Cybersecurity 101

2020-04-21

Introduction

- Hi, I’m moe 👋
- I tried to occupy the construction site of a coal plant once
- I don’t consider myself to be a “cybersecurity expert”

Agenda

- Why is this important?
- How to assess risks
- Computer stuff
  - The Basics
  - Transport Layer vs. End to End Encryption
  - Passwords
  - Disk Encryption
  - Communication
- Choosing your providers

Why is this important for me?

“I am not doing anything illegal / I have nothing to hide.”

- Would that hold true if you doing exactly the same in mexico/philippines/hungary/bavaria?
- Do you have international allies from places that are less secure for activists?
- Do you plan acts civil disobedience where it’s crucial that some aspects of your plan are kept secret?
- Is there a right-wing movement in your country that attacks climate activists?
- How interested has the police/secret services in your country been in the “anarchist eco scene” recently?

Why is this important for me?

“It’s useless to care for security, they can access anything anyway.”

- That does definitely not hold true for every adversary.
- It’s hard to gather insight of the different state actors, their interests, capabilities, legal boundaries (and if they are followed) and budgets.
- Some security measures do not hurt anyone, not doing them would be irresponsible.
- With other measure we can assess how much they “cost” us.
- Caring and protecting us, our friends and partners is a must. Fatalism does not help.

Risk Assessment

Risk Assessment (Also known as **threat modelling**)

Ask yourself the following questions:

- What do I want to protect?
- Who do I want to protect it from? (What are their capabilities?)
- How bad are the consequences if I fail?
- How likely is it that I will need to protect it?
- How much trouble am I willing to go through to try to prevent potential consequences?

https://ssd.eff.org/en/module/your-security-plan

Risk Assessment Example 1

Alice has a well known twitter account where she posts about climate justice.

- What do I want to protect?
  Her real name, address and workplace
- Who do I want to protect it from?
  Right-wing online trolls are threatening her.
- How bad are the consequences if I fail?
  She knows about cases of doxing, shit storms, telephone calls or even swatting.
- How likely is it that I will need to protect it?
  She suspects that there are specific chat groups to target activists like her. Some of the trolls may have light knowledge about hacking, others are good at researching online accounts.

Risk Assessment Example 1

Alice has a well known twitter account where she posts about climate justice.

How much trouble am I willing to go through to try to prevent potential consequences?

- Separate twitter account/mail from all other social networks/services.
- Review privacy settings
- Do not add friends and colleagues to her activist account.
- Use a strong and unique password as well as two-factor-authentication.
- Be careful about posting images and context information.
- ~~Delete her linkedin profile.~~
- ~~Only connect to twitter via Tor.~~

https://ssd.eff.org/en/playlist/want-security-starter-pack#protecting-yourself-social-networks

Risk Assessment Example 2

A local affinity group wants to do a banner drop from a cargo ship that transports SUVs.

- What do I want to protect?
- Who do I want to protect it from?
- How bad are the consequences if I fail?
- How likely is it that I will need to protect it?
- How much trouble am I willing to go through to try to prevent potential consequences?

Apart from the action, what would the group want to protect “all the time”?

Basics

Basics

Using cool secret communication tools only helps if your computer is not running malware:

- Keep your software updated, especially Operating System and Browser
- Use Browser extensions/features to protect yourself:
  - HTTPS Everywhere
  - uBlock Origin
  - Incognito mode
- Be very careful with email attachments
- (Use two-factor authentication)

