The Linux Integrity Measurement Architecture and TPM-Based Network Endpoint Assessment

Linux Security Summit August 2012 San Diego

http://www.strongswan.org/lss2012.pdf

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?

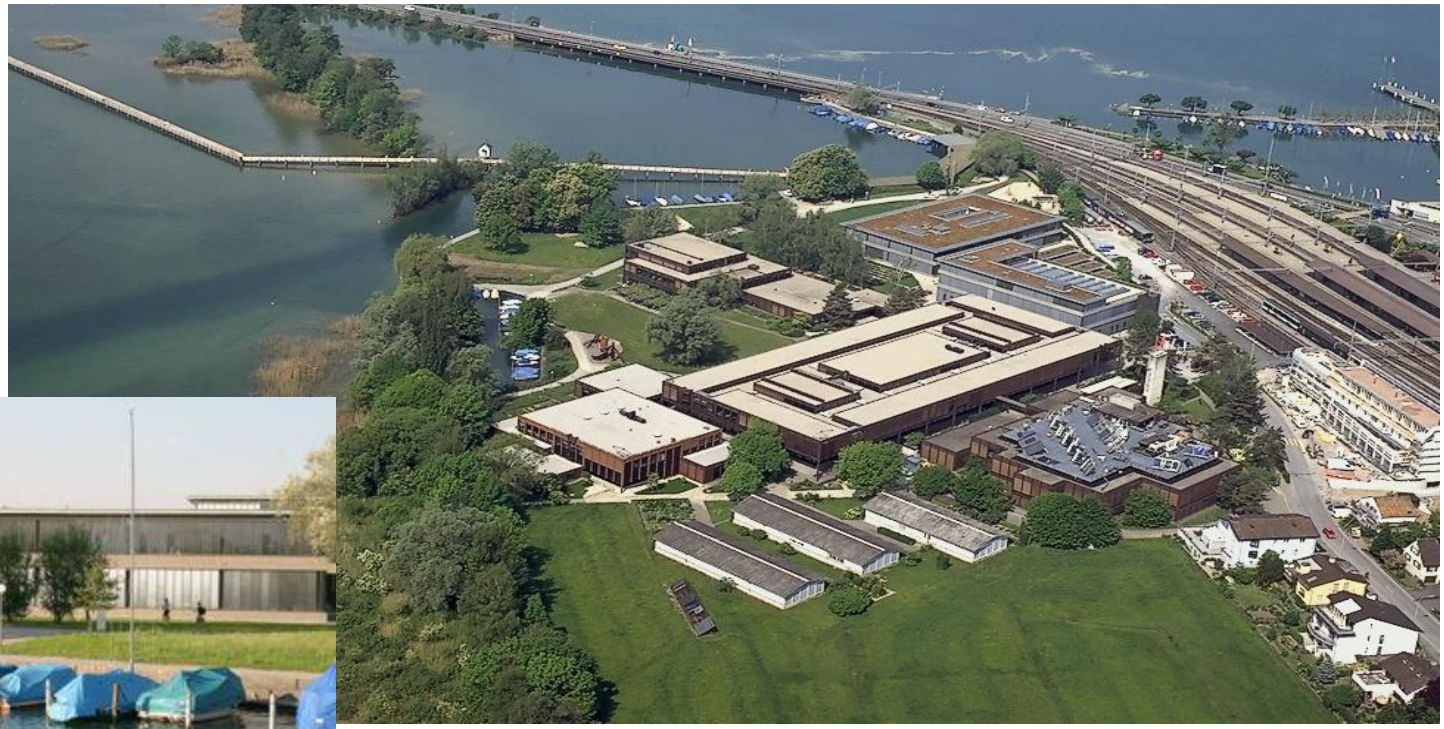
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

