TPM-Based Attestation of IoT Devices

Cyber-Security Event Singapore, March 10

Prof. Andreas Steffen
Institute for Networked Solutions
HSR University of Applied Sciences Rapperswil
andreas.steffen@hsr.ch

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

strongswan

Where the heck is Rapperswil?

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

HSR - Hochschule für Technik Rapperswil

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

- University of Applied Sciences with about 1500 students
- Faculty of Information Technology (300-400 students)
- Bachelor Course (3 years), Master Course (+1.5 years)

Our Lab

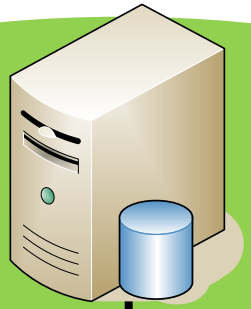
Research Building

strongSwan – the OpenSource VPN Solution

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

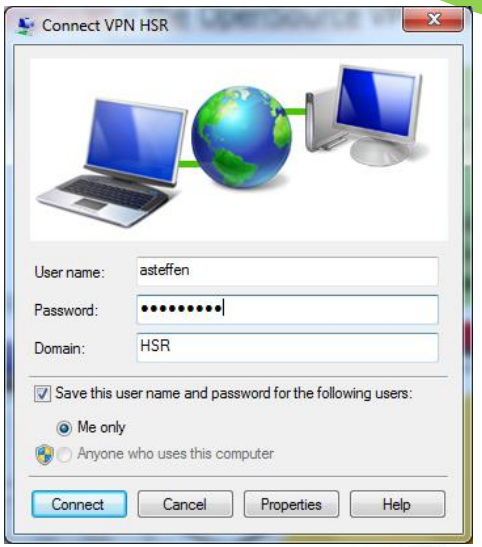
Windows Active Directory Server

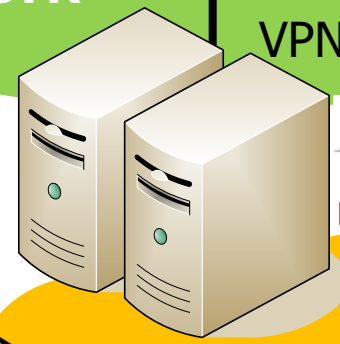


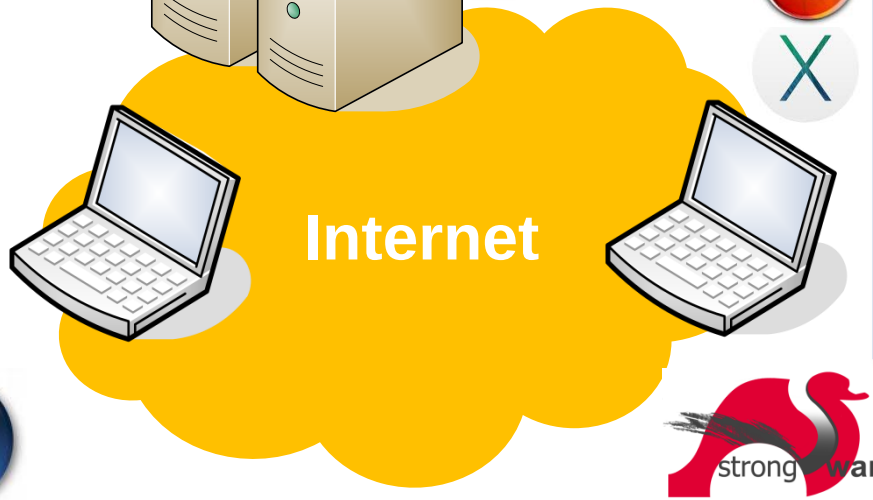
Linux FreeRadius Server

Corporate Network

High-Availability strongSwan VPN Gateway





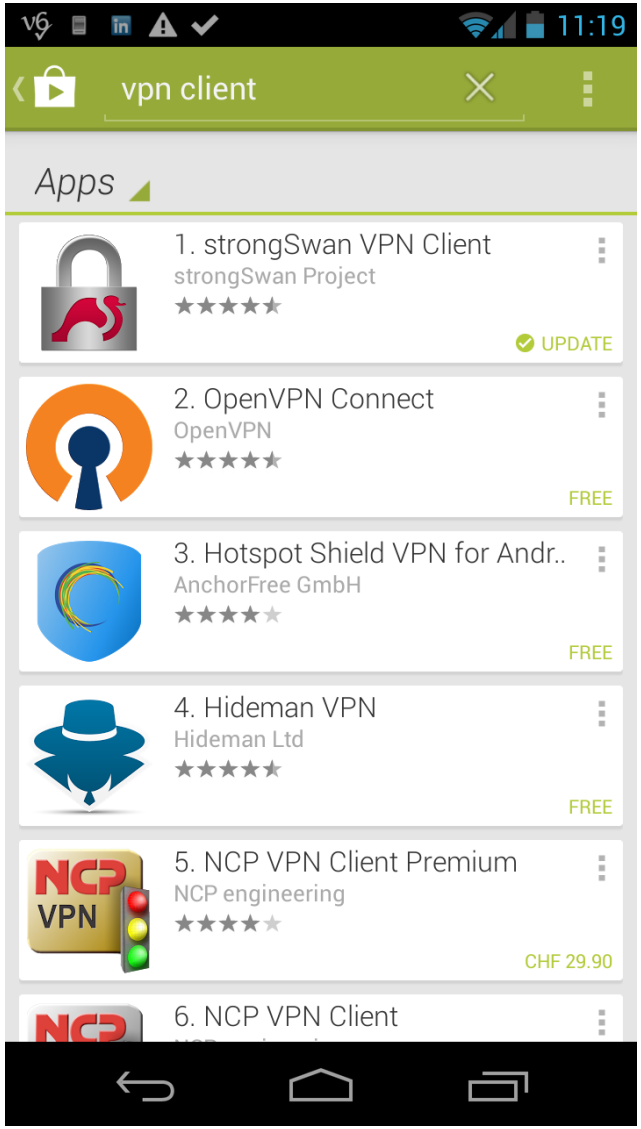


Windows 7/8/10 Agile VPN Client

strongSwan Linux Client

Free Download from Google Play Store

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz



October 16, 2016:
21’816 installations

☑	United States	5,434	24.91%
☑	China	2,640	12.10%
☑	Germany	2,043	9.36%
☐	United Kingdom	1,333	6.11%
☐	Canada	858	3.93%
☐	Russia	735	3.37%
☐	France	722	3.31%
☐	Netherlands	477	2.19%
☐	Australia	465	2.13%
☐	Japan	445	2.04%
	Others	6,664	30.55%

TPM-Based Attestation of IoT Devices

Cyber-Security Event Singapore, March 10

Attestation of IoT Devices based on
Trusted Network Connect (TNC)

