Starke Identität und Sicherheit von IoT Geräten

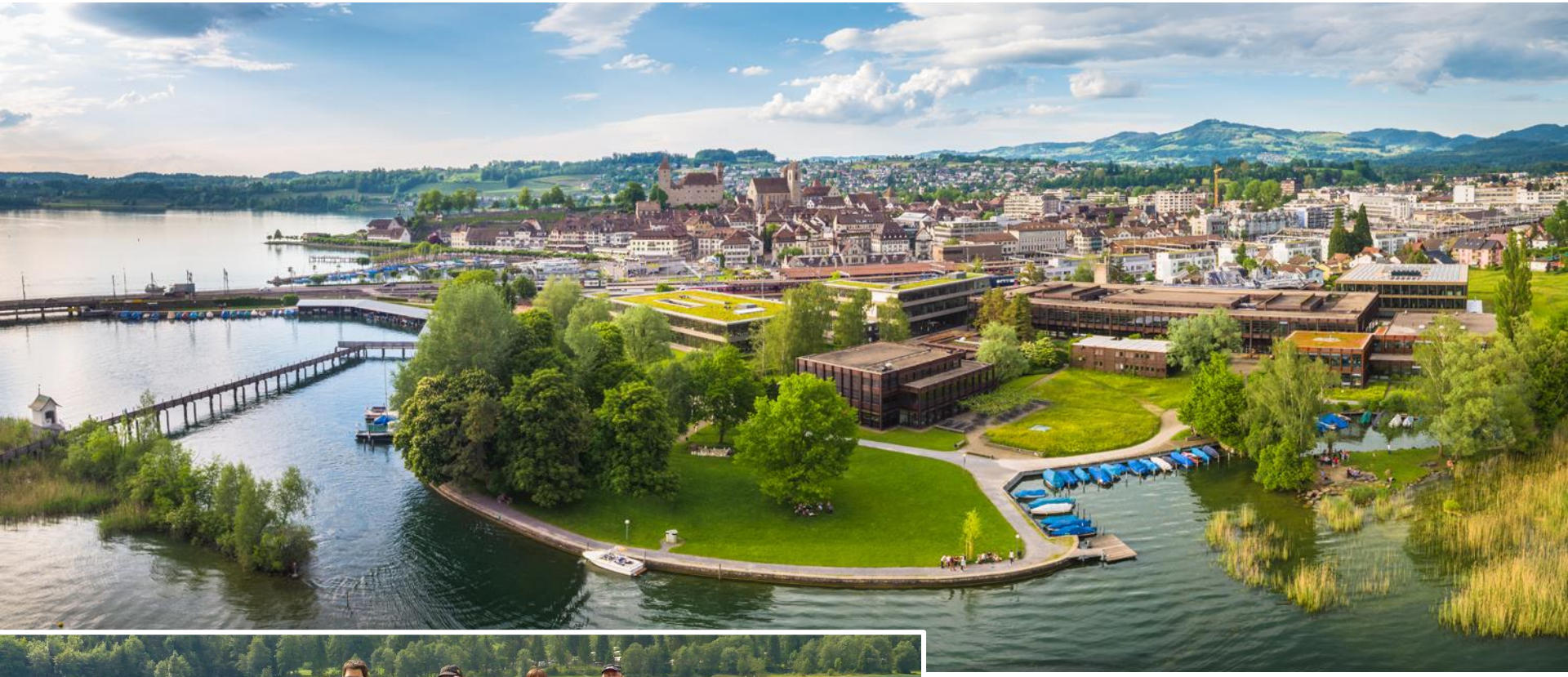
Information Security in Healthcare, 7. Juni 2018, Rotkreuz

Prof. Dr. Andreas Steffen
Institute for Networked Solutions
HSR Hochschule für Technik Rapperswil

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

HSR - Hochschule für Technik Rapperswil

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz



Internet of Things (IoT)

Angriffe auf IoT Geräte und Netzwerke

- Überwachung der Netzwerkkommunikation
  - Abhilfe: Verschlüsselung der Kommunikation (z.B. via SSL/TLS, IPsec)
- Gezielte Manipulation der Netwerkkommunikation
  - Abhilfe: Datenintegrität der Kommunikation (z.B. via SSL/TLS, IPsec)
- Einschleusen von fremden, potentiell bösartigen IoT Geräten
  - Abhilfe: Starke Geräte-Identität (X.509 Zertifikate, Device Secrets)
- Unterwanderung eigener IoT Geräte durch Malware
  - Abhilfe: Überprüfen des Gesundheitszustands (Attestation)

Kritische IoT Anwendungen

- Erzeugung und Verteilung von Energie (Energy Grid)
  - Totalausfall führt innert Tagen zum Zerfall unserer Zivilisation (Blackout)
- Transportwesen
  - Angriffe auf autonome Fahrzeuge (Lastwagen und Personenwagen)
- Flugzeugindustrie
  - Einbau von Kill-Switches bei der Flugzeug-Fertigung (Boeing, Airbus)
- Prozesssteuerung
  - Sabotage von Produktionsprozessen (z.B. Stuxnet im Iran)
- Gebäudeautomatisation
  - Erpressung via Übernahme von Sensoren und Steuerungen
- HealthTech
  - Angriffe auf Herzschrittmacher, Insulinpumpen und weitere medizinische IoT Geräte

