Mutual Attestation of IoT Devices and TPM 2.0 Support

TCG Members Meeting June 2016 Vienna

Prof. Andreas Steffen
Institute for Internet Technologies and Applications
HSR University of Applied Sciences Rapperswil
andreas.steffen@hsr.ch

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

strongSwan

Where the heck is Rapperswil?

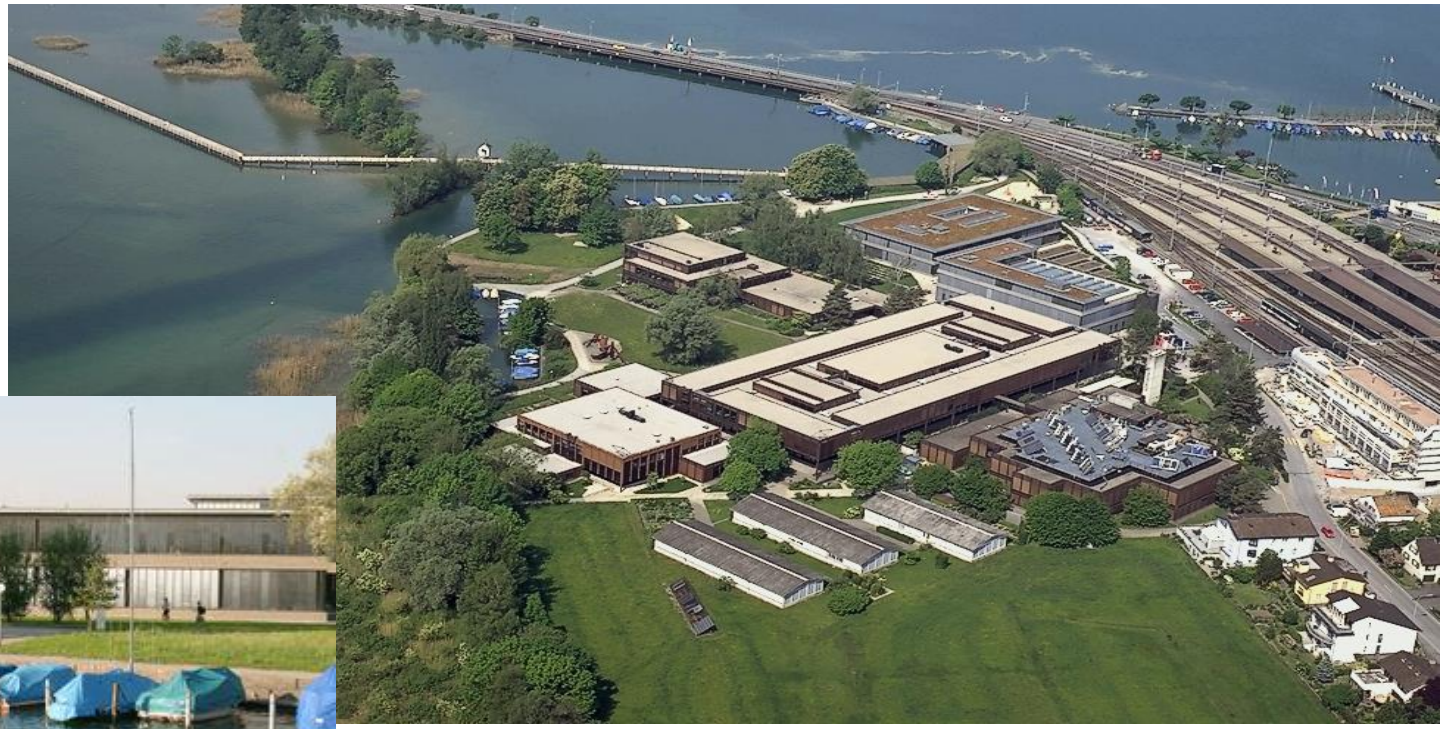
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