see https://securityinabox.org/en/guide/malware

Two-factor authentication

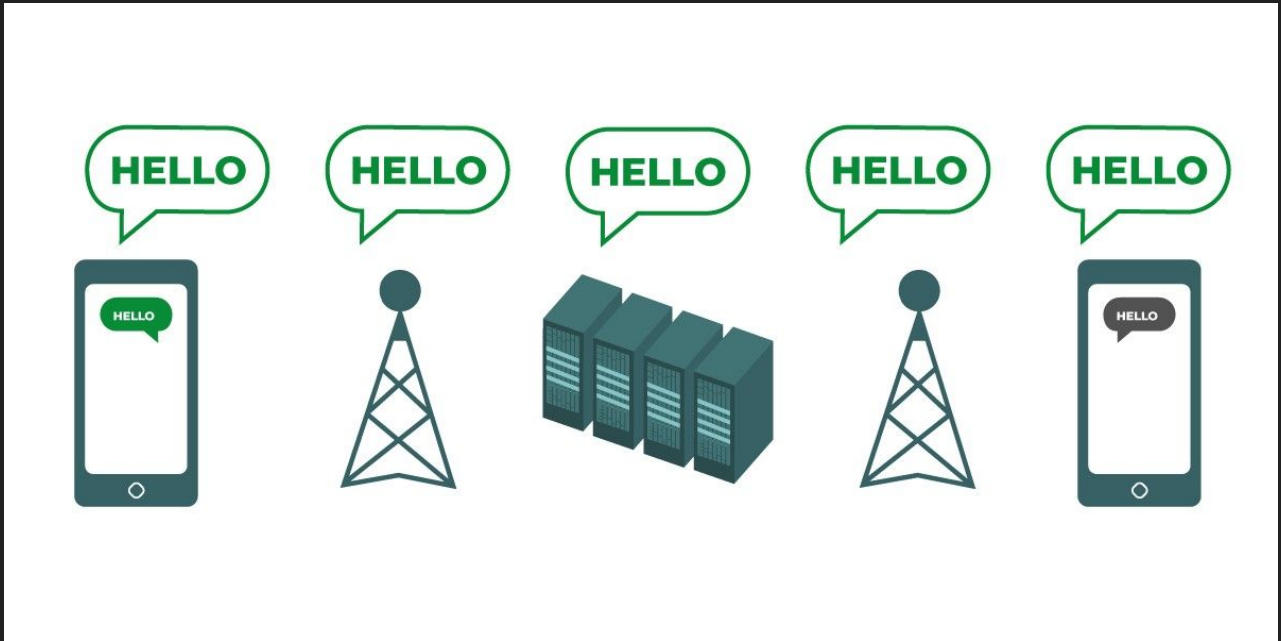
Adds a ‘second factor’ needed to log in

- First factor: password
- Second factor: e.g. ownership of a mobile device (most banking services)
- Adds security when the password gets compromised
  Example: BKA Telegram ‘hack’

see https://ssd.eff.org/en/module/how-enable-two-factor-authentication

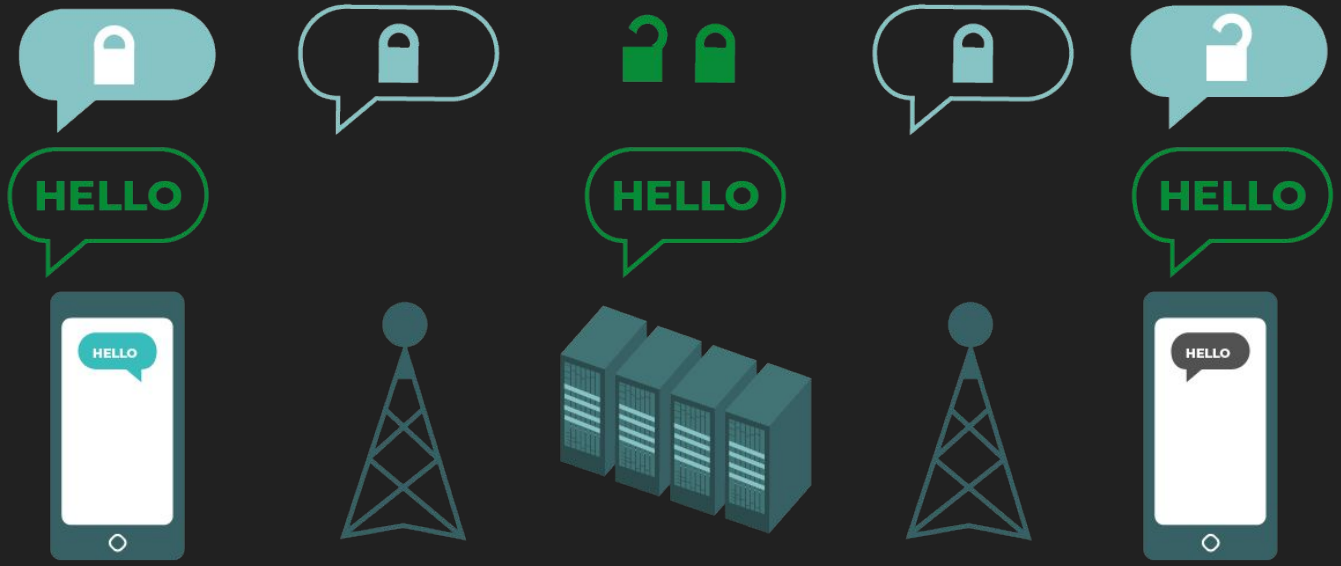
Transport Layer vs. End to End Encryption