Starke Identität und Sicherheit von IoT Geräten

Information Security in Healthcare, 7. Juni 2018, Rotkreuz

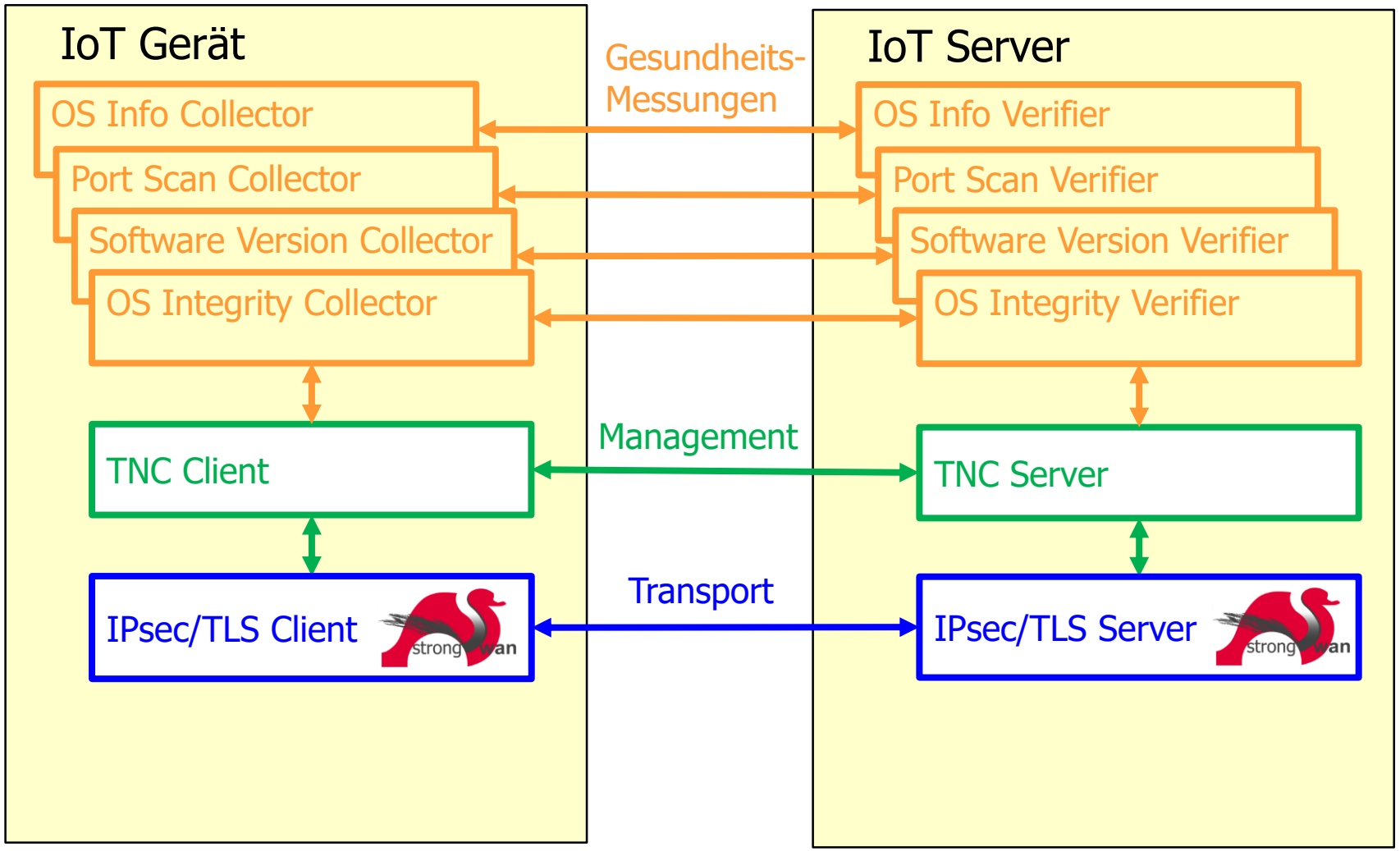
Starke HW-Identität und Attestation via Trusted Platform Modul (TPM)

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

strongswan

Trusted Network Connect (TNC) Architektur



www.trustedcomputinggroup.org
www.strongswan.org/tnc

IETF Network Endpoint Assessment (NEA)

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- TNC Messdaten

```
[IMV] operating system name is 'Android' from vendor Google
[IMV] operating system version is '4.2.1'
[IMV] device ID is cf5e4cbcc6e6a2db
```

- TNC Mess-Protokoll — PA-TNC (RFC 5792)

```
[TNC] handling PB-PA message type 'IETF/Operating System' 0x000000/0x00000001
[IMV] IMV 1 "OS" received message for Connection ID 1 from IMC 1
[TNC] processing PA-TNC message with ID 0xec41ce1d
[TNC] processing PA-TNC attribute type 'IETF/Product Information' 0x000000/0x00000002
[TNC] processing PA-TNC attribute type 'IETF/String Version' 0x000000/0x00000004
[TNC} processing PA-TNC attribute type 'ITA-HSR/Device ID' 0x00902a/0x00000008
```

