Sicherheit für alle:

Was kann ein TPM ?

Andreas Fuchs
Fraunhofer-Insitut für Sichere Informationtechnologie

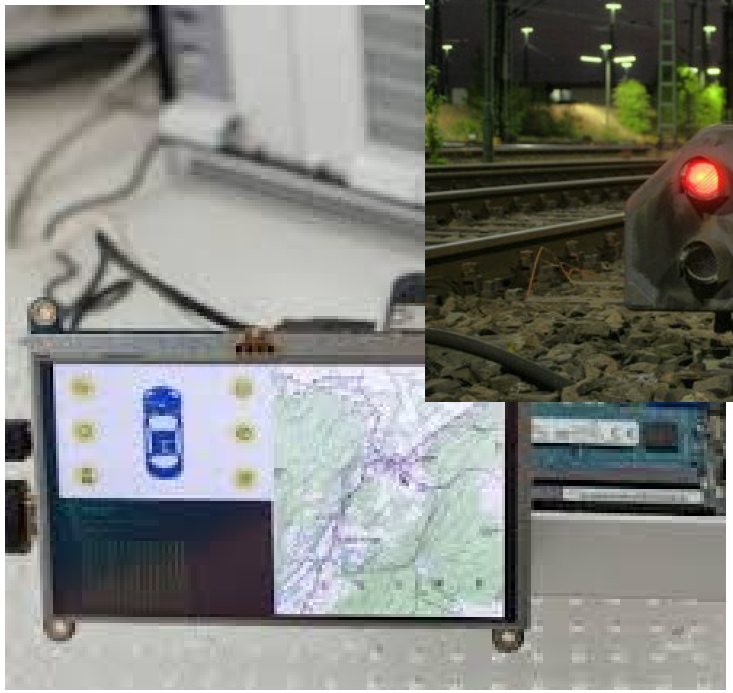
2020-01-22 – Berlin
OmniSecure 2020

Vorstellung

- **Andreas Fuchs (@sit.fraunhofer.de)**
  - Deputy Head of Department Cyber-Physical Systems and Automotive Security
  - Head of Research Group Trustworthy Platforms
- **TPM-consumer for 13 years**
- **TCG (Trusted Computing Group) member**
  - TSS (TPM Software Stack) workgroup chair
  - 2017 TCG leadership award
- **tpm2-software project maintainer**
  - tpm2-tss
  - tpm2-tss-engine
  - tpm2-totp

