Android BYOD Security using Trusted Network Connect Protocol Suite

Prof. Andreas Steffen
HSR University of Applied Sciences Rapperswil
andreas.steffen@hsr.ch

The Trusted Computing Conference

AWARENESS IMAGINATION COLLABORATION AND SECURITY

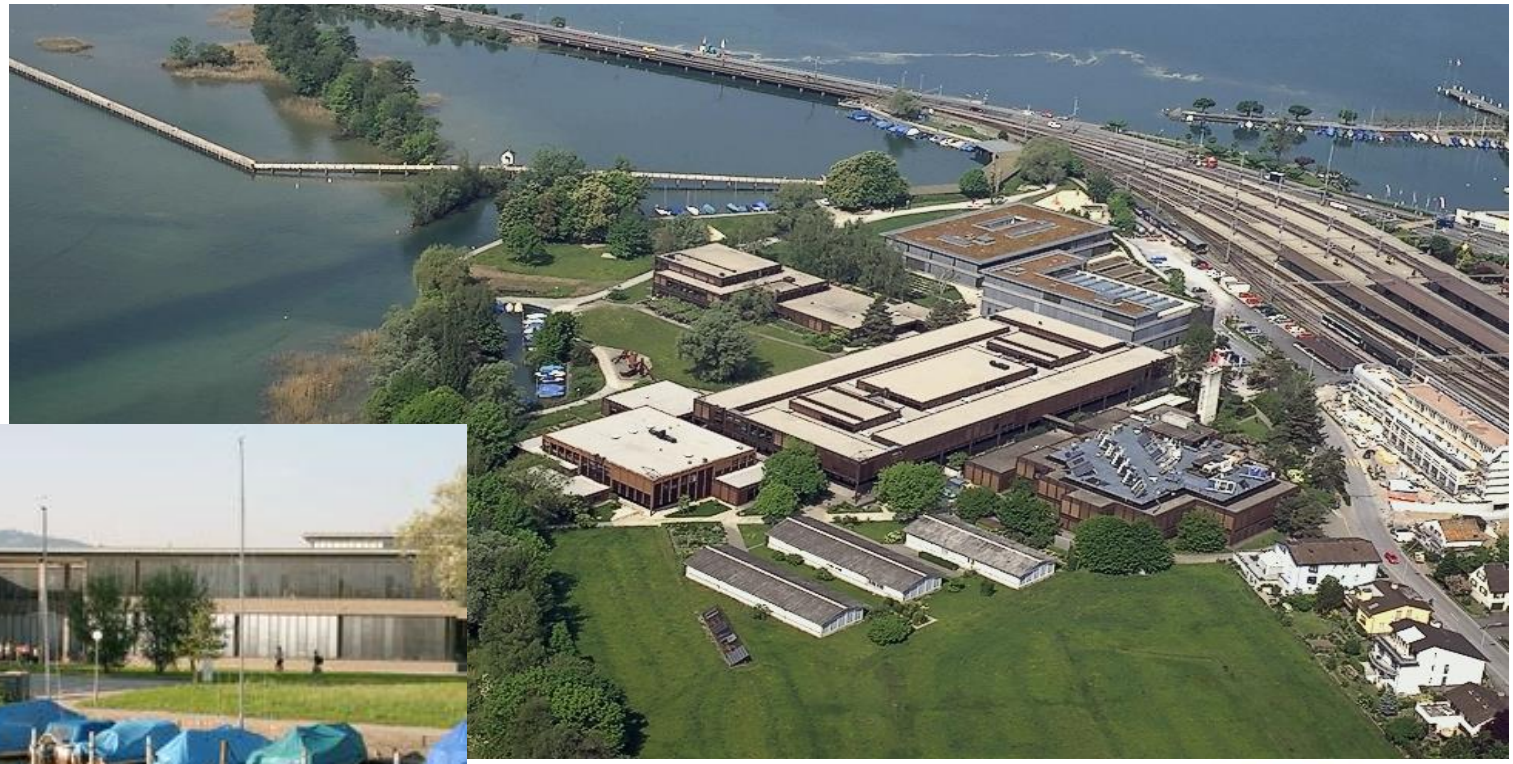
Where the heck is Rapperswil?