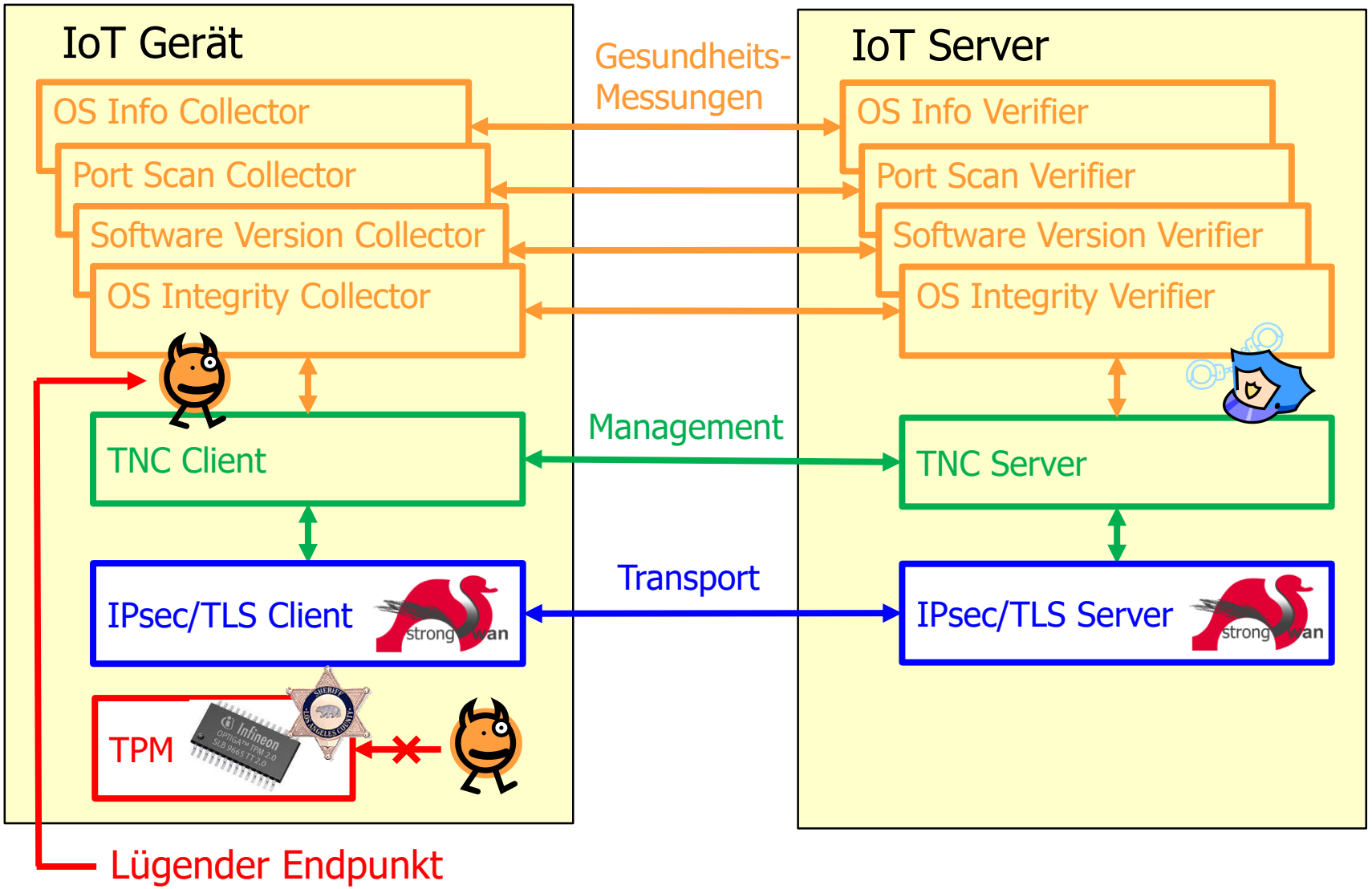
- TNC Client-Server-Protokoll — PB-TNC (RFC 5793)

```
[TNC] received TNCCS batch (160 bytes) for Connection ID 1
[TNC] PB-TNC state transition from 'Init' to 'Server Working'
[TNC] processing PB-TNC CDATA batch
[TNC] processing PB-Language-Preference message (31 bytes)
[TNC] processing PB-PA message (121 bytes)
[TNC] setting language preference to 'en'
```

- TNC Transport-Protokoll — PT-TLS (RFC 6876), PT-EAP (RFC 7171)

```
[NET] received packet: from 152.96.15.29[50871] to 77.56.144.51[4500] (320 bytes)
[ENC] parsed IKE_AUTH request 8 [ EAP/RES/TTLS ]
[IKE] received tunneled EAP-TTLS AVP [EAP/RES/PT]
```

