



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







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 Netzwerkkommunikation
 - **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

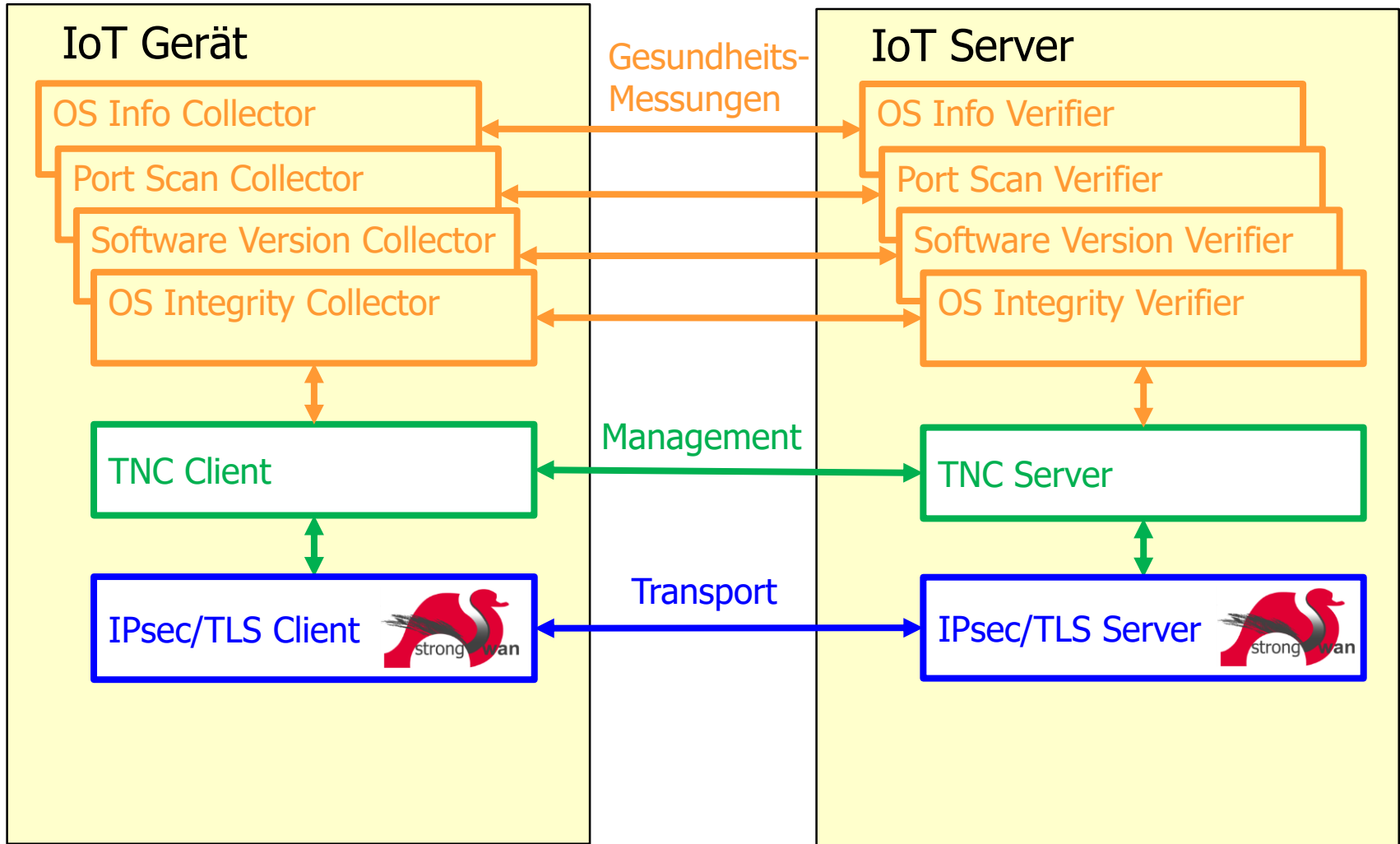
Information Security in Healthcare, 7. Juni 2018, Rotkreuz

