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

Max & Peter
05. Oktober 2022

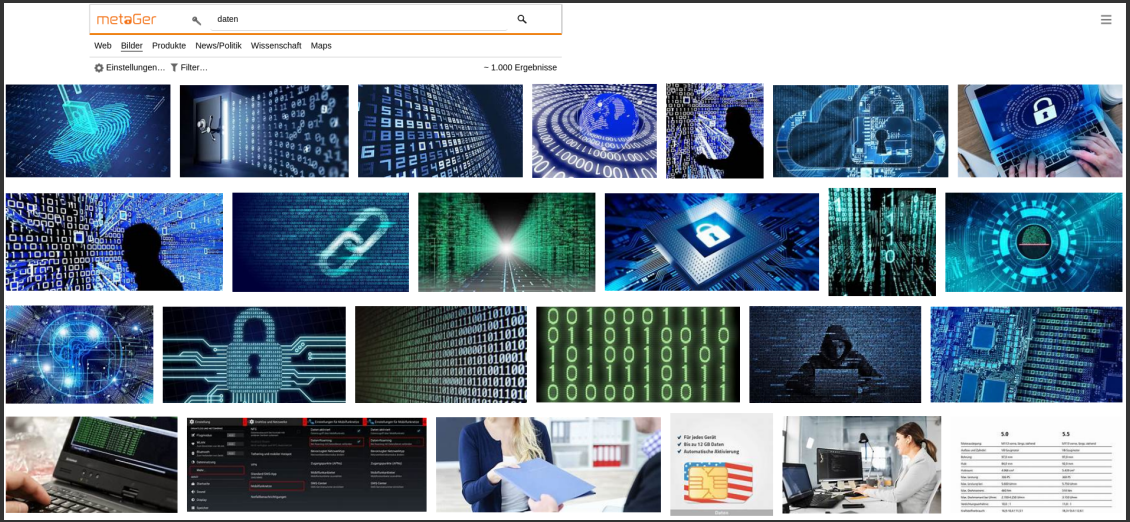
Vorstellung

>>> Vorstellung

* AG Link - AG für kritische Informatik
* seit 2018
* Website: ag-link.xyz
* Email: ag-link@riseup.net

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.
* Firmen
* Behörden

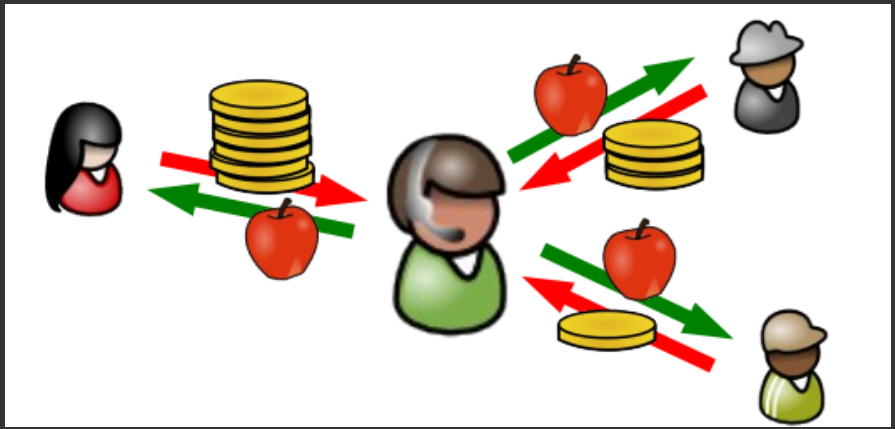


Abbildung: Profitmaximierung durch Perfect Price Discrimination

>>> Wer verwendet meine Date? - 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[1]

