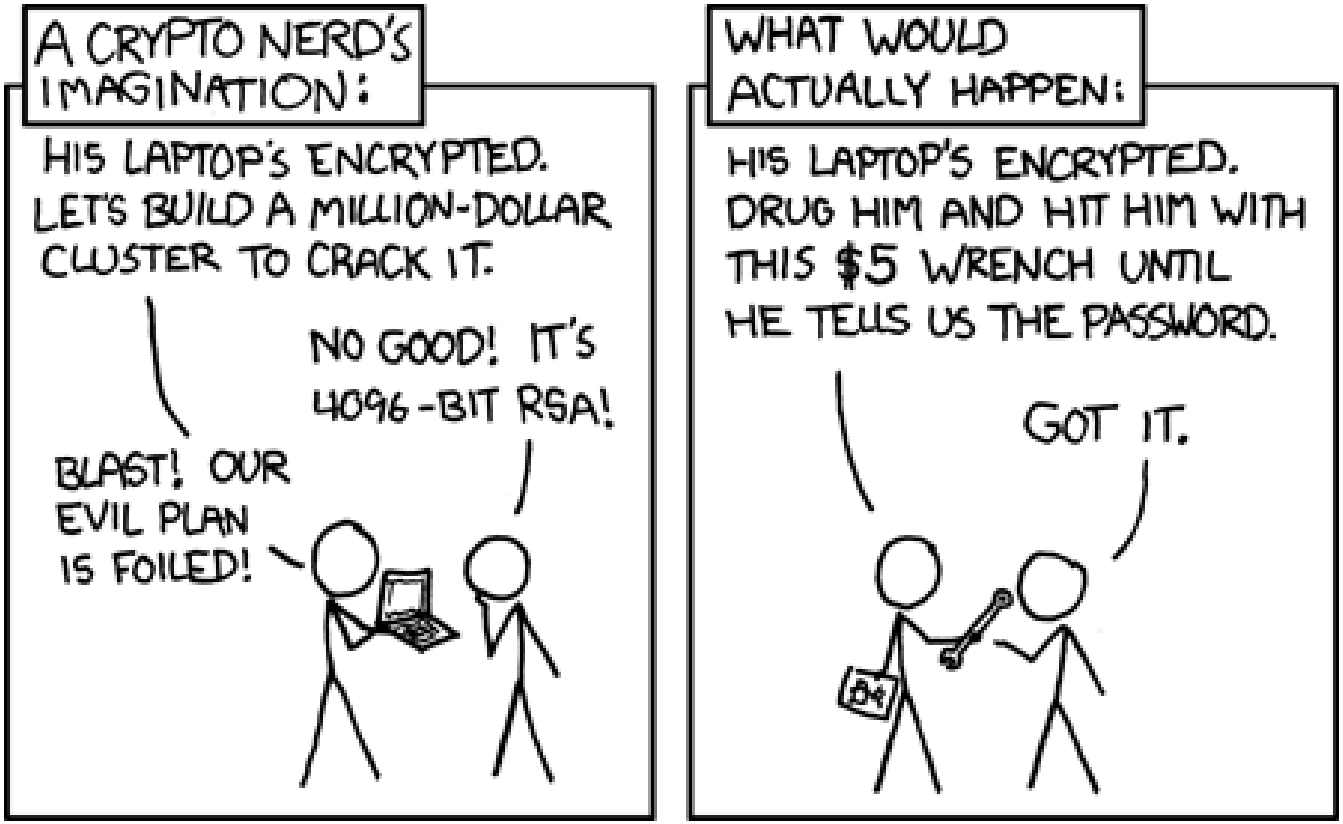
Internet privacy workshop

Pinknoise

June 29, 2015


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.

Why workshop and why privacy?

- Because want share knowledge and help people to use privacy tools to make online privacy more accesible.
- Because we think you should be able to be in control of what data/information you share and with whom.
- Because invasion of our privacy makes us more vulnerable and submissive.
- more reasons why privacy is important

Stuff we can help you with:

- Alternatives to commercial services and software.
- Technical tools to help protect your information and privacy.

Stuff that cannot be fixed with technical tools:

- Things you publish yourself.
- giving away huge amounts of info (of yourself and your network) when using social media
- giving away huge amounts of info when using google or other commercial services

Stuff that cannot be fixed with technical tools:

- selling out your visitors when using google analytics/ jsdelivr.net (grotebroek.nl)
- Grotebroek snitching on all the visitors of our privacy workshop.

Basics

- Use free (libre, as in speech, as in freedom, not as in beer) software.
- Use strong passwords.
- Encrypt all your harddrives/ usb drives/ floppy disks / tapes, etc.
- no cloud crap (keep your data on your own machine)

Software

- Know where your software comes from
- Can you trust the developers?
- Free software / open protocols
- Package manager (signed packages, updates)
- Keep software up-to-date
- Only use software that is maintained
- Free software / open protocols
- Because commercial software, like all commercially produced goods, is designed to generate profit - not to guarantee your privacy.
- more reasons free software should be used?

