Personal FREEDOM in digital millenium

Sergey Kozlukov

INTRO

Contact info

- Sergey Kozlukov <rerumnovarum@openmailbox.org>
- GPG: **B986D856**
- Sources and examples are available at `https://github.com/RerumNovarum/vsu.en`

{}

Github

- Again, sources and examples are available at `https://github.com/RerumNovarum/vsu.en`
- Feel free to Fork, report an Issue and send a Pull-Request

Subject

FREEDOM in digital millenium

- Threats and threat models
- Protection

Threats and threat models

WHY?

It's always about money and influence
And sometimes just about hostility

Privacy. Opensource information

> *Privacy is completely and utterly dead, and we killed it*
> *(c) Steven Rambam*

All the personal info is now opensource

- Name, bd, home address
- Political views, sexual orientation
- Photos, geotags

These are contributed by people themselves
This information makes you and your neighbourhood vulnerable to social engineering attacks
Also, hope you're not used to specify your real city or birthdate as an answer to these "secure questions", like some people in Voronezh like to do?

Privacy. Recording

> *Privacy is completely and utterly dead, and we killed it*
> *(c) Steven Rambam*

Every single movement of a person is recorded in some database

- Medical records
- Criminal records
- Border crossings
- Employment history
- Bank records
- 24/7 tracking via goddamn mobile phone

And ALL of these are cross-linked

Privacy. Recording

All these things you or somebody has contributed into public
domain will NEVER EVER be deleted
Think of it before you post in the blog

Proliferated malicious services, soft and hardware

Malicious soft and hardware nowadays is extremely widespread. It is often proprietary products, enforced by governments and multiple monopolies. People are usually chained in Closed standards (forcing ppl to use malicious software from e.g. Microsoft)

Proliferated malicious services, soft and hardware

- Document circulation (e.g. proprietary MS .doc)
- Correspondence
  - Proprietary mail/chat services with surveillance enabled by-default
  - Even worser, services, that require to execute malicious code on your machine, with backdoors included, e.g. Skype
- Mobile telephony, all these CDMA, &c
  - Almost no encryption, vulnerable to everyone who got hardware
  - Just a blackbox living it's own life
    - You cannot disable this module even by unplugging battery
    - Probably these modules have access to host
  - 24/7 tracking, while you're walking among cells

Proliferated malicious services, soft and hardware

Figure 1: Upgrade from Windows

Proliferated malicious services, soft and hardware

Hardware backdoors

- Intel ME
  - Full access to RAM
  - Screen monitoring
  - Access to peripherals
  - Can NOT be disabled (except for extremely old chips)
- Reported backdoors in WD hard drives' firmwares
- Mobile phones. Just a goddamn uncontrollable blackbox which spies on you
- Secure boot and other digital restriction means
  - Supposed to be a security feature, but used instead to restrict user's freedom

Proliferated malicious services, soft and hardware

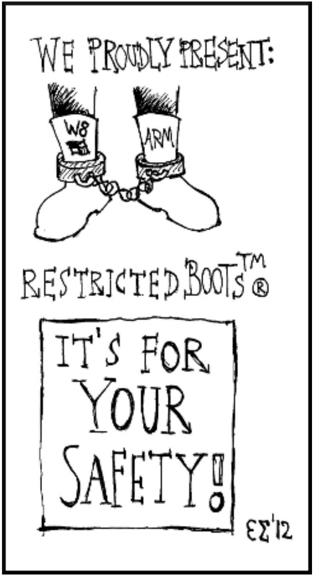


Figure 3: restricted boots

Proliferated malicious services, soft and hardware

Proprietary services

- Put you in a jail of legal traps
- In 2009 Amazon massively ERASED copies of Orwell's 1984 from ebooks of it's users
- Apple uploads to the cloud and deletes local copies of audio files w/o user's permission. And you'll never get exact copies back, only lossy versions
- Microsoft got killswitch to delete arbitrary program from your machine
- All of these – compliant with their EULA. In particular, Apple is not responsible for any bogus behaviour of it's service

