No IT security without Free Software

How openness contributes to security

Max Mehl – Programme Manager – @mxmehl

3 July 2019 – Pass the SALT

Free Software Foundation Europe is a charity that empowers users to control technology.

Free Software

fsfe

USE

The software can be used for any purpose without restrictions.

STUDY

The software and its code can be analysed by anyone

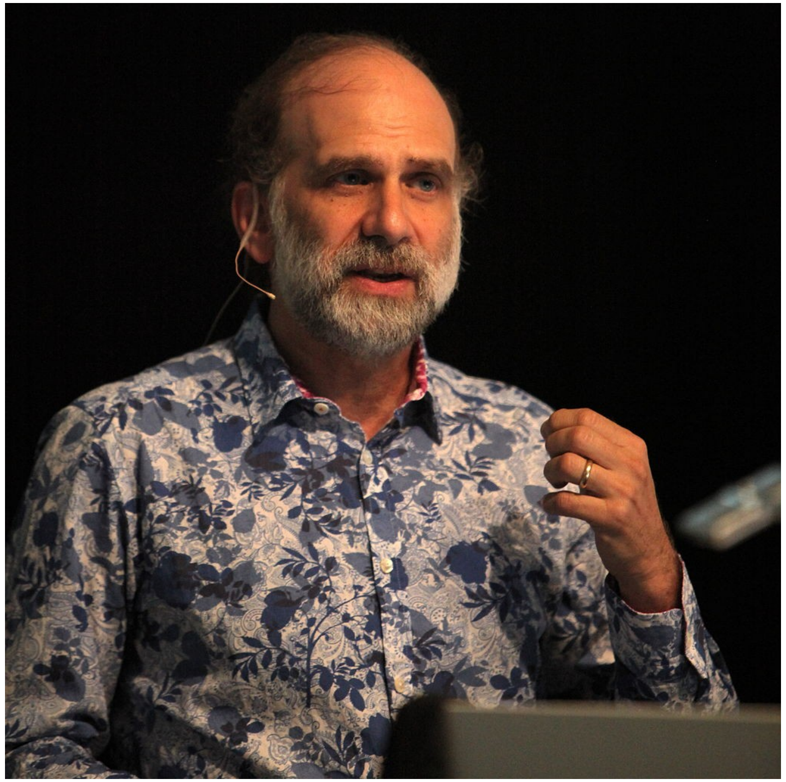
SHARE

The software can be shared without limitations. The price doesn’t matter.

IMPROVE

The software can be modified by you or others to give back to the community.

What is IT security?