Passwords

- Strong passwords are long, highly random and don't use dictionary words, or...
- Use lots of words (passphrases)
- Do not reuse passwords, especially not between offline (disk encryption) and online (email) stuff
- You could use a password manager (on a trusted computer), for example KeepassX(cross platform)
- Never use your passwords on machines you do not trust (any machine that is not yours)

Hardware

- TEMPEST (leaking electromagnetic/sound/etc. waves)
- Keyloggers
- Hardware actually contains a lot of software
- The Evil Maid!
- Police Raid
- Loss of hardware

Storage

- Encrypt your harddrives, usbsticks, etc. , keeps your data safe when computer is turned off
- Storage encryption does NOT work on computers that are turned on.
- Never mount your encrypted storage on public computers.
- Be aware that anything you delete from a harddrive, sd card, or usb stick, is still there and very easy to recover, so encrypt ALL your media.
- Get rid of metadata before you publish something (MetadateAnonymisationToolkit) (https://mat.boum.org/).
- When your computer is suspended, disk encryption doesn't work.

Online

- Avoid commercial services
- Use encrypted connections (SSL/TLS)
- Hide the location you are connecting from (tor)
- It is almost impossible to make your browser not unique, so use torbrowser or tails

Browser Plugins

- Adblock plus/edge/whatever
- Noscript
- Https everywhere

Mobile phones

- They give away your location
- All communications are easily interceptable
- Don't use them
- separation between modem and application processor
- http://redmine.replicant.us/projects/replicant/wiki/SamsungGalaxyE
- New versions of android have full disk encryption, you should turn it on (and use a good screenlock password).
- There is: replicant, guardian project, signal

Frequently Asked Questions about quitting facebook.

- Q: How to communicate with your friends without facebook?
- A: You don't have to, because you will lose all your friends
-
- Q: How do i know when is the birthday of my friend without using facebook?
- A: Before you quit your facebook account you can write down their birthday in you agenda. Anyway, after you quit they are not your friend anymore so you don't have to give them a present.
-
- Q: How do i know when there is a nice party without using facebook?
- A: There is no way, people without facebook can't be invited for events.
-
- Q: How do i contact people i lost contact with?
- A:
-

Cryptography

- is the practice and study of techniques for secure communication in the presence of third parties
- various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation[4] are central to modern cryptography.
- Symmetric cryptography means Alice and bob both have the same key

Assymetric cryptograpy / Public/private-key cryptography

- Used in: SSL, OTR, GPG
- Makes it possible to securely communicate with people without agreeing on a shared secret before
- You can sign messages

Virtual Private Network / Proxy Servers

- A vpn routes your traffic trough a server in a different location in the internet
- Protects your traffic against people sniffing the internet connection you are connected to
- Can be used to avoid censorship

Peer to peer networks / darknets

- gnunet (filesharing, vpn, phone, social network)
- i2p, the invisible internet project (anonymous overlay network)
- tor hidden services (anonymous overlay network)
- freenet (filesharing)
-

The onion router

- Hides your IP adres from the destination website
- Hides the browsing destination from your ISP and others
- Circumvents local censorship
- You can still identify yourself through information you share with websites (logging in, etc)

GnuPG

- Free software implementation of openPGP
- Private/Public Key system
- Encryption
- Digital signatures (software distribution)
- Public key can be published (key servers)
- Web of trust
- Choose a keyserver you trust and that is encrypted.
- https://help.riseup.net/en/security/message-security/openpgp/best-practices

jabber / xmpp

- protocol for chatting with people
- you are not bound to 1 service provider like with skype,facebook,etc.
- most xmpp clients support OTR (pidgin, chatsecure, etc.)
- OTR in 2 clients signed in at same moment does NOT work

audio / video calls conferencing

- mumble
- ostel
- zrtp

OTR

- Off The Record
- For us with various chat clients and different services
- Session keys, Perfect Forward Secrecy.

Keysigning

- Sign some GPG or OTR keys
- Everybody puts their gpg fingerprint + otr fingerprint + any other fingerprints + email address on a pad and sends their public key to the coordinator from the email address listed in the key.
- Everybody will make a copy of the pad and store it locally
- When everybody did that, the list will be projected
- We will make a round, and everybody has to verify that their fingerprint is correct (read it out loud), people will check on their own copy of the list if it has the same fingerprint.
- All keys that could not be verified will be removed from the list (also do that on your local copy).
- The coordinator will send all the keys to everybody
- Everybody will verify the keys (using their verified copy of the list), and sign them (local signatures, except when people explicitly requested public signatures)

Questions

- Questions?
- Now we will do practical sessions on various subjects (depending on what you want to learn).
-
- Check out:
- https://pn.puscii.nl/privacyworkshop
- www.puscii.nl
- we.laglab.org