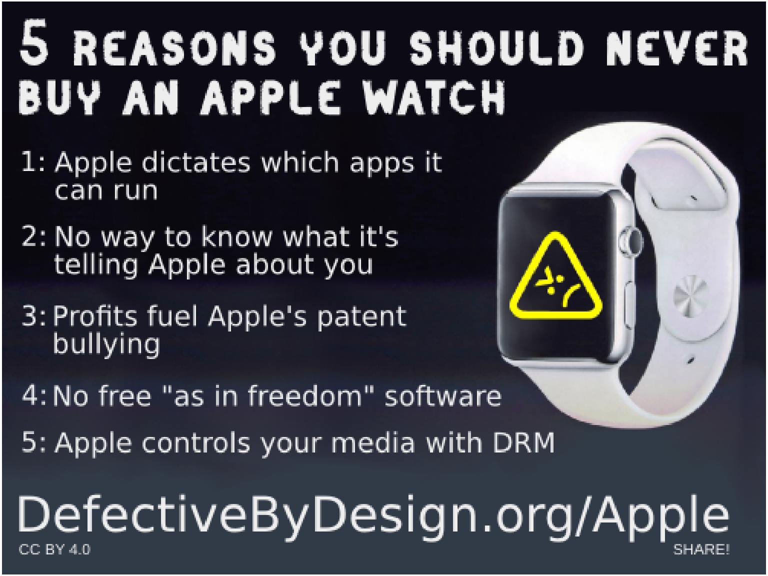
Proliferated malicious services, soft and hardware

Proprietary operating systems

- Have throughout control over user's computer
  - Automatic installation or "upgrading" w/o user intervention
- Full access to file system
  - Didn't you disable Skydirve?
  - Your whole "Documents" folder has been legally uploaded to MS servers
- Remote code execution
- Installations log, keylogging, whatever
- Licensing traps
  - MS (Apple, Amazon, all of them, you can read) can LEGALLY delete any of your files or programs

All of these are MALWARE

Proliferated malicious services, soft and hardware



5 REASONS YOU SHOULD NEVER BUY AN APPLE WATCH

1: Apple dictates which apps it can run

2: No way to know what it's telling Apple about you

3: Profits fuel Apple's patent bullying

4: No free "as in freedom" software

5: Apple controls your media with DRM

DefectiveByDesign.org/Apple

CC BY 4.0

SHARE!

Figure 4: Apple watch is defective by design

Digital Restrictions Management (DRM)

- Technical means to restrict user's freedom to use it's media (and not only media)
- Based on legal enforcement of manufacturers (and users) to include malicious code blobs to the software
- Based on infamous "Security through obscurity" approach
- Main ideas:
  - Money of out the air, never let the user own content, instead license temporarily to stream

Digital Restrictions Management (DRM)

It's certainly easier to implement bad security and make it illegal for anyone to notice than it is to implement good security. (c) Bruce Schneier

Digital Restrictions Management (DRM)

DRM (also patents, partially copytight, &c) actually reduces to the following:

Corporation is trying to establish a monopoly and to restrict people to use only it's service and only in the way Corp. wants to. Via lobbyists Corp. makes government to support and protect Corp.'s intention to threat people

In the result, to protect an ill-meaning minority, gov-t forces entire Majority to install and use proprietary and closed malicious hard and software, that potentially (i.e. almost always) contains backdoors &c

Such a nonsense

Digital Restrictions Management (DRM)

Nowadays multiple Evil-corps, including e.g. Microsoft, Netflix, others are trying hard to make DRM part of HTML5 standard

Vulnerable services

Whoever you are i’m sure there is in your chat logs some evidence of criminal offence you’ve had commited, some “pirate” content, or some private photos

Most of the services you use aren’t secured

Vast majority of them tightly cooperate with special services

And almost all of them collect statistics and sell info about you to whoever gonna pay

Vulnerable services

And most of them weren't developed with security in mind

Most of the android applications ignore certificate checking, which makes them vulnerable to MiTM attacks

Fundamental technologies themselves like SSL are defective, they're based on centralised CA's, which makes special services able to perform MiTM transparently

Vulnerable services

BTW, these “special services” cannot cope with community via technical means. So governments are trying to restrict community legally

For example 5Eyes countries are up to legally forbid end-to-end encryption

And in Russia e.g. Hardware Security modules were prohibited a while ago

Also Russian gov-t prohibited any open wireless stations, which also means more secured and robust networking solutions like meshnetworking are prohibited

Vulnerable services

Services advertised as security concerned can be vulnerable
E.g. widely-advertised Telegram messenger is flawe by-default since it depends on mobile network operator and gives access to your account to anyone in the company who can e.g produce new sim card
Also it is technically possible to intercept the SMS

Vulnerable services

All the widespread desktop operating system have totally broken security system
E.g.