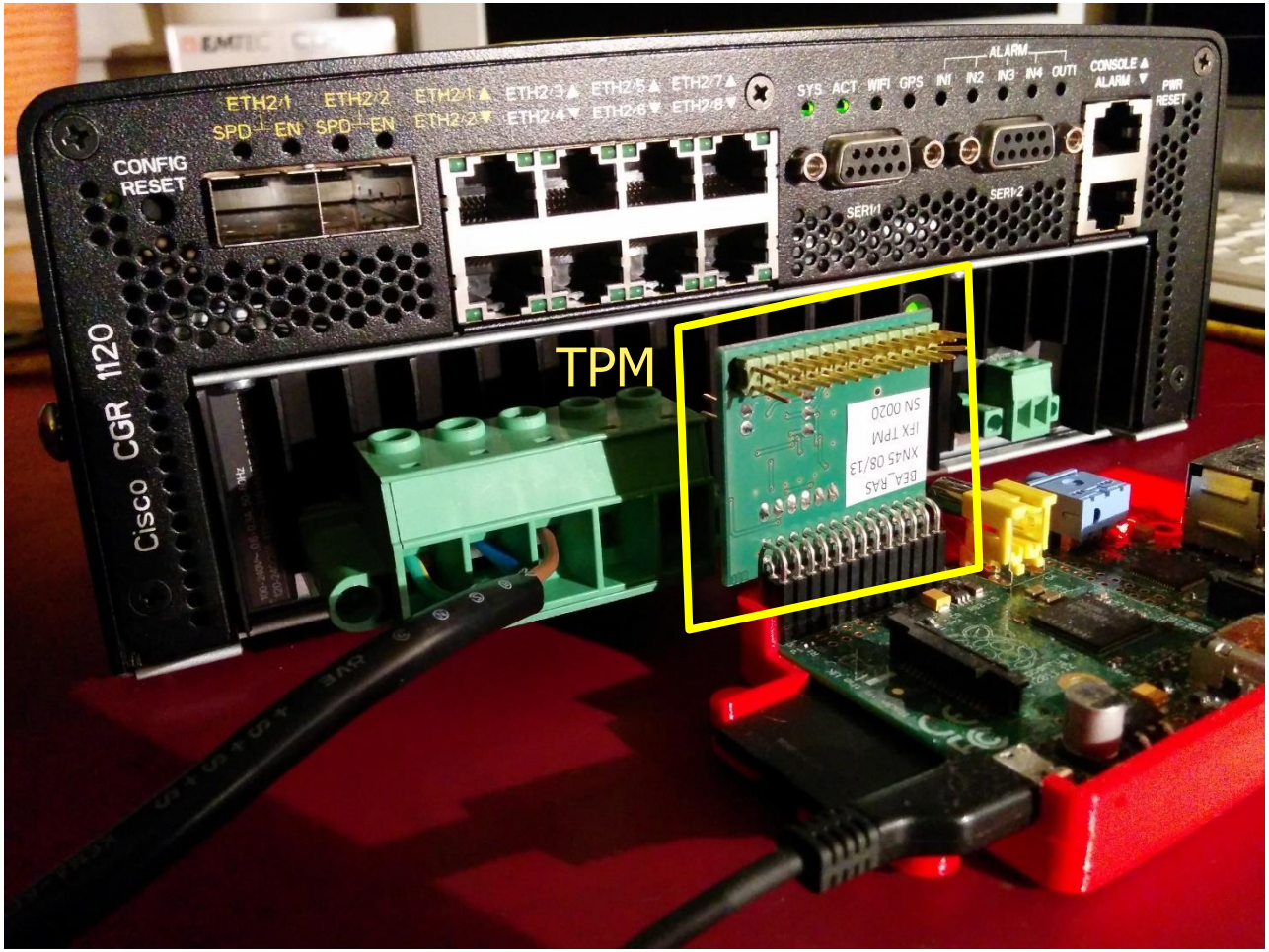
Problem des lügenden Endpunkts



Trusted Platform Module (TPM)

- Die meisten PCs haben ein TPM 2.0!
  - Microsoft verlangt ein TPM 2.0 für Windows 10.
  - TPM Chip Hersteller: Infineon, Nuvoton, STMicroelectronics.
  - Intel Core Prozessoren enthalten seit der vierten Generation (Haswell) ein Firmware TPM 2.0 (Platform Trust Technology - PTT).
  - TPM 2.0 Firmware läuft auch in der TrustZone eines ARM Prozessors.
- Features
  - Sichere Speicherung von privaten Schlüsseln und dazugehörigen X.509 Zertifikaten, die für eine starke Geräte-Identifikation verwendet werden können.
  - Vertrauenswürdiges Messen von Systemdateien über SHA256 Hashwerte, die durch das TPM in Platform Configuration Register (PCR) akkumuliert und mit einem Attestation-Schlüssel signiert werden.