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





Trusted Network Connect (TNC) Architektur



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



- 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'
```

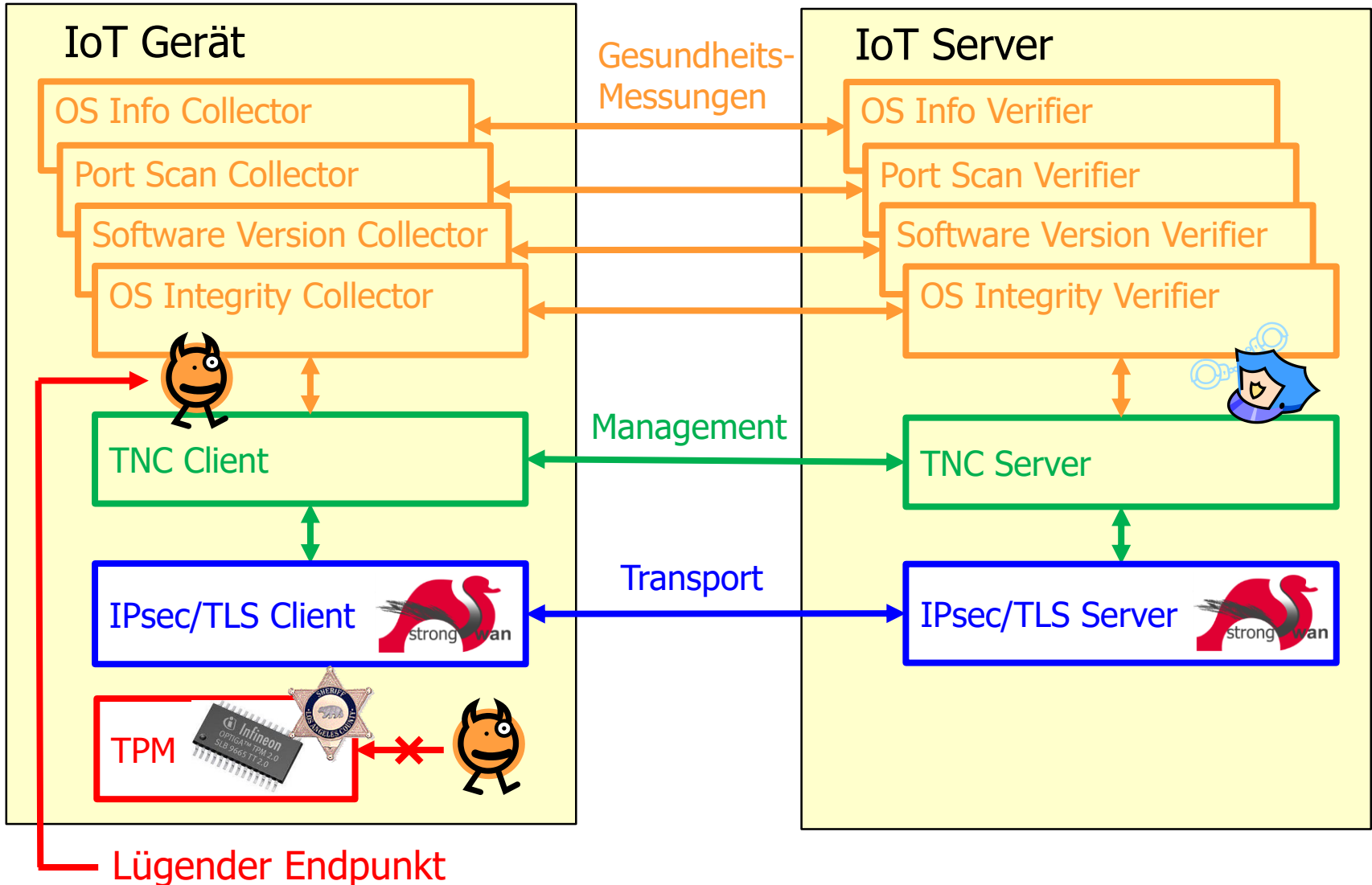
- TNC Transport-Protokoll

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





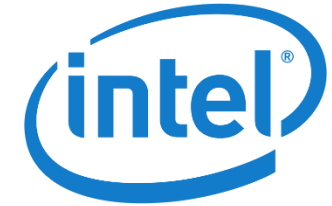
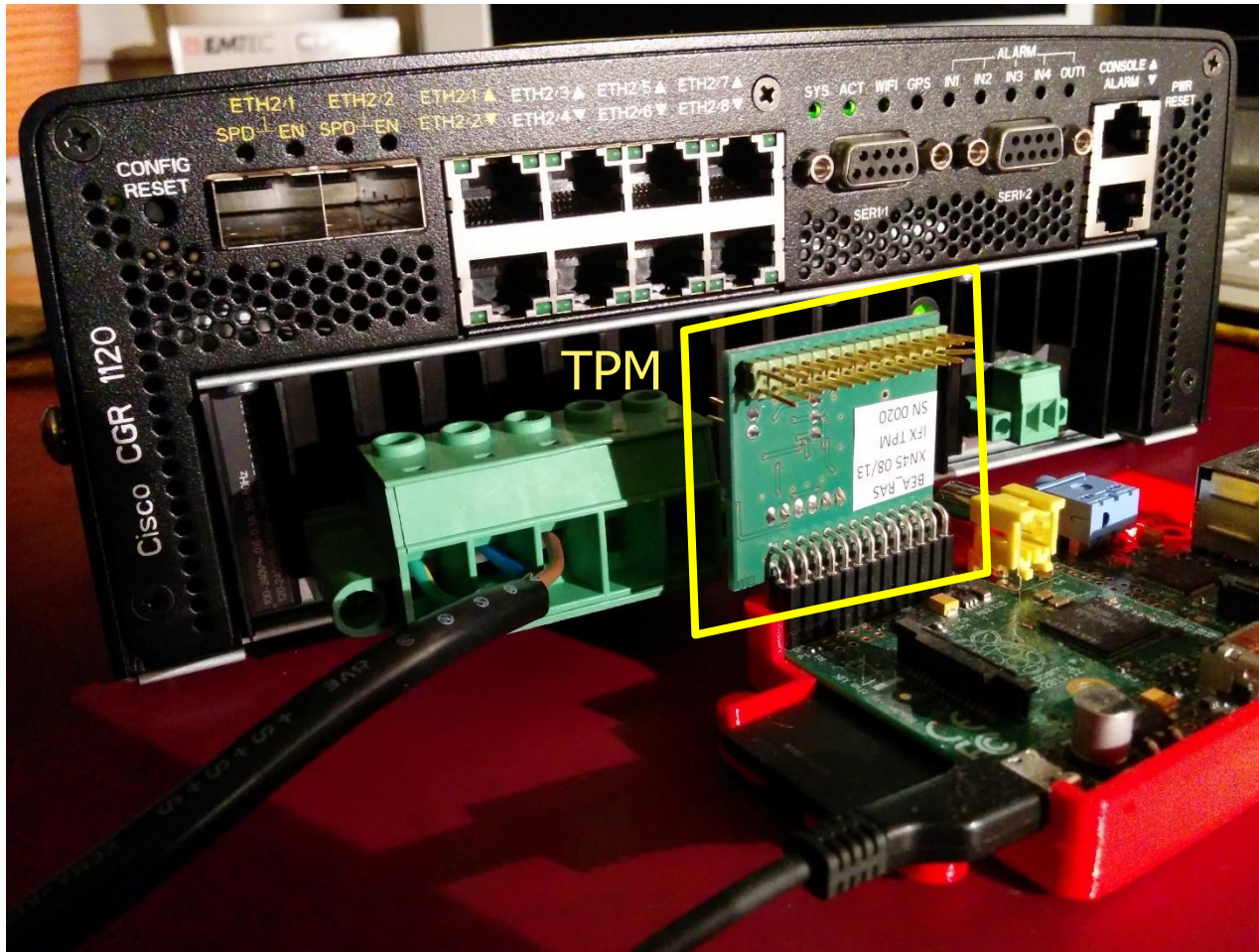
Trusted Platform Module (TPM)

- 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.
 - Vertrauenswürdigen 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.

The screenshot shows the strongTNC web interface. The browser address bar displays the URL `https://tnc.strongswan.org/files/163836#page=0`. The interface includes a sidebar with navigation options like Overview, Groups, Policies, and Enforcements. The main content area is titled "File wget" and shows a list of files under the path `/usr/bin/wget`. A "File info" section for `/usr/bin/wget` is visible, along with a "Delete" button. Below this is a table titled "File Size and Hashes" with columns for Product, Version, Size, Algo, and Hash. The table lists various Debian packages and their associated hashes.