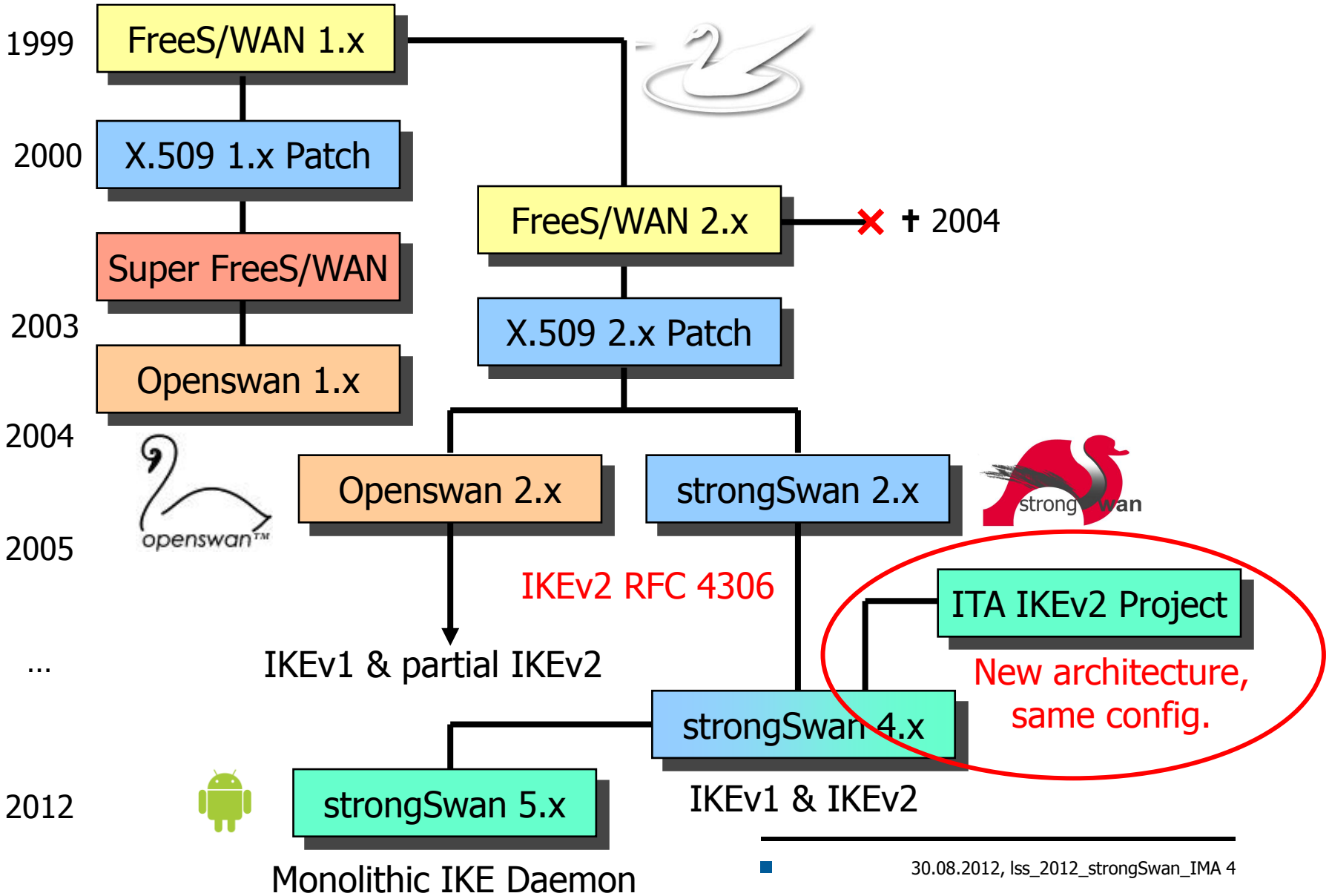
HSR - Hochschule für Technik Rapperswil

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)



The strongSwan Open Source VPN Project



The Linux Integrity Measurement Architecture and TPM-Based Network Endpoint Assessment

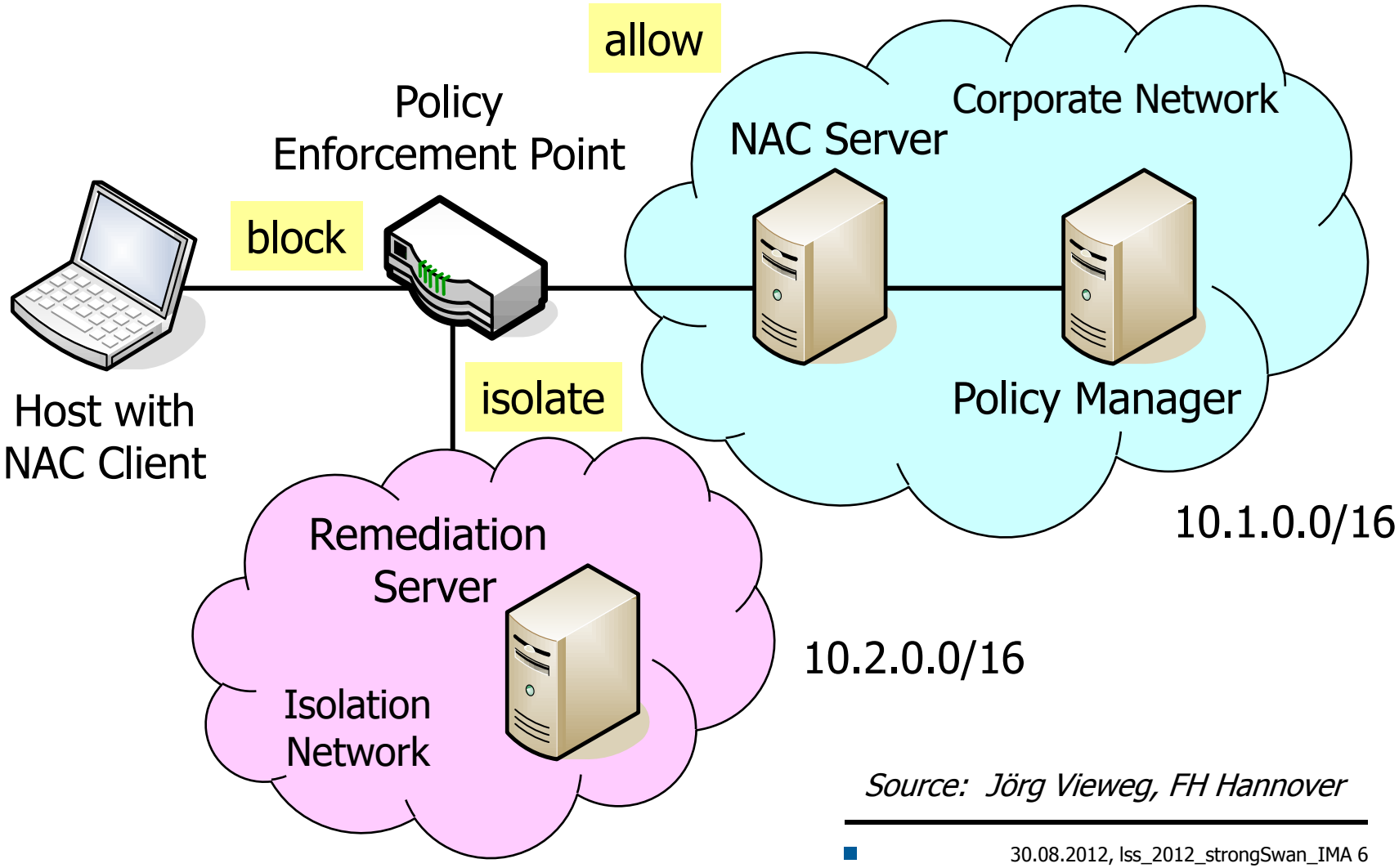
Linux Security Summit August 2012 San Diego