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

>>> Wer verwendet meine Daten? - Hacker

Entity	Year	Records	Organization type	Method	Sources
Iberdrola	2022	1,300,000	energy	poor security	[200]
International Committee of the Red Cross	2022	515,000	humanitarian	unknown	[204][205][206]
Morinaga Confectionery	2022	1,648,922	online shopping	ransomware hacked	[250]
Twitter	2022	5,400,000	tech	hacked	[308]
50 companies and government institutions	2022	6,400,000	various	poor security	[411] [412]
IKEA	2022	95,000	retail	accidentally published	[413]
Ancestry.com	2021	300,000	web	poor security	[23]
Ankle & Foot Center of Tampa Bay, Inc.	2021	156,000	healthcare	hacked	[25]
Apple, Inc./BlueToad	2021	12,367,232	tech, retail	accidentally published	[32]
Apple	2021	275,000	tech	hacked	[33]
Apple Health Medicaid	2021	91,000	healthcare	poor security	[34]
Atraf	2021	unknown	dating	hacked	[38]
CyberServe	2021	1,107,034	hosting provider	hacked	[98][99]
Dedalus	2021	500,000	health	poor security	[103]
Health Service Executive	2021	unknown	healthcare	unknown	[187]
Microsoft Exchange servers	2021	unknown	software	zero-day vulnerabilities	[241]
NEC Networks, LLC	2021	1,600,000	healthcare	hacked	[255]
T-Mobile	2021	45,000,000	telecom	hacked	[341]
Twitch	2021	unknown	tech	hacked/misconfiguration	[348]
500px	2020	14,870,304	social networking	hacked	[7]
Accendo Insurance Co.	2020	175,350	healthcare	poor security	[8][9]
Animal Jam	2020	46,000,000	gaming	hacked	[24]
Betsson Group	2020	unknown	gambling	unknown	[54]
Capcom	2020	350,000	game	hacked	[70]
CheckPeople	2020	56,000,000	background check	unknown	[80]
Clearview AI	2020	unknown (client list)	information technology	hacked	[87][88][89]

Abbildung: kürzliche Datenlecks[2]

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

>>> Wer verwendet meine Daten? - Behörden

Abbildung: Prognose von Rückfallwahrscheinlichkeiten[3]

[3] https://www.heise.de/newsticker/meldung/Studie-Algorithmen-prognostizieren-Rueckfallkriminalitaet-besser-als-Laien-4661585.html

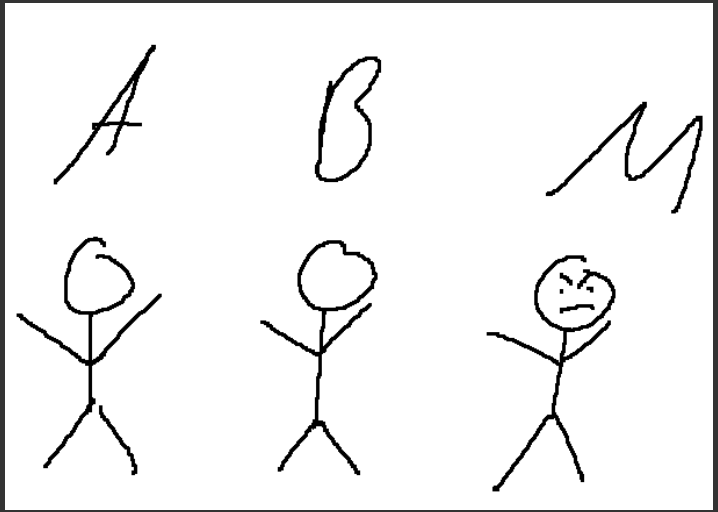
>>> Wer verwendet meine Daten? - Behörden

Abbildung: Behörden fragen Daten von Telegram an[4]

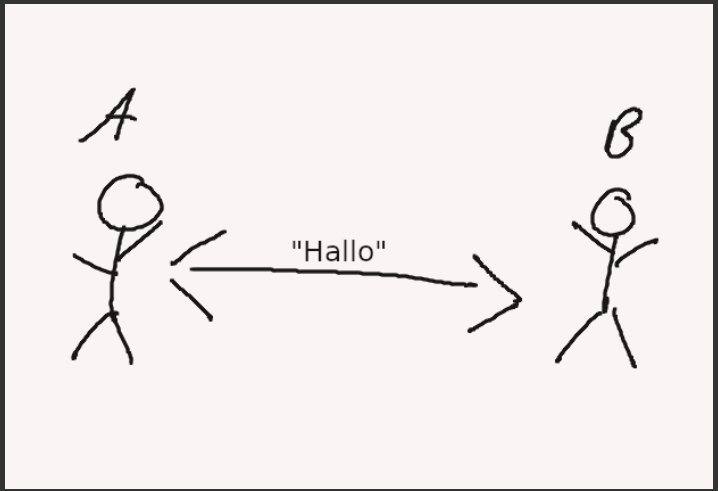
[4] https://www.handelsblatt.com/dpa/extremismus-telegram-uebermittelte-daten-an-deutsche-sicherheitsbehoerden/28666622.html