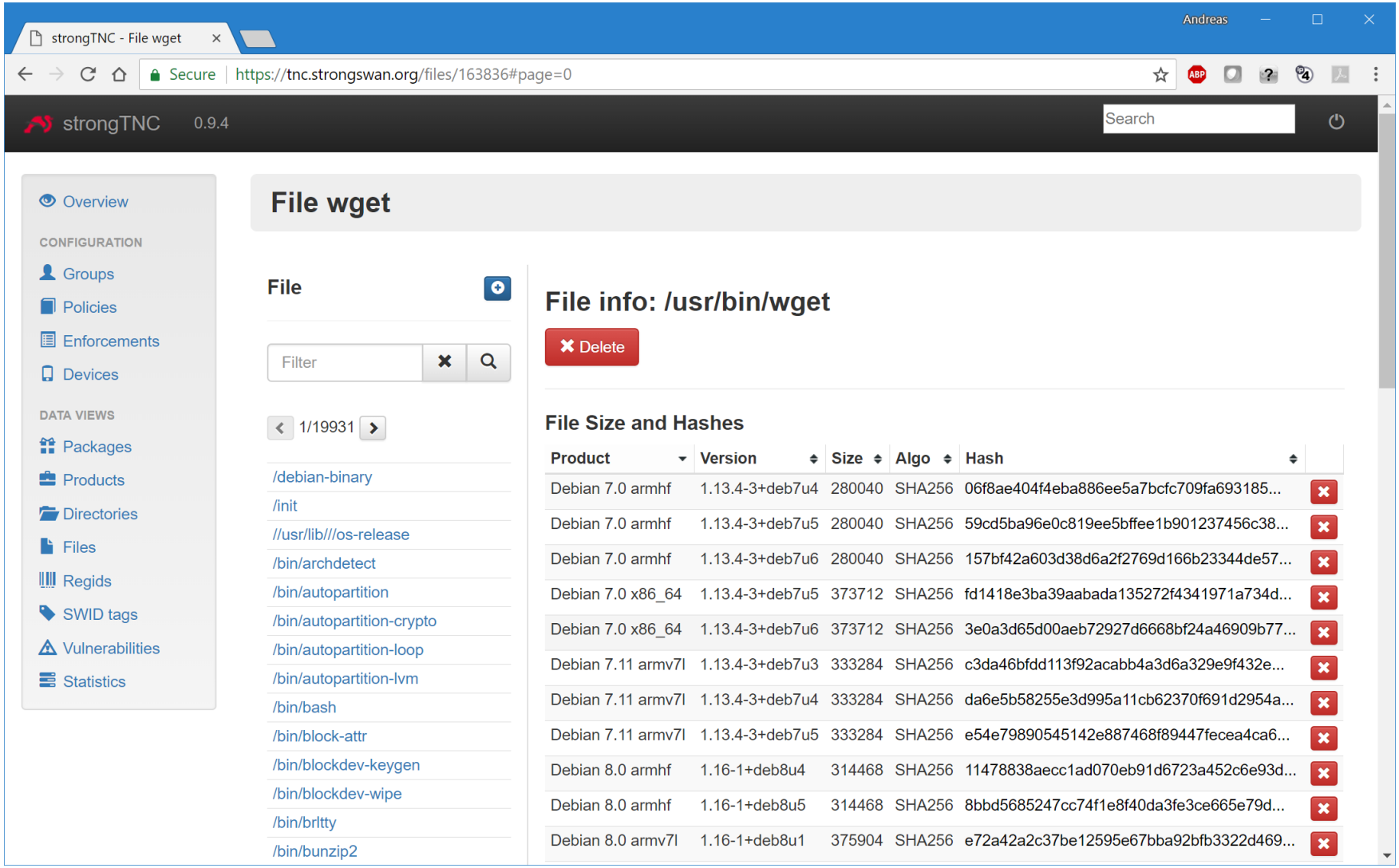
RSA Security Conference 2015, San Francisco



Cisco 1120 Connected Grid Router mit strongSwan
Mutual Attestation auf einem Linux Gast-OS.

