Privacy, security & anonimity

Foo-Manroot

Foo-Manroot

https://foo-manroot.github.io/

Foo_Manroot

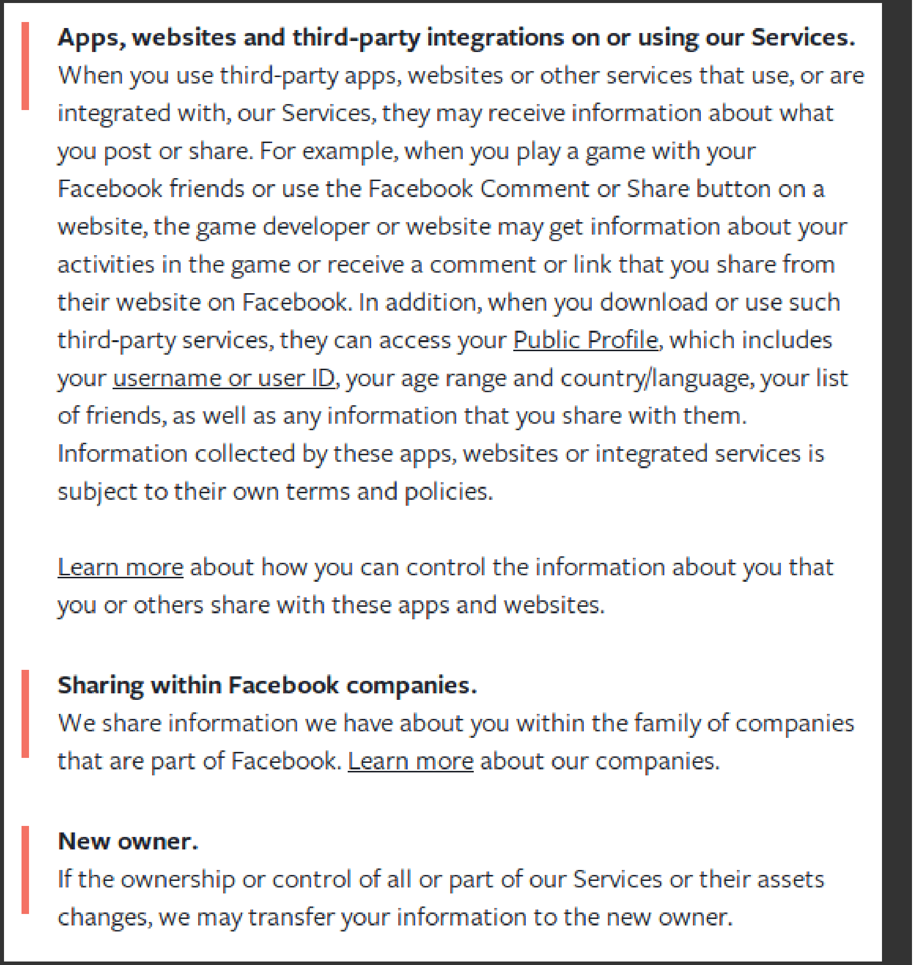
The need of security on Information Systems

- CIA:
  - Confidentiality
  - Integrity
  - Availability

Defined on ISO 27000

- Surveillance programs:
  - PRISM (U.S.A): revealed by E. Snowden in 2013.
  - Data Retention Directive (E.U.): The telecommunications data has to be stored for 6 to 24 months to be accessed by the police and security agencies (declared invalid on 2014)
  - Facebook, Google, Microsoft, Apple… all follow the U.S.A. laws (at least, when it suits them → *PRISM* vs *San Bernardino*).

- Enterprises sell and buy personal information:
  - On ToS there are usually clauses where the enterpirse is granted permission to share data with third parties to “provide an optimal experience”
- Common criminals:
  - *Phising*, *malware*…
  - Easy attacks. Greater threat than state agents



Apps, websites and third-party integrations on or using our Services.
When you use third-party apps, websites or other services that use, or are integrated with, our Services, they may receive information about what you post or share. For example, when you play a game with your Facebook friends or use the Facebook Comment or Share button on a website, the game developer or website may get information about your activities in the game or receive a comment or link that you share from their website on Facebook. In addition, when you download or use such third-party services, they can access your Public Profile, which includes your username or user ID, your age range and country/language, your list of friends, as well as any information that you share with them. Information collected by these apps, websites or integrated services is subject to their own terms and policies.