Daten übertragen

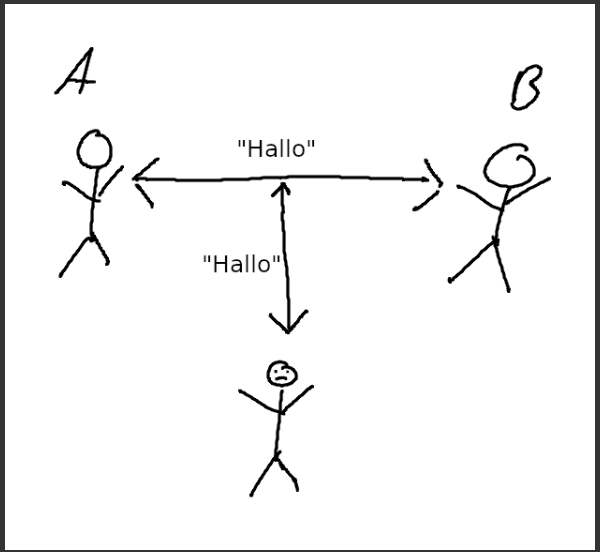
>>> Datenübertragungen



>>> Was bedeutet Datenübertragung?

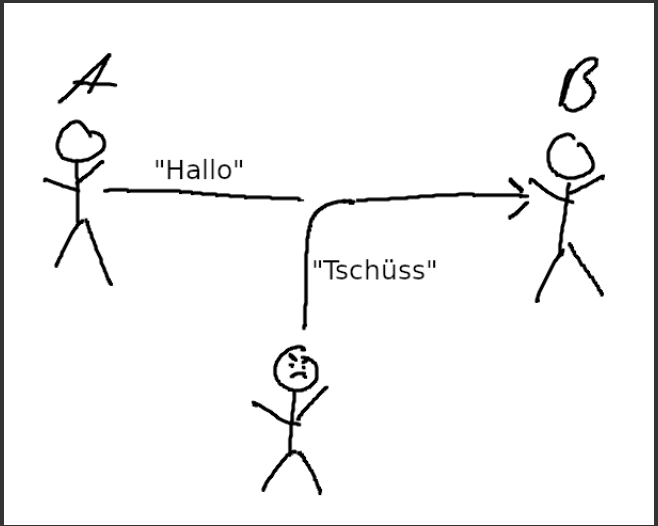


>>> Was sind Gefahren bei der Datenübertragung?



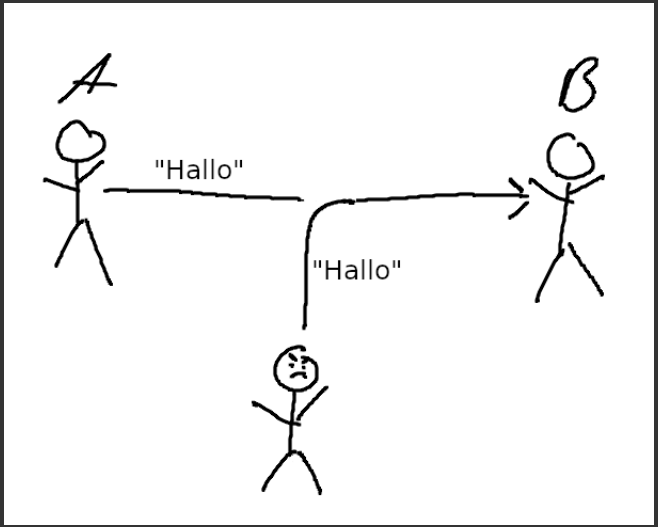
Gefahr: Lauschangriff

>>> Was sind Gefahren bei der Datenübertragung?