strongTNC Security Automation - Referenzwerte

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

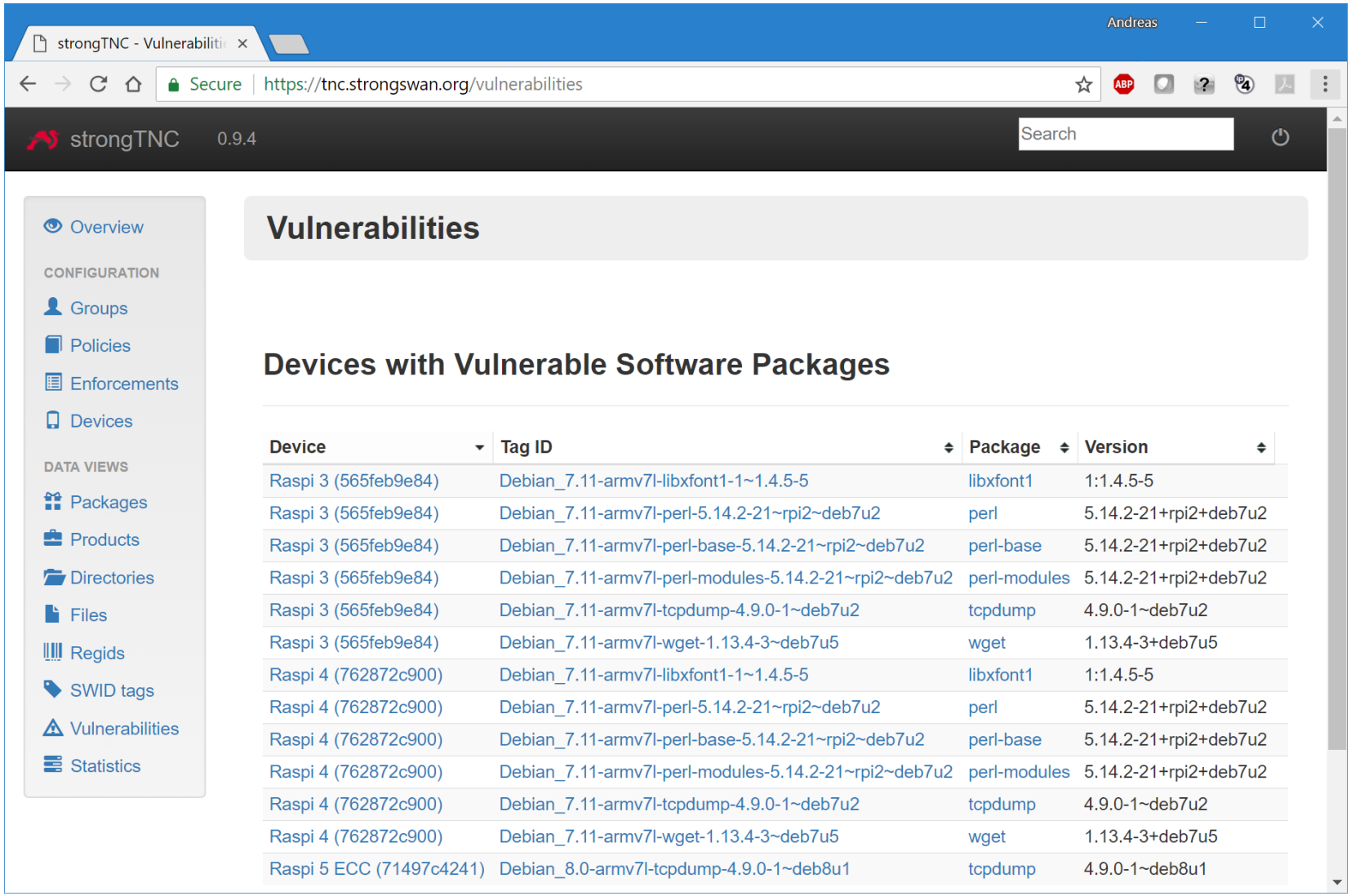


Software Management mit SWID Tags

- ISO/IEC 19770-2:2015 Software Asset Management Part 2: Software Identification Tag

```
<SoftwareIdentity xmlns="http://standards.iso.org/iso/19770/-2/2015/schema.xsd"
   xmlns:SHA256="http://www.w3.org/2001/04/xmlenc#sha256"
   xmlns:n8060="http://csrc.nist.gov/schema/swid/2015-extensions/swid-2015-extensions-1.0.xsd"
   name="libssl1.0.0" tagId="Debian_8.0-x86_64-libssl1.0.0-1.0.1t-1~deb8u8"
   version="1.0.1t-1+deb8u8" versionScheme="alphanumeric">
  <Entity name="strongSwan Project" regid="strongswan.org" role="tagCreator"/>
  <Meta product="Debian 8.0 x86_64"/>
  <Payload>
    <Directory name="x86_64-linux-gnu" root="/usr/lib">
      <File SHA256:hash="4de8f1690122d3ac5e836d0c60c8cf63c6e3bab20b5c8c385a8ea20774cc26d6"
        name="libcrypto.so.1.0.0" size="2070912"/>
      <File SHA256:hash="79f8dc203a5b81fe04c8bd37fa10dc92ee6cc92ae3f6cda1086028fc2aa907c4"
        name="libssl.so.1.0.0" size="395176"/>
    </Directory>
    <Directory name="engines" root="/usr/lib/x86_64-linux-gnu/openssl-1.0.0">
      <File SHA256:hash="1961870c4350e742c130187c62c93e0d096e4fd8c124e0a98cdd52416e42ddb2"
        name="lib4758cca.so" size="19512"/>
      ...
      <File SHA256:hash="a97cc3c75e2f59373b90ab1a431821bc94b755eba6643bdad59a047503257d03"
        name="libubsec.so" size="19784"/>
    </Directory>
    ...
  </Payload>
</SoftwareIdentity>
```

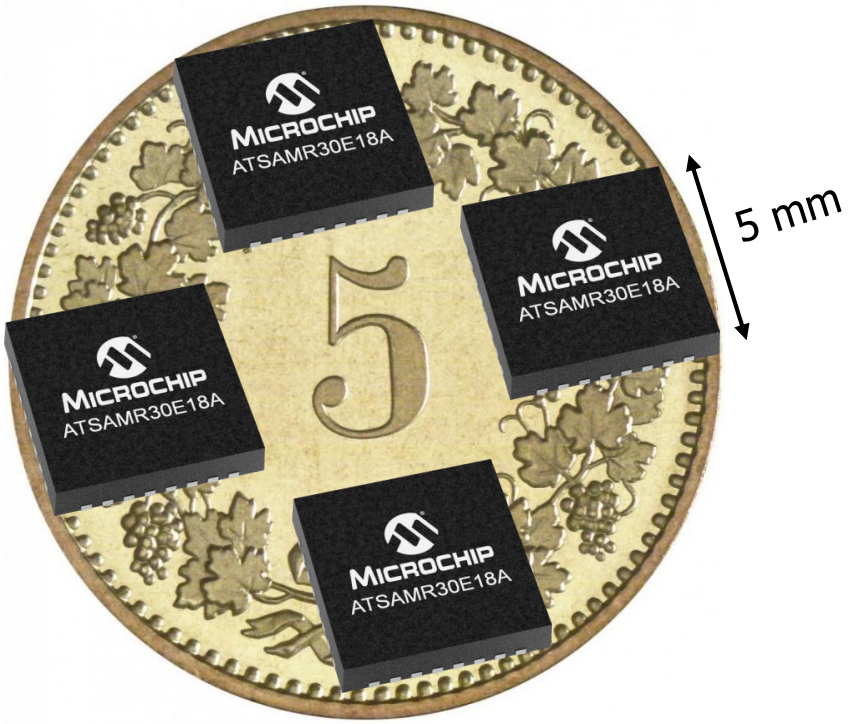
strongTNC Security Automation - Schwachstellen



