

strongSwan TNC Activities Update

TCG Members Meeting June 2013 Dublin

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

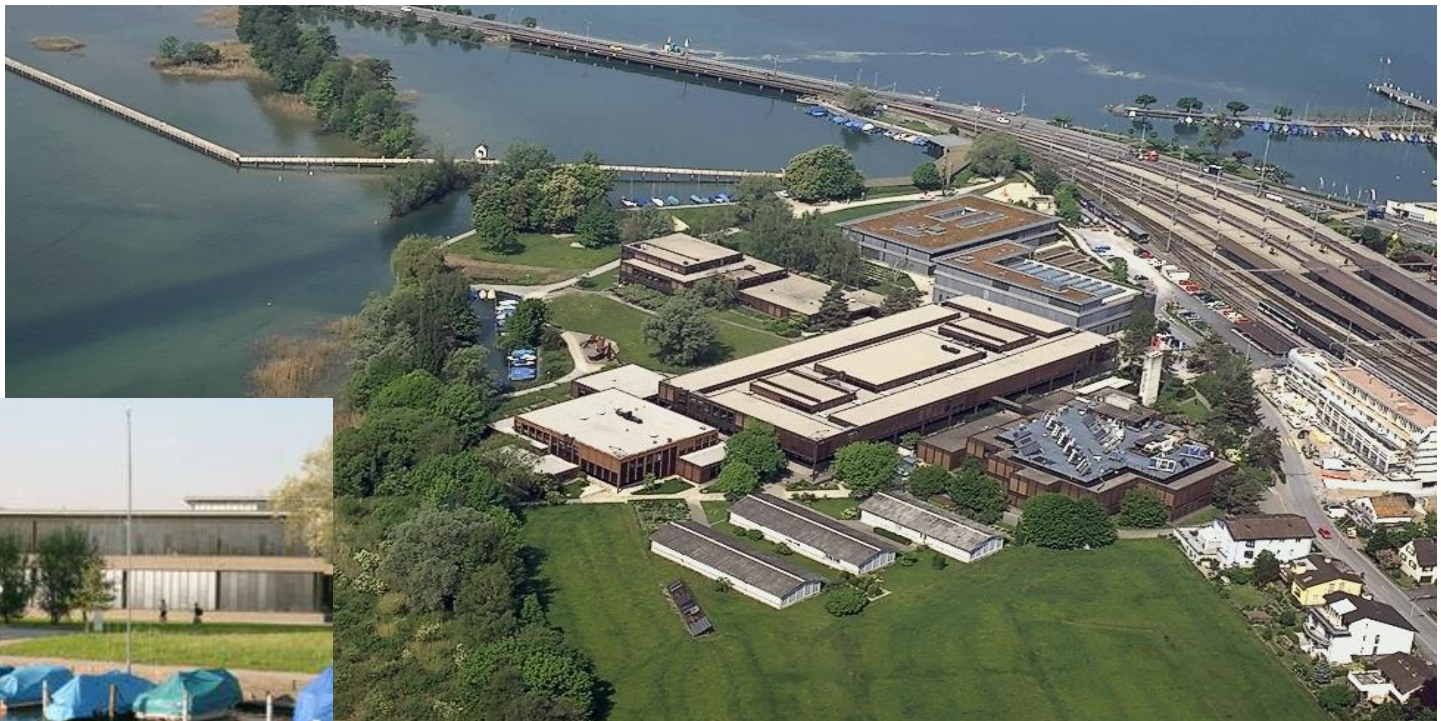


Where the heck is Rapperswil?



HSR - Hochschule für Technik Rapperswil

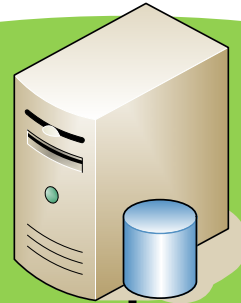
- University of Applied Sciences with about 1500 students
- Faculty of Information Technology (300-400 students)
- Bachelor Course (3 years), Master Course (+1.5 years)



strongSwan – the OpenSource VPN Solution



Windows Active Directory Server

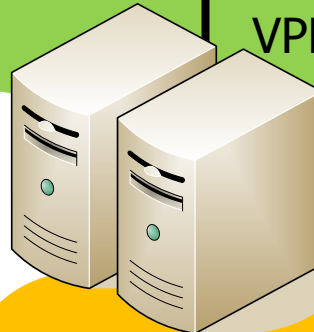
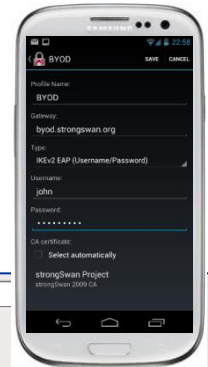


