

CYBER party

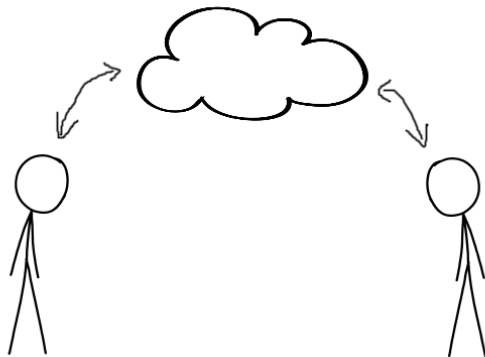
Martin Rey

Verschlüsselung - Was?

Verschlüsselung 101:

- ▶ Für alle lesbaren Text so umwandeln, dass er nicht mehr lesbar ist, wenn man keine Berechtigung dazu hat

Verschlüsselung - Warum?



- ▶ Man möchte nicht, dass alle wissen, was man macht
- ▶ Vertrauliche Daten und Personen schützen

Verschlüsselung - Warum?

Beispiel 1: Verlust

Ihr verliert euren Notebook im Zug. Durch Verschlüsselung eurer Festplatten verhindert ihr, dass unberechtigte Dritte die Informationen, die auf eurer Festplatte sind, erhalten.

Beispiel 2: Vertraulichkeit

Ihr wollt miteinander mit der Sicherheit kommunizieren, dass nur berechtigte Personen mitlesen können. Durch verschlüsselte Kommunikationswege macht ihr es schwerer, abgehört zu werden.

Verschlüsselung - Wie?

- ▶ Open Source: Alle können nachprüfen, wie die Verschlüsselung funktioniert und die Sicherheit liegt nur im Schlüssel.
- ▶ Aktuelle & geprüfte Kryptographie: Die Verschlüsselungs-Methode ist bereits länger in Crypto-Kreisen bekannt und es wurden keine Schwächen gefunden.










Verschlüsselung - Wie?

- ▶ Open Source: Alle können nachprüfen, wie die Verschlüsselung funktioniert und die Sicherheit liegt nur im Schlüssel.
- ▶ Aktuelle & geprüfte Kryptographie: Die Verschlüsselungs-Methode ist bereits länger in Crypto-Kreisen bekannt und es wurden keine Schwächen gefunden.

Sinnvoll zu haben:

- ▶ Ende-zu-Ende (E2E): Die Verschlüsselung reicht vom Sender bis zum Empfänger.
- ▶ Glaubhafte Abstreitbarkeit (plausible deniability): Man kann glaubhaft abstreiten, von der Existenz einer Nachricht zu wissen.
- ▶ perfect forward secrecy: Auch wenn in Zukunft ein Schlüssel kompromittiert wird, ist alte Kommunikation nicht entschlüsselbar.

Verschlüsselung - Womit? (Messenger)

| |  |  |  |  |  |  |  |  |  |
|---------------|---|---|---|---|---|---|---|---|---|
| Offen | - | - | - | + | + | + | + | + | + |
| Crypto | + | - | + | ~ | + | + | + | + | + |
| Infrastruktur | - | - | - | - | ~ | ~ | + | + | + |
| Desktop | ~ | + | - | + | ~ | + | + | - | + |
| "Features" | + | + | + | + | ~ | + | ~ | - | ~ |

weitere Infos auf <https://www.securemessagingapps.com/>

Verschlüsselung - Womit? (Messenger)

- ▶ Signal - <https://www.signal.org>
- ▶ Wire - <https://app.wire.com>
- ▶ Conversations (Jabber, Android) - <https://conversations.im>
- ▶ Gajim (Jabber, Desktop) - <https://gajim.org>
- ▶ Briar - <https://briarproject.org>
- ▶ Deltachat (E-Mail, Android) - <https://delta.chat>

Verschlüsselung - Womit? (E-Mail)

Wer benutzt denn noch E-Mails?

Verschlüsselung - Womit? (E-Mail)

Wer benutzt denn noch E-Mails?