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

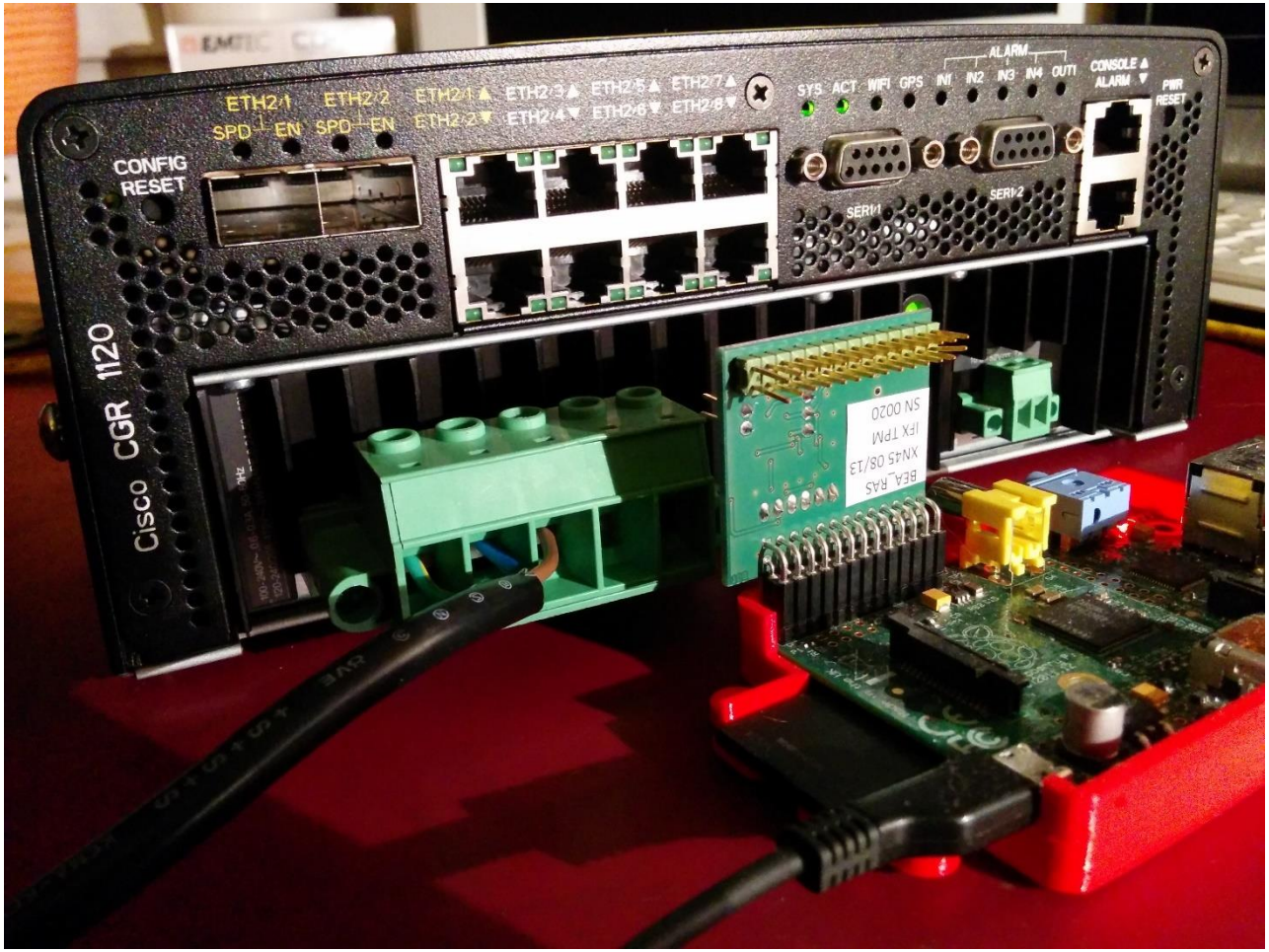
The Energy Grid

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

Network devices and SCADA components controlling the energy grid are extremely vulnerable to cyber attacks!