Product	Version	Size	Algo	Hash
Debian 7.0 armhf	1.13.4-3+deb7u4	280040	SHA256	06f8ae404f4eba886ee5a7bcfc709fa693185...
Debian 7.0 armhf	1.13.4-3+deb7u5	280040	SHA256	59cd5ba96e0c819ee5bffee1b901237456c38...
Debian 7.0 armhf	1.13.4-3+deb7u6	280040	SHA256	157bf42a603d38d6a2f2769d166b23344de57...
Debian 7.0 x86_64	1.13.4-3+deb7u5	373712	SHA256	fd1418e3ba39aabada135272f4341971a734d...
Debian 7.0 x86_64	1.13.4-3+deb7u6	373712	SHA256	3e0a3d65d00aeb72927d6668bf24a46909b77...
Debian 7.11 armv7l	1.13.4-3+deb7u3	333284	SHA256	c3da46bfd113f92acabb4a3d6a329e9f432e...
Debian 7.11 armv7l	1.13.4-3+deb7u4	333284	SHA256	da6e5b58255e3d995a11cb62370f691d2954a...
Debian 7.11 armv7l	1.13.4-3+deb7u5	333284	SHA256	e54e79890545142e887468f89447feca4ca6...
Debian 8.0 armhf	1.16-1+deb8u4	314468	SHA256	11478838aecc1ad070eb91d6723a452c6e93d...
Debian 8.0 armhf	1.16-1+deb8u5	314468	SHA256	8bbd5685247cc74f1e8f40da3fe3ce665e79d...
Debian 8.0 armv7l	1.16-1+deb8u1	375904	SHA256	e72a42a2c37be12595e67bba92bfb3322d469...



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>
```



