschlüsselung

>>> Verschlüsselung – der einfache Fall

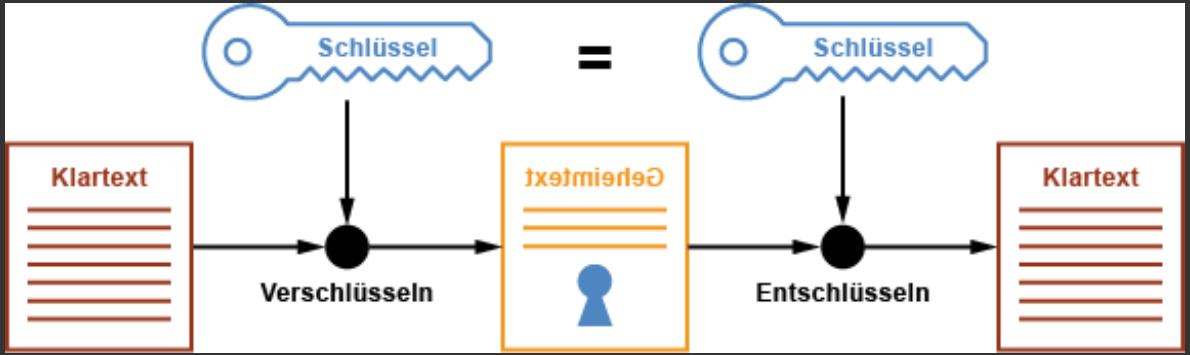
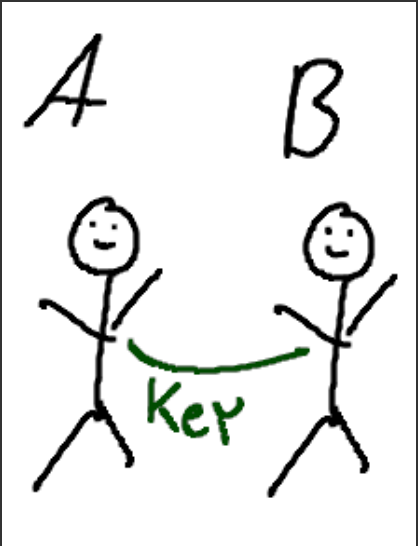


Abbildung: Symmetrische Verschlüsselung

>>> Verschlüsselung - der einfache Fall



>>> Verschlüsselung – der einfache Fall

AES Online Encryption

Enter text to be Encrypted

123

OR

Choose File No file chosen

Select Mode

CBC

Key Size in Bits

128

Enter IV (Optional)

1234567898765432

Enter Secret Key

1234123456789878

Output Text Format: Base64 Hex

Encrypt

AES Encrypted Output:

4573BF2C65009DF18FAF9421B5D0E789

AES Online Decryption

Enter text to be Decrypted

4573BF2C65009DF18FAF9421B5D0E789

Input Text Format: Base64 Hex

Select Mode

CBC

Enter IV Used During Encryption(Optional)

1234567898765432

Key Size in Bits

128

Enter Secret Key

1234123456789878

Decrypt

AES Decrypted Output **(Base64)**:

MTIz

Decode to Plain Text

123

>>> Verschlüsselung - Sicherheit?

* AES 256-Bit Verschlüsselung

-> 2^{256} mögliche Kombinationen

-> Dauer Entschlüsselung ohne Wissen des Passwort = ca. $3,3 \times 10^{56}$ Jahre

  * vgl. Alter des Universums: $13,8 \times 10^{9}$

>>> Verschlüsselung - Sicherheit?

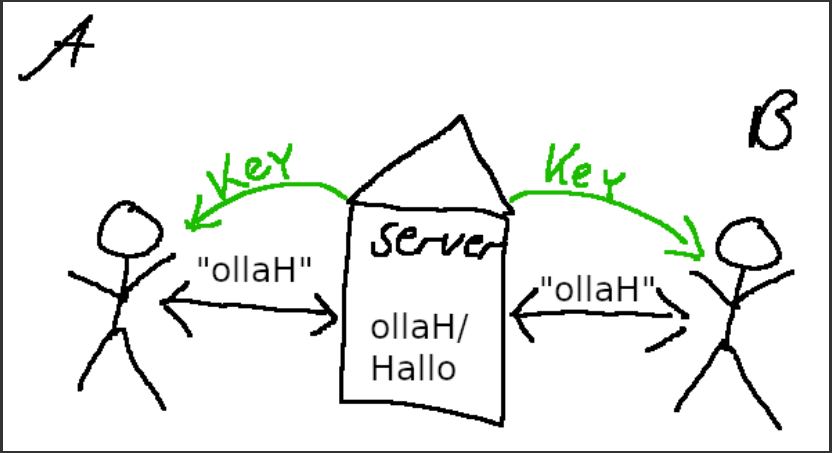
* AES 256-Bit Verschlüsselung

-> 2^{256} mögliche Kombinationen

-> Dauer Entschlüsselung ohne Wissen des Passwort = ca. $3,3 \times 10^{56}$ Jahre