Learn more about how you can control the information about you that you or others share with these apps and websites.

Sharing within Facebook companies.
We share information we have about you within the family of companies that are part of Facebook. Learn more about our companies.

New owner.
If the ownership or control of all or part of our Services or their assets changes, we may transfer your information to the new owner.

ToS de Facebook

There’s no perfect security, but the risk can be minimized.
Security policies can’t be applied with retroactive effect → After a breah, there’s little than can be done

Some previous definitions

- *Software*
  - *Free Software* (as in ‘freedom’)
- VPN
- Privacy ≠ anonimity
- Encryption
  - OpenPGP standard

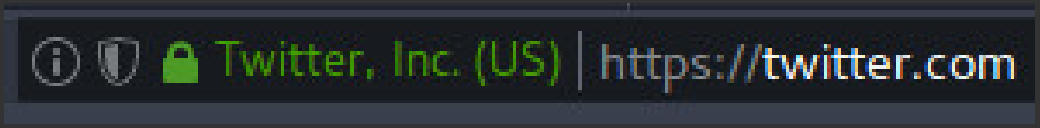
Personal security

Good practices

- The objective is to minimize the exposition surface.

- Keep software up to date.

- Use HTTPS:
  - Available on ~41% of web pages
  - Guarantees confidentiality (even though the ISP can still see the traffic's destination), integrity and authenticity
  - It's important to check the certificate (very easy)



Twitter, Inc. (US) | https://twitter.com

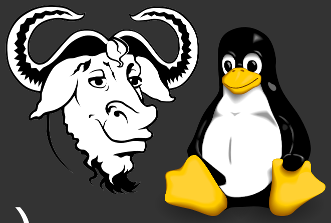
- Full disk encryption:
  - Easy and transparent
  - Guarantees confidentiality if the system is physically compromised (stolen, requisitioned by the police…)
  - Tool to encrypt disks: VeraCrypt

- Passwords (complemented by 2FA):
  - One password per website
  - Use phrases or multiple words concatenated
  - Eased by a password manager:
    - Only the master password has to be remembered
    - There are a lot of options (*open-source*):
      - Keepass (very popular, with a lot of *plugins*)
      - Gnome password manager
      - (…)
      - Even an encrypted file with GPG can be used (handled with care)
      - It’s very important that the code of the password manager is available, to verify it

- Mobile phones (mostly Android):
  - Turn wi-fi off when out of range
  - Avoid Google Apps (Gmail, Drive, Calendar…):
    - The minimum to still have the essential functionalities is the core (base system, installler, Play Store...)
    - It’s preferable to use OpenGAapps (*open-source*… kind of):
      - Some part of Google’s code can be found on their repositories
      - There’s also MicroG; but there may be some problems (Gapps’s impersonation, the little *hack* used to get it working) or use experience
    - Some *open-source* alternativs can be found on F-Droid + Yalp (interface with Google Play)
  - Turn GPS off (it’s not needed most part of the time)
  - Control permissions:
    - Permissions granularity (global, by application…)
    - If an application asks for a lot of permissions, suspect...
    - If an application asks for permissions that seems unnecessary, suspect…
  - Remember that Android is developed by Google
    - Alternative S.O. (if available): LineageOS → *Free software*

- Look after your image:
  - Profiles on Twitter, Instagram, Facebook...
    - OSINT *(Open Source INTelligence):*
      - If a profile is public, milliones of people (and *bots*) can access your information (download images, control activity…)
    - Make the accounts private
    - Control the information that is proportioned (i.e., don’t show your keys in a photo)
    - *If a product is free, you are the product*:
      - Enterpirses sell your data (usage habits, demographic profile…) and link accounts from different services (Facebook and Whatsapp, for example)
      - Services like 10minutemail can be used to help prevent this
  - Block cameras when not in use

- Use *free software*:
  - Their respect for privacy can be verified.
  - Mozilla Firefox:
    - Similar funcionalities and performance as Google Chrome (developed by Google), with a record of fighting for a free internet.