The Trusted Computing Conference

HSR Hochschule für Technik Rapperswil

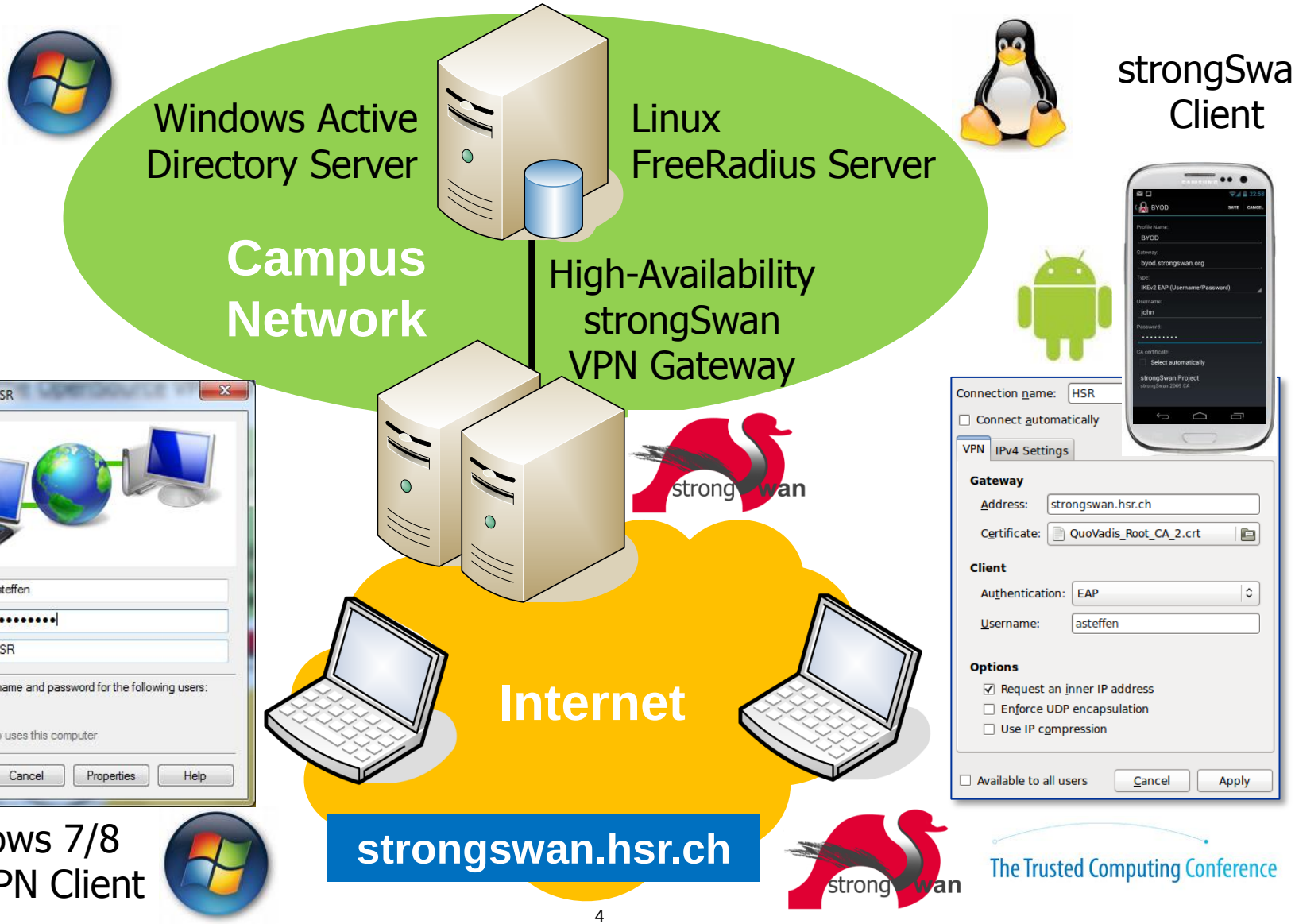
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