Vorstellung

- **My job: “Put TPMs into things”**

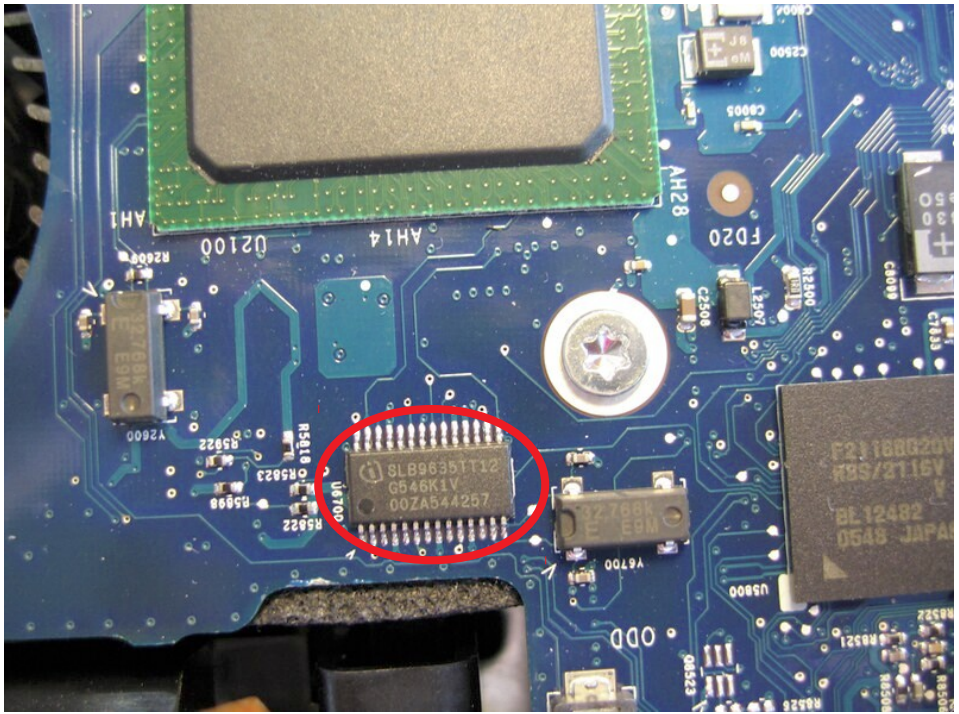


Agenda

- **Was ist ein TPM ?**
- **Was kann ein TPM ?**
- **Was kann man mit einem TPM machen ?**
- **Wie geht es weiter ?**

Was ist ein TPM (2.0) ?

- **Security Chip on Mainboard**
- **Part of every Windows-Logo PC.**
- **(Pretty) High security**
  - Common Criteria and such
  - except RSA-prime, tpm.fail, ...
- **Capable of crypto, (some) storage and recording boot’s hash values**
- **It’s passive !**



Picture by Paolo Attivissimo via flickr CC-BY

Was ist ein TPM ?

- **TPMs reputation**

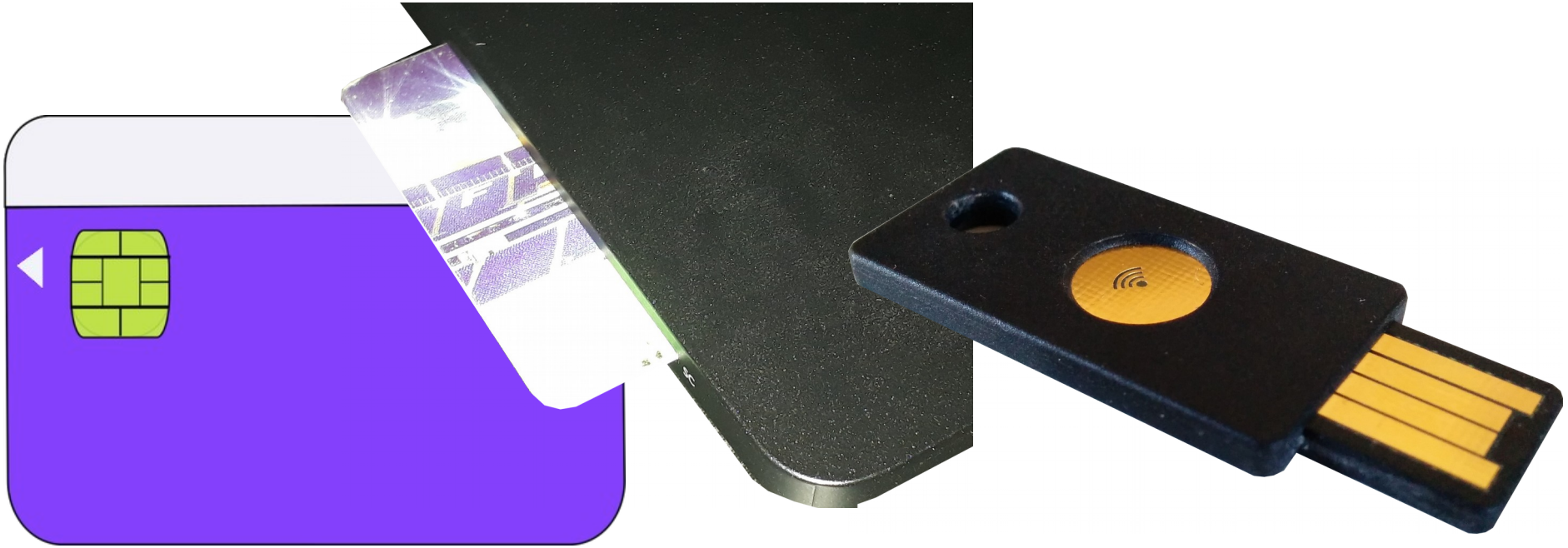
  “DRM devices that remote control our PCs”