  - GNU/Linux:
    - User-friendly distributions (Ubuntu, Fedora, Mint…)
    - Greater control over your machine
    - There’s no need for sysadmin experience (the infamous *terminal*).
  - Messaging: Signal, Keybase, Protonmail...
  - In absence of alternatives, at least *software* that expresses their respect for privacy:
    - Search providers: DuckDuckGo o Ixquick (recommended by EU)
    - There’s no other choice than to trust these services

Paranoid mode (justified)

- Surfing the web:
  - Turn tracking protection on
  - Turn JavaScript off
  - Don’t use outdated technology (Flash, Java applets…) → HTML5 solved these need for interactivity long time ago
  - Reject cookies. JS is more used for tracking and analytics, but some sites still use cookies for tracking. Nowadays, cookies que are usually for security (CSRF) or authentication

- Instant messaging (extended later):
  - Problems with Whatsapp:
    - Property of Facebook → Uses the metadata with Facebook to suggest relationships (“people you may know”).
    - Closed-source → The correct implementation of the end-to-end encryption can’t be verified
    - Messages are stored in clear on */data/data/com.whatsapp/databases* → If the terminal is compromised, anybody can access to all the history of messages
  - Problems with Telegram:
    - By default, conversations aren’t encrypted end-to-end → The company can see the content of the messages
      - Only secret chats are encrypted end-to-end → Using their own protocol, that hasn’t been tested independently
    - Like Facebook selling data to another companies and gobernments (U.S.A and allies), Telegram does it (presumably) with russian companies and russiand allies
    - Telegram claims to be secure, but doesn’t provide enough means and abnormal restrictions to test it (date limits, scenarios reduced to very specific cases) → Propagandistic strategy

- Use of VPNs:
  - Mask IPs to the end server (anonymity):
  - The VPN provider controls all the traffic:
    - Trust is transferred from one provider (ISP) to another (VPN)
    - The problem (to evade traffic control) remains
  - Usually they’re not free. If one VPN is free, they’re most probably selling your data (or smething worse...)
  - ToR / I2P / etc.:
    - *Free software*
    - Intermediate nodes can’t see the data, and the end node can’t know who is performing the request
      - Aimed to obtain anonimity on the web
      - The exit node can still see the data (privacy is not guaranteed)
    - Real identities are discovered because of human errors:
      - Turn on JavaScript, Flash…
      - Download and execute files
      - Using personal accounts (Gmail, YouTube, Facebook…) → Silk Road (Ross Ulbricht)

- Encrypt and sign messages on a regular way:
  - Encrypt and sign message and attached files
  - PGP (GPG, Keybase..)
  - Guarantees confidentiality, integrity and authenticity

“Total paranoid” mode

- Techniques widely used on big companies, especially on higher levels

- Air-gap electronic devices:
  - Turn off networking (flying mode)
  - Remove power supply (battery, plug…)
    - Usually, that’s enough
      - Si se hubiera introducido un elemento de escucha que siguiera funcionando sin esta alimentación principal, seguramente se notarían desperfectos en la carcasa.
    - If it’s not enough → Faraday cage (box with tinfoil, microwave oven…)
  - Sometimes, manufacturers introduce direct access tha can be exploited:
    - IME (Intel)

- File encryption (apart from full disk encryption):
  - Backups
  - USB
  - Folders on a shared terminal

- Effective removal of files: shred

- USB (or similar) to unlock terminal (2FA)

Security in groups

Communication

- Instant messaging:
  - Needs:
    - Confidentiality
    - Integrity
    - Authentication
    - Repudiation
    - Access to the code
    - In some cases, message destruction
  - It’s advisable to use different methods, according to the needs:
    - Avoids all information to be on the same place → To link the activity of different methods is harder

	Whatsapp	Telegram	Signal	Facebook Messenger	Wickr
Confidentiality, integrity and authentication	Signal protocol. Without independent reviews	No encryption (except secret chats)	Signal protocol. Public and reviewed	No encryption (except secret chats)	Wickr protocol. Público and reviewed
Open-source	No	Only clients	🟩	No	Yes (privative license)
Message destruction	No	Can be erased (by hand)	Self-destruct messages	No	Self-destruct messages
Comments	Owned by Facebook	⬛	Protocol reviewed by independent parties	Owned by Facebook	• Protocol reviewed by independent parties • P2P

Some other options has been ommited, to maintain the table manageable.
The rest of applications (the most used ones) has similar characteristics than Whatsapp and Telegram.