Gefahr: Manipulation

>>> Was sind Gefahren bei der Datenübertragung?



Gefahr: Authentizität

Was tun?

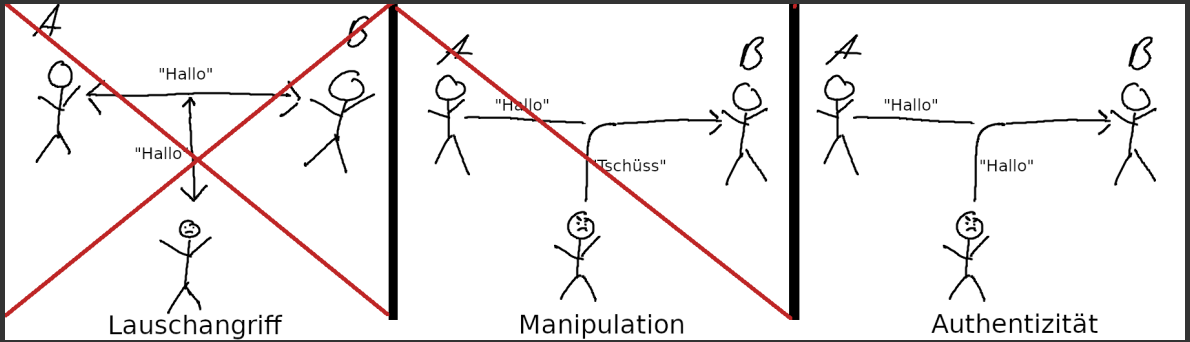


Abbildung: Probleme gelöst durch Verschlüsselung

>>> Verschlüsselung - der einfache Fall

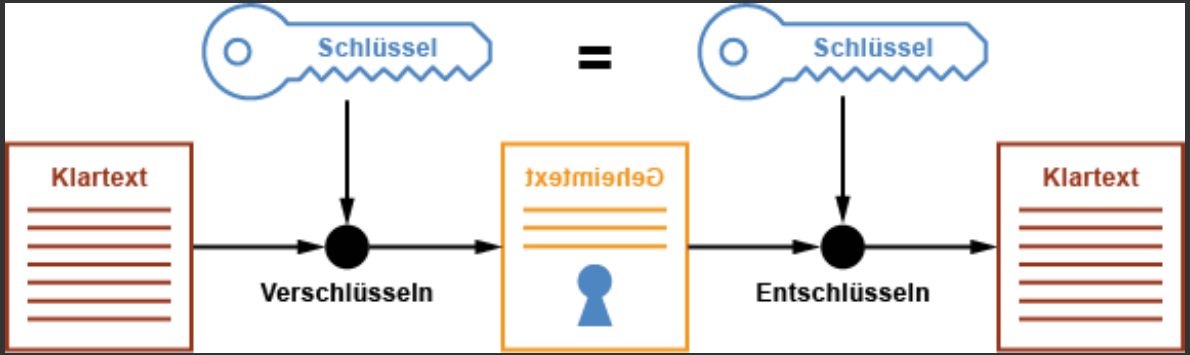
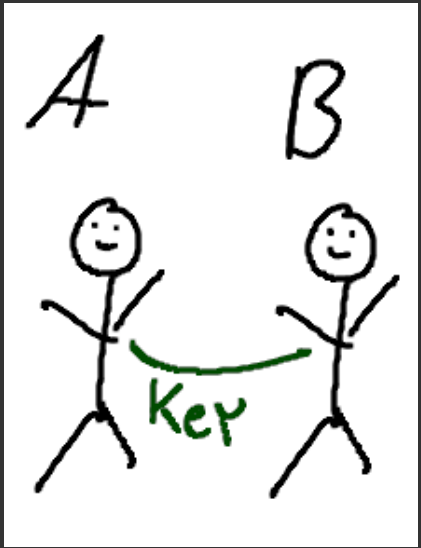
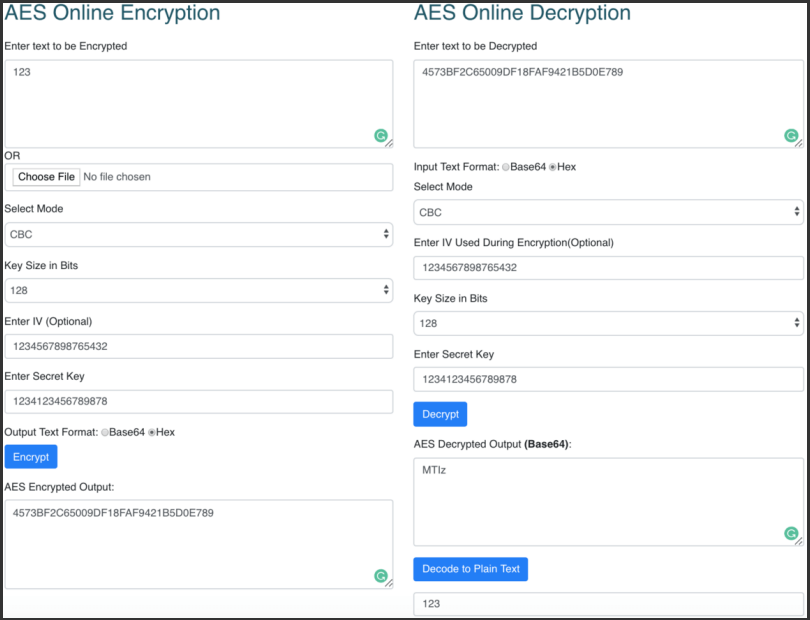