- **TPMs in reality**
  - “Embedded SmartCards”
  - Integrity reporting / attestation capabilities
- **Stallman/GNU**

  [..] Therefore, we conclude that the “Trusted Platform Modules” available for PCs are not dangerous, and there is no reason not to include one in a computer or support it in system software. [..] https://www.gnu.org/philosophy/can-you-trust.en.html

Was ist ein TPM ?

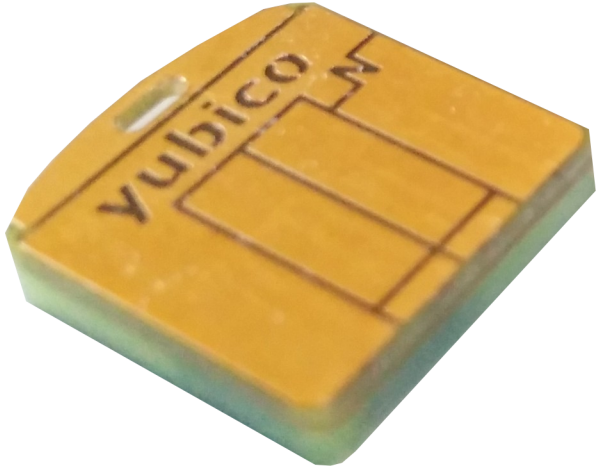
- **Something like a SmartCard**



Yubikey by Wikipedia-Commons / Autopilot CC-BY-SA

Was ist ein TPM ?

- **A allways-on SmartCard**



Yubikey by Wikipedia-Commons / Autopilot CC-BY-SA

Was kann ein TPM ?

- **Secure storage for (cryptographic) keys**
  - (Main-CPU) Software never knows the keys (during storage)
- **Secure en/decryption and signature operations**
  - (Main-CPU) Software never knows the keys (during usage)
- **Secure key generation**
  - (Main-CPU) Software never knows the keys (during generation)
- **Secure data storage**
  - … for small amounts of data (a few hundred bytes)

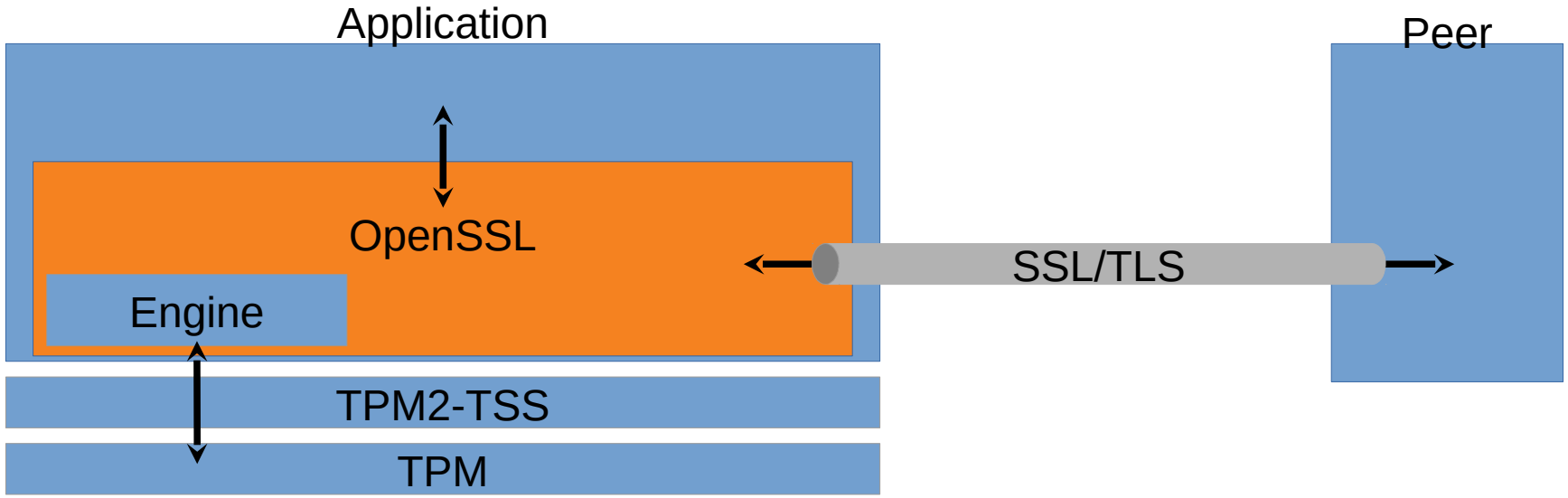
Was kann ein TPM ?