Transport Layer vs End to End Encryption



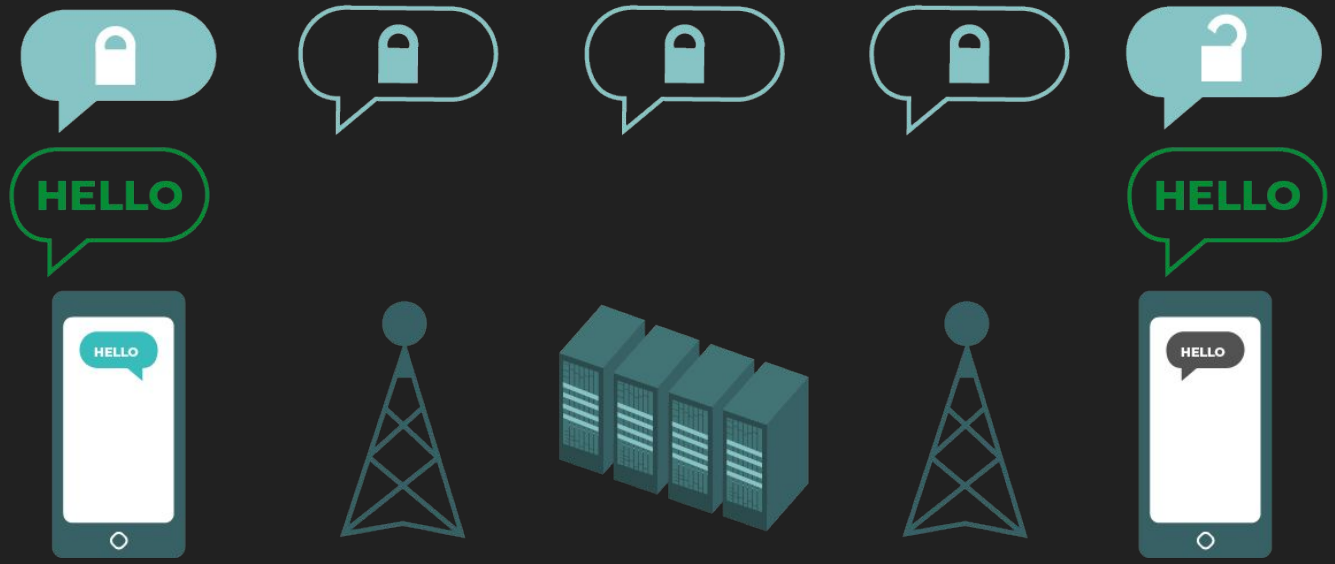
No encryption (http connections)

Transport Layer vs End to End Encryption



Transport Layer encryption (e.g. https websites, etherpads)

Transport Layer vs End to End Encryption



End to End encryption (signal, pgp)

Image source and details: https://ssd.eff.org/en/module/what-should-i-know-about-encryption

Passwords

Passwords

Some of the most common passwords:

```
123456{7,8,9}
password
qwerty
letmein
```

You can to better! Two strategies for good passwords:

- Combination of (12+) characters, symbols, numbers (e.g. following a sentence a poem, …)
- Use a **random** sequence of words

https://ssd.eff.org/en/module/creating-strong-passwords

Passwords

- Do not reuse passwords:
  - Login data regularly gets ‘lost’. Check at https://haveibeenpwned.com/
- Use a password manager (e.g. KeePassX) to create unique and strong passwords for each account that you don’t have to remember
- You still need to remember a small amount of passwords (disk encryption, password manager)

Secure your devices

Secure your devices

- Use encryption to secure resting data on all your devices (Smartphones, Computers, …)
- Full disk encryption is preferred (harder to make mistakes) and available for most OS. (On windows only available through professional edition)
- Tools like Veracrypt allow to encrypt certain files on you computer
- Useful in combination with a screen lock
- In doubt turn your device off

Secure your communication

Secure your communication

Use End-to-End Encryption whenever possible!