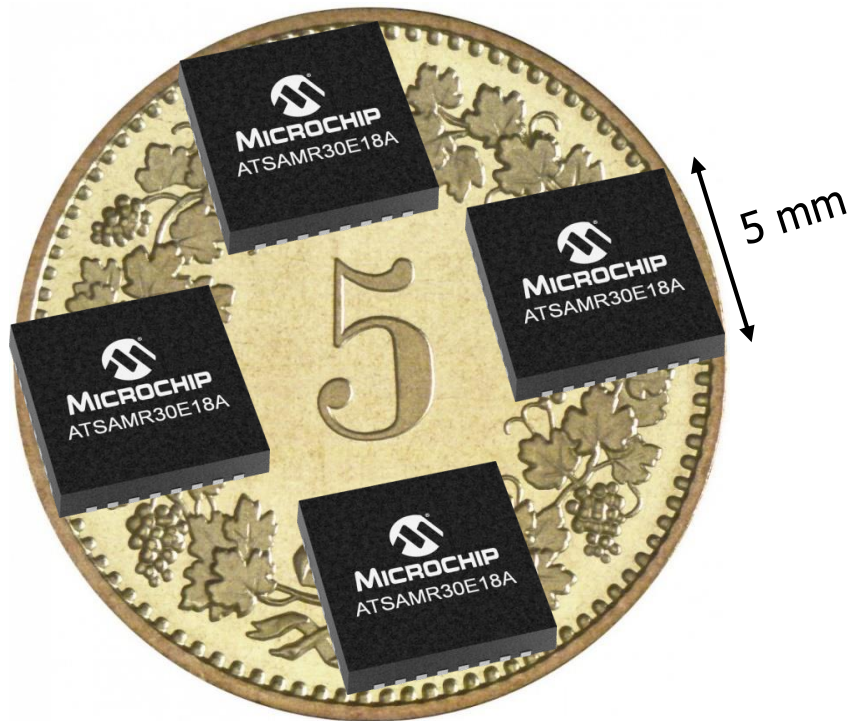

The screenshot shows the strongTNC web interface. The browser address bar displays <https://tnc.strongswan.org/vulnerabilities>. The page title is "strongTNC 0.9.4". A search bar is visible in the top right. The main content area is titled "Vulnerabilities" and contains a sub-section "Devices with Vulnerable Software Packages". Below this is a table with the following data:

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

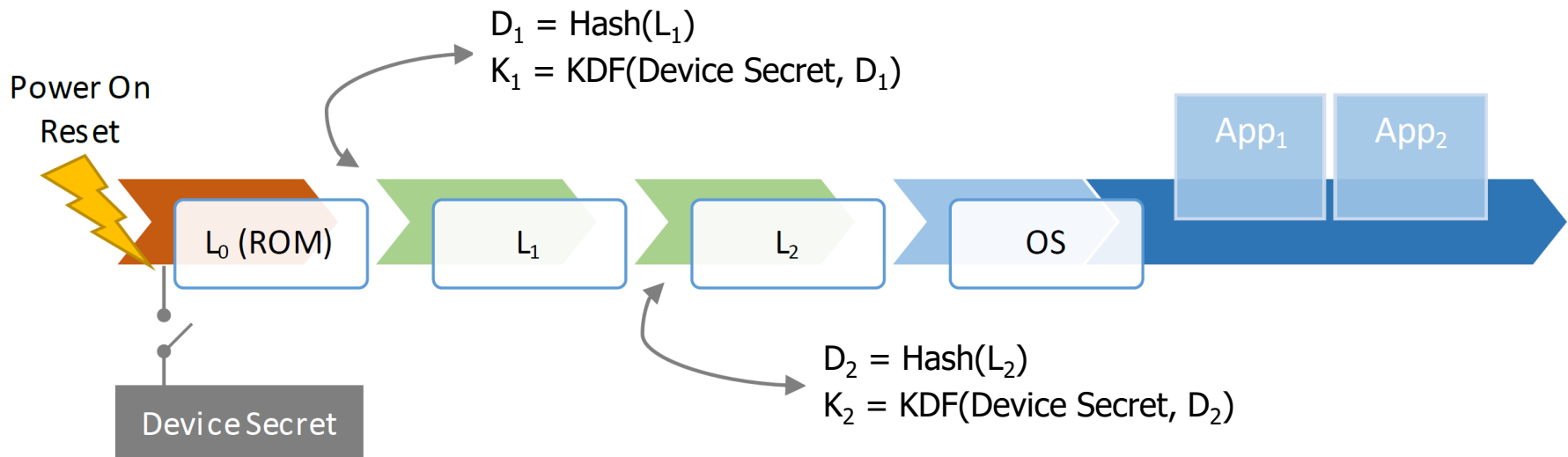
Information Security in Healthcare, 7. Juni 2018, Rotkreuz