Network Access Control

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

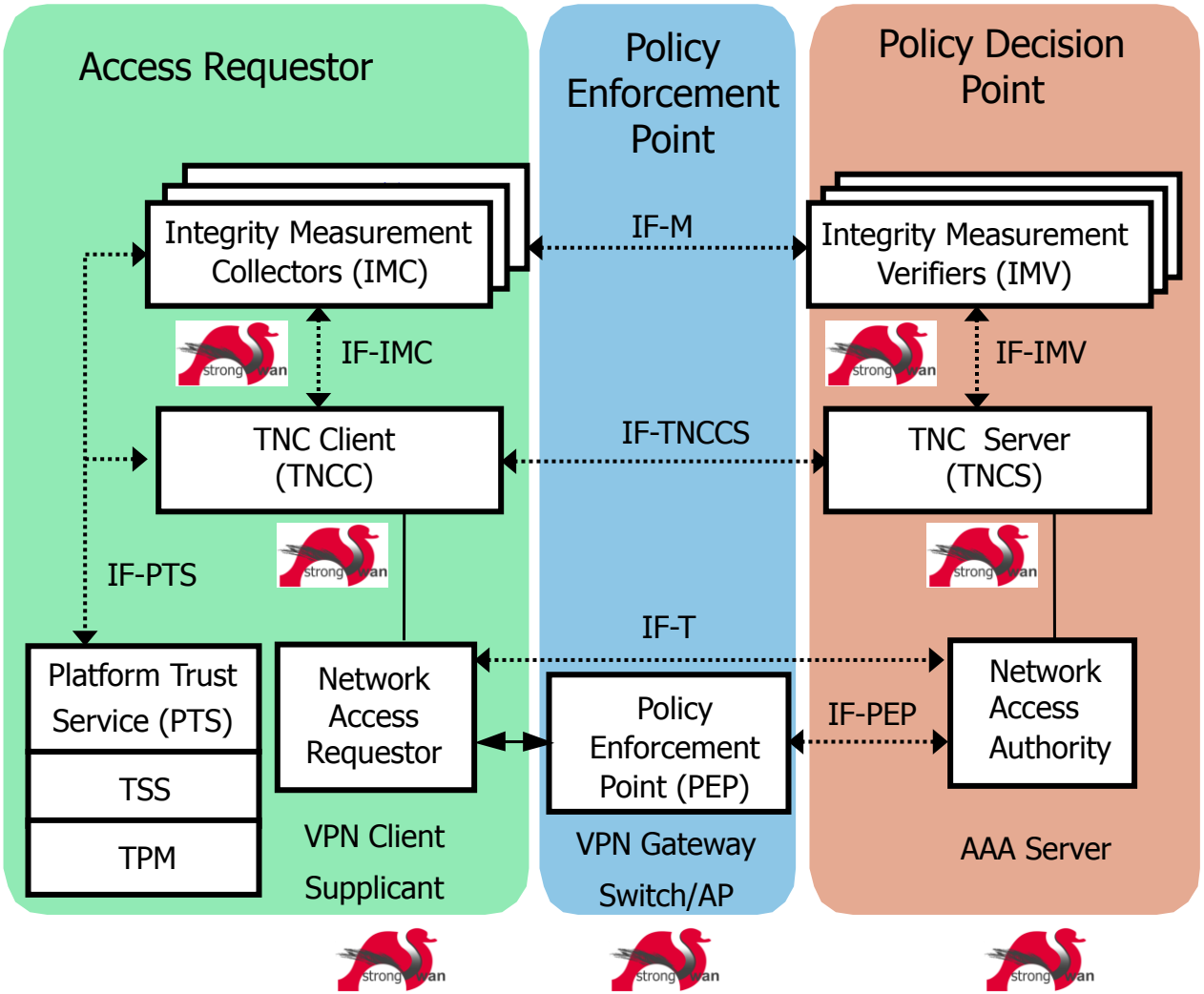
FHO Fachhochschule Ostschweiz

Network Access Control (NAC)