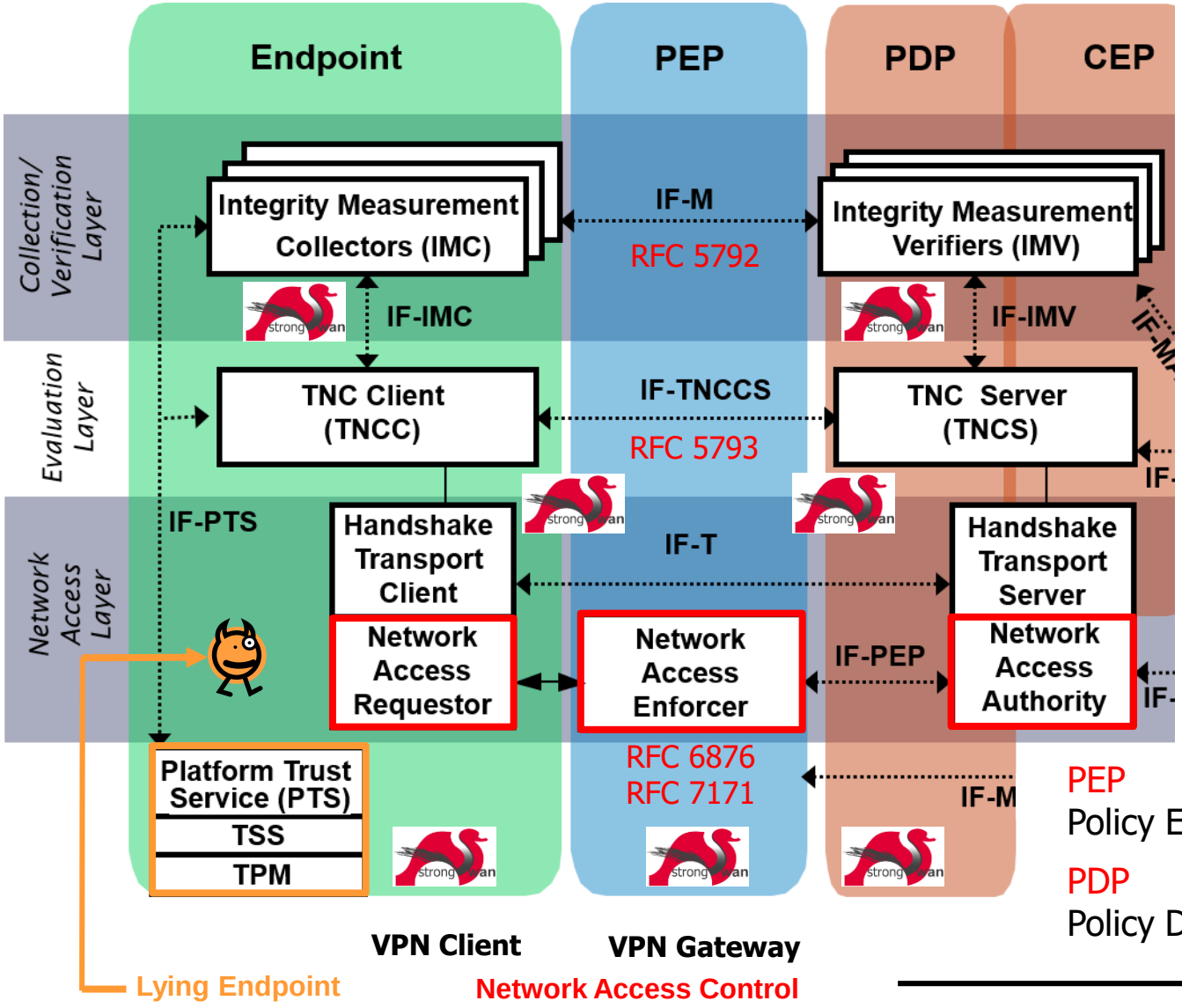
It is important to be able to detect malware embedding itself into IoT firmware.

RSA 2015 Security Conference San Francisco



Cisco 1120 Connected Grid Router with strongSwan running on Linux Guest OS

Trusted Network Connect (TNC) Architecture



PEP
Policy Enforcement Point

PDP
Policy Decision Point

Layered TNC Protocol Stack

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

- TNC Measurement Data

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

- IF-M Measurement Protocol 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
```

- IF-TNCCS TNC Client-Server Protocol 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'
```