Linux FreeRadius Server



Campus Network

High-Availability strongSwan VPN Gateway



Internet



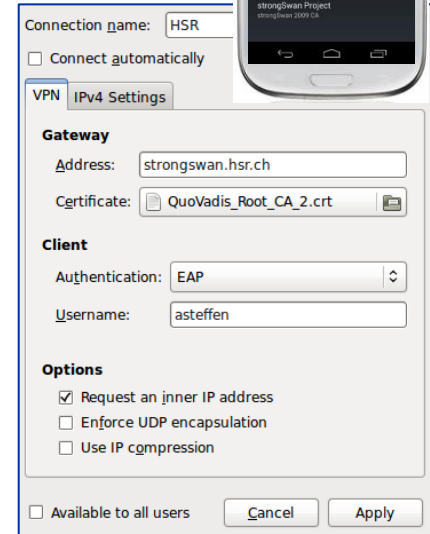
strongswan.hsr.ch



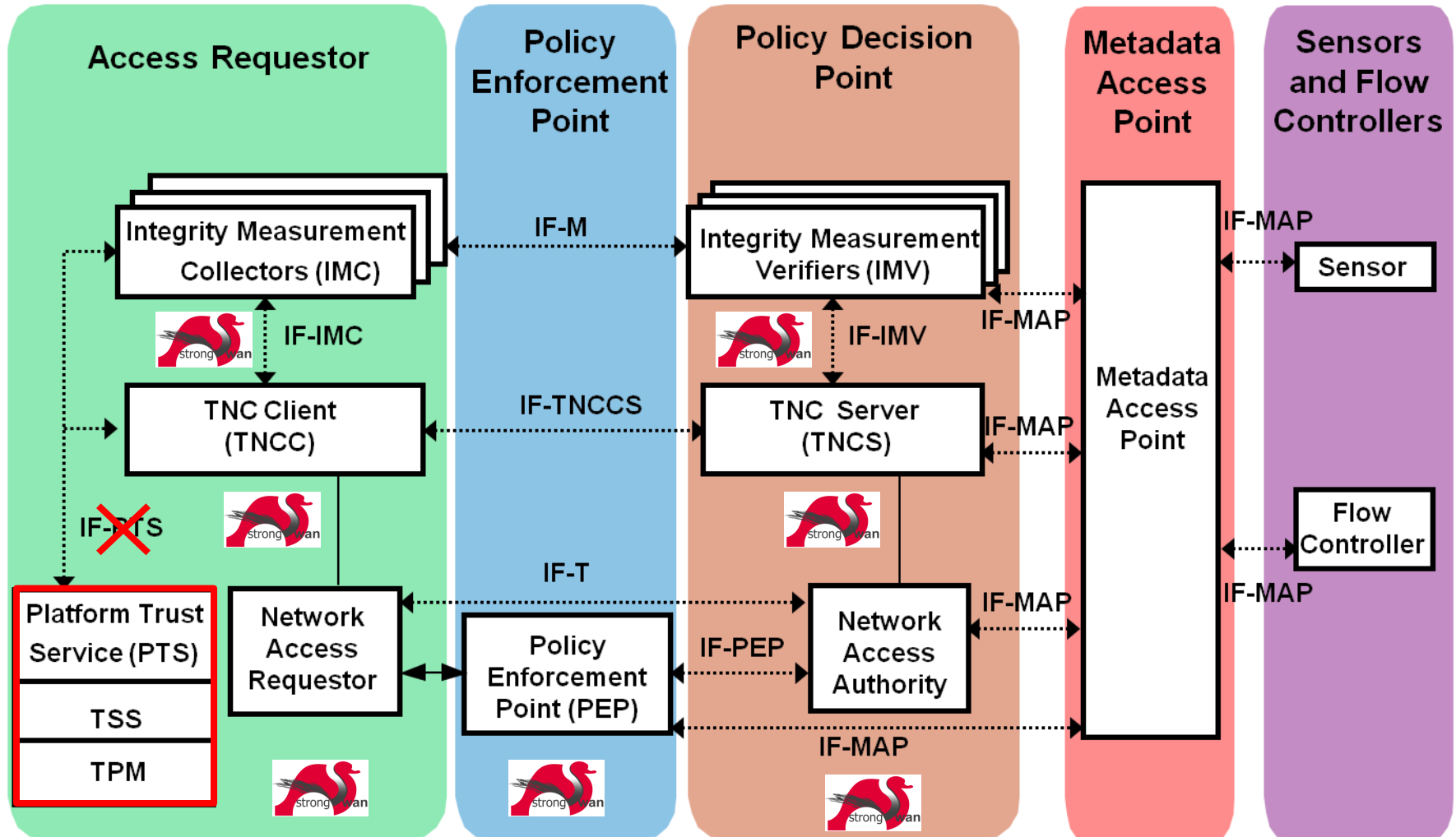
strongSwan Linux Client



Windows 7/8 Agile VPN Client



Trusted Network Connect (TNC) Framework



strongSwan TNC Activities Update

TCG Members Meeting Juni 2013 Dublin

strongSwan IMC/IMV Pairs

- **Objective**
 - Get Operating System Information
- **Subscribed IF-M Subtype**
 - IETF/Operating System
- **Supported IF-M Attributes**
 - IETF/Attribute Request
 - IETF/Product Information, IETF/String Version, IETF/Numeric Version
 - IETF/Operational Status (**Linux Uptime**)
 - IETF/Installed Packages (**Android, Debian, Ubuntu**)
 - IETF/Forwarding Enabled
 - IETF/Factory Default Password Enabled
 - IETF/Assessment Result
 - IETF/Remediation Instructions
 - IETF/IF-M Error
 - ITA/Device ID (**Android ID, Linux D-Bus ID, TPM AIK Fingerprint**)
 - ITA/Get Settings, ITA/Settings
 - ITA/Start Angel, ITA/Stop Angel (**Fragmentation of Installed Packages**)

Scanner IMC/IMV Pair

- **Objective**
 - Scan open listening TCP and UDP ports
- **Subscribed IF-M Subtype**
 - IETF/VPN
- **Supported IF-M Attributes**
 - IETF/Attribute Request
 - IETF/Port Filter
 - IETF/Assessment Result
 - IETF/Remediation Instructions
 - IETF/IF-M Error

- **Objective**