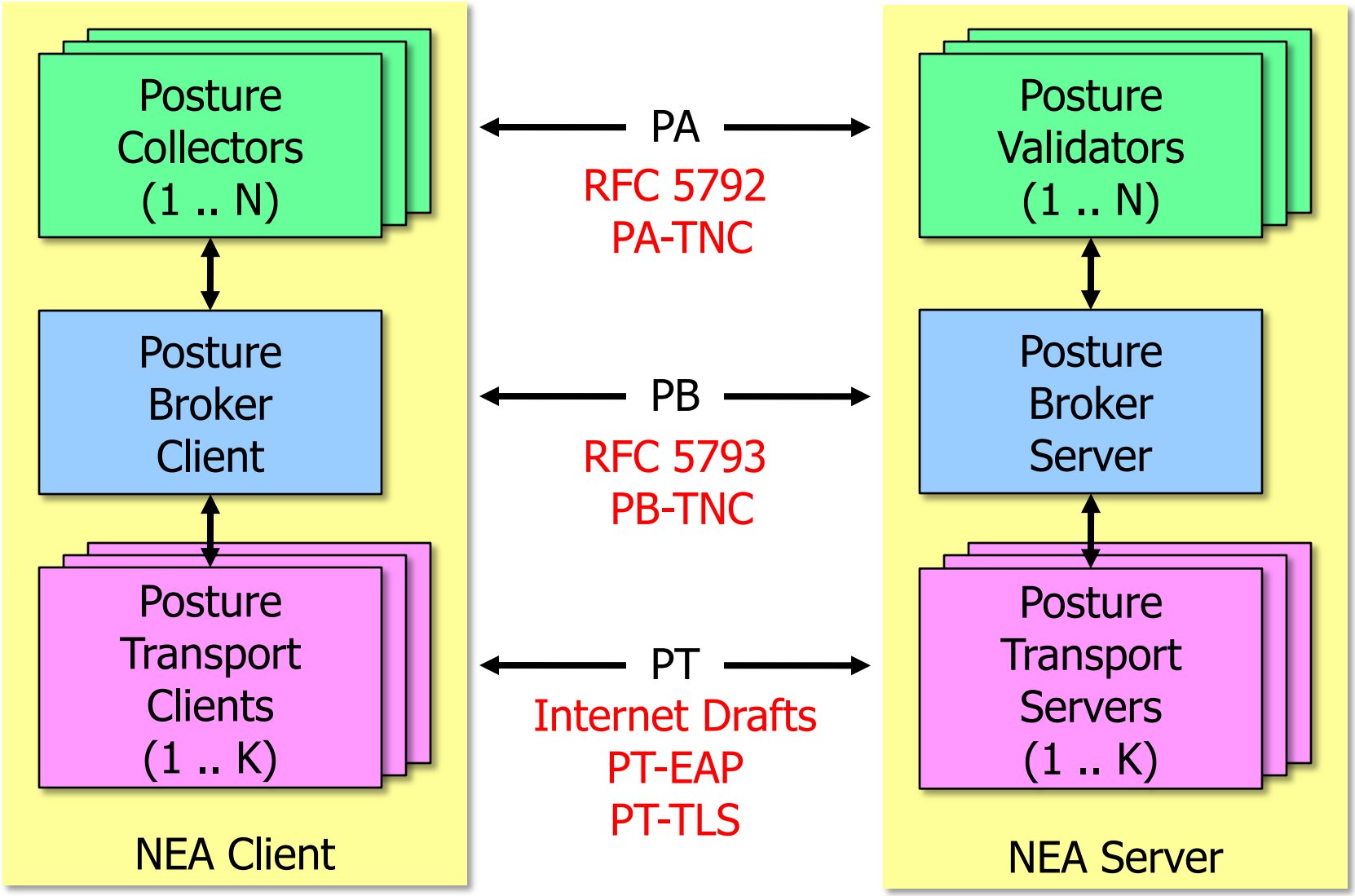
Source: Jörg Vieweg, FH Hannover

Trusted Network Connect (TNC) Framework

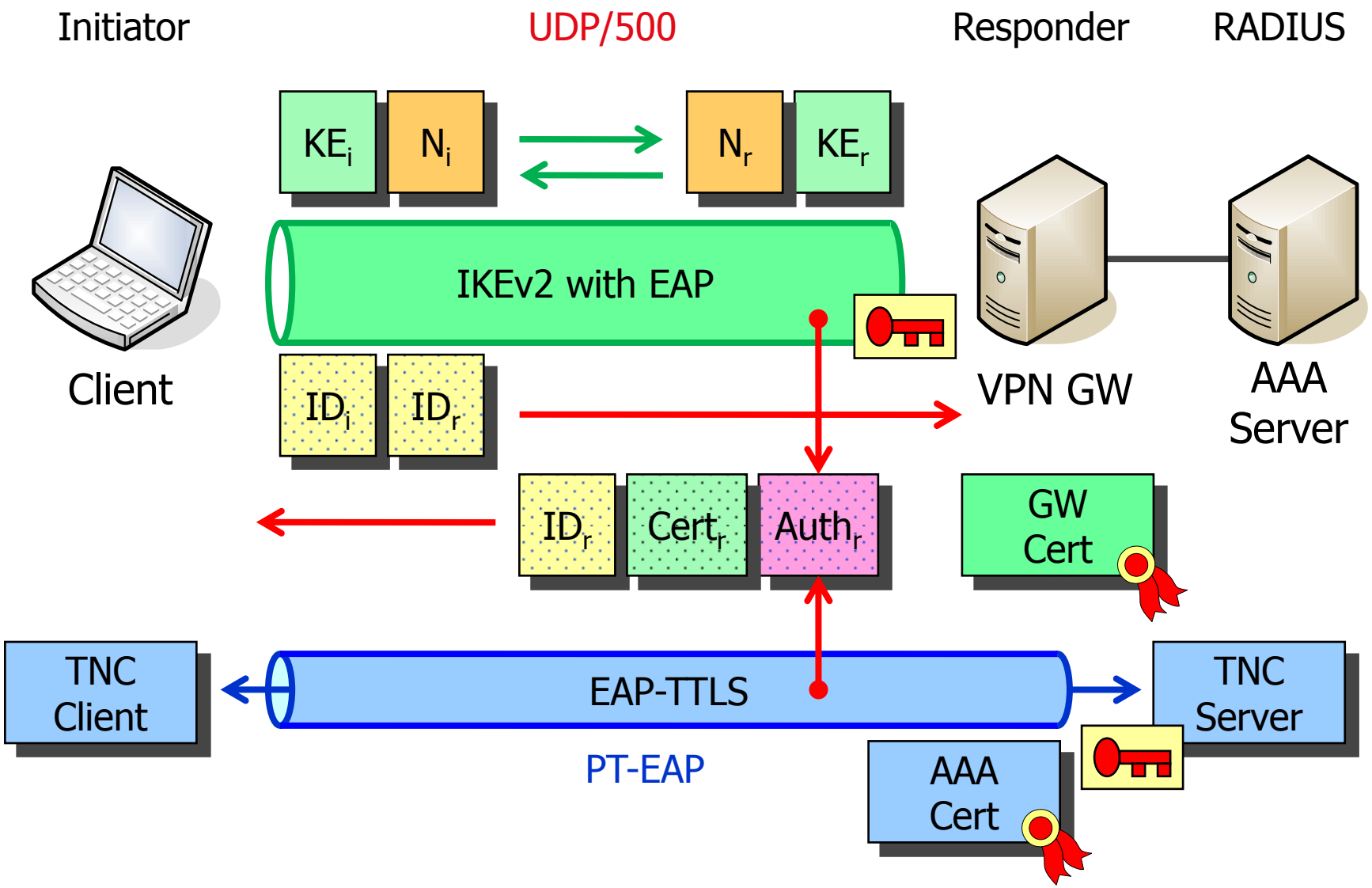


Source: Trusted Computing Group (TCG)

Network Endpoint Assessment (RFC 5209)



PT-EAP Transport over IKEv2 EAP-TTLS



The Linux Integrity Measurement Architecture and TPM-Based Network Endpoint Assessment