Device	Tag ID	Package	Version
Raspi 3 (565feb9e84)	Debian_7.11-armv7l-libxfont1-1~1.4.5-5	libxfont1	1:1.4.5-5
Raspi 3 (565feb9e84)	Debian_7.11-armv7l-perl-5.14.2-21~rpi2~deb7u2	perl	5.14.2-21+rpi2+deb7u2
Raspi 3 (565feb9e84)	Debian_7.11-armv7l-perl-base-5.14.2-21~rpi2~deb7u2	perl-base	5.14.2-21+rpi2+deb7u2
Raspi 3 (565feb9e84)	Debian_7.11-armv7l-perl-modules-5.14.2-21~rpi2~deb7u2	perl-modules	5.14.2-21+rpi2+deb7u2
Raspi 3 (565feb9e84)	Debian_7.11-armv7l-tcpdump-4.9.0-1~deb7u2	tcpdump	4.9.0-1~deb7u2
Raspi 3 (565feb9e84)	Debian_7.11-armv7l-wget-1.13.4-3~deb7u5	wget	1.13.4-3+deb7u5
Raspi 4 (762872c900)	Debian_7.11-armv7l-libxfont1-1~1.4.5-5	libxfont1	1:1.4.5-5
Raspi 4 (762872c900)	Debian_7.11-armv7l-perl-5.14.2-21~rpi2~deb7u2	perl	5.14.2-21+rpi2+deb7u2
Raspi 4 (762872c900)	Debian_7.11-armv7l-perl-base-5.14.2-21~rpi2~deb7u2	perl-base	5.14.2-21+rpi2+deb7u2
Raspi 4 (762872c900)	Debian_7.11-armv7l-perl-modules-5.14.2-21~rpi2~deb7u2	perl-modules	5.14.2-21+rpi2+deb7u2
Raspi 4 (762872c900)	Debian_7.11-armv7l-tcpdump-4.9.0-1~deb7u2	tcpdump	4.9.0-1~deb7u2
Raspi 4 (762872c900)	Debian_7.11-armv7l-wget-1.13.4-3~deb7u5	wget	1.13.4-3+deb7u5
Raspi 5 ECC (71497c4241)	Debian_8.0-armv7l-tcpdump-4.9.0-1~deb8u1	tcpdump	4.9.0-1~deb8u1

Demonstriert am IETF Prag Hackathon im Juli 2017
auf Bitte von NIST und NSA

Low Power Single Chip IoT Devices



Cortex M0+ MCU & IEEE 802.15.4 Transceiver in a single package

256 KB flash / 32KB RAM, 8 KB Low Power Mode retained RAM

Ultra-low power consumption: 700 nA typical with RTC

Hardware AES Crypto Accelerators, True Random Number Generator

Price: 3.50 EUR

Starke Identität und Sicherheit von IoT Geräten

Information Security in Healthcare, 7. Juni 2018, Rotkreuz

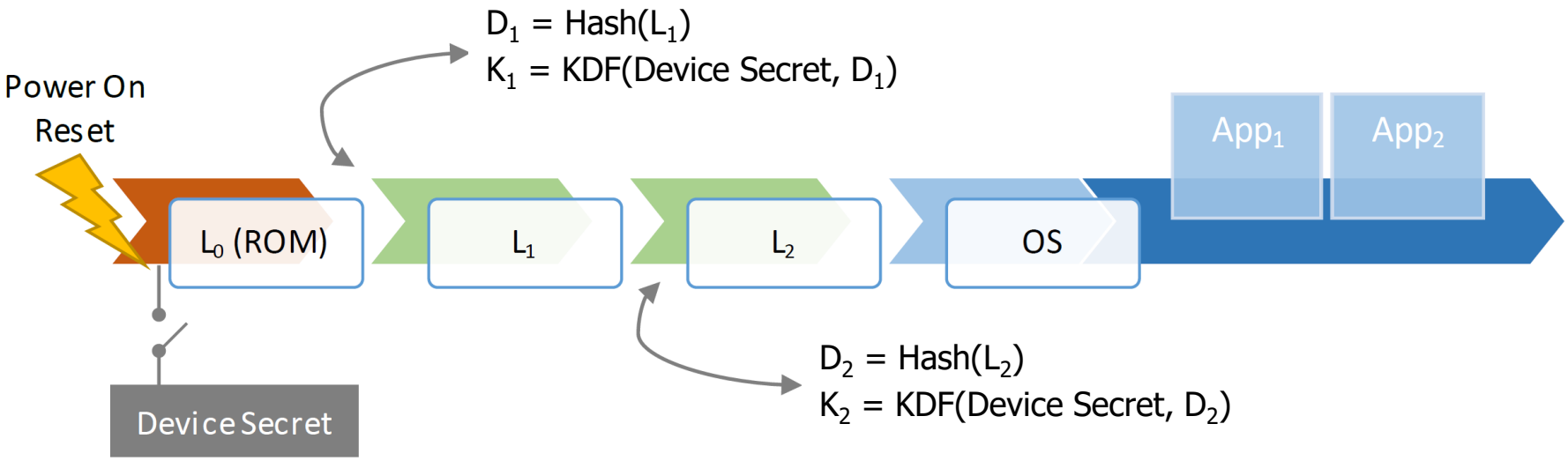
Starke HW-Identität und Attestation via RIoT (Robust IoT)

