

CYBER party

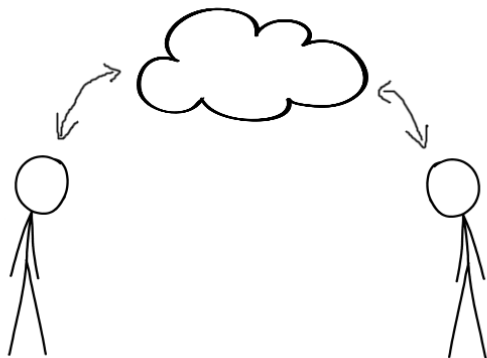
Verschlüsselung gegen Überwachung & Hausdurchsuchungen

Verschlüsselung - Was?

Verschlüsselung 101:

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

Verschlüsselung - Warum?



- ▶ Allgemein: mensch möchte nicht, dass alle wissen was es tut
- ▶ Hier konkret: Repression umgehen, andere Menschen schützen

Verschlüsselung - Warum?

Beispiel 1: Hausdurchsuchung

Bei euch gibt es eine Hausdurchsuchung. Durch Verschlüsselung eurer Festplatten verhindert ihr, dass ihr Repression durch die Informationen, die auf eurer Festplatte sind, erhaltet.

Beispiel 2: Abhören

Ihr plant eine Aktion. Durch Kommunikation durch verschlüsselte Wege macht ihr es schwerer abgehört zu werden und eure Aktion bleibt so nur unter euch.

Schützt eure Mitmenschen durch Verschlüsselung!

(Hier nicht behandelt: Schutz vor Geheimdiensten. Das ist wahrscheinlich nicht euer Problem. Wenn ihr wissen wollt, wie es sich anfühlt, Ziel von Geheimdiensten zu sein, schaut diesen Talk: https://media.ccc.de/v/rc3-11512-cia_vs_wikileaks

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 (Deniability): Mensch kann glaubhaft abstreiten eine Nachricht gesendet zu haben.
- ▶ Perfect forward secrecy: Auch wenn in Zukunft ein Schlüssel kompromittiert wird ist alte Kommunikation nicht entschlüsselbar.

Verschlüsselung - Womit? (Messenger)

	WhatsApp	Threema	Telegram	Signal	Wire	Conversations	Element/Riot	Briar	Deltachat
Open Source	-	+	+	+	+	+	+	+	+
Verschlüsselung	~	+	-	+	+	+	+	+	+
Metadaten	-	-	-	-	-	~	~	+	~
Pseudonym	-	-	-	-	+	+	+	+	+
Desktop-Client	~	-	+	~	+	+	+	-	+
"Benutzbarkeit"	+	+	+	~	+	~	-	-	~

Weitere Infos: <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: `riseup.net`, `systemli.org`, ...
- ▶ 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: `riseup.net`, `systemli.org`, ...
- ▶ schlechte Beispiele: `gmail.com`, `hotmail.com`, ...

E-Mail-Verschlüsselung mit PGP kurzgesagt:






A screenshot of a tweet from Joseph Bonneau (@josephbonneau) dated September 1, 2015. The tweet contains a quote from Phil Zimmermann regarding PGP decryption. The tweet has 253 likes and 268 replies.

 **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 (Android-App)
- ▶ K9-Mail (Android-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.

Verschlüsselung - Womit? (Daten)

Problem: Je nach Gerät anders :(

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

Verschlüsselung - Womit? (Daten)

System	Programm
Windows/Linux	Veracrypt*
Linux	LUKS
Android	Device Encryption
iOS	Device Encryption
Alle gängigen OSes	Cryptomator**

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

**<https://cryptomator.org/>

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.
- ▶ Wie häufig ist es, dass das System nicht mehr funktioniert nach einem Softwareupdate?

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.
- ▶ Wie häufig ist es, dass das System nicht mehr funktioniert nach einem Softwareupdate?
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.
- ▶ Wie häufig ist es, dass das System nicht mehr funktioniert nach einem Softwareupdate?
Das ist nicht vorhersagbar, aber selten.
- ▶ Soll ich es trotzdem 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.
- ▶ Wie häufig ist es, dass das System nicht mehr funktioniert nach einem Softwareupdate?
Das ist nicht vorhersagbar, aber selten.
- ▶ Soll ich es trotzdem 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.
- ▶ Wie häufig ist es, dass das System nicht mehr funktioniert nach einem Softwareupdate?
Das ist nicht vorhersagbar, aber selten.
- ▶ Soll ich es trotzdem installieren?
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.
- ▶ Wie häufig ist es, dass das System nicht mehr funktioniert nach einem Softwareupdate?
Das ist nicht vorhersagbar, aber selten.
- ▶ Soll ich es trotzdem installieren?
Ja.
- ▶ Wieso?
Wenn dein System kompromittiert ist bringt dir sämtliche Verschlüsselung nichts?

Sicherheit - Passwörter

- ▶ Benutzt nie, nie, nie 2x dasselbe Passwort
- ▶ Benutzt einen Passwortmanager (KeePass, ...)
- ▶ Wählt Passwörter zufällig (d.h. verwendet ein Programm)

Sicherheit - Passwörter

UNCOMMON (NON-GIBBERISH) BASE WORD

ORDER UNKNOWN

Trøub4dor & 3

CAPS? COMMON SUBSTITUTIONS NUMERAL PUNCTUATION

(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)

~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**

correct horse battery staple

FOUR RANDOM COMMON WORDS

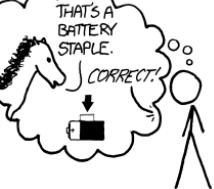
~44 BITS OF ENTROPY

$2^{44} = 530 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

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.



Workshop!

Jetzt seid ihr dran!

Fragen?

Braucht ihr Hilfe bei der Installation oder beim Benutzen?

Wir sind für euch da :)

Danke fürs zuhören!