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

Max & Peter
04. Oktober 2023

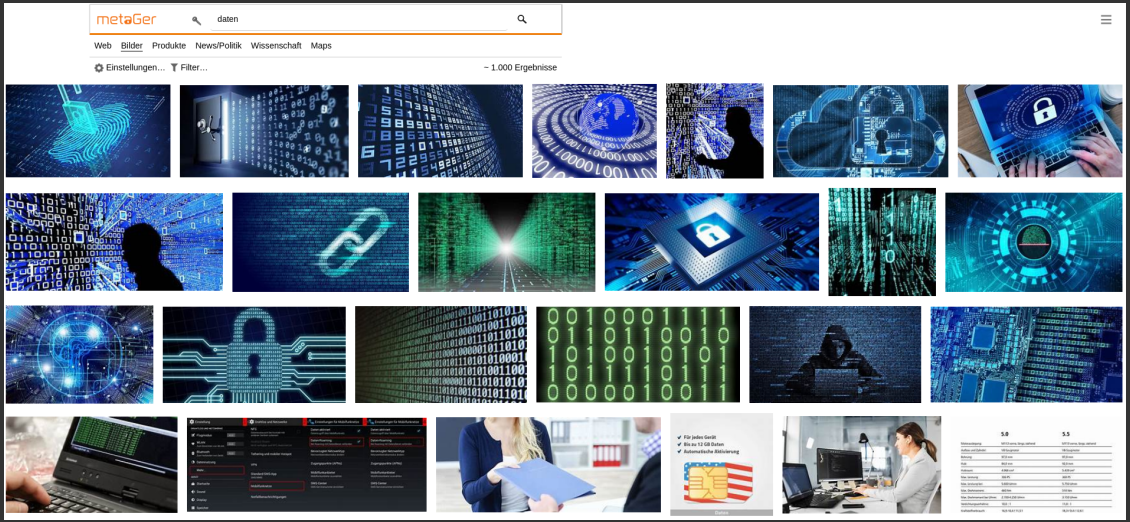
Vorstellung

>>> Vorstellung

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

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 +
  Freunde,
  Familie,
  Bekannte

>>> Wer verwendet meine Daten?

* ich + Freunde, Familie, Bekannte
* Hacker, Erpresser, etc.

Entity	Year	Records	Organization type	Method	Sources
Bangladesh Government website data breach	2023	50,000,000+	government	data leak due to security vulnerabilities	[46]
Duolingo	2023	2,676,696	educational services	hacked	[10][123]
Evide data breach	2023	1,000	computer services for charities	ransomware hacked	[141][142] [143][144][145]
Manipulated Caiman	2023	40,000,000	financial	hacked	[247][248]
NTT Docomo	2023	5,960,000	telecoms	hacked	[285]
Tesla	2023	75,000	transport	inside job	[352]
Tic Hosting Solutions	2023	unknown	hosting provider	hacked	[355]
T-Mobile	2023	37,000,000	telecom	hacked	[362]
Consumer Financial Protection Bureau	2023	256,000	bureau	poor security	[440]
Directorate General of Immigration of Indonesia	2023	34,900,867	Government	hacked and published	[441]
Directorate General of Population and Civil Registration (Dukcapil)	2023	337.225.463	Government	leaked and published	[442]
Iberdrola	2022	1,300,000	energy	poor security	[213]
International Committee of the Red Cross	2022	515,000	humanitarian	unknown	[217][218][219]
Medibank & AHM	2022	9,700,000	healthcare	hacked	[6][9][11][12]

Abbildung: kürzliche Datenlecks 2023[a]

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

>>> Wer verwendet meine Daten?

* ich + Freunde, 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 + Freunde, Familie, Bekannte
* Hacker, Erpresser, etc.
* Firmen

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?