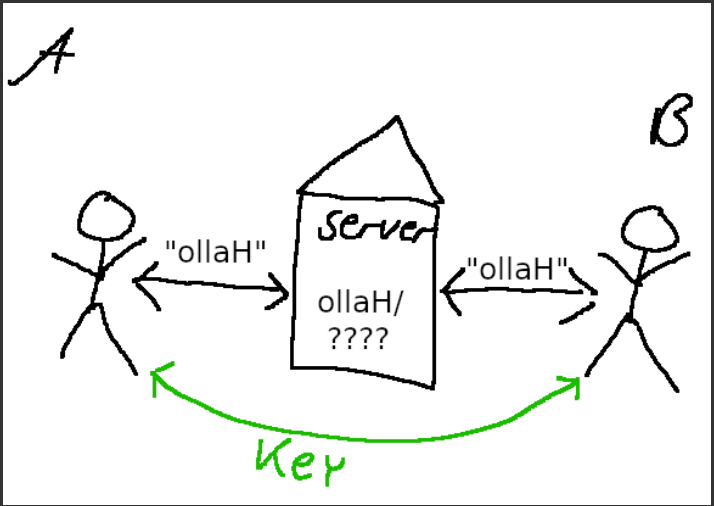
  * vgl. Alter des Universums: $13,8 \times 10^{9}$

>>> Transportweg-Verschlüsselung (TLS)



Transportwegverschlüsselung (kein E2E) = schlecht

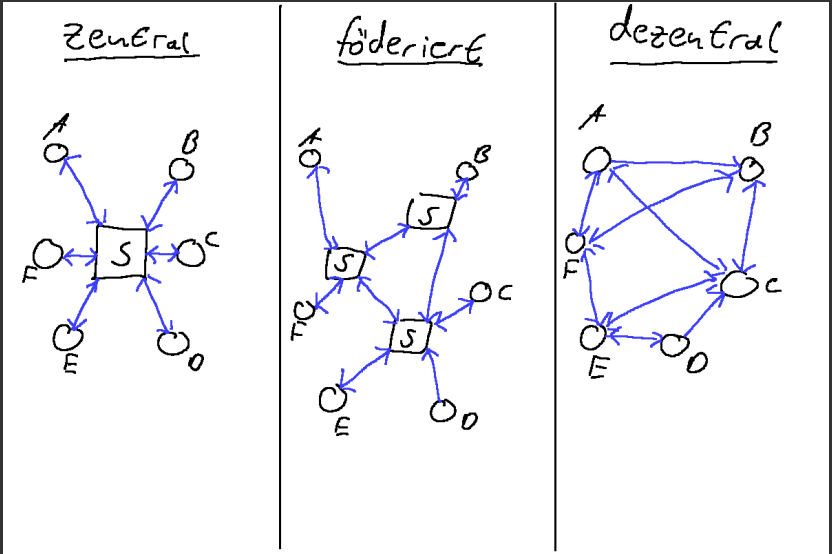
>>> Ende-zu-Ende-Verschlüsselung (E2E)



E2E = gut

Messenger

>>> Messenger Konzepte



>>> Was sind gute Messenger?

	WhatsApp	Telegram	Signal	Threema	Element	Briar
Verschlüsselung						
Vertrauenswürdig						
Open-Source						
Dezentral						
Metadaten						
Kostenlos						

>>> Unsere Empfehlung

Signal

Element

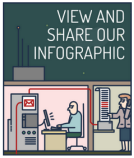
Briar

>>> Und sonst? - E-Mails

>>> E-Mail Verschlüsselung

EMAIL SELF-DEFENSE

LANGUAGE ▾ | SET UP GUIDE | TEACH YOUR FRIENDS | THIS SITE'S TOR ONION SERVICE | SHARE



Bulk surveillance violates our fundamental rights and makes free speech risky. This guide will teach you a basic surveillance self-defense skill: email encryption. Once you've finished, you'll be able to send and receive emails that are scrambled to make sure a surveillance agent or thief intercepting your email can't read them. All you need is a computer with an Internet connection, an email account, and about forty minutes.

