InfoSec Workshop @ Hearts' Fear

by resist.berlin

Nov 8 2018, 7-10 PM

Before we start...

- InfoSec-Workshop: every 2nd and 4th Thursday of the month, 7-10 PM @ Wildenbruchstr. 24
- Today: no specific topic. Future dates will have topics announced in advance.
- Language: English (unless everyone speaks German)
- 60 min presentation
- 15 min discussion, short break
- 90 min individual questions, hands-on workshop
- Bring your own hardware :)

Before we start...

- berlin.freifunk.net (free WiFi) should be available
- Please buy drinks/food and donate to support Hearts‘ Fear
- Take some flyers with you and spread the word to support resist.berlin
- Check soze44.noblogs.org for more information about the new Social Center Neukölln
- Next date: Nov 22, 7–10 PM

Outline for today

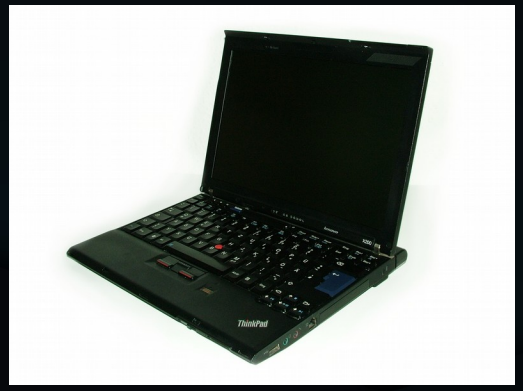
- Introduction
- What is InfoSec? The basics
- What can you do immediately?
- Topics for the next dates
- Discussion / Questions

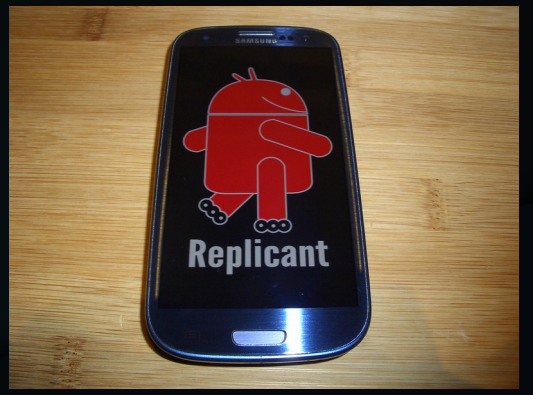
Introduction

- resist.berlin: project founded in April 2018
- Located in Kreuzberg, near Hermannplatz
- Activist-friendly hardware & consulting: „libre tools for cyberpunk activism“
- Ideals: Free Software, InfoSec, usability, sustainability
- Web: https://resist.berlin
- E-Mail: resist.berlin@posteo.de
- GPG Fingerprint: 5A77 422F 3B22 28E3 3D39 E152 D7FE A87B 9354 9E52

Introduction

- Libreboot-Laptops
- Replicant-Phones
- Freifunk
- Accessories
- Autonomous infrastructure
- Creative Commons
- Upgrades/Repairs
- **Workshops**





freifunk.net

Tails
theamnesicincognitolivesystem

tm

The libre embedded GNU/Linux distro

What is InfoSec?

„Information security […] is the practice of preventing **unauthorized** access, use, disclosure, disruption, modification, inspection, recording or destruction of information.“

(https://en.wikipedia.org/wiki/Information_security)

What is InfoSec?

- InfoSec is a concept known from the corporate world or from spy agencies (NSA, BND)
- We can take the same concepts & strategies to fight back: against surveillance capitalism and state repression
- The important word is „unauthorized“. We can be the ones who decide.
- We can be in control of our computing and our communications
- InfoSec includes CryptoParty stuff, but goes beyond that (it also covers e.g. video surveillance)

Basics

- Free Software
- Data Reduction
- Decentralisation
- Anonymity
- Encryption, Authentication
- Location Tracking

Basics – Free Software

- Free as in „Freedom“, not as in „Free Beer“
- 4 essential freedoms:
  - 0: The freedom to run the program as you wish, for any purpose
  - 1: The freedom to study how the program works, and change it so it does your computing as you wish
  - 2: The freedom to redistribute copies so you can help others
  - 3: The freedom to distribute copies of your modified versions to others
- More info: https://www.gnu.org/philosophy/free-sw.en.html

Basics – Free Software

- Free Software attempts to be ethical, not convenient
- Free Software is **always** „open source“, but not vice versa
- Free Software allows you to have control over your computing, because you know exactly what instructions your computer is executing
- Free Software is the only known defense against malware and backdoors, which are often included in proprietary (non-free) software
- Using Free Software is a precondition for good InfoSec practices!