- 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 Trusted Computing Conference

strongSwan – the Open Source VPN Solution

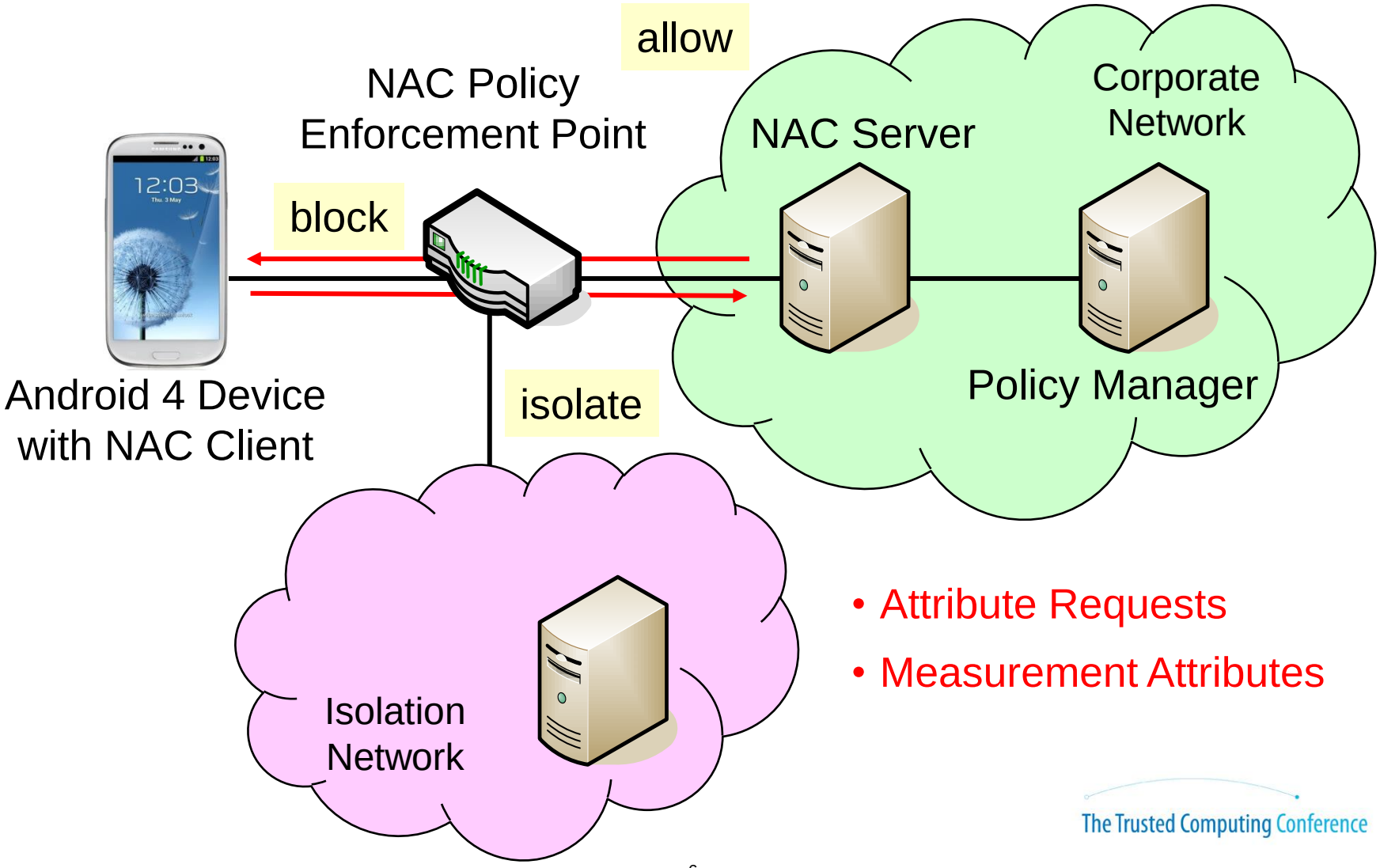


BYOD – Bring Your Own Device

Security Issues

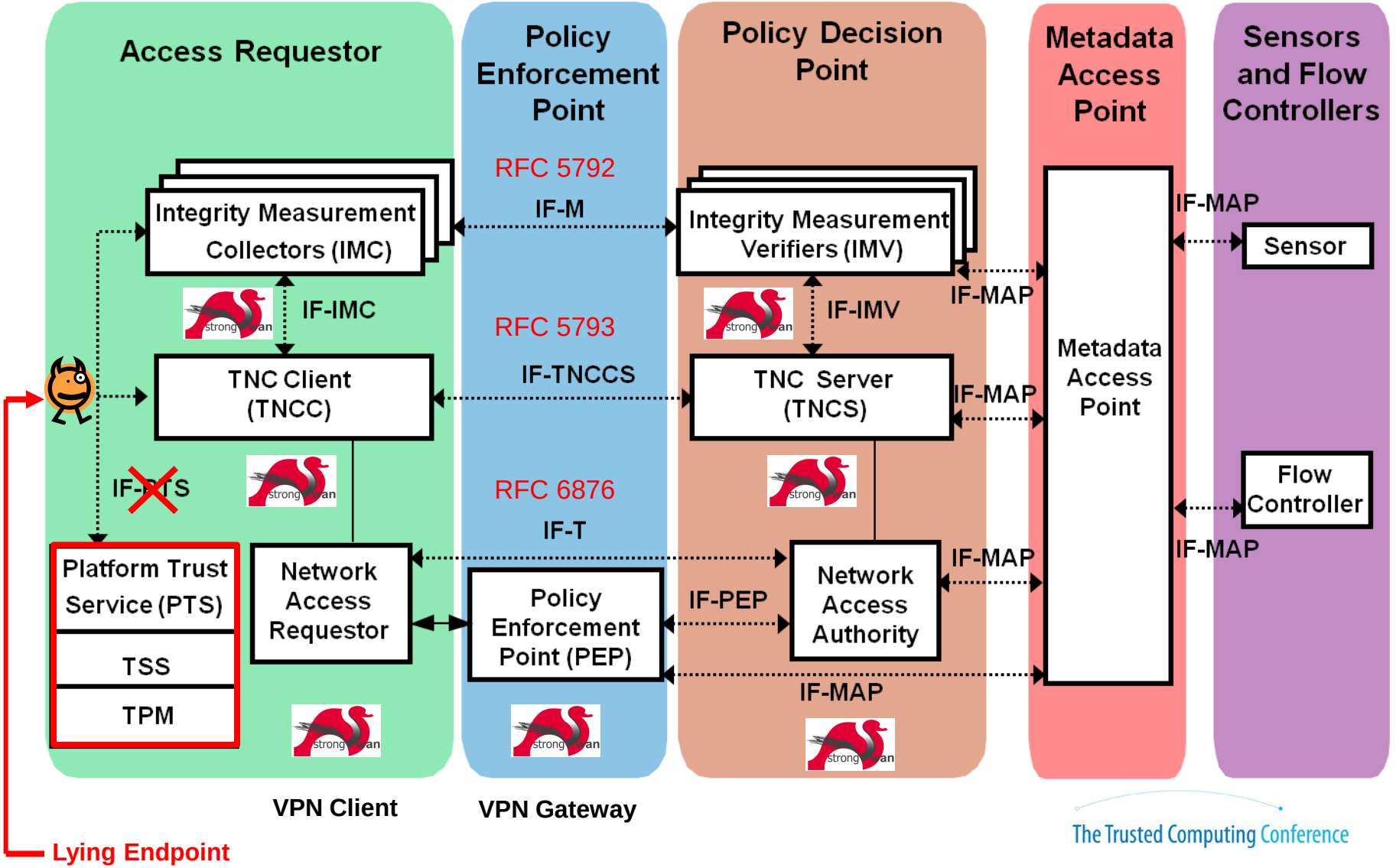
- Users do not protect access to their devices or use weak passwords or login methods.
- Users download and install dangerous software packages containing malware from unknown sources.
- Users do not regularly apply security updates to the installed software packages and operating system.
- Users run server applications potentially giving third parties access to the corporate network and/or sensitive data
- Malware might embed itself into the operating system, modifying system commands and libraries.