HSR - Hochschule für Technik Rapperswil

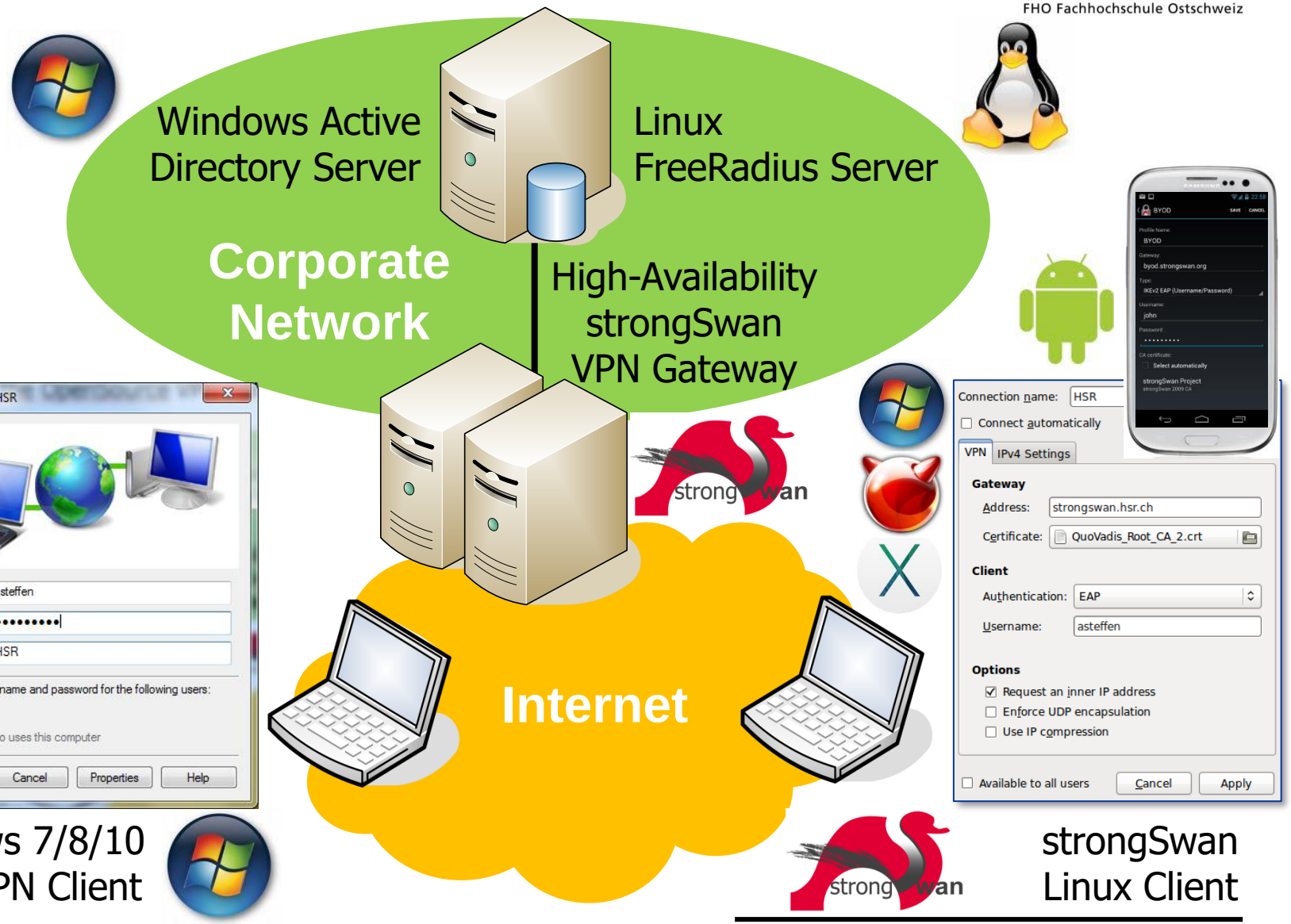
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