- the concept of “superuser”, i.e. elevating program’s rights to do whatever it wants
- lack of isolation
- &c

Poisoned in foundation

Most of contemporary communications and computing systems
are extremely vulnerable and fragile
Mainly because of centralisation

Poisoned in foundation. IP

1. Global routing table is so huge for a single router
2. Centralisation; a few registered organisation control entire internet
   - 2.1 Political influence: governments are already using centralisation to build up an iron maiden

   E.g. when egyptians risen up, egyptian government just had the Internet shut down, to prevent events coverage

   - 2.2 Fragility: you only need to destroy a few objectives to start an apocalypse

Poisoned in foundation. DNS

(for technical limitations) there are only 13 DNS clusters serving ENTIRE internet

Again vulnerable to both political repressions and all the kinds of denial of service attacks

Poisoned in foundation. SSL

Uses multiple Central Authorities for verification

These are ruled by corporations and governments, you by definition cannot trust them

Star topology

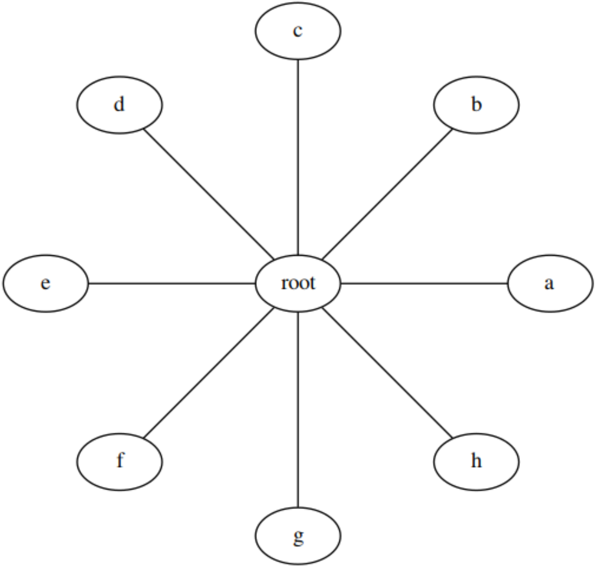


Figure 6: star connected

Star topology

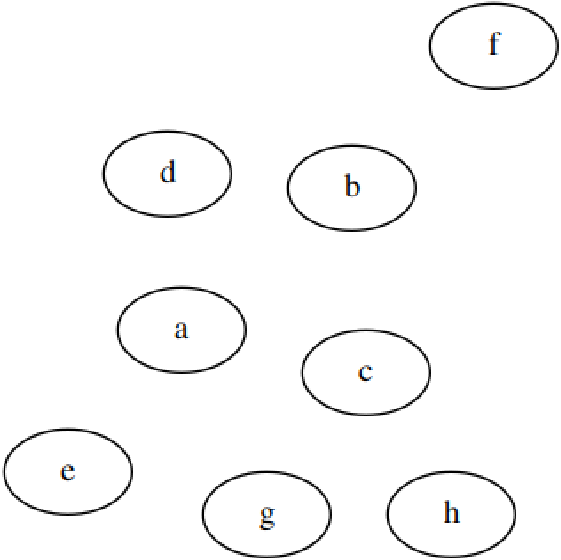


Figure 7: star disconnected

Protection

Free software

First of all, REJECT all the software and hardware that restricts your freedom
In eighties RMS started GNU movement, for developing GNU system, which would respect four main user' freedoms

0. Freedom to run program as you wish
1. Freedom to study program and to change it so it does what you wish
2. Freedom to redistribute exact copies
3. Freedom to distribute modified versions

Free software