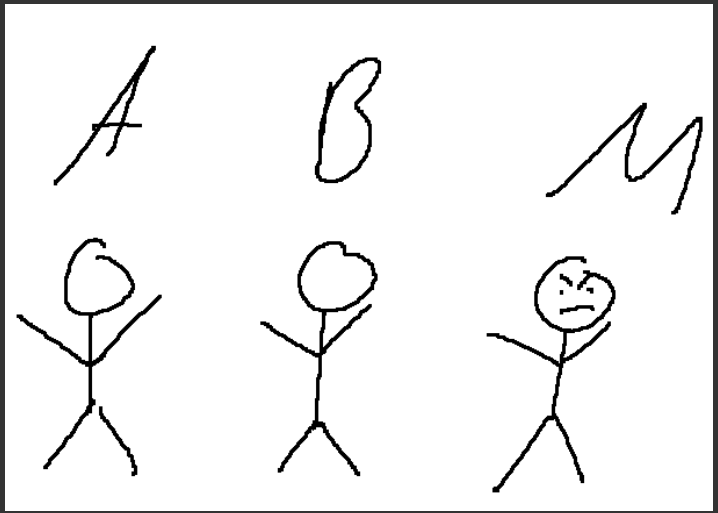
* ich + Freunde, Familie, Bekannte
* Hacker, Erpresser, etc.
* Firmen
* **Behörden**

Abbildung: Behörden fragen Daten von Telegram an[a]

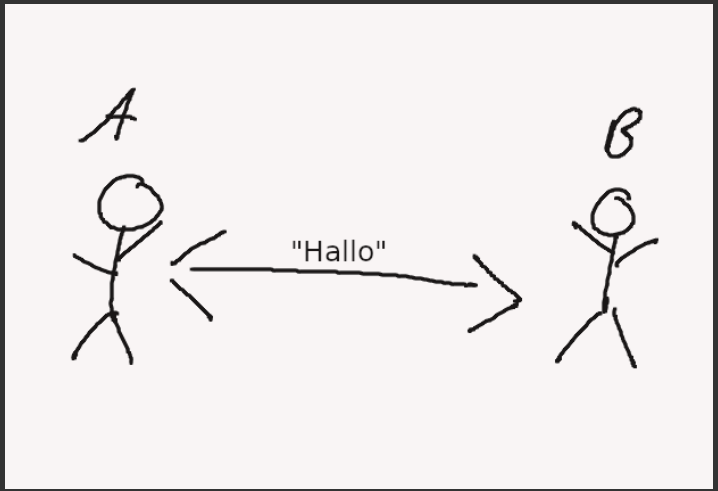
[a] https://www.handelsblatt.com/dpa/extremismus-telegram-uebermittelte-daten-an-deutsche-sicherheitsbehoerden/28666622.html

Gefahren bei der Datenübertragung

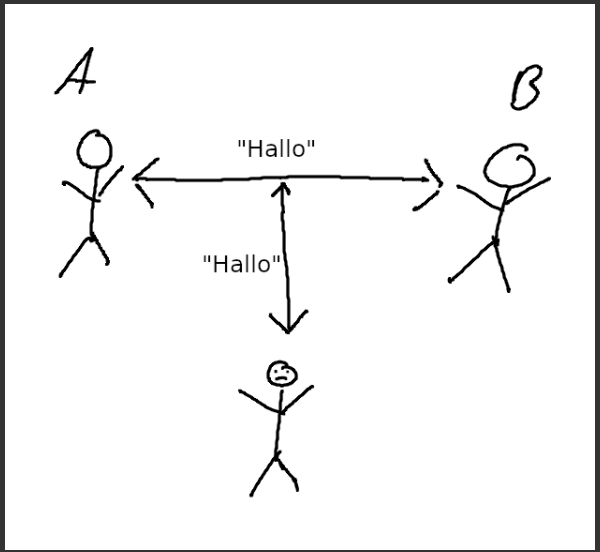
>>> Datenübertragungen



>>> Was bedeutet Datenübertragung?