Android BYOD with Network Access Control



- Attribute Requests
- Measurement Attributes

TCG Trusted Network Connect (TNC) Architecture



Layered TNC Protocol Stack

- IF-T Transport Protocol — PT-TLS (RFC 6876) or PT-EAP

```
[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/TNC]
```

- 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'
```

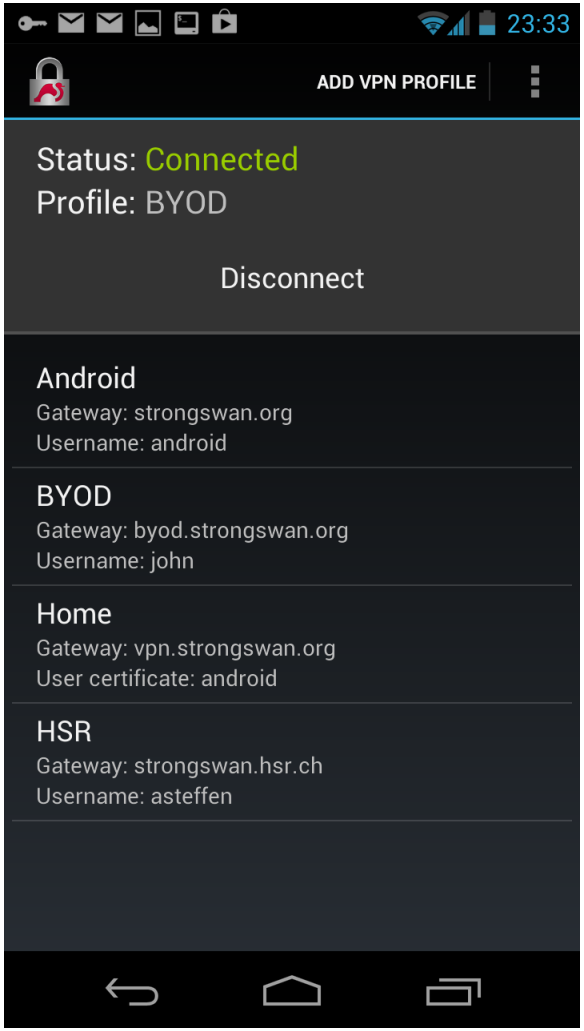
- IF-M Measurement Protocol — PA-TNC (RFC 5792)

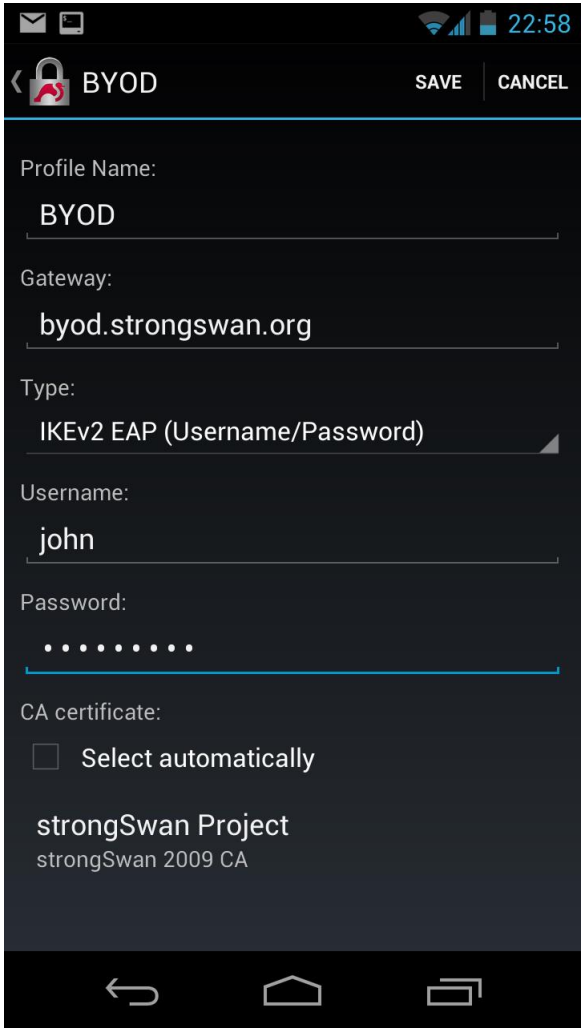
```
[TNC] handling PB-PA message type 'IETF/Operating System' 0x000000/0x00000001
[IMV] IMV 1 "OS" received message for Connection ID 1 from IMC 1
[TNC] processing PA-TNC message with ID 0xec41ce1d
[TNC] processing PA-TNC attribute type 'IETF/Product Information' 0x000000/0x00000002
[TNC] processing PA-TNC attribute type 'IETF/String Version' 0x000000/0x00000004
[TNC} processing PA-TNC attribute type 'ITA-HSR/Device ID' 0x00902a/0x00000008
```

- 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
```

