Towards A Clean Slate

Digital Sovereignty in the Post Snowden Era

Alexander von Gernler

<gernler@genua.de>

Munich Internet Research Retreat

Raitenhaslach, November 24/25, 2016

Disclaimer

The views presented in this talk are rather my own as
GI Junior Fellow and Open Source activist
than the ones of my company.

And nothing presented here is new.
It is just mostly overlooked or forgotten.

So prepare for a quick recapitulation.

Digital Sovereignty

Attempt of Definition

- Term Digitale Souveränität in use in German politics and media since Snowden's revelations of NSA attack on communication infrastructure
- exact meaning unclear, but tries to suggest security
- usually employed synonymously with Staatliche Digitale Souveränität
  - cf. Hack of German Bundestag
  - cf. ensuring „cyber" capabilities of German military
  - cf. more budget for state agencies
- But! Mostly left out: Personal Digital Sovereignty
- What is that? We try covering this in the rest of the talk!

Symptom: Hardware no longer trustworthy

Laptop, Workstation, Server, Smartphone, Tablet? Does not matter – you're 0wned.

- Intel Management Engine (ME): Black Box in every computer
- UEFI: Uncontrollable Monster that also boots your machine
- Controllers everywhere: graphics, keyboard, hard disk, SD card
- Digital Rights Management (DRM)
- „Secure" Boot: Mostly your vendor's platform lockin strategy

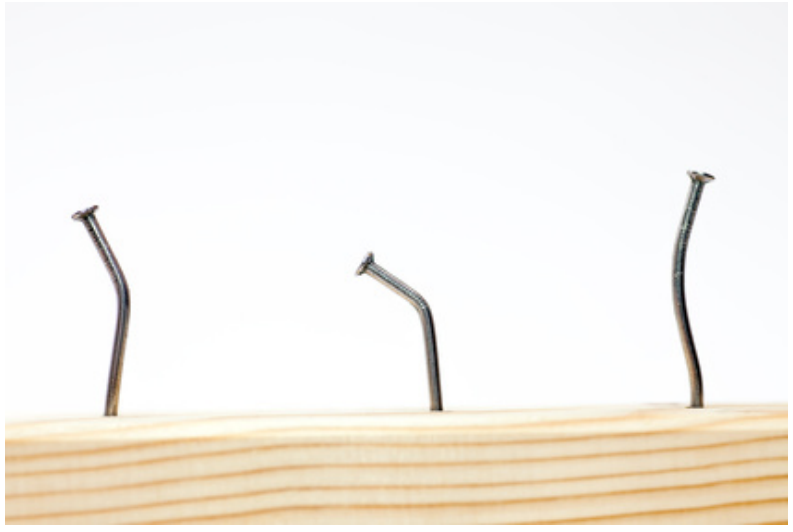
$\Rightarrow$ The user is now only a guest on his very own computer

Symptom: Always On, Full Service

Switching off your machine was yesterday

- DOS-based PC from the early nineties
  - hard disk would make loud noise upon activity
  - was switched off at night
  - could do (mostly) one task at a time
  - no big source of surprise to average user
- today's Smartphone/Tablet/Ultrabook
  - always on
  - battery non-removable
  - (mostly) always online
  - software running without user's control or consent

Personal Digital Sovereignty: Who cares, anyway?



- Not my department?
  - Meh, what's the worst that could happen?
  - Some vendors controlling my computer, so what?
  - Don't you have more serious problems?

Gazing into the abyss

- computers/mobile devices today indispensable
  - personal diary
  - container of personal correspondence
  - access to your bank account
  - place of forming your political opinion
  - German: *Kernbereich privater Lebensgestaltung*
  - home of your digital persona
  - oracle to answer all your open questions
- without trustworthy platform: democracy at stake!
  - free access to information without being watched
  - free expression of opinion and discrete exchange with other people

The Consequences

Chilling Effects: Users adjust their behaviour when they suspect being watched. A study of Canadian Researchers (Heise, April 2016) indicates that after Snowden's revelations, specific pages on Wikipedia are 30% less accessed than before – mainly pages on bombs, terrorism and the like.

Enter the Stakeholders

If you install a feeder, the pigs will gather


...

- Internet giants performing a lock in strategy
  - Each and every transaction should stay on *their* platform
  - They don't mind having access to your device, if unavoidable
- On your computer, elections are decided!
  - citizens gather information using computers: filter bubble
  - discuss political issues using computers: chilling effects
- Civil Liberties at Stake!
  - your device trojaned by default for your own security?
  - actually imaginable, cf. *National Security Letters* in the US
  - In Germany only restricted through missing resources, not ethical hesitations

What should be done?

- In my opinion, integrity and confidentiality of people's very own computing platforms should be an inalienable human right
- German federal constitutional court established this as a German basic right
- It is mostly overlooked by now
- Devices required to be neat and shiny, not secure and trustworthy
- Clean Slate Approach seems to be promising
- And we (that is, you) should start working on it today

Ways out, anyone?

Purism

- Open Hardware: Purism Librem, Novena, RISC-V, Raptor Talos
- Open Source Software: Linux, *BSD, L4 family
- Sensible Designs of Systems: Microkernels, Capabilities
- Waking up society: The revolution will not be televised (unfortunately)

RISC-V

TALOS™


mitmischen.de
Flirten, Lästern, Tratschen.
Und niemand hört mit.
»Dem Fernmeldegeheimnis unterliegen der Inhalt
der Telekommunikation und ihre näheren Umstände [...]«
§ 85 Abs. 1 Telekommunikationsgesetz, beschlossen vom Deutschen Bundestag
Entscheidungen für die Freiheit. Deutscher Bundestag.