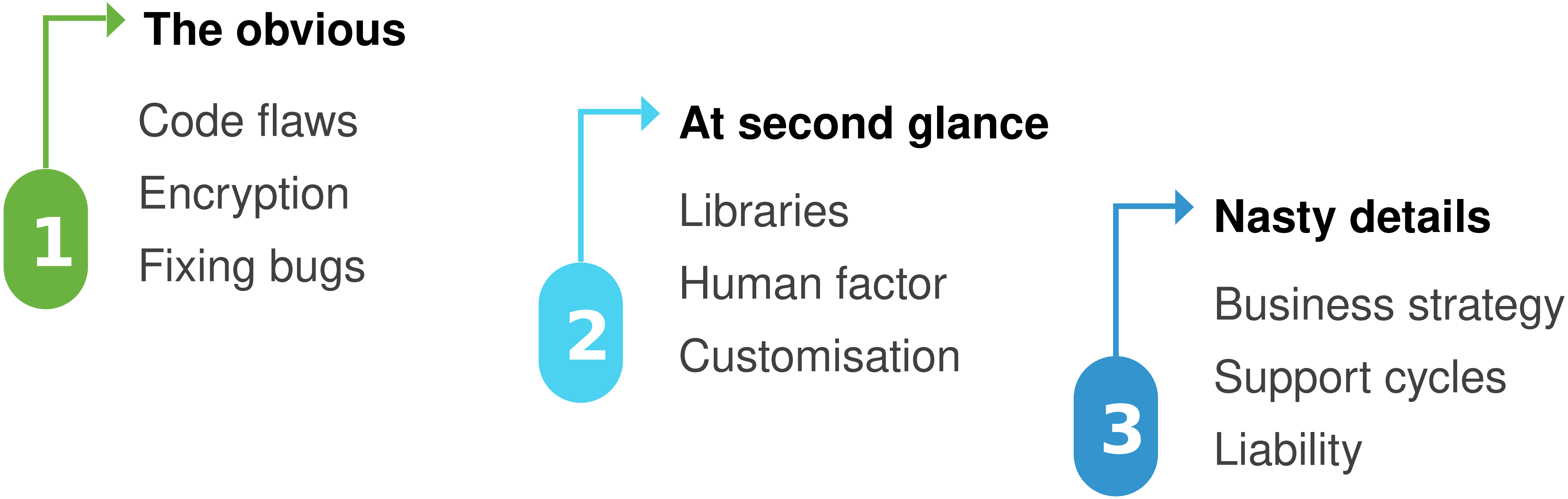


„Security is not a product;
it itself is a process.“

– Bruce Schneier in „Secret & Lies“, 2000

Photograph by Rama, Wikimedia Commons, Cc-by-sa-2.0-fr

IT security as a process



1 **The obvious**

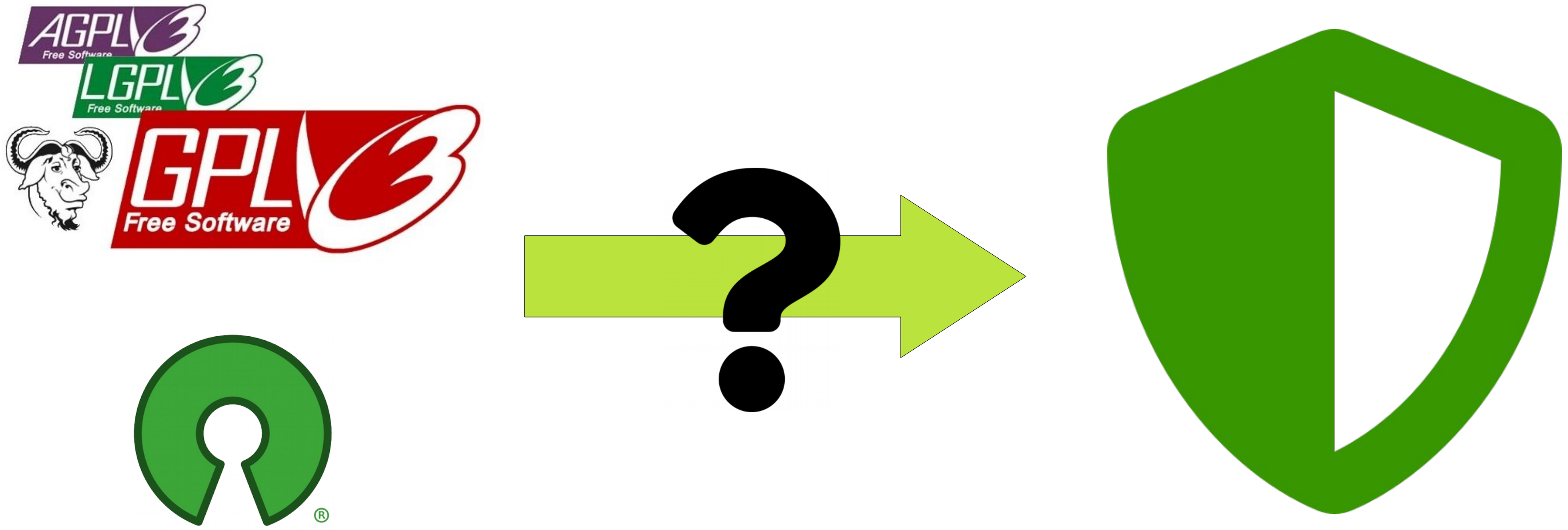
- Code flaws
- Encryption
- Fixing bugs

2 **At second glance**

- Libraries
- Human factor
- Customisation

3 **Nasty details**

- Business strategy
- Support cycles
- Liability


AGPLv3
Free Software
LGPLv3
Free Software
GPLv3
Free Software
?
®

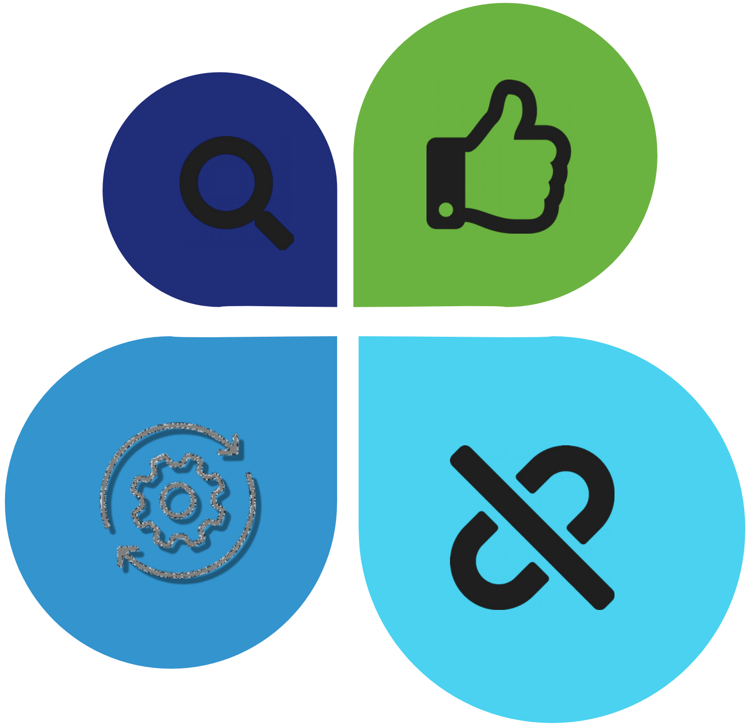
Security benefits through Free Software

Transparency for all

Independent security audits increase trust, also internally.

Outside pressure

When publishing code, one better look a bit closer.



Sharing synergies

Other users and the community take interest and contribute.

Independence

Issues can be solved on one’s own, or a project forked if necessary.

Free Software is a necessary, but not sufficient component of IT security

Considerations

Responsibilities

Who is responsible for security in shared projects? How to deal with external libraries?

Degree of reuse

Usage of many external Free Software modules, or rather smaller but custom software?

„National security“

Is there software whose release would be disadvantageous?

Other components

Free Hardware, reproducible builds, and other security processes are important as well.

Common counterarguments

fsfe

„Free Software only with non-critical things!“

NO, trust and open processes are all the more crucial for critical and public infrastructure.

„Free Software is only by and for hobbyists!”

NO, see Linux kernel, RedHat, Apache, Microsoft, virtualisation, CMSs...

„Public source code = Risk”

NO, “security by obscurity” has been proven wrong. Source code can often be reconstructed.
→ Kerckhoffs’ principle

“Business secrets”

Yes and no, but usually not problematic, often even beneficial.

Example Huawei

Concerns with 5G infrastructure

- Free Software fosters trust
- Independent security audits possible
- Agencies can share work
- Competition as additional pressure
- Also important: reproducability, free hardware
- Unrealistic? Perhaps today, but not in the intermediate and long term.

Advantages of Free Software

Thank you!

fsfe

Thanks to all FSFE supporters who enable our work. Join them!

fsfe.org/support

Max Mehl | max.mehl@fsfe.org | @mxmehl (Mastodon, Twitter...)