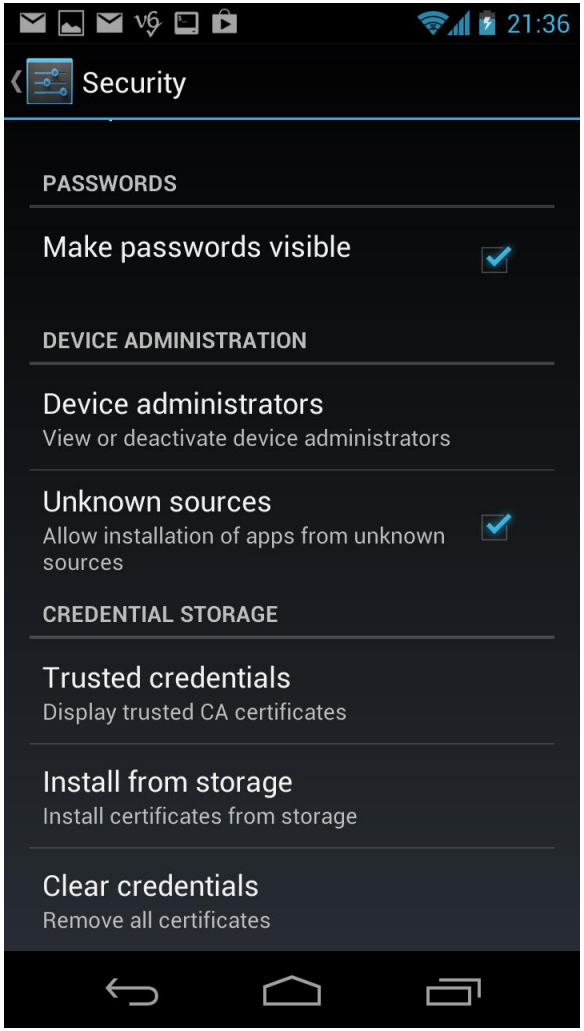
strongSwan Android VPN Client: Easy to Connect