 - File/Directory Measurements and TPM-based Remote Attestation
- **Subscribed IF-M Subtypes**
 - TCG/PTS, IETF/Operating System (IMV only, requires an OS IMC)
- **Supported IF-M Attributes**
 - TCG/Request PTS Protocol Capabilities, TCG/PTS Protocol Capabilities
 - TCG/PTS Measurement Algorithm Request/Response
 - TCG/Request File Measurement, TCG/File Measurement
 - TCG/Request File Metadata, TCG/Unix-Style File Metadata
 - TCG/D-H Nonce Parameters Request/Response, TCG/D-H Nonce Finish
 - TCG/Get TPM Version Information, TCG/TPM Version Information
 - TCG/Get Attestation Identity Key, TCG/Attestation Identity Key
 - TCG/Request Functional Component Evidence
 - TCG/Generate Attestation Evidence
 - TCG/Simple Component Evidence, TCG/Simple Evidence Final (Quote)
 - IETF/IF-M Error, IETF/Attribute Request
 - IETF/Product Information, IETF/String Version
 - IETF/Assessment Result, IETF/Remediation Instructions

strongSwan TNC Activities Update

TCG Members Meeting Juni 2013 Dublin

Linux Integrity Measurement Architecture (IMA)



HSR

HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

- **Linux Security Summit 2012 Paper**
 - Presented in September at LinuxCon in San Diego
 - The transfer and database lookup of 1200 file measurements amounting to about 120 kB of IMA measurements and certified by a Quote2 TPM signature takes about 20 seconds.
 - <http://www.strongswan.org/lss2012.pdf>