Allgemeines zu E-Mails:

- ▶ benutzt Alternativen zu "kostenlosen" E-Mail-Anbietern
- ▶ gute Beispiele: `mailbox.org`, `posteo.de`, ...
- ▶ schlechte Beispiele: `gmail.com`, `hotmail.com`, ...

Verschlüsselung - Womit? (E-Mail)

Wer benutzt denn noch E-Mails?

Allgemeines zu E-Mails:

- ▶ benutzt Alternativen zu "kostenlosen" E-Mail-Anbietern
- ▶ gute Beispiele: `mailbox.org`, `posteo.de`, ...
- ▶ schlechte Beispiele: `gmail.com`, `hotmail.com`, ...

E-Mail-Verschlüsselung mit PGP kurz gesagt:



Joseph Bonneau

@josephbonneau



Email from Phil Zimmerman: "Sorry, but I cannot decrypt this message. I don't have a version of PGP that runs on any of my devices"

7:55 PM - Sep 1, 2015

♡ 253 💬 268 people are talking about this



Verschlüsselung - Womit? (E-Mail)

Autocrypt (<https://autocrypt.org/>) ist ein Standard, der Menschen PGP einfacher macht, indem es die Programme "automatisch" verschlüsseln lässt.

Welche E-Mail-Programme unterstützen das gerade?

- ▶ Deltachat (App)
- ▶ K9-Mail (App)
- ▶ Enigmail (Thunderbird Plugin)

Und wie benutze ich das nun?

- ▶ Lade das Programm herunter und richte dein E-Mail-Konto darin ein. Fertig. Jetzt werden alle E-Mails von und zu Menschen die auch Autocrypt verwenden mit PGP verschlüsselt.

Daten

Verschlüsselung - Womit? (Daten)

Problem: Je nach Gerät anders :(

- ▶ Aber: Prinzip ist gleich
- ▶ Man nutzt ein Programm, dass das Gerät verschlüsselt
- ▶ Nur welches Programm?

Verschlüsselung - Womit? (Daten)

| System | Programm |
|---------------|-------------------|
| Windows/Linux | Veracrypt* |
| Linux | LUKS |
| Android | Device Encryption |
| iOS | Device Encryption |

*<https://www.veracrypt.fr>

Sicherheit - Softwareupdates

Euer System wird euch (hoffentlich) sagen, wenn es Updates gibt. Und wenn es sie gibt, installiert sie.

FAQ:

- ▶ Muss ich wirklich alle installieren?

Sicherheit - Softwareupdates

Euer System wird euch (hoffentlich) sagen, wenn es Updates gibt. Und wenn es sie gibt, installiert sie.

FAQ:

- ▶ Muss ich wirklich alle installieren?
Ja.

Sicherheit - Softwareupdates

Euer System wird euch (hoffentlich) sagen, wenn es Updates gibt. Und wenn es sie gibt, installiert sie.

FAQ:

- ▶ Muss ich wirklich alle installieren?

Ja.

(oder prüfen, ob im changelog keine security updates sind)

Sicherheit - Softwareupdates

Euer System wird euch (hoffentlich) sagen, wenn es Updates gibt. Und wenn es sie gibt, installiert sie.

FAQ:

- ▶ Muss ich wirklich alle installieren?
Ja.
(oder prüfen, ob im changelog keine security updates sind)
- ▶ Wie häufig ist es, dass das System nach einem Softwareupdate nicht mehr funktioniert?

Sicherheit - Softwareupdates

Euer System wird euch (hoffentlich) sagen, wenn es Updates gibt. Und wenn es sie gibt, installiert sie.

FAQ:

- ▶ Muss ich wirklich alle installieren?
Ja.
(oder prüfen, ob im changelog keine security updates sind)
- ▶ Wie häufig ist es, dass das System nach einem Softwareupdate nicht mehr funktioniert?
Das ist nicht vorhersagbar, aber selten.

Sicherheit - Softwareupdates

Euer System wird euch (hoffentlich) sagen, wenn es Updates gibt. Und wenn es sie gibt, installiert sie.