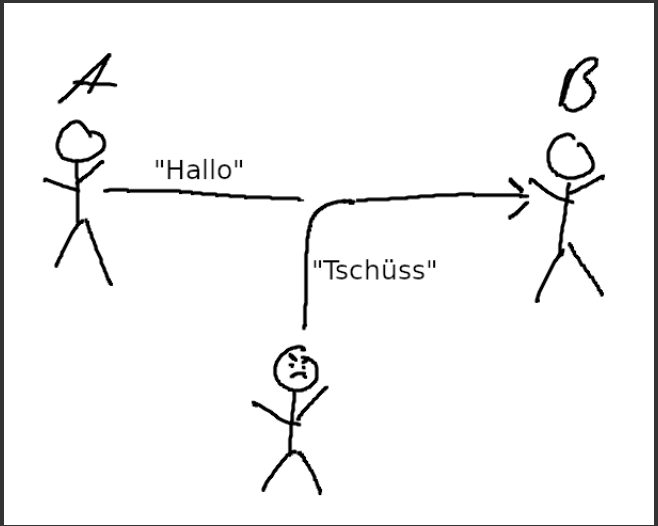


>>> Was sind Gefahren bei der Datenübertragung?



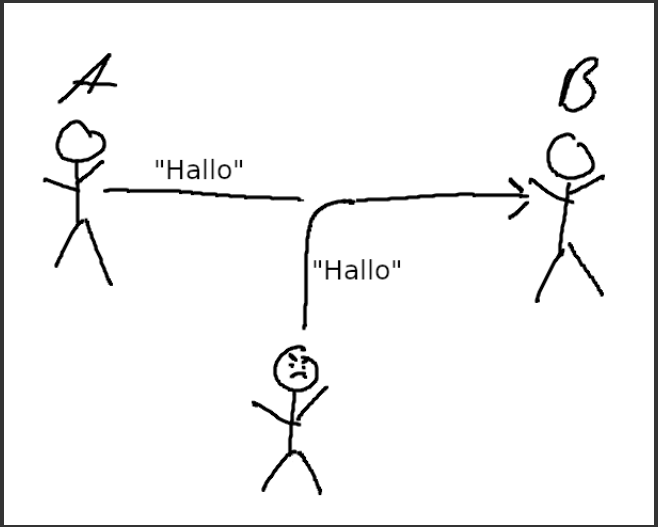
Gefahr: Lauschangriff

>>> Was sind Gefahren bei der Datenübertragung?



Gefahr: Manipulation

>>> Was sind Gefahren bei der Datenübertragung?



Gefahr: Authentizität

Was tun?