- 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]
```

- 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 be 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
	


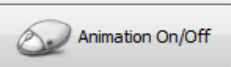



strongSwan TNC Activities Update

TCG Members Meeting Juni 2013 Dublin

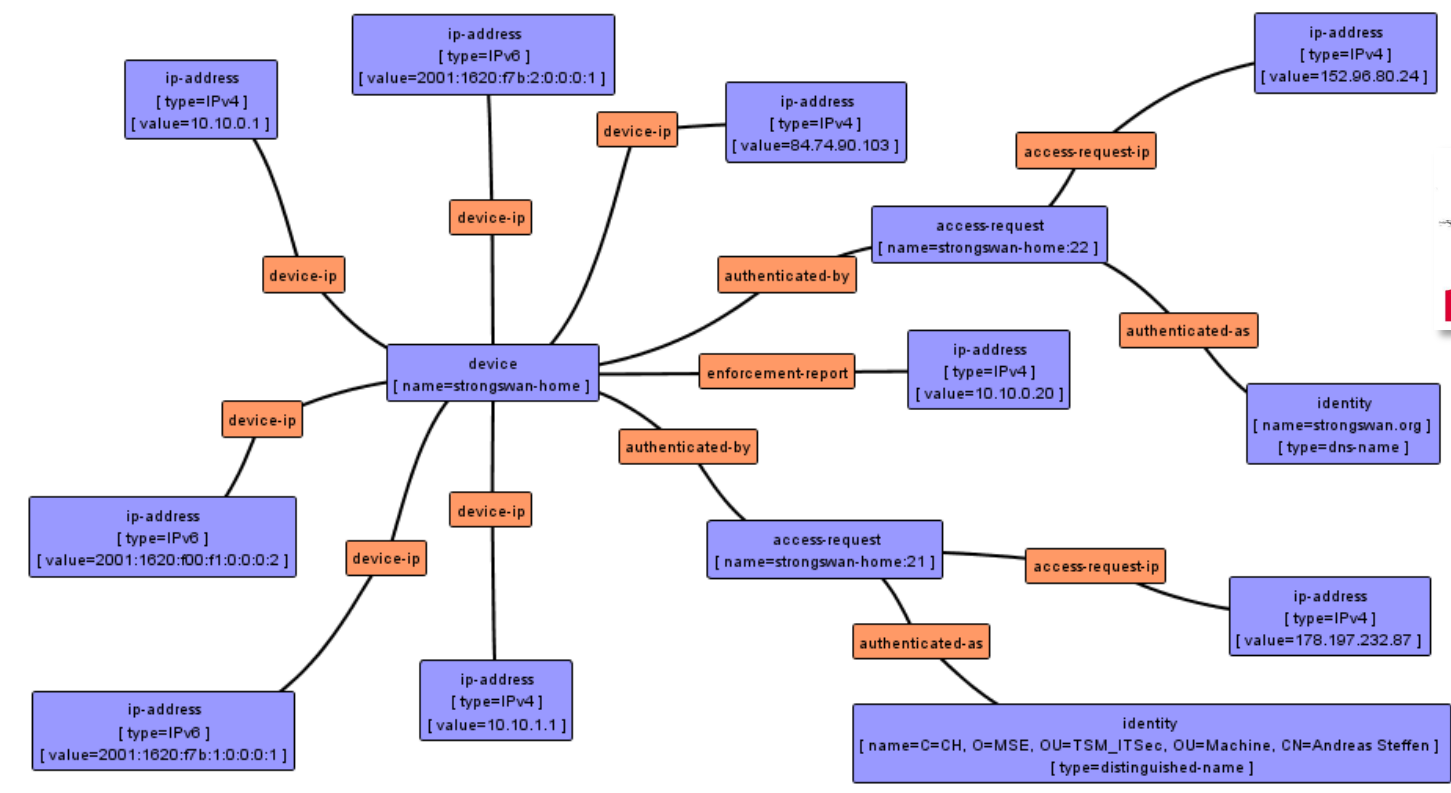
strongSwan PDP as an IF-MAP Client

Open Source TNC IF-MAP Products

IRONGUI 0.3.0

Trust@FHH IRON



meta:device-ip [ifmap-publisher: strongSec_2007_CA-11058845081 ifmap-timestamp: 2011-09-06T06:56:25+02:00 ifmap-cardinality: singleValue]