- **Enhanced Authorization Policies**
  - A (logical expression) policy language with AND and OR
  - Enables e.g. for 4-eye principle or access deference
  - Efficient implementation, yet easy definition language in JSON
- **Store a measurement of started software and sign it (Remote Attestation)**
  - Only stores a hash-chain of values reported by the CPU (no active inspection of the CPU)
  - Signing of hash-chain is used as Integrity Evidence

Was kann ich mit einem TPM machen ?

- **Example: Key protection**
  - Keys in RAM are always dangerous → “Heartbleed”
  - Keys on Disk are always dangerous
    - You can protect them with user passwords
      but they can be bruteforced
    - Servers have no unlock step for user interaction
    - Embedded devices have no unlock step
  - Thus keys are at risk for
    - Offline-copying or online-extraction
    - Consequences: Device impersonation or cloning

Was kann ich mit einem TPM machen ?
Example OpenSSL



- **Aufbau eines OpenSSL-Servers / Clients**

Was kann ich mit einem TPM machen ?
Example OpenSSL: tpm2-tss-engine

- **Generate a key**

  tpm2tss-genkey mykey-engine.pem

- **Generate a (self-signed) certificate**

  openssl req -new -x509 -engine tpm2tss -key mykey-engine.pem -keyform engine -out mykey-engine.crt

- **Configuring nginx**
  - /etc/nginx/sites-enabled/default:

    ssl_certificate = /home/andreas/mykey-engine.crt;
    ssl_certificate_key = engine:tpm2tss:/home/andreas/mykey-engine.pem;
  - /etc/nginx/nginx.conf:

    ssl_engine = tpm2tss;

Was kann ich mit einem TPM machen ?

- **Hard-Disk encryption (with or without password)**
  - “Bitlocker for Linux” with shorter passwords
  - Data Center: Prevent stealing of HDDs from the rack
  - Secure embedded devices’ storage
- **Credential protection**
  - VPN access security (OpenConnect and OpenVPN via tpm2-pkcs11)
  - SSH connection protection (via tpm2-pkcs11)

Common theme: Prevent credential leaks

Wie geht es weiter ?

- **TPMs are becoming the most general and generic Security Solution**
  - Unified (security) functionality set
  - Unified hardware interfaces (via SPI bus)
  - Unified software interfaces (the TSS)
  - Universal software interfaces
    - C/C++, python, rust, go, ...
  - Universal application inclusions
    - OpenSSL (most HTTPS servers), PKCS11 (most HTTPS clients), VPNs (OpenConnect, OpenVPN, ...), ...

Wie geht es weiter ?

- **https://tpm2-software.github.io**
- **https://tpm2-software.github.io/software**

Question time