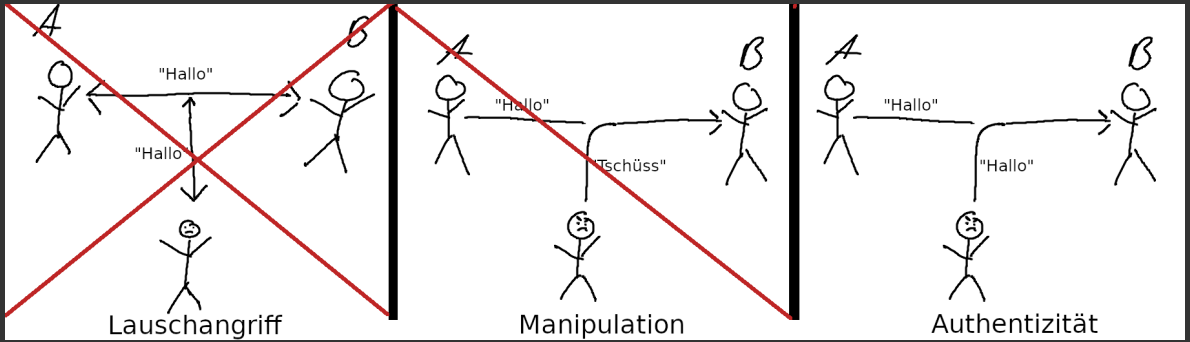


Abbildung: Probleme gelöst durch Verschlüsselung

>>> Verschlüsselung - der einfache Fall

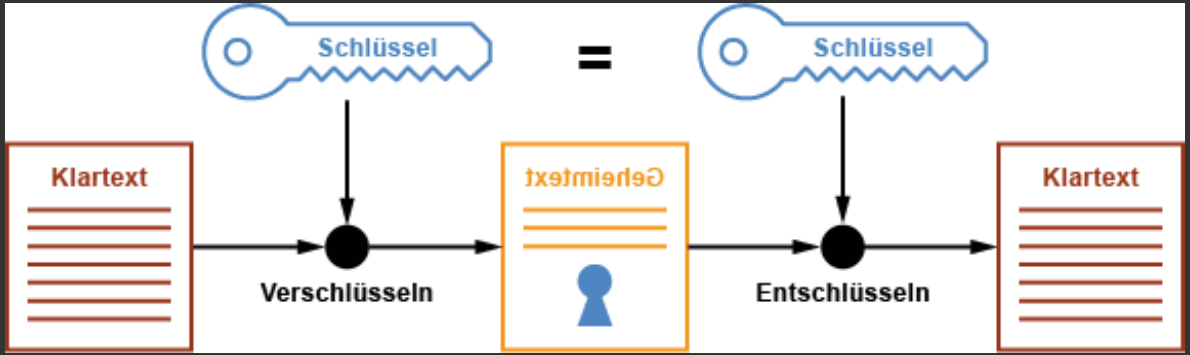
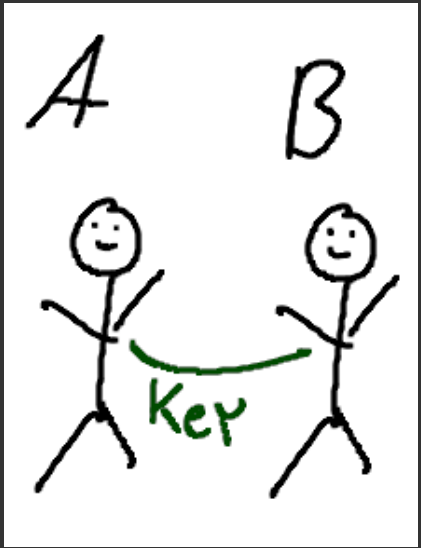
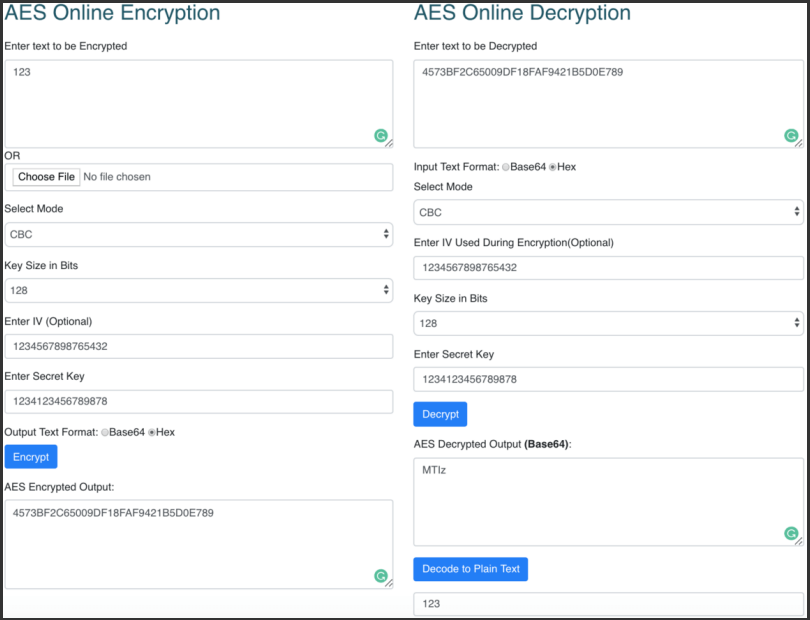


Abbildung: Symmetrische Verschlüsselung

>>> Verschlüsselung - der einfache Fall



>>> Verschlüsselung - der einfache Fall



>>> 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?