Element	Value / Attribute-Name	Attribute-Value

Last update: 07-09-2011 20:39:37



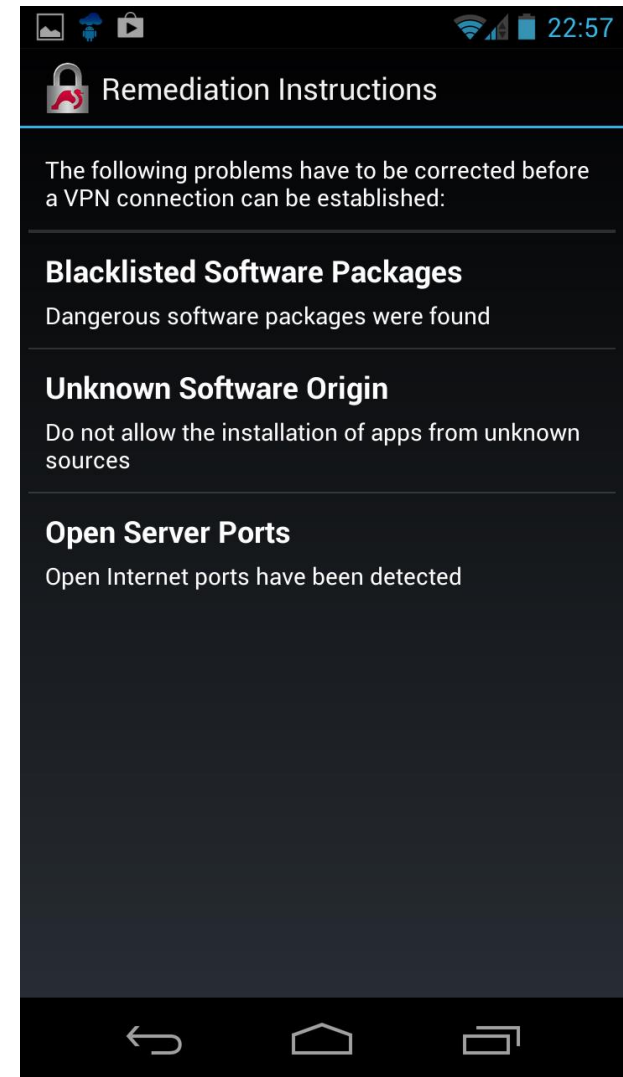
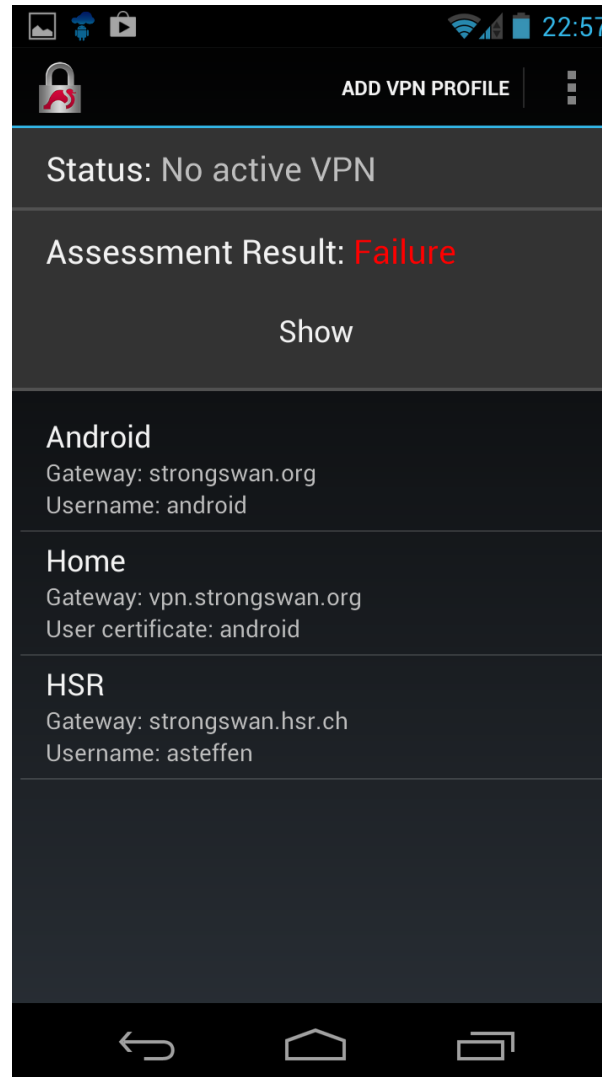
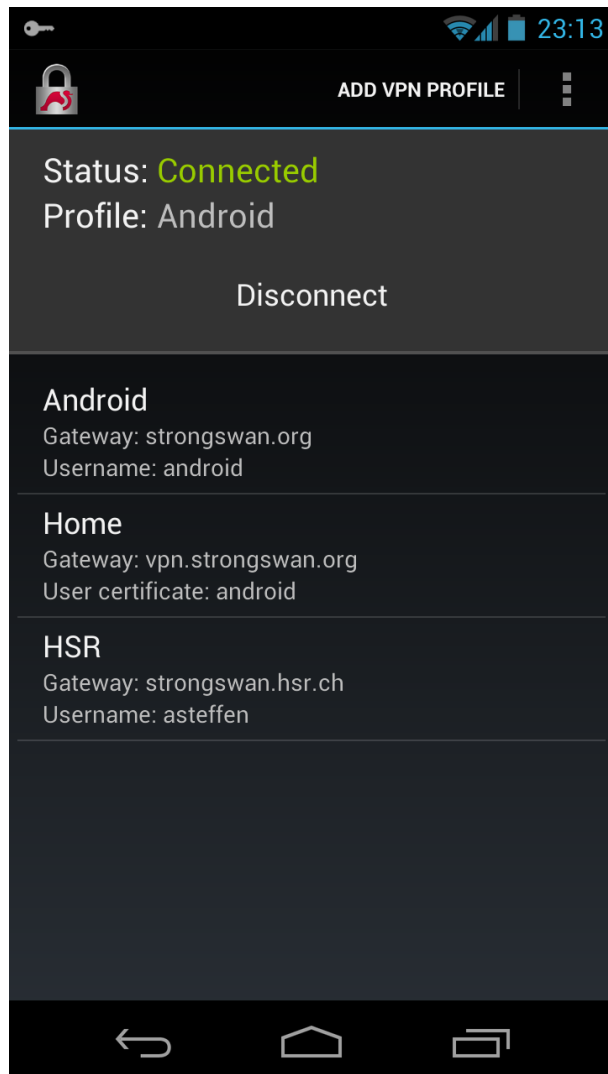
MAP-Client

strongSwan TNC Activities Update

TCG Members Meeting Juni 2013 Dublin

strongSwan BYOD Android VPN Client

strongSwan Android BYOD VPN Client

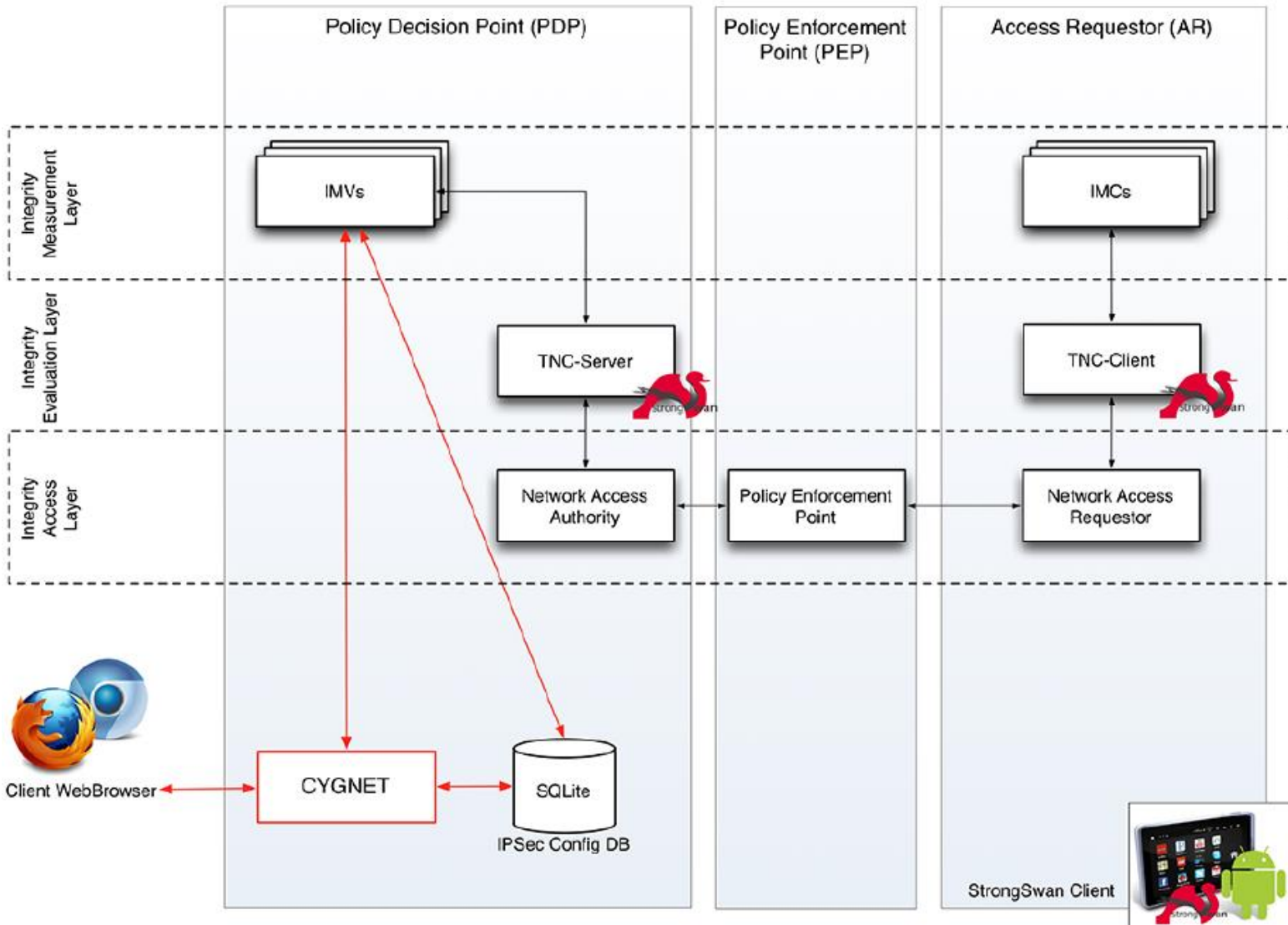


strongSwan TNC Activities Update

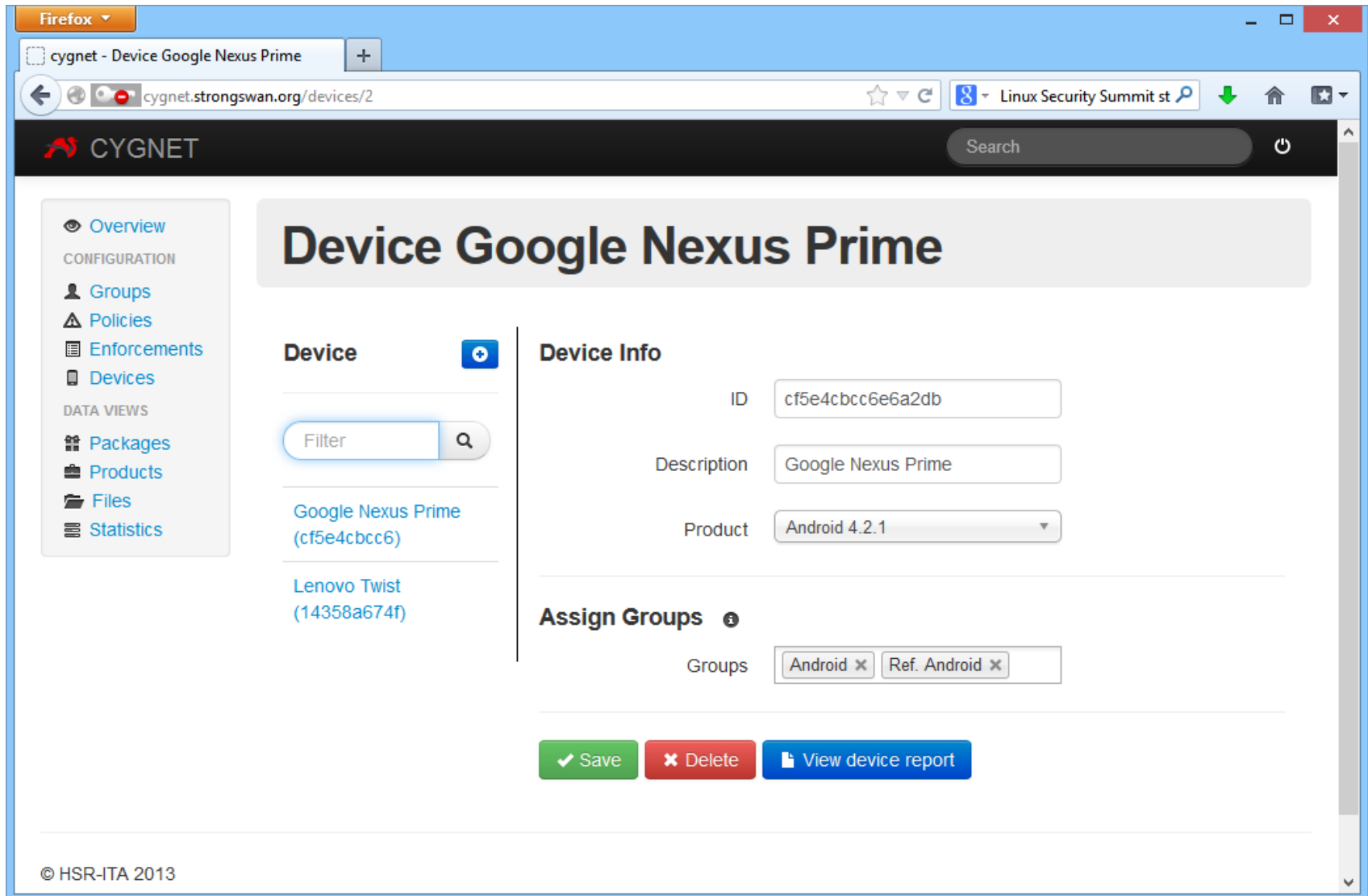