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



strongSwan – the OpenSource VPN Solution

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz



Mutual Attestation of IoT Devices and TPM 2.0 Support

TCG Members Meeting June 2016 Vienna

Trusted Network Communications (TNC)

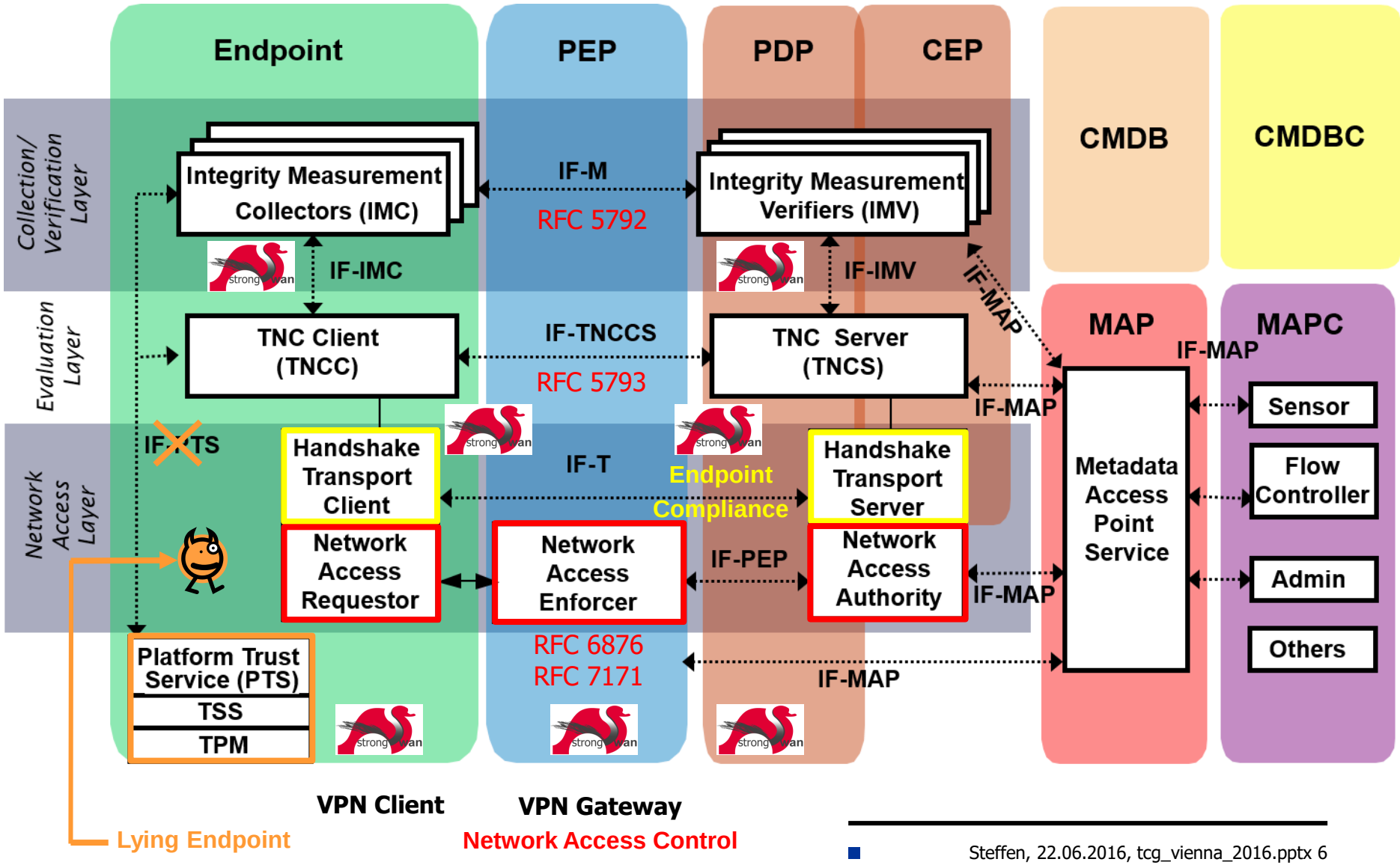
Current Use Cases:

Network Access Control & Endpoint Compliance

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

TNC Architecture



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]
```

TPM-based Attestation

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

2010 Implemented the TCG TNC IF-TNCCS 2.0 Client/Server and TCG TNC IF-M Measurement protocols.

2011 Implemented the TCG Attestation Protocol Binding to TNC IF-M using TrouSerS stack under Linux [later ported to Windows].

2012 Implemented TPM 1.2 based attestation using the Linux Integrity Measurement Architecture (IMA).

2015 Implemented the TCG TNC IF-M Segmentation Protocol allowing the transport of huge IF-M attributes over IF-T for EAP Methods. IF-T for TLS transport also profits from large buffer savings.

2016 Implemented TPM 2.0 based Attestation using the Intel TSS2 SAPI under Linux and an Intel PTT firmware TPM.

➔TSS 2.0 requires an update of the Attestation Binding to IF-M !!!

Mutual Attestation of IoT Devices and TPM 2.0 Support

TCG Members Meeting June 2016 Vienna

Trusted Network Communications (TNC)

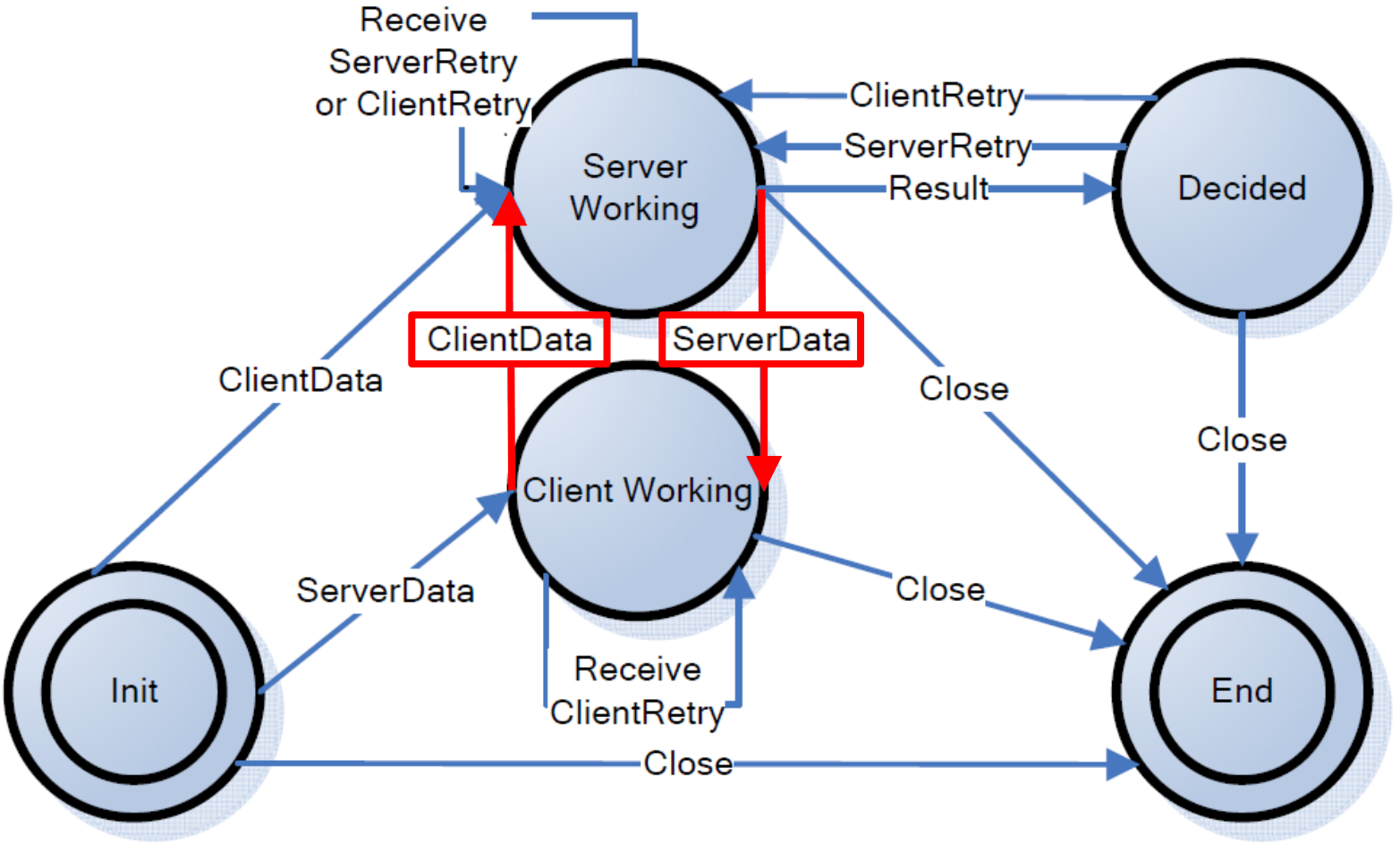
New Use Case:

Mutual Measurements of Endpoints

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

PB-TNC / IF-TNCCS 2.0 State Machine



Exchange of PB-TNC Client/Server Data Batches containing PA-TNC Messages

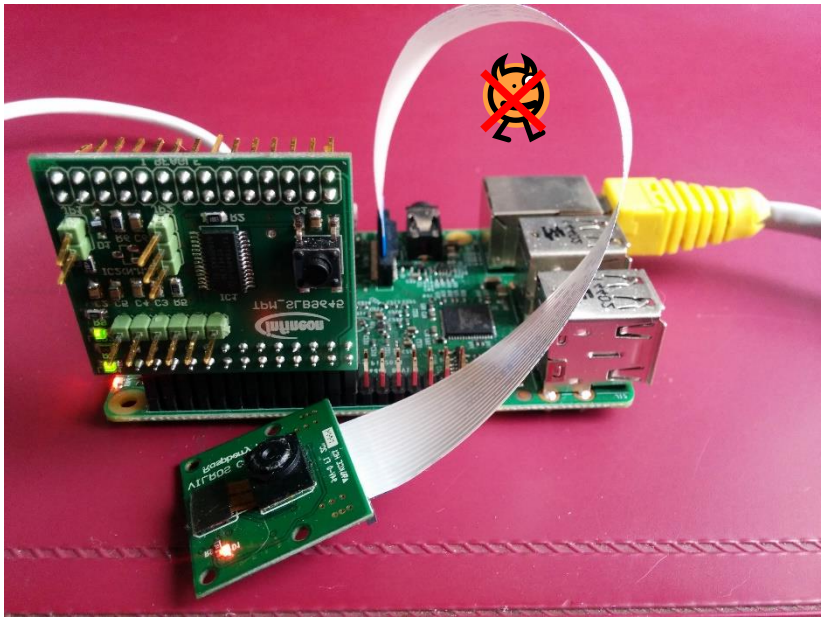
Mutual Measurements in Half-Duplex Mode

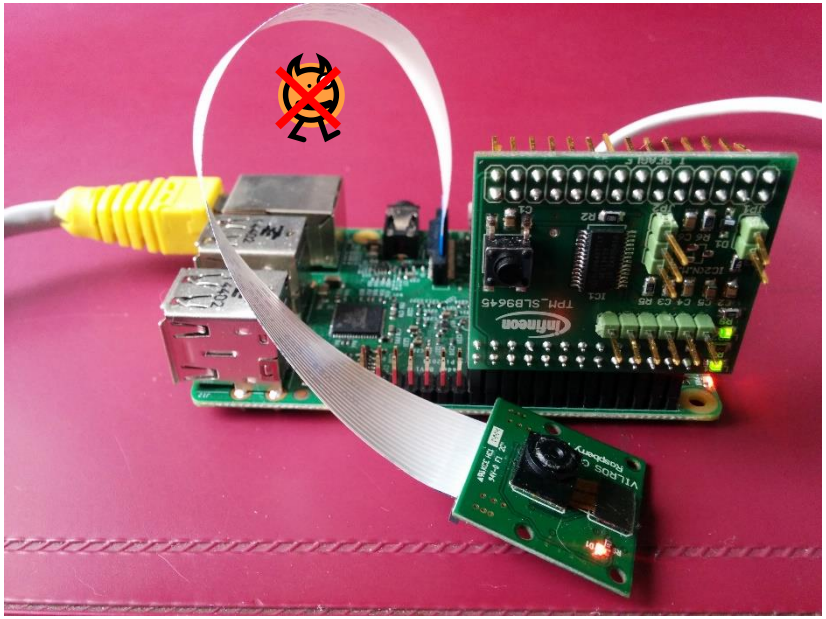
HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

Initiator		PB-TNC Batch[PB-TNC Messages]		Responder