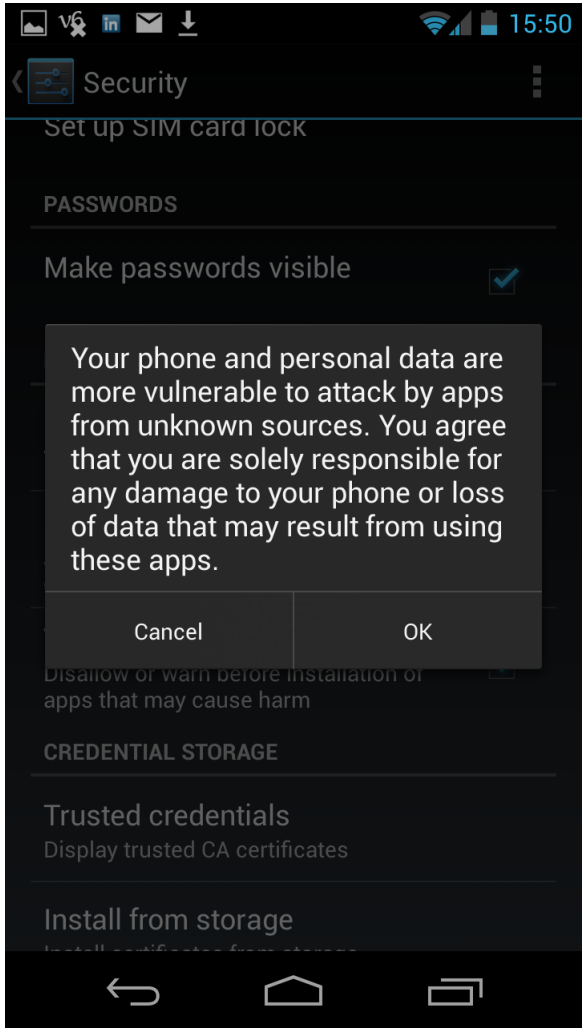




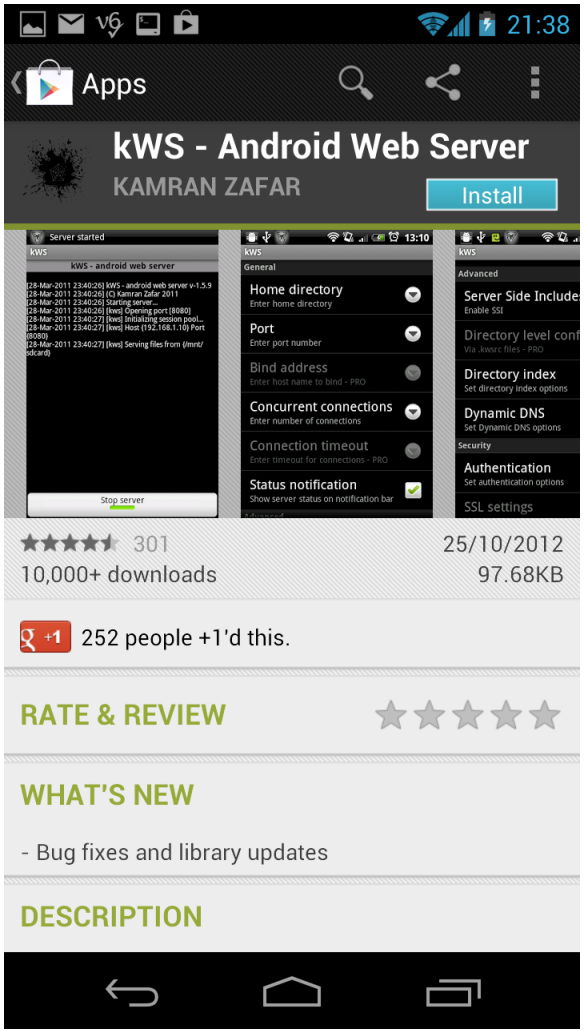
The Trusted Computing Conference

Dangerous: Allow Download from Unknown Sources