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

strongwan

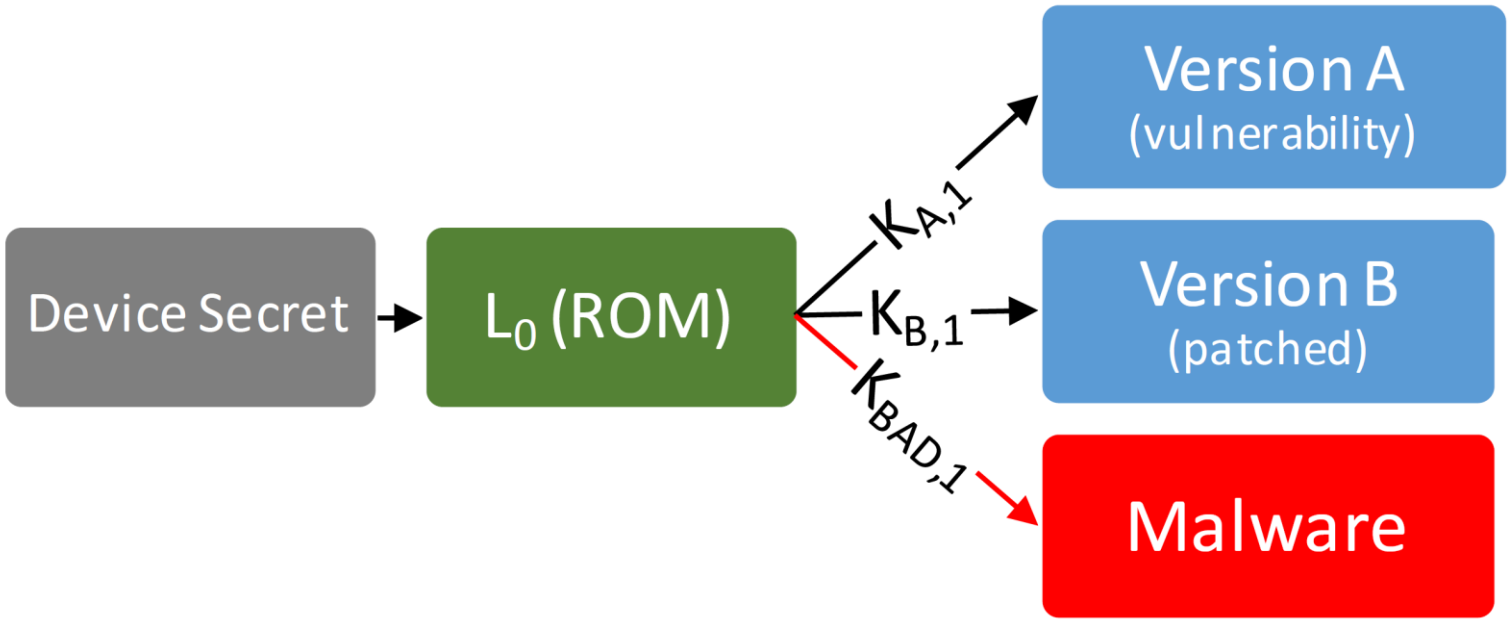
RIoT (Robust IoT) von Microsoft Research*



- Device Secret: 256…512 Bit unlöschbarer, zufällig generierter Geräteschlüssel, der nur durch die ROM Bootstufe L_0 lesbar ist.
- Hash Function: z.B. SHA256
- Key Derivation Function (KDF): z.B. HMAC-SHA256

*www.microsoft.com/en-us/research/publication/riot-a-foundation-for-trust-in-the-internet-of-things/

Einfache RIoT-basierte Attestation



- Kann auf Low Power IoT Devices realisiert werden (Hash/HMAC)
- Device Secrets werden auf einem zentralen Server gespeichert
- Single-Point of Attack ➔ Kann alle Device Secrets kompromittieren
- Falls die Rechner-Ressourcen ausreichen, sind aus dem Device Secret abgeleitete Public Keys (RSA/ECDSA) möglich.

Zusammenfassung

- TPM-basierte HW-Identität und Attestation verfügbar mit strongSwan/strongTNC Open Source Software
- RIoT-basierte HW-Identität und Attestation verfügbar für ausgewählte STMicroelectronics IoT Plattformen ab Herbst 2018
- Modulare Erweiterung auf weitere IoT Plattformen geplant

Fragen?