Ψηφιακή Ανωνυμία και Ασφάλεια

I Insurrection Festival **insurrectionfestival@riseup.net**

Athens, 12 – 14 November 2017 **insurrectionfestival.noblogs.org**

DANGERS

NOTHING is secure

You are not alone

Adversaries

- Hackers
- Your own comrades
- Yourself!
- Internet services
- ISP – OTE, Cyta
- Mass surveillance. Google's AI. Big data. They know you better than yourself

Make them work hard.

Data retention: zeit.de/datenschutz/malte-spitz-data-retention

Transparency report: transparencyreport.google.com

TYPES OF ATTACK

- brute force – howsecureismypassword.net
- bots, algorithms – better than brute force
- AI – better than bots
- Quantic – many times faster than all the computers that have ever existed put together
- Man-in-the-middle – they can be in every step of the path between you and the server; even between steps, tapping the cable
- physical access – USB sticks
- rubber hose (google it!)

... who to trust?

GOOD PRACTICES

Protect

- your *IDENTITY* – WHO you are
- your *LOCATION* – WHERE you are
- your *ACTIVITY* – WHAT you are doing or saying
- your *NETWORK* – remember, you are not alone

GENERAL

Who owns who?

All phones release data every 5 s. Companies make 8000€/y by selling your data; censorship; control

Free software. 4 freedoms

(0) to run the program

(1) to study and change the program's source code

(2) to redistribute exact copies

(3) to distribute modified versions

Directory. directory.fsf.org

Professional OS – based on UNIX

- Non-free: MacOS, Android, iOS
- Free: GNU/Linux, Replicant

Use the command line and your life will be better

Threat model

1. ***WHAT do I have at home that is worth protecting?*** *List your assets*
2. ***WHO do I want to protect it from?*** *List your adversaries*

3. ***HOW LIKELY is it that I will need to protect it?*** *List which threats you are going to take seriously, and which may be too rare or harmless (or too difficult to beat) to worry about*
4. ***HOW BAD are the consequences if I fail?*** *List the things your adversary can do with your private data*
5. ***HOW MUCH TROUBLE am I willing to go through to prevent these consequences?*** *List the options you have available to help mitigate your threats. Note if you have any financial, technical, or social constraints*

INTERNET

Browsing

Tracking
- Browser id techniques
  - Panopticlick: panopticlick.eff.org

Virus – NOT with free software
Phishing
Ransomware
ID theft
Scripts
Zombie machines and botnets

Solutions
- Use Firefox or Chromium
- Delete history
- Cookies
- Private browsing
- Alternatives to Google: **DuckDuckGo**
- Alternatives to Facebook: **DumDarac**
- Disable scripts
- Different users
- Virtual machines: **VirtualBox**
- Extensions: **HTTPS-Everywhere**, **U-Block**, **DoNotTrackMe**
- MAC address spoofing
- Cover your camera
- Don't connect to random open WIFI networks
- VPN: **OpenVPN**
- Open downloaded files offline or on G-Drive

Deep web. Dark Net. Hidden Wikipedia. **Tor** protects your *IDENTITY* and *LOCATION*.
- De-anon Tor users

thenextweb.com/insider/2016/03/11/mouse-movements-can-reveal-identity-even-tor-cant-hide

news.softpedia.com/news/tor-users-can-be-tracked-based-on-their-mouse-movements-501602.shtml

Tails. Live OS (it runs inside a USB stick) based on security and privacy. Includes Tor by default, MAC spoofing, etc.

Communications

Email

Server. **riseup.net**, **autistici.org**, **protonmail.com** (non-free)
Client. **Thunderbird**

Messaging

End-to-end encryption vs. transport encryption. **Riot. Signal. Telegram**

Voice

VoIP – **Signal. Jitsi. CSIPSimple**

Google hangouts ??

Encryption

It protects part of your *ACTIVITY*, but not your *LOCATION* or *IDENTIY*.

Man-in-the-middle attack: tails.boum.org/doc/about/warning/index.en.html#man-in-the-middle

- Strong ***passwords***. Use dice word charts for randomness. Don't recycle. Password manager - **KeepassX**

  Test your password: passwordmeter.com
- Change your passwords often

- Use 2-factor authentication (but careful if you link your credentials to a SIM card)
- Full drive encryption
- Hide files with **Veracrypt**

Wiping and Shredding

Deleted files don't disappear from the drive. Use **shred** instead.

secure-delete has four tools:

srm - securely delete an existing file
smem - securely delete traces of a file from RAM
sfill - wipe all the space marked as empty on your drive
sswap - wipe all the data from you swap space

Encrypting SWAP space

ibm.com/support/knowledgecenter/en/linuxonibm/liaai.securesles/liaaisecureencryptswappsles.htm

PGP

Encrypting, decrypting – Combination of public key + private key + password. Protect the content of the conversation, but NOT THE METADATA.

Signing. Prove it's really you.

Web of trust. Trusted peers can sign each other's public keys.

P2P

Bittorrent **–** thepiratebay.org

Cloud computing – NASA

Blockchain – **Bitcoin, FairCoin** – fair.coop is a public, anonymous and ultra-secure financial system for economic disobedience

MOBILE PHONES

Do not use them

Not designed for security. They are tracking devices with additional features. The more advanced, the worse they get.

There may or may not have *backdoors* (you don't know), so even if you close an app it might continue working secretly and connecting with your ISP or others.

Aware of the dangers but still decide to use it? Fine.

- Hide your *LOCATION*. Disconnect from networks: GSM, WIFI, bluetooth, GPS, radio FM
- Root your phone, or buy a rooted phone anonymously with faircoin market.fair.coop/shop/brands?brand=174
- **Fdroid** is an alternative to Google's Play Store
- Phone mic access – possible even when phone is off
- Wiping files – you can't! (SSD ≠ HDD). But you can encrypt
- Use anonymous SIM cards
- Don't store your (or your comrade's) private data in the phone. Protect your *NETWORK*
- Exchange your device randomly with someone

HARDWARE

Hardware compatible with free software – h-node.org

Internet of things

- Ways to hack a printer – hacking-printers.net
- Soon in your life: connected refrigerators, cars, clothes, contact lenses with camera, your dog… – fuck that shit right there

RESOURCES

- **Starter pack:** ssd.eff.org/en/playlist/want-security-starter-pack
- **Resources**: fsf.org/resources

HACKING

- Hackback's DIY guide: gist.github.com/tfairane/fe22d64508bd057e9cdb8b6d5a7d27bd#file-ht_en-txt
- Stalker tools: stalkertools.com/category/caller-id-spoofing-methods/#sthash.4C1qPfKK.dpbs

Happy hacking!