- Instant messaging:
  - Best options seem to be Signal y Wickr
  - Both can be used:
    - Signal for daily usage
    - Wickr to complement (additional conversations, like side discussions that don’t belong to the main group)
    - (or vice versa)
  - Poor adoption of these applications:
    - Whatsapp and Telegram still dominate the market

- Another option is to use decentralized networks:
  - XMPP:
    - Communication standard
      - Multiple applications can implement this standard → More flexibility
  - Matrix:
    - More modern than XMPP
    - Has “bridges” to other protocols (IRC, XMPP...)
  - If you have the needed resources, you can have your own server → No dependency of third parties

- E-mail:
  - Same needs than instant messaging
  - Easier solution is to encrypt and sign all mails (including attached files) using PGP
    - There are a lot of easy to use implementations:
      - Keybase
      - GPG
      - OpenKeychain
    - Some mail clientes (like K-9 mail) integrates easily with this tools to encrypt/decrypt and sign/verify messages

Social networks

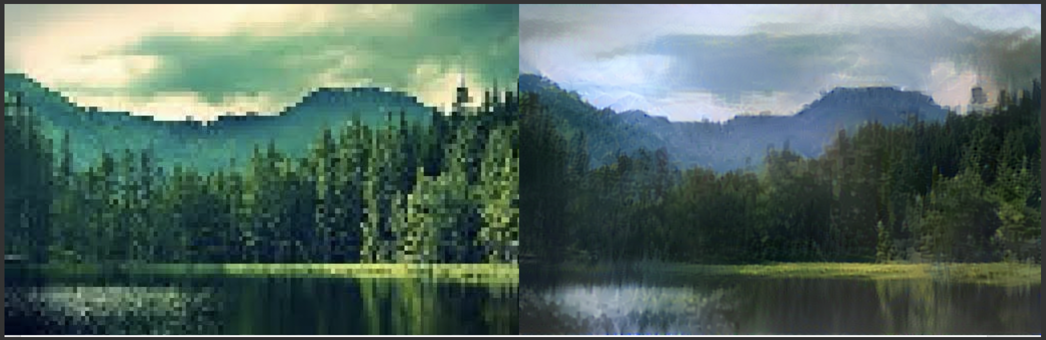
- Alternatives to traditional networks that respect privacy:
  - Facebook → Diaspora
  - Twitter → Mastodon
- Decentralized networks and *open-source*
- Problem: little adoption by the public

mastodon

diaspora*

Miscellaneous

- Distributing images:
  - Check metadata
  - If some information has to be hidden, do not pixelate (information can be recovered), but paint on top of it
- If PGP is used, distribute correctly the keys:
  - Some implementations (like Keybase) ease this task
  - Check the keys in person
- Use *free software*:
  - Search alternatives to traditional services (Google, Microsoft, etc.):
    - Email
    - Colaborative document editing
    - Cloud storage



Conclussions

- Review of proposed tools (other options and recommendations can be found on the internet):
  - Password manager:
    - Keepass
  - Instant messaging:
    - Signal $\vee$ Wickr $\vee$ XMPP
  - Email
    - Provider:
      - ProtonMail $\vee$ OpenMailBox $\vee$ Tutanota
    - Client:
      - K-9 mail (mobile)
      - Thunderbird (pc)
    - Encrypt with PGP (there are plugins to ease the task)
  - PGP:
    - Keybase $\veebar$ GPG (to handle keys)

- Review of proposed tools (cont.):
  - GNU/Linux:
    - User-friendly and stable distros:
      - Ubuntu
      - Fedora
      - Mint
    - Disk encryption (with the O.S.'s tools, or with external ones like VeraCrypt)
    - Encrypt personal folder
  - Firefox:
    - Review plugins and addons:
      - Turn off Flash, Java, JavaScript…
      - Control HTTPs
      - Extensions for PGP and Keepass
    - Tracking protection enabled and third-party cookies disabled
    - Use DuckDuckGo ⋁ Ixquick
  - VPN (paying) ⊻ ToR / I2P / Freenet (high latency)

- To avoid unjustified paranoia:
  - Review code (to learn is easy)
  - Monitor traffic
  - Ask experts on the field

- Distribute information:
  - Limits the impact when a system is compromised
  - Increases the exposition surface
- Control public information
  - Know (or deduce) where your information could be

<u>There’s no perfect security</u>

You have to stay always alert

Demo time!