- IF-T Transport Protocol 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]
```

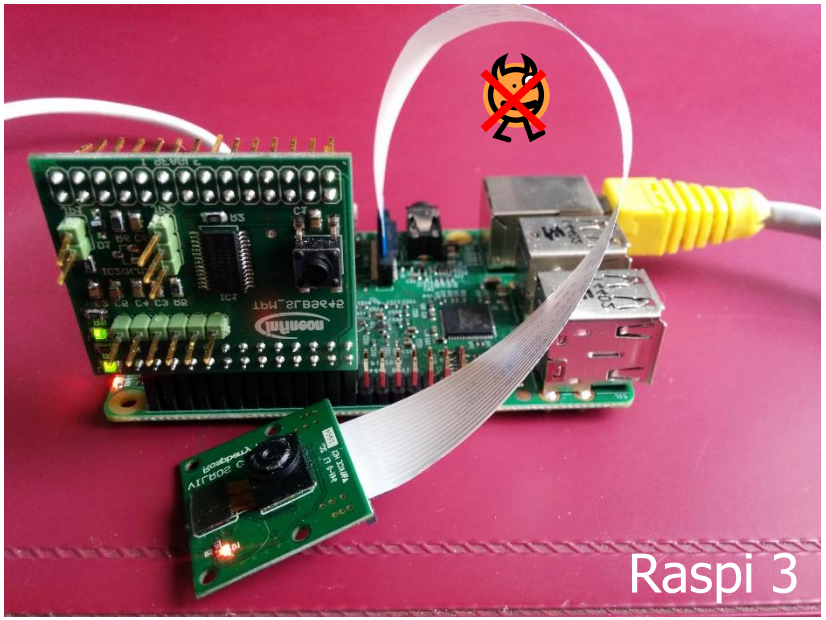
Demo: Mutually Trusted Video Phones

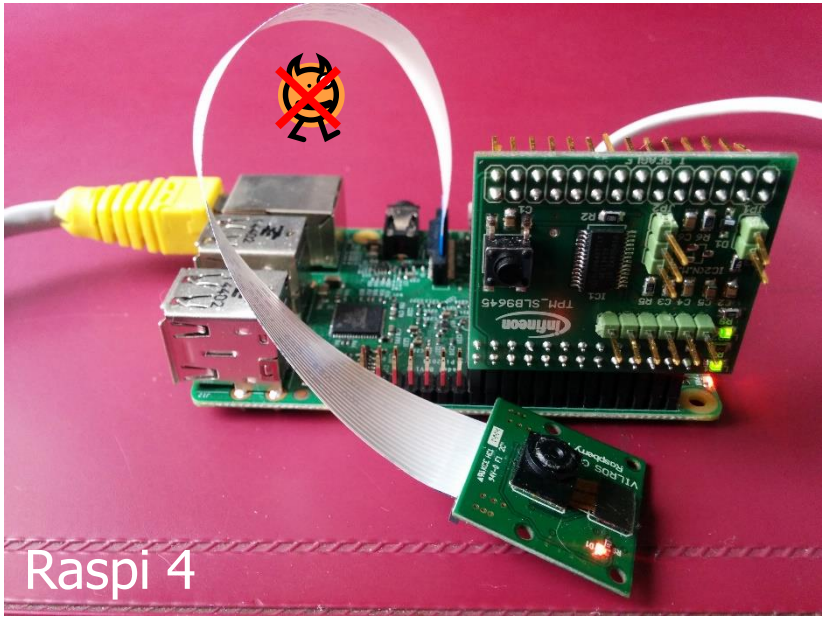
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

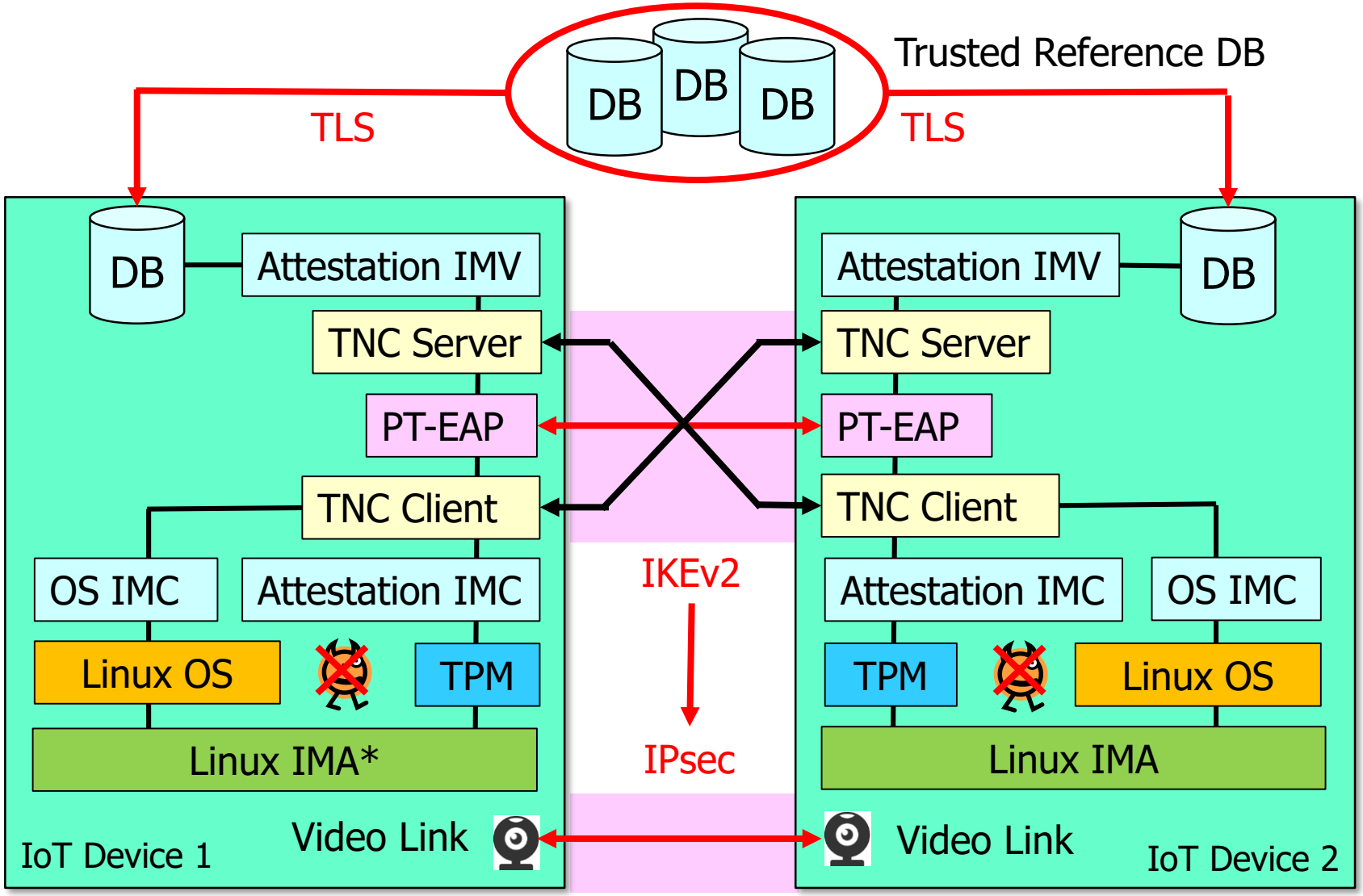
CeBIT 2016 Hannover:

Raspberry Pi 2 IoT Platform
Raspian OS (Debian 8)
Intel TSS 2.0 Stack
Infineon HW TPM 2.0





Mutual Attestation of IoT Devices



* IMA: Integrity Measurement Architecture

File Version Management using SWID Tags

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- ISO/IEC 19770-2:2015 Software Asset Management Part 2: Software Identification Tag
- NISTIR 8060 Guidelines for the Creation of Interoperable SWID Tags