FAQ:

- ▶ Muss ich wirklich alle installieren?
Ja.
(oder prüfen, ob im changelog keine security updates sind)
- ▶ Wie häufig ist es, dass das System nach einem Softwareupdate nicht mehr funktioniert?
Das ist nicht vorhersagbar, aber selten.
- ▶ Soll ich es trotzdem installieren/prüfen?

Sicherheit - Softwareupdates

Euer System wird euch (hoffentlich) sagen, wenn es Updates gibt. Und wenn es sie gibt, installiert sie.

FAQ:

- ▶ Muss ich wirklich alle installieren?
Ja.
(oder prüfen, ob im changelog keine security updates sind)
- ▶ Wie häufig ist es, dass das System nach einem Softwareupdate nicht mehr funktioniert?
Das ist nicht vorhersagbar, aber selten.
- ▶ Soll ich es trotzdem installieren/prüfen?
Ja.

Sicherheit - Softwareupdates

Euer System wird euch (hoffentlich) sagen, wenn es Updates gibt. Und wenn es sie gibt, installiert sie.

FAQ:

- ▶ Muss ich wirklich alle installieren?
Ja.
(oder prüfen, ob im changelog keine security updates sind)
- ▶ Wie häufig ist es, dass das System nach einem Softwareupdate nicht mehr funktioniert?
Das ist nicht vorhersagbar, aber selten.
- ▶ Soll ich es trotzdem installieren/prüfen?
Ja.
- ▶ Wieso?

Sicherheit - Softwareupdates

Euer System wird euch (hoffentlich) sagen, wenn es Updates gibt. Und wenn es sie gibt, installiert sie.

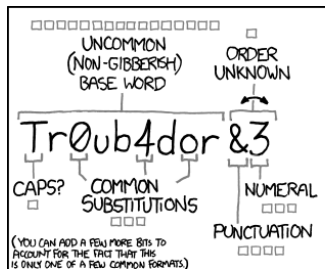
FAQ:

- ▶ Muss ich wirklich alle installieren?
Ja.
(oder prüfen, ob im changelog keine security updates sind)
- ▶ Wie häufig ist es, dass das System nach einem Softwareupdate nicht mehr funktioniert?
Das ist nicht vorhersagbar, aber selten.
- ▶ Soll ich es trotzdem installieren/prüfen?
Ja.
- ▶ Wieso?
Wenn dein System kompromittiert ist, bringt sämtliche Verschlüsselung nichts.

Sicherheit - Passwörter

- ▶ Benutzt Passwörter nie, nie mehrmals
- ▶ Generiert zufällige Passwörter (d.h. verwendet ein Programm)
- ▶ Benutzt einen Passwortmanager (KeePassXC, password-store, ...)

Sicherheit - Passwörter



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

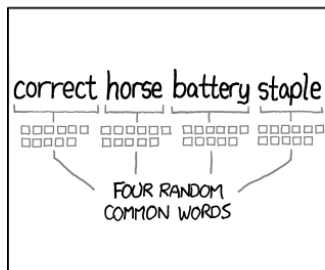
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE O's WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: **YOU'VE ALREADY MEMORIZED IT**

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Sicherheit - Datensparsamkeit

A CRYPTO NERD'S IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

NO GOOD! IT'S
4096-BIT RSA!

BLAST! OUR
EVIL PLAN
IS FOILED!



WHAT WOULD ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

GOT IT.



Anonymität

Ist an sich keine Verschlüsselung, sondern wie man sich anonym im Internet verhält.

Was ist Anonymität?