Even if you have nothing to hide, using encryption helps protect the privacy of people you communicate with, and makes life difficult for bulk surveillance systems. If you do have something important to hide, you're in good company; these are the same tools that whistleblowers use to protect their identities while shining light on human rights abuses, corruption, and other crimes.

In addition to using encryption, standing up to surveillance requires fighting politically for a reduction in the amount of data collected on us, but the essential first step is to protect yourself and make surveillance of your communication as difficult as possible. This guide helps you do that. It is designed for beginners, but if you already know the basics of GnuPG or are an experienced free software user, you'll enjoy the advanced tips and the guide to teaching your friends.

FSF FREE SOFTWARE FOUNDATION

We fight for computer users' rights, and promote the development of free (as in freedom) software. Resisting bulk surveillance is very important to us.

Please donate to support Email Self-Defense. We need to keep improving it, and making more materials, for the benefit of people around the world taking the first step towards protecting their privacy.

DONATE

SIGN UP

Enter your email address to receive our monthly newsletter, the Free Software Supporter

SUBSCRIBE ME

#1 GET THE PIECES

⇒ komplette Anleitung unter: https://emailselfdefense.fsf.org

>>> Dateien verschicken

* sichere Messenger
* verschlüsselte E-Mails
* Clouds:
    * „Nextcloud"[1] (eigen, oder extern[2])
    * Uni Cloud (max. 5GB) + Cryptomator[3]
    * Dropbox/ GoogleCloud/ etc. mit verschlüsselten Dateien
* Geheimtipp: Onion-Share[4]

---

[1] https://nextcloud.com/
[2] https://riseup.net/de/security/resources/radical-servers
[3] https://www.urz.uni-leipzig.de/servicedesk-und-hilfe/hilfe-zu-unseren-services/it-sicherheit/datenverschluesselung-mit-cryptomator
[4] https://onionshare.org/

Informationen sicher speichern

>>> Gefahr durch unverschlüsselte Daten

Daten werden immer noch oft unverschlüsselt gespeichert.

* login Passwort schützt nicht ohne weiteres Daten
* Daten *vollständig* zu löschen ist nicht einfach

>>> Welche Daten sind potentiell unverschlüsselt?

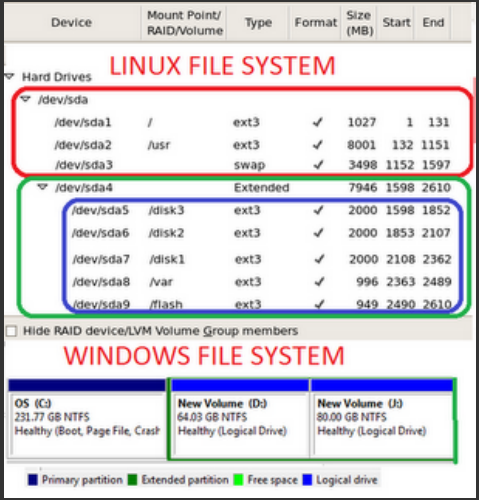


Abbildung: Wo werden Daten gepseichert?

>>> Gefahr durch unverschlüsselte Daten

Angenommen du verlierst deinen Laptop.

Bist du dir sicher, dass niemand auf deine persönlichen Daten zugreifen kann?

>>> Vorteile von Verschlüsselung

Kümmert euch **aktiv** um die Verschlüsselung eurer Daten!

* Speicherort spielt dann keine Rolle mehr
* keine Gefährdung bei Verlust
* Verschlüsselung ist sehr schwer bis gar nicht zu knacken

>>> Welche Daten sind bereits verschlüsselt?

Standardmäßig nicht zwangsläufig verschlüsselt:

* Windows
* macOS
* Linux
* externe Festplatten
* USB-Sticks
* SSD
* Cloud-Speicher

Standardmäßig verschlüsselt:

* Android, iOS, spezielle Speichermedien (Self-Encrypting Drives)
    * Achtung! Was ist mit SD-Karte?

>>> Verschlüsselungsprogramme

Wie verschlüssele ich meine Daten?