Abbildung: Symmetrische Verschlüsselung

>>> 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?

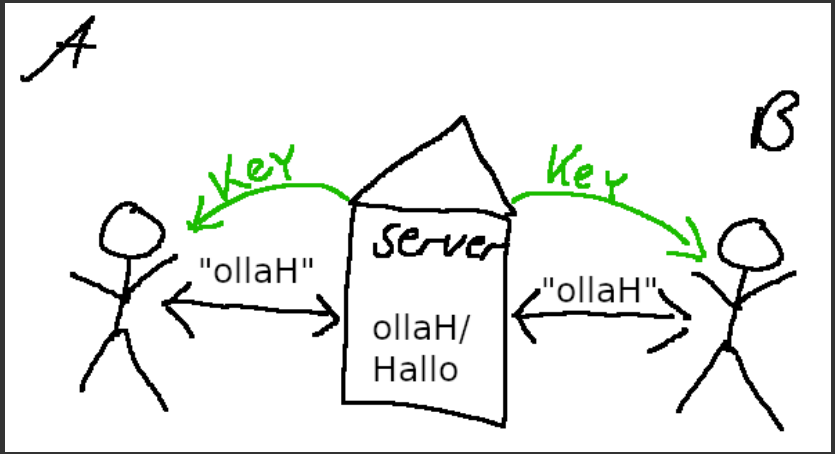
* AES 256-Bit Verschlüsselung

-> 2^{256} mögliche Kombinationen

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

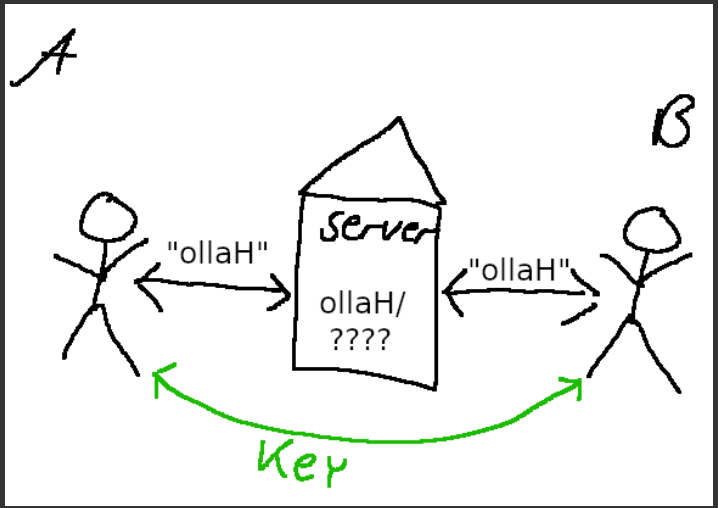
  * vgl. Alter des Universums: $13,8 \times 10^{9}$