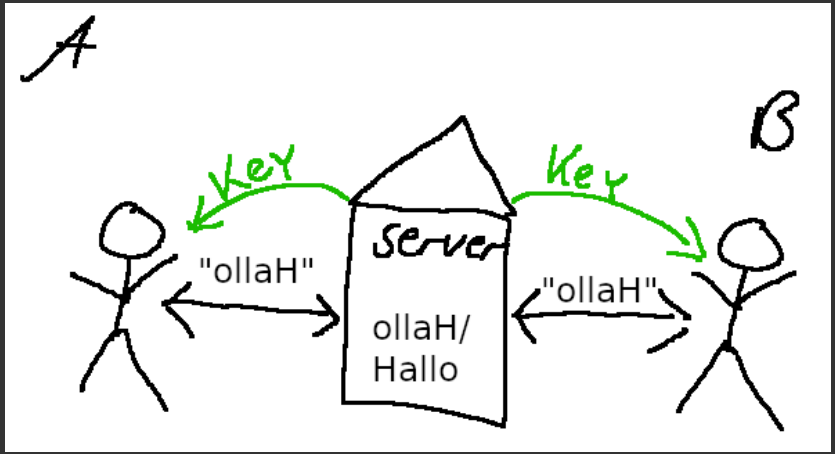
* AES 256-Bit Verschlüsselung

-> 2^{256} mögliche Kombinationen

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

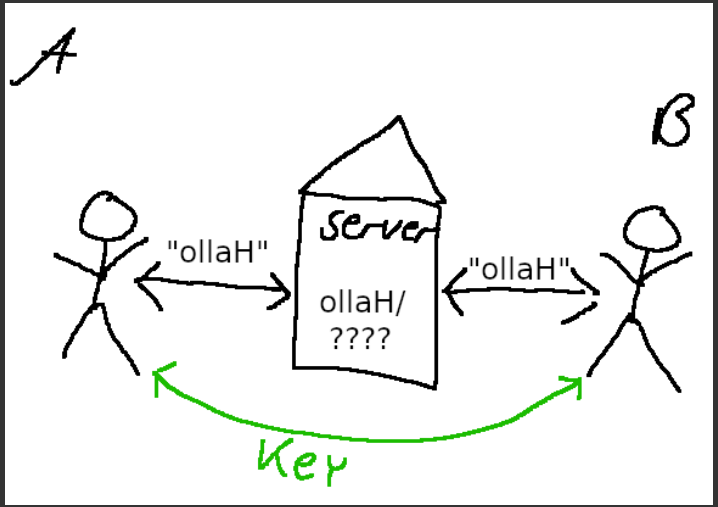
  * vgl. Alter des Universums: $13,8 \times 10^{9}$

>>> Transportweg-Verschlüsselung (TLS)