TNC Client	→	CDATA[PB-MUTUAL, PB-PA]	→	TNC Server
TNC Client	←	SDATA[PB-MUTUAL, PB-PA]	←	TNC Server
TNC Server	→	SDATA[]	→	TNC Client
TNC Server	←	CDATA[PB-PA]	←	TNC Client
TNC Client	→	CDATA[PB-PA]	→	TNC Server
TNC Client	←	RESULT[PB-ASSESSMENT]	←	TNC Server
TNC Server	→	SDATA[PB-PA]	→	TNC Client
TNC Server	←	CDATA[PB-PA]	←	TNC Client
TNC Server	→	RESULT[PB-ASSESSMENT]	→	TNC Client
TNC Server	←	CLOSE[]	←	TNC Client
TNC Client	→	CLOSE[]	→	TNC Server

- The initiating TNC client sends CLOSE batch last
- Works over PT-EAP and PT-TLS

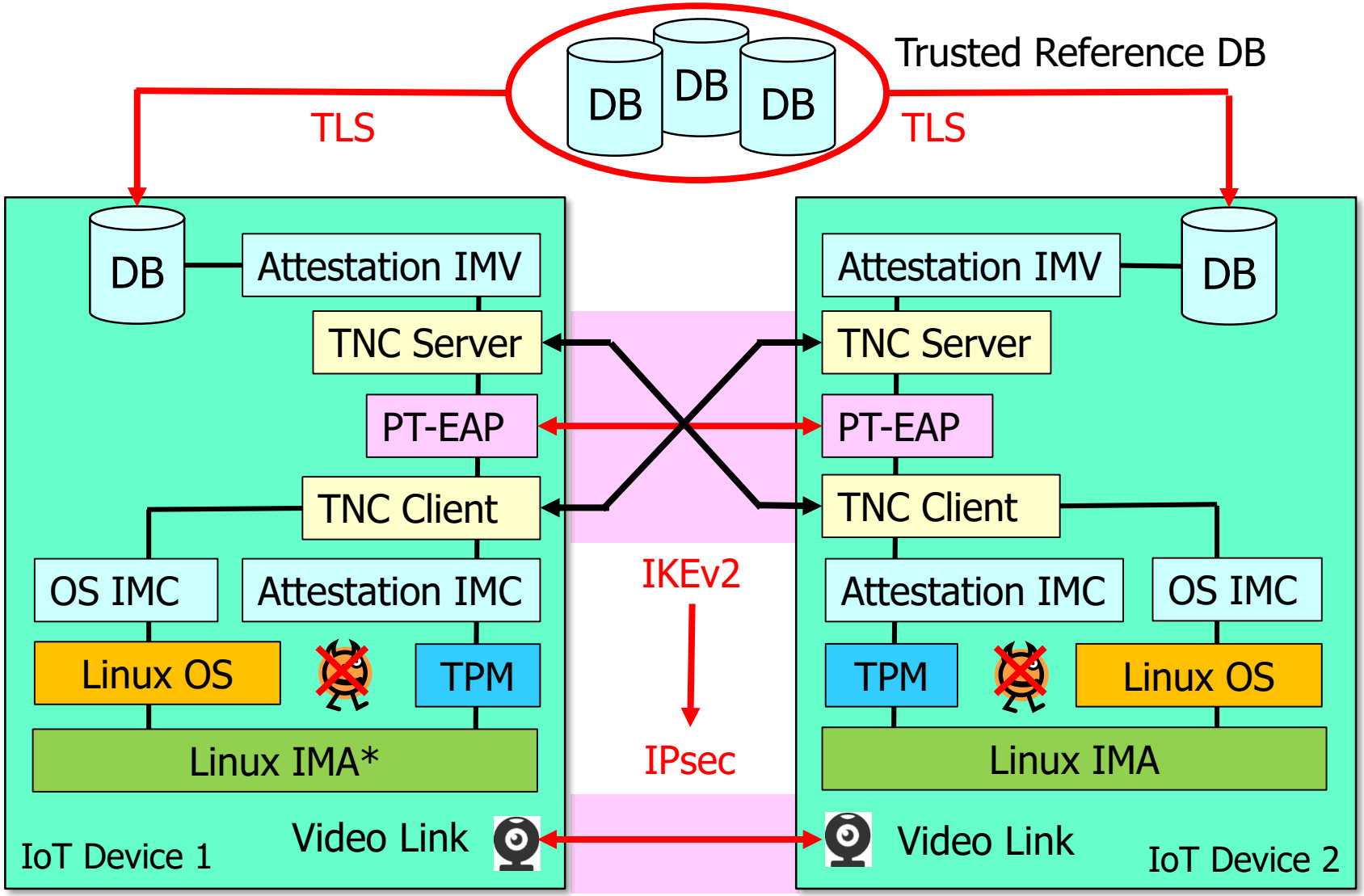
Example: Mutually Trusted Video Phones





Mutual Attestation of IoT Devices

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz



* 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:

```
<SoftwareIdentity xmlns=http://standards.iso.org/iso/19770/-2/2015/schema.xsd
   name="libssl1.0.0" uniqueId="Ubuntu_14.04-x86_64-libssl1.0.0-1.0.1f-1ubuntu2.15“
   version="1.0.1f-1ubuntu2.15" versionScheme="alphanumeric">
  <Entity name="strongSwan Project" regid="regid.2004-03.org.strongswan“ role="tagcreator"/>
  <Payload>
    <File location="/lib/x86_64-linux-gnu" name="libcrypto.so.1.0.0"/>
    <File location="/lib/x86_64-linux-gnu" name="libssl.so.1.0.0"/>
    <File location="/usr/share/doc/libssl1.0.0" name="copyright"/>
    <File location="/usr/share/doc/libssl1.0.0" name="changelog.Debian.gz"/>
    <File location="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines" name="libpadlock.so"/>
    <File location="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines" name="libcswift.so"/>
    <File location="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines" name="lib4758cca.so"/>
    <File location="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines" name="libaep.so"/>
    <File location="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines" name="libubsec.so"/>
    <File location="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines" name="libchil.so"/>
    <File location="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines" name="libgost.so"/>
    <File location="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines" name="libgmp.so"/>
    <File location="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines" name="libcapi.so"/>
    <File location="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines" name="libnuron.so"/>
    <File location="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines" name="libsureware.so"/>
    <File location="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines" name="libatalla.so"/>
  </Payload>
</SoftwareIdentity>
```

Thank you for your attention!

Questions?

www.strongswan.org/tnc/