>>> Transportweg-Verschlüsselung (TLS)



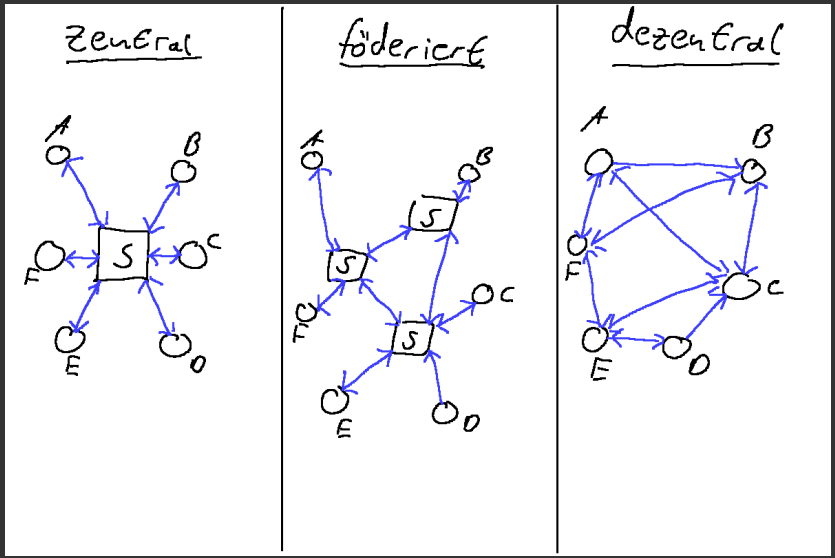
Transportwegverschlüsselung (kein E2E) = schlecht

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



E2E = gut

Daten verschicken


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

>>> Was sind gute Messenger?

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

>>> Einschub: TOR-Netzwerk

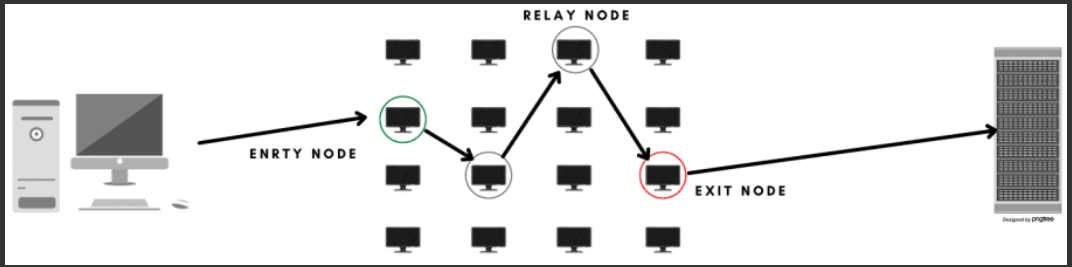


Abbildung: Aufbau und Ablauf TOR-Netzwerk

>>> Was sind gute Messenger?

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

>>> Was sind gute Messenger?

Signal

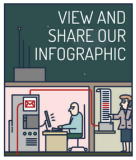
Element

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"[5] (eigen, oder extern[6])
    * Uni Cloud (max. 4GB) + Cryptomator[7]
    * Dropbox/ GoogleCloud/ etc. mit verschlüsselten Dateien
* Geheimtipp: Onion-Share[8]

---

[5] https://nextcloud.com/

[6] https://riseup.net/de/security/resources/radical-servers

[7] https://www.urz.uni-leipzig.de/servicedesk-und-hilfe/hilfe-zu-unseren-services/it-sicherheit/datenverschluesselung-mit-cryptomator

[8] https://onionshare.org/

>>> Was noch? - Betriebssysteme

* Betriebssysteme sind große Sicherheitslücken!