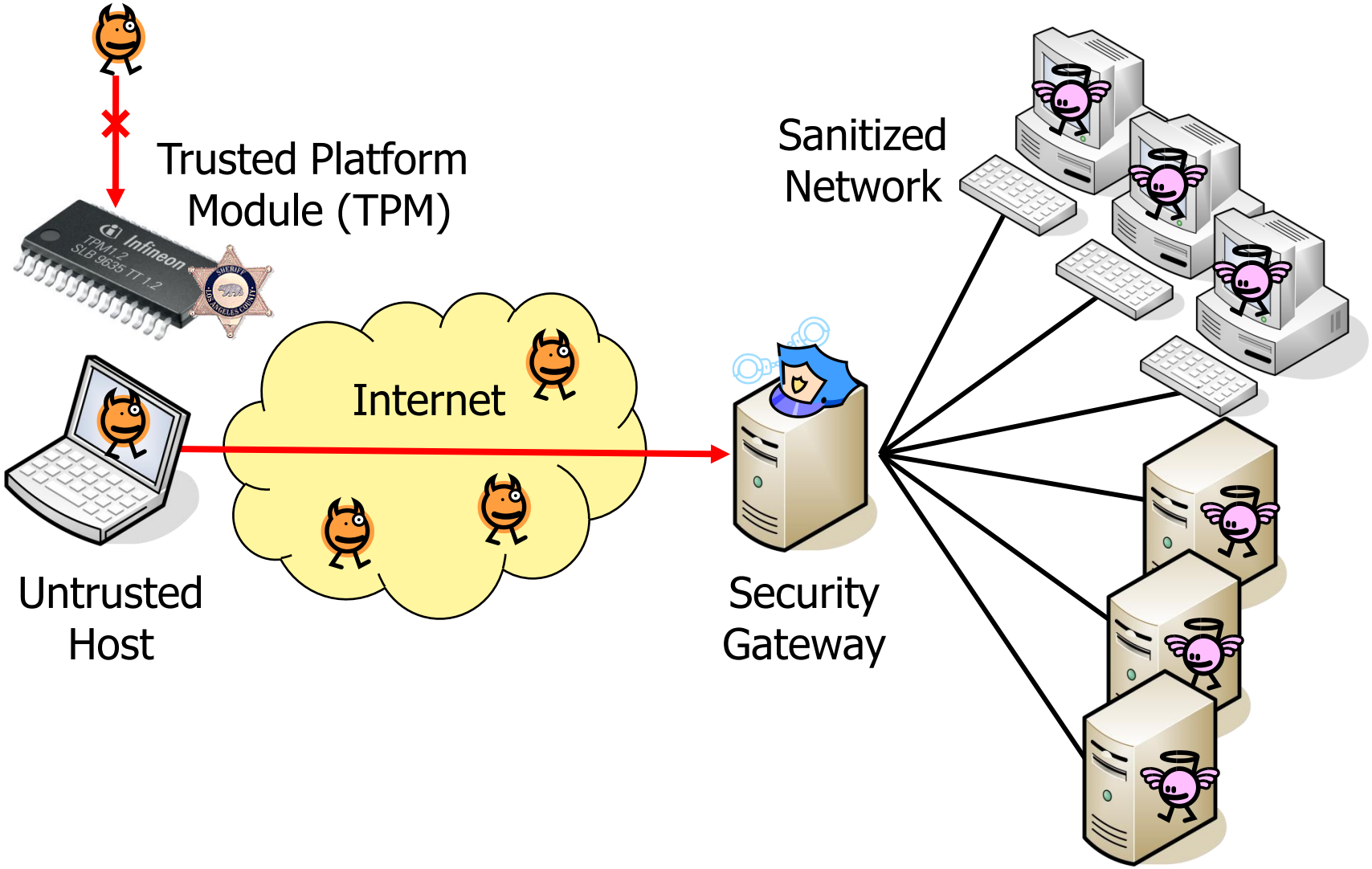
Linux Security Summit 2012 San Diego

Platform Trust Services

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

TPM stablishes Trust in Measurements



Linux IMA - BIOS Measurements

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

- BIOS is measured during the boot process
  - Many Linux distributions enable BIOS measurement by default when a TPM hardware device is detected.
  - BIOS measurement report with typically 20…130 entries is written to /sys/kernel/security/tpm0/ascii_bios_measurements
  - BIOS measurements are extended into PCRs #0..7

```
PCR  SHA-1 Measurement Hash                          Comment
  0 4d894eef0ae7cb124740df4f6c5c35aa0fe7dae8 08 [S-CRTM Version]
  0 f2c846e7f335f7b9e9dd0a44f48c48e1986750c7 01 [POST CODE]
    ...
  7 9069ca78e7450a285173431b3e52c5c25299e473 04 []
  4 c1e25c3f6b0dc78d57296aa2870ca6f782ccf80f 05 [Calling INT 19h]
  4 67a0a98bc4d6321142895a4d938b342f6959c1a9 05 [Booting BCV Device 80h, - Hitachi HTS723216L9A360]
  4 06d60b3a0dee9bb9beb2f0b04aff2e75bd1d2860 0d [IPL]
  5 1b87003b6c7d90483713c90100cca3e62392b9bc 0e [IPL Partition Data]
```

Linux IMA - Runtime Measurements

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

- Executable files, dynamic libraries and kernel modules are measured when loaded during runtime.
  - With current Linux distributions either IMA must be activated via the boot parameter ima_tcb or the kernel must by manually compiled with CONFIG_IMA enabled
  - The IMA runtime measurement report with about 1200 entries is written to /sys/kernel/security/ima/ascii_runtime_measurements
  - IMA runtime measurements are extended into TPM PCR #10

```
PCR  SHA-1 Measurement Hash                          SHA-1 File Data Hash                          Filename
 10 d0bb59e83c371ba6f3adad491619524786124f9a ima 365a7adf8fa89608d381d9775ec2f29563c2d0b8 boot_aggregate
 10 76188748450a5c456124c908c36bf9e398c08d11 ima f39e77957b909f3f81f891c478333160ef3ac2ca /bin/sleep
 10 df27e645963911df0d5b43400ad71cc28f7f898e ima 78a85b50138c481679fe4100ef2b3a0e6e53ba50 ld-2.15.so
                        ...                                           ...
 10 30fa7707af01a670fc353386fcc95440e011b08b ima 72ebd589aa9555910ff3764c27dbdda4296575fe parport.ko
                        ...                                           ...
```

Custom IMA Measurement Policy

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

- The IMA kernel interface allows to set a custom policy defining which files are to be measured
  - A dracut initramfs replaces the default policy by the custom one defined in /etc/sysconfig/ima-policy at an early stage during the boot process
  - SE Linux file system labeling allows to fine-tune which system files are to be measured.

```
# PROC_SUPER_MAGIC
dont_measure fsmagic=0x9fa0
# SYSFS_MAGIC
dont_measure fsmagic=0x62656572
# DEBUGFS_MAGIC
dont_measure fsmagic=0x64626720
# TMPFS_MAGIC
dont_measure fsmagic=0x01021994
# SECURITYFS_MAGIC
dont_measure fsmagic=0x73636673
measure func=BPRM_CHECK
measure func=FILE_MMAP mask=MAY_EXEC
# SE Linux
measure func=PATH_CHECK mask=MAY_READ obj_type=modules_object_t
```

TCG Attestation PTS Protocol

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

- The TCG PTS protocol defines a collection of IF-M attributes allowing an Attestation IMC/IMV pair to exchange
  - PTS capabilities and configuration parameters
  - Diffie-Hellman nonces and AIK certificates
  - File measurements and metadata
  - Bulk integrity measurement data
  - TPM Quote signatures

  in a standardized way.
- strongSwan implements a subset of PTS IF-M attributes , needed to transfer TLV-based Simple Component Evidence measurement data and Linux/Unix-style file metadata in an efficient way.
- Verbose XML-based Integrity Reports, corresponding Reference Manifests, Verification Results, as well as Windows-style file metadata and registry entries are currently not supported.