Universell:

* VeraCrypt
    * Container, Laufwerke, Partitionen
    * Kommt zu unserem Workshop

Windows:

* BitLocker (closed Source)

macOs:

* FileVault (closed Source)

Linux:

* LUKS (Linux Unified Key Setup)

Cloud-Speicher:

* cryptomator

>>> Cloudverschlüsselung

„Cloud" als Spezialfall, da wir Festplatte nicht selbst verschlüsseln können.

Abbildung: Prinzip Cryptomator

>>> Passwörter

Symmetrische Verschlüsselung hängt von einem Schlüssel (meist Passwort) ab.

* Wer sollte potentiell Zugriff auf euren Schlüssel haben?
    * Microsoft?
    * Google?
    * Apple?
* Besser: Passwörter selber verwalten → Passwortmanager

>>> Passwortmanager

Gute Open Source Passwortmanager:

* KeePassXC
    * Offline (Synchronisation zwischen Geräten in eigener Verantwortung)
    * Browser Add-Ons verfügbar
* Bitwarden
    * Server basiert (Account notwendig)
    * Server kann selbst gehosted werden
* pass
    * Offline (Synchronisation zwischen Geräten in eigener Verantwortung)
    * Erfordert Willen sich mit zugrunde liegenden Prinzipien ausinanderzusetzen
    * Unix Philosphy mit gpg Verschlüsselung

>>> Single Sign On und integrierte Passwortmanager?

Was ist mit SSO Diensten von Unternehmen wie, Apple, Google, Microsoft und integrierten Passwortmanagern von Firefox, Chrome, Safari, etc.?

* Wie leicht wird dadurch Zugriff auf Accounts (z.B. zum Autofill)?
    * → Masterpasswort verwenden
* Plattformbindung
* prinzipiell besser als kein Passwortmanager
* trotzdem sollten starke Passwörter verwendet werden

>>> Was ist ein gutes Passwort?

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

How did we make this? Learn at hivesystems.com/password

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

HIVE SYSTEMS

› Hardware: 12 x RTX 4090 | Password hash: bcrypt

Das wars an Input! :)

unsere weiteren KEW-Veranstaltungen

>>> VeraCrypt Workshop

* Workshop: Einführung in Festplatten & USB-Stick Verschlüsselung mit VeraCrypt
* **Wann**: (Do.) 12.10.2023, 15:00-17:00Uhr
* **Wo**: S017
* **Was ihr braucht**: Laptop (+ optional USB-Stick/ externe Festplatte)
* **Event-Link**: https://ag-link.xyz/event/2023/10/12/handson-digitale-selbstverteidigung.html

>>> offenes Kennenlern-Treffen

* Kommt vorbei und lernt uns kennen!
* **Wann:** (Mi.) 30.10.2024, 18:00–20:00Uhr
* **Wo:** P801 (Paulinum, 8. Etage, Hauptcampus)

Letzte Anmerkungen

>>> Software-Übersichten

* PrivacyToolsIO - https://www.privacytools.io/
* Awesome-Privacy - https://github.com/Lissy93/awesome-privacy
* AlternativeTo - https://alternativeto.net/
* Liste von Services wie riseup.net - https://riseup.net/de/security/resources/radical-servers

>>> What to read next?

* Video: Datenschutz für Anfänger*innen[6]
* DigitalCourage[7]
* BigBrotherAward[8]
* Netzpolitik[9]
* AlgorithmWatch[10]
* Capulcu[11]

---

[6] https://media.ccc.de/v/ds20-11314-datenschutz_fur_aktivist_innen
[7] https://digitalcourage.de/
[8] https://bigbrotherawards.de/
[9] https://netzpolitik.org/
[10] https://algorithmwatch.org/en/
[11] https://capulcu.blackblogs.org/

>>> Bildnachweise

* https://www.elektronik-kompendium.de/sites/net/1907041.htm
* https://praxistipps.chip.de/was-ist-ein-bit-byte-einfach-erklaert_42267
* https://security.stackexchange.com/questions/69163/what-are-the-risks-of-using-tor-browser
* https://thesecmaster.com/detailed-anatomy-of-the-tor-network-structure-of-the-tor-network/
* https://www.paubox.com/blog/how-to-get-employees-to-use-encrypted-email/
* https://www.pngall.com/backup-png/download/30379
* https://cdn.comparitech.com/wp-content/uploads/2015/11/cryptomator-768x273.jpg
* https://imgbb.com/YLxM90K
* https://linuxexplore.com/wp-content/uploads/2012/10/primary-extended-logical-linux-windows-file-system.png

Fragen?