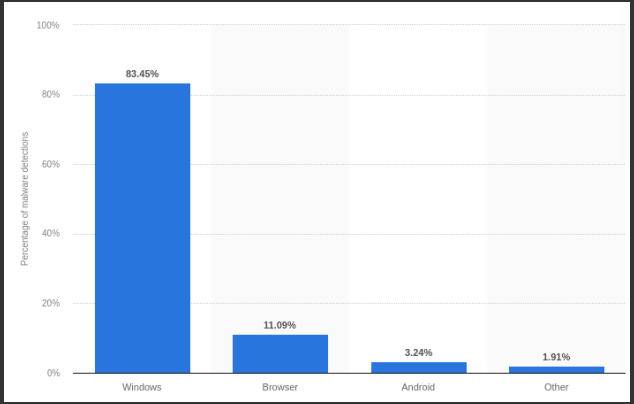


Abbildung: Fundorte von Malware (01.-04.2022)[9]

[9] https://www.statista.com/statistics/680943/malware-os-distribution/

>>> Was noch? - Betriebssysteme

* Betriebssysteme sind große Sicherheitslücken!
* Empfehlungen:
  * bitte kein Windows verwenden
  * irgendeine Linux-Distribution verwenden (z.B. Linux Mint, PopOS, ...)
  * Hart-auf-Hart: Tails[9]

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

Daten verschlüsselt speichern

>>> Gefahr durch unverschlüsselte Daten

Daten werden immer noch oft unverschlüsselt gespeichert.

* Nutzer*innen Passwort schützt nicht ohne weiteres eure Daten
* Daten *vollständig* zu löschen ist nicht einfach
    * → „Datenreste" bergen Gefahr, dass gelöscht geglaubte Informationen wieder auftauchen

>>> Vorteile von Verschlüsselung

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

>>> Vorgehen

Was folgt:

Was erstmal offen bleibt:

>>> Vorgehen

Was folgt:

* „Safe Place" auf eigenem Computer einrichten, mittels verschlüsselten Containern

Was erstmal offen bleibt:

>>> Vorgehen

Was folgt:

* „Safe Place" auf eigenem Computer einrichten, mittels verschlüsselten Containern

Was erstmal offen bleibt:

* Daten verschlüsselt mit Cloud-Speicher synchronisieren
* Prozess-, Marketing- und Nutzer*innen-Daten von Webdiensten
* Datensicherung (z. B. Backups)

>>> 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)

>>> Verschlüsselungsprogramme

Wie verschlüssele ich meine Daten?

Universell:

* VeraCrypt
    * Container, Laufwerke, Partitionen

Windows:

* BitLocker (closed Source)

macOs:

* FileVault (closed Source)

Linux:

* LUKS (Linux Unified Key Setup)

Cloud-Speicher:

* cryptomator

>>> Let's Encrypt

Warum VeraCrypt?

* Open Source (keine backdoors, prüfbar, fortführbar auch nach Entwicklungsstopp)
* weite Verbreitung und Anerkennung
* unabhängige Audits, unter anderem vom Bundesamt für Sicherheit[10]
* einfach anzuwenden

Zum Projekt:

* Vom Unternehmen IDRIX betreut[11]
* Nachfolge vom TrueCrypt Projekt

---

[10] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Veracrypt/Veracrypt.html

[11] https://www.idrix.fr/Root/

>>> Arten der Verschlüsselung in VeraCrypt

In VeraCrypt gibt es zwei Arten der Verschlüsselung:

* 1. File als Container
    * können wie normale Files behandelt werden (verschoben, gelöscht, unbenannt)
    * Metadaten fallen an
* 2. (Gesamte) Partition als Container
    * Möglichkeit der Vollverschlüsselung
    * keine unverschlüsselten Reste auf der Festplatte

Problem von Containerbasierter Verschlüsselung: Container können verschlüsselt nur als ganzes übertragen werden.

>>> Weitere Anwendungsmöglichkeiten

* Versteckte verschlüsselte Partitionen (mit plausible deniability)

Workshop - VeraCrypt

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[12]
* DigitalCourage[13]
* BigBrotherAward[14]
* Netzpolitik[15]
* AlgorithmWatch[16]
* Capulcu[17]

[12] https://media.ccc.de/v/ds20-11314-datenschutz_fur_aktivist_innen
[13] https://digitalcourage.de/
[14] https://bigbrotherawards.de/
[15] https://netzpolitik.org/
[16] https://algorithmwatch.org/en/
[17] 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