IMA Measurement Reference Database

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- For each Linux version more than 10'000 reference measurements are generated and stored in an SQLite DB using about 200 attest calls.

```
#!/bin/sh
# executable files with absolute filenames
ipsec attest --add --product "Ubuntu 12.04 LTS i686" --sha1-ima --dir /sbin
ipsec attest --add --product "Ubuntu 12.04 LTS i686" --sha1-ima --dir /usr/sbin
ipsec attest --add --product "Ubuntu 12.04 LTS i686" --sha1-ima --dir /bin
ipsec attest --add --product "Ubuntu 12.04 LTS i686" --sha1-ima --dir /usr/bin
...
# dynamic libraries with relative filenames
ipsec attest --add --product "Ubuntu 12.04 LTS i686" --sha1-ima --rel --dir /lib
ipsec attest --add --product "Ubuntu 12.04 LTS i686" --sha1-ima --rel --dir /usr/lib
ipsec attest --add --product "Ubuntu 12.04 LTS i686" --sha1-ima --rel --dir /lib/i386-linux-gnu
...
# applications using different versions of Linux system libraries
for file in /usr/lib/firefox/*.so
do
ipsec attest --add --product "Ubuntu 12.04 LTS i686" --sha1-ima --rel --file $file
done
...
# kernel modules with relative filenames
for file in `find /lib/modules/3.2.21ima/kernel -name *.ko`
do
ipsec attest --add --product "Ubuntu 12.04 LTS i686" --sha1-ima --rel --file $file
done
```

PTS Functional Component Evidence I

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- The Attestation IMC attached to TNC client carol receives a Functional Component Evidence Request for the ITA-HSR Linux IMA component with qualifiers Trusted Platform and Operating System, respectively.
- The Generate Attestation Evidence attribute triggers the start of the component measurements.

```
carol charon: 16[TNC] processing PA-TNC message with ID 0x184fd6d0
carol charon: 16[TNC] processing PA-TNC attribute type 'TCG/Request Functional Component Evidence
carol charon: 16[TNC] processing PA-TNC attribute type 'TCG/Generate Attestation Evidence'
carol charon: 16[IMC] evidence requested for 2 functional components
carol charon: 16[PTS] * ITA-HSR functional component 'Linux IMA' [K.] 'Trusted Platform'
carol charon: 16[PTS] loaded '/sys/kernel/security/tpm0/binary_bios_measurements' (126 entries)
carol charon: 16[PTS] * ITA-HSR functional component 'Linux IMA' [K.] 'Operating System'
carol charon: 16[PTS] loaded '/sys/kernel/security/ima/binary_runtime_measurements' (1248 entries)
```

PTS Functional Component Evidence II

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- The Attestation IMV attached to TNC server moon first receives 126 Simple Component Evidence attributes containing BIOS measurements.
- The boot_aggregate IMA measurement is a SHA-1 hash of the contents of PCRs 0..7 where the 126 BIOS measurements were extended into.

```
moon charon: 09[TNC] processing PA-TNC attribute type 'TCG/Simple Component Evidence
moon charon: 09[PTS] ITA-HSR functional component 'Linux IMA' [K.] 'Trusted Platform'
moon charon: 09[PTS] measurement time: Jul 30 19:28:11 2012
moon charon: 09[PTS] PCR 0 extended with: 4d:89:4e:ef:0a:e7:cb:12:47:40:df:4f:6c:5c:35:aa:0f:e7:da:e8
...
moon charon: 09[TNC] processing PA-TNC attribute type 'TCG/Simple Component Evidence'
moon charon: 09[PTS] ITA-HSR functional component 'Linux IMA' [K.] 'Trusted Platform'
moon charon: 09[PTS] measurement time: Jul 30 19:28:11 2012
moon charon: 09[PTS] PCR 5 extended with: 1b:87:00:3b:6c:7d:90:48:37:13:c9:01:00:cc:a3:e6:23:92:b9:bc
moon charon: 09[PTS] checking 126 ITA-HSR 'Linux IMA' BIOS evidence measurements

moon charon: 09[TNC] processing PA-TNC attribute type 'TCG/Simple Component Evidence
moon charon: 09[PTS] ITA-HSR functional component 'Linux IMA' [K.] 'Operating System'
moon charon: 09[PTS] measurement time: Jul 30 19:28:13 2012
moon charon: 09[PTS] PCR 10 extended with: d0:bb:59:e8:3c:37:1b:a6:f3:ad:ad:49:16:19:52:47:86:12:4f:9a
moon charon: 09[PTS] 'boot_aggregate'
moon charon: 09[PTS] checking ITA-HSR 'Linux IMA' boot aggregate evidence measurement
```

PTS Functional Component Evidence III

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- Next the Attestion IMV attached to TNC server moon receives 1247 Simple Component Evidence attributes containing IMA file measurements.

```
moon charon: 09[TNC] processing PA-TNC attribute type 'TCG/Simple Component Evidence
moon charon: 09[PTS] ITA-HSR functional component 'Linux IMA' [K.] 'Operating System'
moon charon: 09[PTS] measurement time: Jul 30 19:28:13 2012
moon charon: 09[PTS] PCR 10 extended with: 76:18:87:48:45:0a:5c:45:61:24:c9:08:c3:6b:f9:e3:98:c0:8d:11
moon charon: 09[PTS] '/bin/sleep'

moon charon: 09[TNC] processing PA-TNC attribute type 'TCG/Simple Component Evidence
moon charon: 09[PTS] ITA-HSR functional component 'Linux IMA' [K.] 'Operating System'
moon charon: 09[PTS] measurement time: Jul 30 19:28:13 2012
moon charon: 09[PTS] PCR 10 extended with: df:27:e6:45:96:39:11:df:0d:5b:43:40:0a:d7:1c:c2:8f:7f:89:8e
moon charon: 09[PTS] 'ld-2.15.so'
...
moon charon: 09[TNC] processing PA-TNC attribute type 'TCG/Simple Component Evidence
moon charon: 09[PTS] ITA-HSR functional component 'Linux IMA' [K.] 'Operating System'
moon charon: 09[PTS] measurement time: Jul 30 19:28:13 2012
moon charon: 09[PTS] PCR 10 extended with: 30:fa:77:07:af:01:a6:70:fc:35:33:86:fc:c9:54:40:e0:11:b0:8b
moon charon: 09[PTS] 'parport.ko'
...
```