```
<SoftwareIdentity xmlns="http://standards.iso.org/iso/19770/-2/2015/schema.xsd"
   name="libssl1.0.0" tagId="Ubuntu_16.04-x86_64-libssl1.0.0-1.0.2g-1ubuntu4.6“
   version="1.0.2g-1ubuntu4.6" versionScheme="alphanumeric">
  <Entity name="strongSwan Project" regid="strongswan.org“ role="tagCreator"/>
  <Payload>
    <Directory name="/lib/x86_64-linux-gnu" >
      <File name="libcrypto.so.1.0.0" size=“2361856"
         SHA256:hash="879a98c17952cd00d20cf42e83b1c54b4187f48dccb06cc8cc80ac2505a4db56"/>
      <File name="libssl.so.1.0.0" size="42834“
         SHA256:hash="b46a5c50ee77d7fe59fdb0eb1bae18a724c0e7962b5f228e2d901d6bff93be26"/>
    </Directory>
    <Directory name ="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines">
      <File name="libatalla.so" size= "15488"
         SHA256:hash=" 3e3a07ac750d335555230c1b438c844f7983044a4efcf2c2564670d98549ca9c"/>
      ...
    </Directory>
    <Directory name ="/usr/share/doc/libssl1.0.0">
      <File name="copyright" size= "6547"
         SHA256:hash="df574956b215bcdb0fb9e1b7b1562c9f172f1b5243d03b2f5bab5ecc68300ac5"/>
      ...
    </Directory>
  </Payload>
</SoftwareIdentity>
```

Conclusion

- A Trusted Platform Module (TPM) allows the reliable detection of any unauthorized change in the BIOS and operating system of an IoT device, solving the lying endpoint problem.
- Attestation measurements are digitally signed by the TPM thus asserting the trustworthiness.
- Additionally a TPM offers a secure and trustworthy hardware identity derived from a unique Endorsement Seed permanently programmed into the TPM during the manufacturing or provisioning process.
- Modern Intel and ARM processors offer a built-in firmware TPM based on Intel Platform Trust Technology (PTT) and ARM TrustZone, respectively.
- The strongSwan open source project offers a full implementation of the Trusted Network Connect (TNC) Internet standards, allowing the remote or mutual attestation of IoT devices.

Thank you for your attention!

Questions?

www.strongswan.org/tnc/