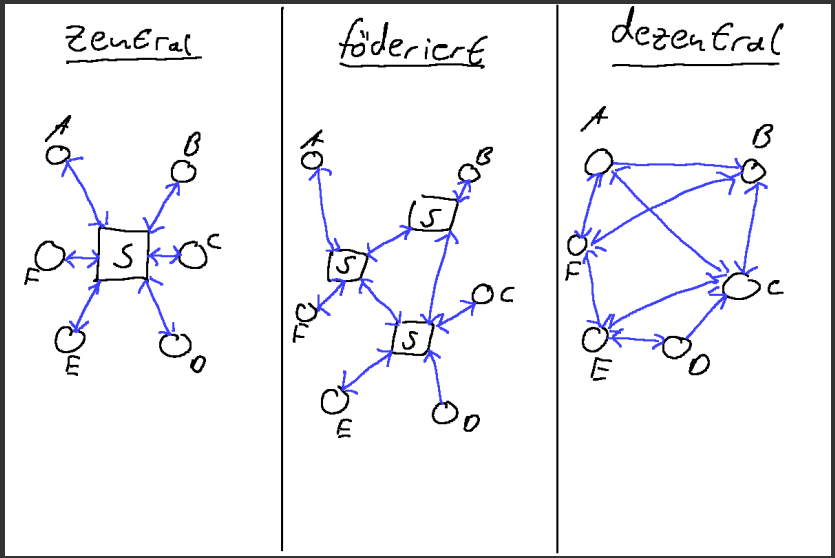
Transportwegverschlüsselung (kein E2E) = schlecht

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



E2E = gut

Messenger


zentral
A
B
C
D
E
S
föderiert
A
B
C
D
E
S
S
S
dezentral
A
B
C
D
E

>>> Was sind gute Messenger?

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

>>> Einschub: TOR-Netzwerk

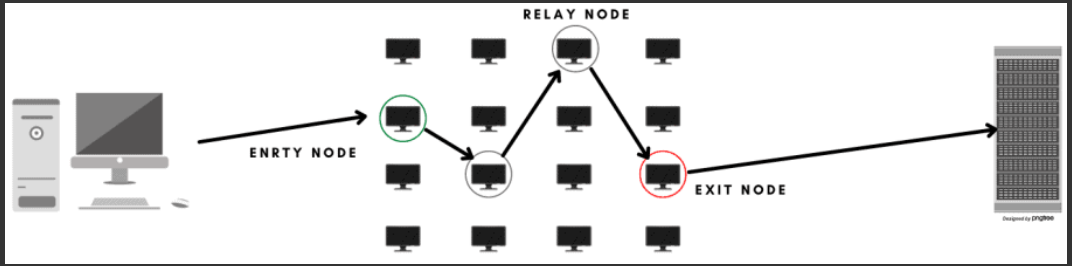


Abbildung: Aufbau TOR-Netzwerk

>>> Einschub: TOR-Netzwerk

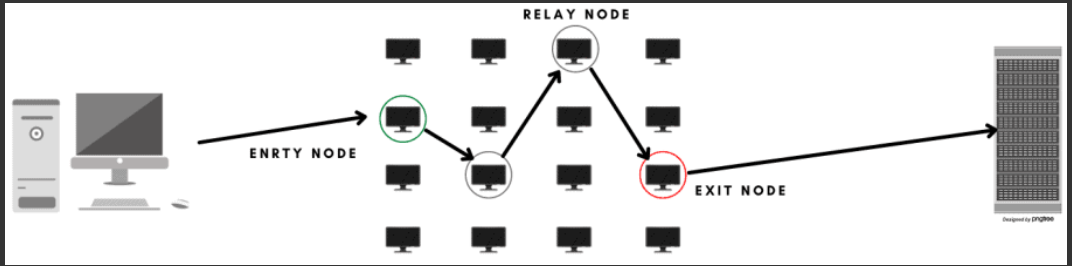


Abbildung: Aufbau TOR-Netzwerk

Nutzung für:

* Cloud Hosting
* Kommunikation
* Anonym P2P File-Sharing
* Website-Hosting
* VPN-Alternative (Geo-Blocks, etc.)