PTS Functional Component Evidence IV

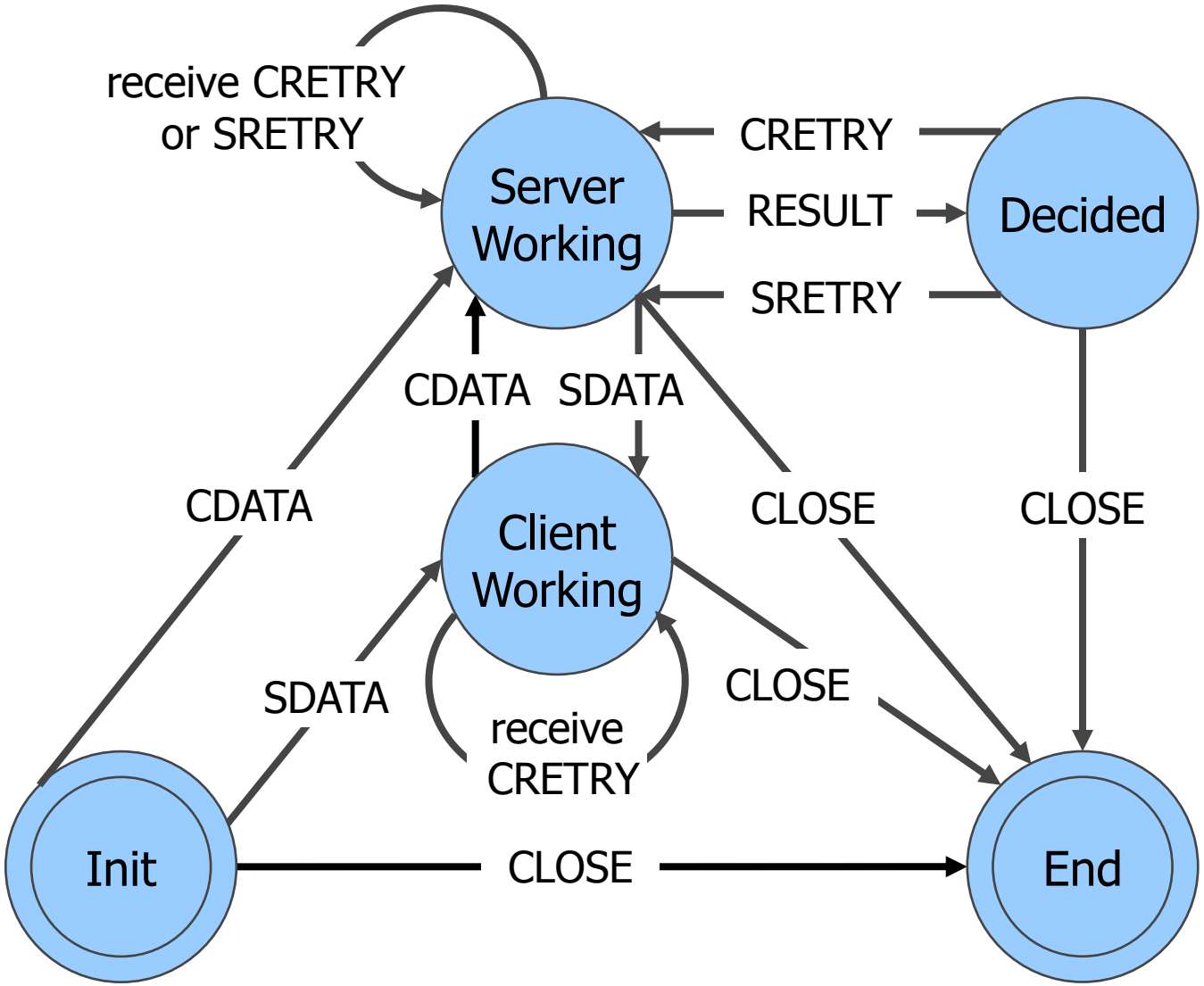
HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- With the Simple Evidence Final attribute the Attestation IMV on TNC client moon receives a TPM Quote2 signature computed over PCRs 0..7 and 10 which can be compared with the final state of the Shadow PCRs maintained by the IMV and which are extended with all the received measurements.
- The lookup of the 1247 IMA file measurements in the database was successful.

```
moon charon: 04[TNC] processing PA-TNC attribute type 'TCG/Simple Evidence Final'
moon charon: 04[PTS] constructed PCR Composite hash:
                     df:07:94:6e:04:72:ee:fe:4d:b0:c3:6e:92:1b:83:dc:e6:49:28:df
moon charon: 04[PTS] constructed TPM Quote Info: => 52 bytes @ 0x8287e2c
moon charon: 04[PTS] 0: 00 36 51 55 54 32 B2 CC 00 38 9D 23 E7 3B 43 D2 .6QUT2...8.#.;C.
moon charon: 04[PTS] 16: 91 88 CE D1 A1 0E 48 F2 B5 54 00 03 FF 04 00 01 ......H..T......
moon charon: 04[PTS] 32: DF 07 94 6E 04 72 EE FE 4D B0 C3 6E 92 1B 83 DC ...n.r..M..n....
moon charon: 04[PTS] 48: E6 49 28 DF .I(.
moon charon: 04[IMV] received PCR Composite matches constructed one
moon charon: 04[IMV] TPM Quote Info signature verification successful

moon charon: 04[PTS] processed 1247 ITA-HSR 'Linux IMA' file evidence measurements:
                     1177 ok, 70 unknown, 0 differ, 0 failed
```

PB-TNC Finite State Machine



PTS Evidence Bulk Data Transfer I

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- 1374 Simple Component Evidence PA-TNC attributes + 1 Simple Evidence Final PA-TNC attribute must be transferred from Attestation IMC to Attestation IMV, amounting to 120k of bulk data.
- Split into 4 PA-TNC messages of 32k each.

```
carol charon: 16[TNC] creating PA-TNC message with ID 0xf3bc541f
carol charon: 16[TNC] creating PA-TNC attribute type 'TCG/Simple Component Evidence'
      charon: last message repeated 380 times
carol charon: 16[TNC] creating PB-PA message type 'TCG/PTS'

carol charon: 16[TNC] creating PA-TNC message with ID 0xa22d16f2
carol charon: 16[TNC] creating PA-TNC attribute type 'TCG/Simple Component Evidence
      charon: last message repeated 346 times
carol charon: 16[TNC] creating PB-PA message type 'TCG/PTS'

carol charon: 16[TNC] creating PA-TNC message with ID 0x0600eabb
carol charon: 16[TNC] creating PA-TNC attribute type 'TCG/Simple Component Evidence
      charon: last message repeated 337 times
carol charon: 16[TNC] creating PB-PA message type 'TCG/PTS'

carol charon: 16[TNC] creating PA-TNC message with ID 0x512bd6ea
carol charon: 16[TNC] creating PA-TNC attribute type 'TCG/Simple Component Evidence
      charon: last message repeated 307 times
carol charon: 16[TNC] creating PA-TNC attribute type 'TCG/Simple Evidence Final'
carol charon: 16[TNC] creating PB-PA message type 'TCG/PTS'
```