TCG Members Meeting Juni 2013 Dublin

CYGNET TNC Policy Manager

CYGNET TNC Policy Manager



CYGNET TNC Policy Manager



The screenshot shows a web browser window with the URL `cygnet.strongswan.org/devices/2`. The page title is "Device Google Nexus Prime". The interface includes a sidebar with navigation options: Overview, CONFIGURATION (Groups, Policies, Enforcements, Devices), and DATA VIEWS (Packages, Products, Files, Statistics). The main content area is titled "Device Google Nexus Prime" and contains a "Device" section with a filter input and a list of devices: "Google Nexus Prime (cf5e4cbcc6)" and "Lenovo Twist (14358a674f)". To the right, the "Device Info" section displays fields for ID (cf5e4cbcc6e6a2db), Description (Google Nexus Prime), and Product (Android 4.2.1). Below this is the "Assign Groups" section, which shows two assigned groups: "Android" and "Ref. Android". At the bottom of the device configuration area, there are three buttons: "Save", "Delete", and "View device report".

© HSR-ITA 2013

● Policy Types

- **PCKGS** Installed Packages
- **UNSRC** Unknown Source
- **FWDEN** Forwarding Enabled
- **PWDEN** Factory Default Password Enabled
- **FREFM** File Reference Measurement
- **FMEAS** File Measurement
- **FMETA** File Metadata
- **DREFM** Directory Reference Measurement
- **DMEAS** Directory Measurement
- **DMETA** Directory Metadata
- **TCPOP** TCP Ports allowed Open
- **TCPBL** TCP Ports to be Blocked
- **UDPOP** UDP Ports allowed Open
- **UDPBL** UDP Ports to be Blocked

Database Schema