Email / PGP

- correctly used it is very secure 👍
- possible to encrypt lists: https://schleuder.org/ 👍
- it’s hard to use it correctly 👎
- if your key gets compromised all your message history can be exposed (no “forward secrecy”) 👎

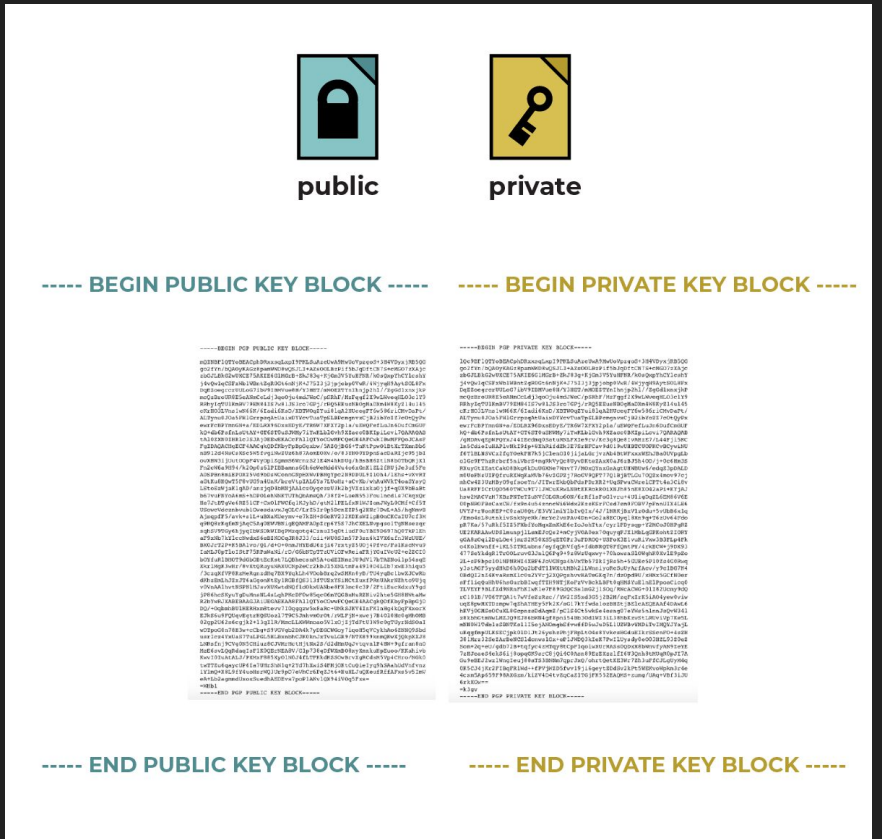
Signal

- recommended by almost everyone 👍
- not suitable for large lists 👎
- currently uses telephone number for identification 👍 / 👎
- forward secrecy 👍

PGP / Asymmetric encryption

“Key”-Concepts

- 🔒 Public key: encrypts a message
  (Use the public key of the recipient)
- 🔑 Private key: decrypts
  (Use your own private key and never give it away)
- Passphrase: additional security for private key



How to choose your provider?

How to choose your provider?

- Large tech companies usually have good security teams. But you have to trust them.
- Open-Source software is preferable.
- Software / servers must be maintained. Setting up own solutions without the right knowledge and capacities can be dangerous.
- If it’s free, you usually pay with your data.
- The internet used to be such a cool place. Now it’s a giant advertisement scheme dominated by a handful of corporations.

Independent tech collectives shape our vision of a decentralized internet and society. (Don’t forget to donate)

Increasing your digital safety is a process.

The choice of tools
and methods is always
a political discussion.

Stuff I have not talked about

- Metadata: https://ssd.eff.org/en/module/why-metadata-matters
- Smartphones and brick phones in general
- Anti virus / malware software
- Being anonymous on the web with VPNs and TOR
- Being tracked on the web by cookies, browser fingerprinting and social networks (https://vimeo.com/249633335)
- Cloud storage
- Etherpads
- Video conferencing and calls (mumble, jitsi)
- Secure deletion of data
- Other chat programs and protocols: Jabber (XMPP), OTR, Riot

Resources

Tutorials

- https://ssd.eff.org 👉 very hands-on, lots of topics
- https://securityinabox.org 👉 similar, may not always be up to date
- https://www.datadetoxkit.org/ 👉 every day tips
- https://holistic-security.tacticaltech.org/ 👉 security in a much broader sense
  “*being physically and emotionally healthy and sustaining ourselves while continuing to do the work that we believe in.*”

Service Providers

- list of tech collectives: https://riseup.net/en/security/resources/radical-servers
- email: https://posteo.de/en