PTS Evidence Bulk Data Transfer II

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- TNC client carol sends PB-TNC CDATA batch with first 32k PB-BA message to TNC server moon.
- Remaining 3 PB-BA messages are put in a queue.
- PT-EAP transport protocol based on EAP-TTLS splits 32k PB-TNC batch into 33 fragments of 1024 bytes each, ready for IKEv2 UDP transport.

```
carol charon: 16[TNC] PB-TNC state transition from 'Client Working' to 'Server Working'
carol charon: 16[TNC] creating PB-TNC CDATA batch
carol charon: 16[TNC] adding PB-PA message
carol charon: 16[TNC] sending PB-TNC CDATA batch (32678 bytes) for Connection ID 1
carol charon: 16[TNC] queued 3 PB-TNC messages for next CDATA batch

carol charon: 16[IKE] sending tunneled EAP-TTLS AVP [EAP/RES/TNC]
carol charon: 16[ENC] generating IKE_AUTH request 16 [ EAP/RES/TTLS ]
carol charon: 16[NET] sending packet: from 192.168.0.254[4500] to 192.168.0.1[4500]
...
carol charon: 03[NET] received packet: from 192.168.0.1[4500] to 192.168.0.254[4500]
carol charon: 03[ENC] parsed IKE_AUTH response 47 [ EAP/REQ/TTLS ]
carol charon: 03[ENC] generating IKE_AUTH request 48 [ EAP/RES/TTLS ]
carol charon: 03[NET] sending packet: from 192.168.0.254[4500] to 192.168.0.1[4500]
```

PTS Evidence Bulk Data Transfer III

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- Attestation IMV hasn't received Simple Evidence Final attribute yet and thus can't produce a final recommendation on the state of health.
- TNC server moon sends an empty PB-TNC SDATA batch to TNC client carol.

```
moon charon: 09[TNC] no recommendation available yet, sending empty PB-TNC SDATA batch
moon charon: 09[TNC] PB-TNC state transition from 'Server Working' to 'Client Working'
moon charon: 09[TNC] creating PB-TNC SDATA batch
moon charon: 09[TNC] sending PB-TNC SDATA batch (8 bytes) for Connection ID 1
moon charon: 09[IKE] sending tunneled EAP-TTLS AVP [EAP/REQ/TNC]
moon charon: 09[ENC] generating IKE_AUTH response 48 [ EAP/REQ/TTLS ]
moon charon: 09[NET] sending packet: from 192.168.0.1[4500] to 192.168.0.254[4500]
```

PTS Evidence Bulk Data Transfer IV

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- TNC client carol sends next 32k PB-PA message in PB-TNC CDATA batch to TNC server moon leaving 2 messages in queue.
- This CDATA/SDATA batch exchange is repeated until the message queue is empty.

```
carol charon: 02[NET] received packet: from 192.168.0.1[4500] to 192.168.0.254[4500]
carol charon: 02[ENC] parsed IKE_AUTH response 48 [ EAP/REQ/TTLS ]
carol charon: 02[IKE] received tunneled EAP-TTLS AVP [EAP/REQ/TNC]
carol charon: 02[TNC] received TNCCS batch (8 bytes) for Connection ID 1
carol charon: 02[TNC] PB-TNC state transition from 'Server Working' to 'Client Working'
carol charon: 02[TNC] processing PB-TNC SDATA batch
carol charon: 02[TNC] PB-TNC state transition from 'Client Working' to 'Server Working'
carol charon: 02[TNC] creating PB-TNC CDATA batch
carol charon: 02[TNC] adding PB-PA message
carol charon: 02[TNC] sending PB-TNC CDATA batch (32695 bytes) for Connection ID 1
carol charon: 02[TNC] queued 2 PB-TNC messages for next CDATA batch
carol charon: 02[IKE] sending tunneled EAP-TTLS AVP [EAP/RES/TNC]
carol charon: 02[ENC] generating IKE_AUTH request 49 [ EAP/RES/TTLS ]
carol charon: 02[NET] sending packet: from 192.168.0.254[4500] to 192.168.0.1[4500]
...
```

PTS Evidence Bulk Data Transfer V

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- Attestation IMV has received all measurement data an provides a recommendation of 'allow ' and an evaluation of 'compliant'.
- TNC server moon sends a PB-TNC RESULT batch to TNC client moon containing a PB-Assessment-Result and a PB-Access-Recommendation message.
- IKEv2 authentication is then completed successfully and client is allowed into the corporate network.

```
moon charon: 04[TNC] IMV 1 provides recommendation 'allow' and evaluation 'compliant'
moon charon: 04[TNC] PB-TNC state transition from 'Server Working' to 'Decided'
moon charon: 04[TNC] creating PB-TNC RESULT batch
moon charon: 04[TNC] adding PB-Assessment-Result message
moon charon: 04[TNC] adding PB-Access-Recommendation message
moon charon: 04[TNC] sending PB-TNC RESULT batch (40 bytes) for Connection ID 1
moon charon: 04[IKE] sending tunneled EAP-TTLS AVP [EAP/REQ/TNC]
moon charon: 04[ENC] generating IKE_AUTH response 143 [ EAP/REQ/TTLS ]
moon charon: 04[NET] sending packet: from 192.168.0.1[4500] to 192.168.0.254[4500]
```

Conclusions

- The suite of TCG Trusted Network Connect protocols which adhere to the IETF Network Endpoint Assessment reference model allow the efficient and robust transfer of Linux IMA measurement data.
- The remote attestion of >1200 IMA file measurements currently takes about 20 seconds.
- The identified bottleneck is the reference measurement lookup in the SQLite database (2 MB size containing 10‘000 entries with optimized filename index).
- A RAM-based reference measurement cache using hashtables might considerably speed up the lookup process.

Thank you for your attention!

Questions?

www.strongswan.org/tnc/