- ▶ Man ist anonym, wenn es nicht identifiziert werden kann

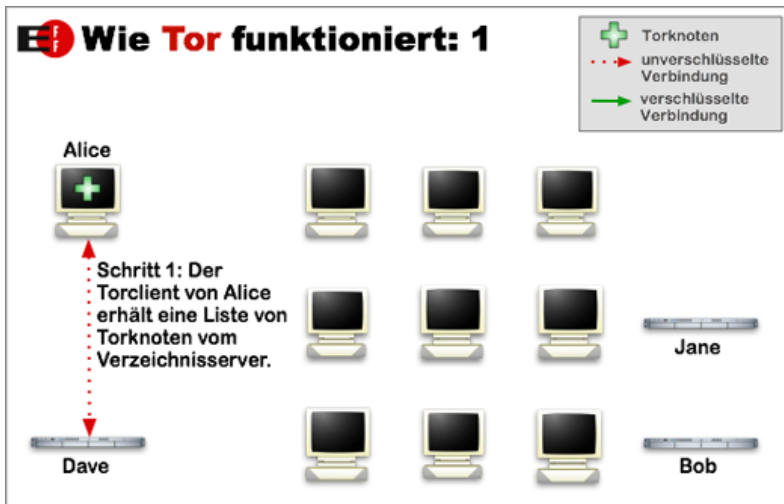
Warum ist das wichtig?

- ▶ Es ist sehr einfach verfolgt zu werden, während man im Internet ist.

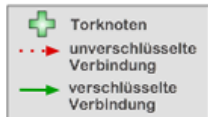
Was ist Tor?

- ▶ Kurz für "The Onion Router"
- ▶ Tor-Browser hilft, anonym zu sein
- ▶ (außerdem gibt es Websites, die man nur mit diesem Browser erreichen kann)
- ▶ Kann man herunterladen auf <https://www.torproject.org/> und einfach starten

Wie funktioniert es?



Wie Tor funktioniert: 2



Alice



Schritt 2: Nachdem der Torclient von Alice die Liste erhalten hat, weiß er, welche Rechner benutzt werden können.



Dave

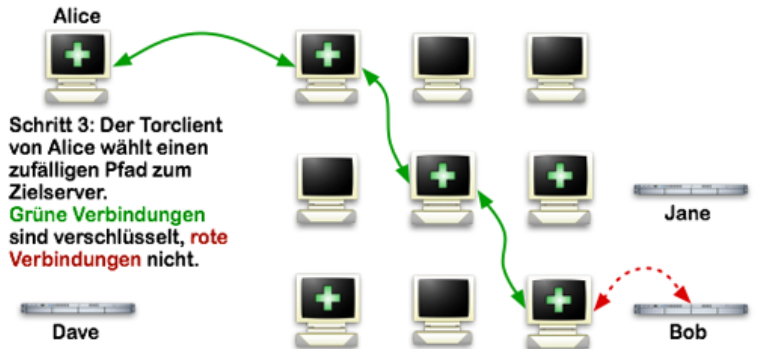


Jane

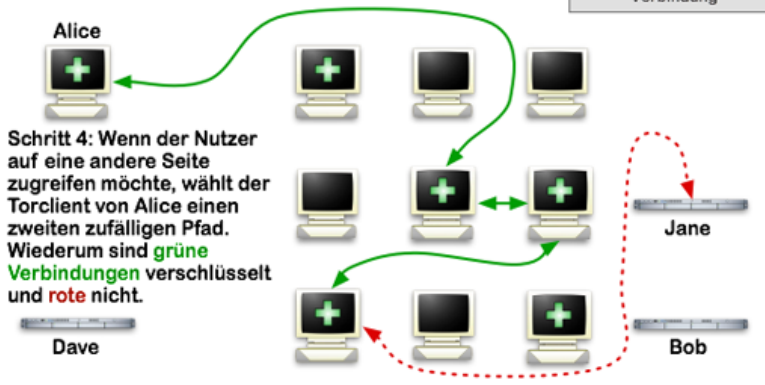


Bob

Wie Tor funktioniert: 3



Wie Tor funktioniert: 4



Was ist das?

- ▶ TAILS ist ein Betriebssystem, das zum Ziel hat, anonymes Verhalten im Internet sicher und einfach zu machen.
- ▶ Tor und andere Werkzeuge vorinstalliert
- ▶ Speichert keinerlei Daten!

Namensnennung

- ▶ xkcd Webcomic - <https://www.xkcd.com>
- ▶ "CYBER" Bild: CC-BY-NC fnordeingang e.V.
<https://fnordeingang.de>