Basics – Free Software

- Many people use free software every day:
  - Mozilla Firefox, Thunderbird
  - LibreOffice
  - VLC Player
  - GIMP
  - Conversations, Wire, Signal
  - GNU/Linux based operating systems
- It is possible to run a computer using 100% Free Software, down to the firmware level
- On phones it‘s more difficult, but almost possible

Basics – Data Reduction

- Data Reduction: reducing attack surface
- Instead of trying to erase data trails, don‘t create them in the first place
- Get rid of unnecessary devices, social media accounts, chat logs, browser history
- Don‘t use cloud storage, unless it‘s provided by yourself (or your group)
- Be aware of where you go and who you communicate with (especially when carrying a phone!)
- Make this a mental exercise: try to keep control over **all** your data. Become a data minimalist!
- If the above is not possible: try to separate your activism stuff as much as possible from work/study (compartmentalisation)

Basics – Decentralisation

- Centralisation means „having everything in one place“
- Centralisation facilitates censorship, surveillance, seizures, repression
- Examples for centralisation: Facebook/Whatsapp, Twitter, Google, Dropbox
- Don‘t create single points of failure!
- Examples for decentralisation: run your own blogs (instead of using Facebook), use federated chat protocols/social networks
- If you can: run your own infrastructure (self-hosting)

Basics – Anonymity

- So far, we have talked about software and data. But there is also **metadata**
- Metadata: not the content of a message, but all surrounding information. For example: phone numbers, IP addresses, time, file size, location
- Metadata is often quite revealing: communication with a doctor, a lawyer, an investigative journalist, a person at Görlitzer Park at midnight…
- Encryption alone does **not help**. Anonymity is a separate issue!
- Tor is a powerful tool to reach reasonable anonymity online

Basics – Encryption

- Encryption: using cryptography to make information unreadable for unauthorized parties
- One of the most well-known building blocks of InfoSec
- https: encrypt the connection to a web server
- End-to-end encryption: encrypt messages so that only the receiver can read them
- Full disk encryption: encrypt your hard drive so you‘re protected in case of theft, loss or seizure
- (this will probably be a workshop on its own)

Basics – Authentication

- Important: encryption is often useless without authentication!
- Encrypted messages can be spoofed (e.g. coming from someone else who might have replaced the message)
- Authentication makes sure the other person/party is really who they pretend to be
- Luckily, encryption and authentication are often well integrated: check the green lock in the browser when using https, check fingerprints when doing end-to-end-encryption
- Always: use strong passphrases!

Basics – Location Tracking

- Location tracking is a relatively new threat that became much worse with the ubiquitous use of mobile phones
- Every phone that is connected to the mobile network is constantly tracked. That information is linked to your identity (via SIM card) and easily accessible by the police
- Increasingly, WiFis are used for tracking as well: BVG, Telekom Hotspots, in-store-tracking
- Location tracking allows to link people together that are otherwise not (yet) linked, e.g. when they go to the same meeting/plenum!
- Remedies: airplane mode (can you trust it?), leaving your phone at home

Basics – Review

- Free Software: the prerequisite for trust
- Data Reduction: reduce attack surface, become minimalist
- Decentralisation: don‘t have everything in one place that is not under your control
- Anonymity: avoid revealing metadata
- Encryption, Authentication: make information inaccessible to others, make sure other parties are who they pretend to be
- Location Tracking: don‘t walk around with a surveillance device revealing your location all the time

What you can do now

- Switch to free software whenever possible
- Close social media accounts (esp. the bad ones), delete all unnecessary stuff
- Switch to a good e-mail provider (e.g. posteo.de, mailbox.org, systemli.org)
- Install Tor Browser (https://www.torproject.org/) on your laptop and use it for browsing sensitive stuff
- Use a free end-to-end-encrypted messenger (e.g. Conversations, Gajim, Signal) instead of making phone calls, sending SMS or writing unencrypted e-mails. Verify fingerprints!
- Leave your phone in airplane mode whenever possible

In the long run

- Switch to a 100% free operating system
- Harden your hardware: install Libreboot, remove cameras/microphones
- Encrypt your hard drive and all your backups
- Use a password manager
- Learn how to use e-mail encryption, build a web of trust
- Self-host your group‘s infrastructure or use a trusted provider
- Install LineageOS or Replicant on your phone, only use apps from the F-Droid store
- Use SIM cards as little as possible. Better install Freifunk routers wherever you can

Questions?

Remember: this was a brief overview. We will go into much more detail in the next weeks!

Proposed topics

- Smartphones: how to run a Google/Apple/Microsoft-free phone, install F-Droid and free software, use end-to-end encryption, avoid tracking
- Anonymity: how to use Tor/Tails/MAT to research and post sensitive information while not leaving traces online
- E-Mail encryption: learn how to use Thunderbird and Enigmail to encrypt and sign mails, exchange keys, build a web-of-trust. Learn about secure chat software on the laptop
- Freifunk: upgrade your *space with a Freifunk router! Provide free, anonymous internet access so people can work and play without using SIM cards
- Mastodon: a federated, free-software based social network. Connect and have fun without the usual downsides

And now...

Discussion, then a short break, then hands-on session (for consulting, urgent problems etc.)

Thank you!

Feel free to visit https://resist.berlin or write an email to resist.berlin@posteo.de.

The slides will be available on the website.

Also check out soze44.noblogs.org for further announcements!