>>> Unsere Empfehlung

Signal

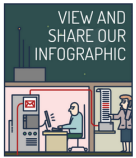
Element

Briar

>>> Und sonst? - E-Mails

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/

Betriebssysteme

File Type	Web (%)	Email (%)
exe	57	26
pdf	10	22
dll	8	-
xls	5	17
lnk	4	2
ps1	3	-
jar	2	-
doc	1	35
…	…	…
docx	-	4
xlsx	-	15

Tabelle: Top Malware Received Globally via Web and Email in 2022[5]

[5] Quelle: https://www.statista.com/statistics/1238996/top-malware-by-file-type/

>>> Betriebssysteme

* Betriebssysteme sind große Sicherheitslücken!
* Empfehlungen:
  * bitte kein Windows verwenden
  * irgendeine Linux-Distribution verwenden (z.B. Linux Mint, Ubuntu, OpenSUSE, PopOS, ...)
  * Hart-auf-Hart: Tails[6]

[6] https://tails.boum.org/

Daten verschlüsselt speichern

>>> Gefahr durch unverschlüsselte Daten

Daten werden immer noch oft unverschlüsselt gespeichert.

* User Passwort schützt nicht ohne weiteres eure Daten
    * Auf Eure Festplatte kann auch an eurem Betriebssystem „vorbei" zugegriffen werden
* Daten *vollständig* zu löschen ist nicht einfach
    * → „Datenreste" bergen Gefahr, dass gelöscht geglaubte Informationen wieder auftauchen

>>> Gefahr durch unverschlüsselte Daten

Wenn euer Handy/Computer jetzt in fremde Hände geraten würde, wäret ihr euch sicher, dass niemand auf eure Daten zugreifen könnte?

>>> 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

Jede symmetrische Verschlüsselung hängt kritisch 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?

Length	Numbers only	Lowercase letters only	Mixed case letters	Numbers and mixed case	And symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 second	5 secs
7	Instantly	Instantly	25 seconds	1 minute	6 mins
8	Instantly	5 seconds	22 minutes	1 hour	8 hours
9	Instantly	2 minutes	19 hours	3 days	3 weeks
10	Instantly	58 minutes	1 month	7 months	5 years
11	2 seconds	1 day	5 years	41 years	400 years
12	25 seconds	3 weeks	300 years	2k years	34k years
13	4 minutes	1 year	16k years	100k years	2m years
14	41 minutes	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100tn years	7qd years

Abbildung: Schätzungen von vor drei Jahren [7]

[7] (vgl. auch https://www.hivesystems.io/password-table)

>>> Was ist ein gutes Passwort?

Abbildung: Wichtig: Gebt eure Passwörter niemals weiter!

Das wars an Input! :)

unsere weiteren KEW-Veranstaltungen

>>> Patriarchale Gewalt im digitalen Raum

* Vortrag: Einführung in das Thema: Patriarchale Gewalt im Netz
* **Wann**: (Mo.) 09.10.2023, 17:00-19:00Uhr
* **Wo**: HS16
* **Event-Link**: https://ag-link.xyz/event/2023/10/09/patriarchale-gewalt-im-digitalen-raum.html

>>> Coding Art

* Workshop zu künstlerischem Programmieren (mit p5.js)
* **Wann:** (Mi.) 11.10.2023, 17:00-19:00Uhr
* **Wo:** S015
* **Event-Link:** https://ag-link.xyz/event/2023/10/11/coding-art.html

>>> 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

* Vorstellung AG-Link & was wir so machen
* Kommt vorbei und lernt uns kennen!
* **Wann:** (Mi.) 18.10.2023, 19:00-21:00Uhr
* **Wo:** P801 (Paulinum, 8. Etage, Hauptcampus)

Checkout

>>> 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[8]
* DigitalCourage[9]
* BigBrotherAward[10]
* Netzpolitik[11]
* AlgorithmWatch[12]
* Capulcu[13]

[8] https://media.ccc.de/v/ds20-11314-datenschutz_fur_aktivist_innen
[9] https://digitalcourage.de/
[10] https://bigbrotherawards.de/
[11] https://netzpolitik.org/
[12] https://algorithmwatch.org/en/
[13] 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

Fragen?