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





RIoT (Robust IoT) von Microsoft Research*

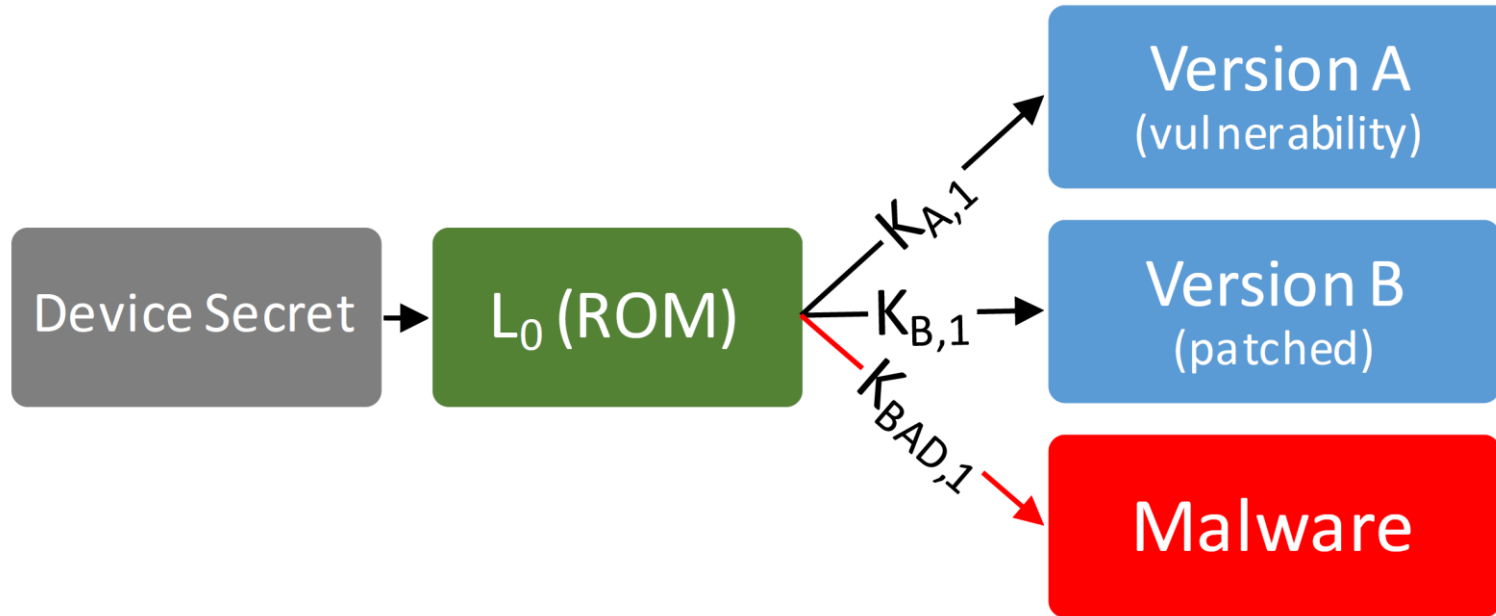


- Device Secret: 256...512 Bit unlöschbarer, zufällig generierter Geräteschlüssel, der nur durch die ROM Bootstufe L_0 lesbar ist.
- Hash Function: z.B. SHA256
- Key Derivation Function (KDF): z.B. HMAC-SHA256

*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?