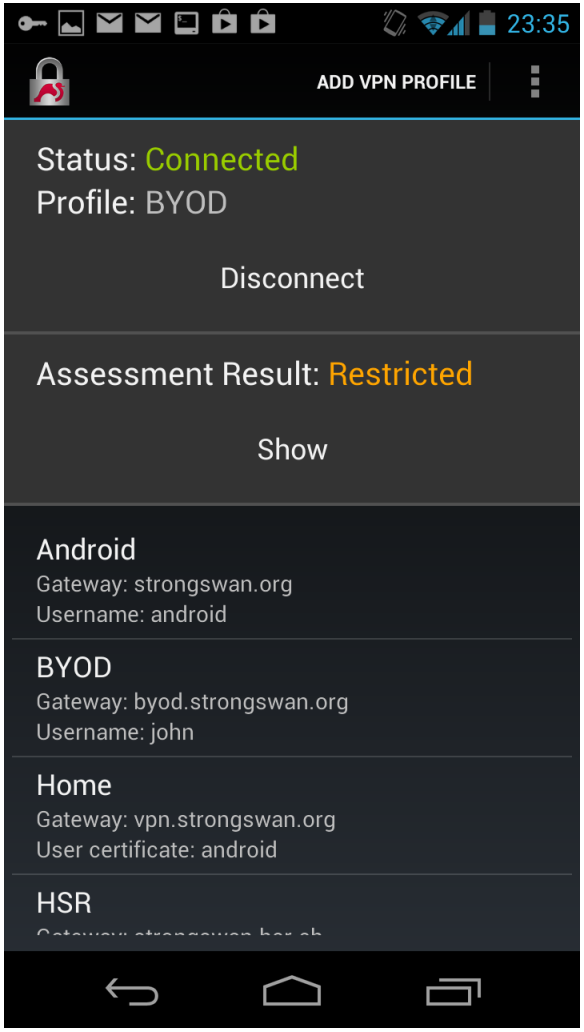


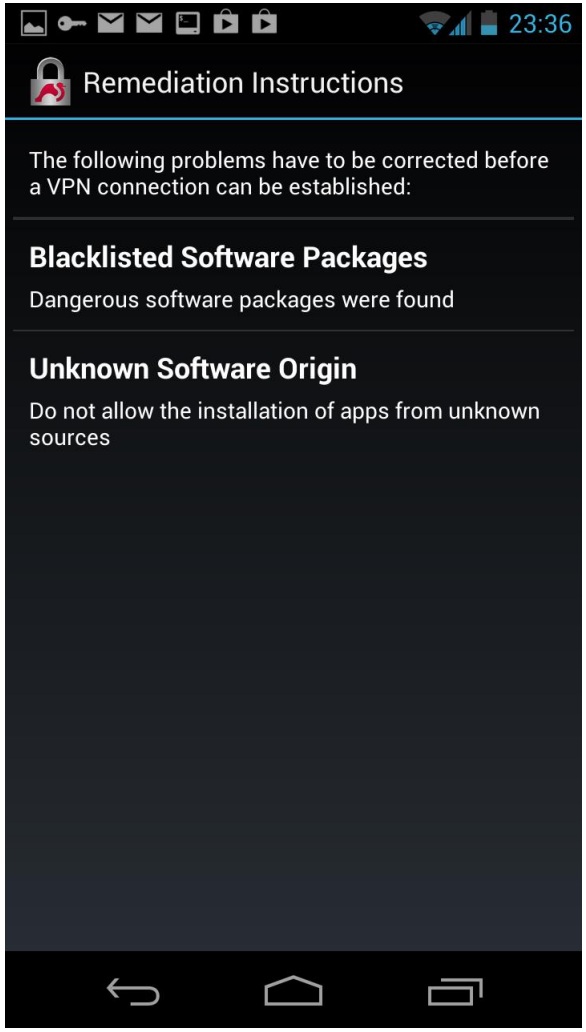
Install Blacklisted Android Web Server Package

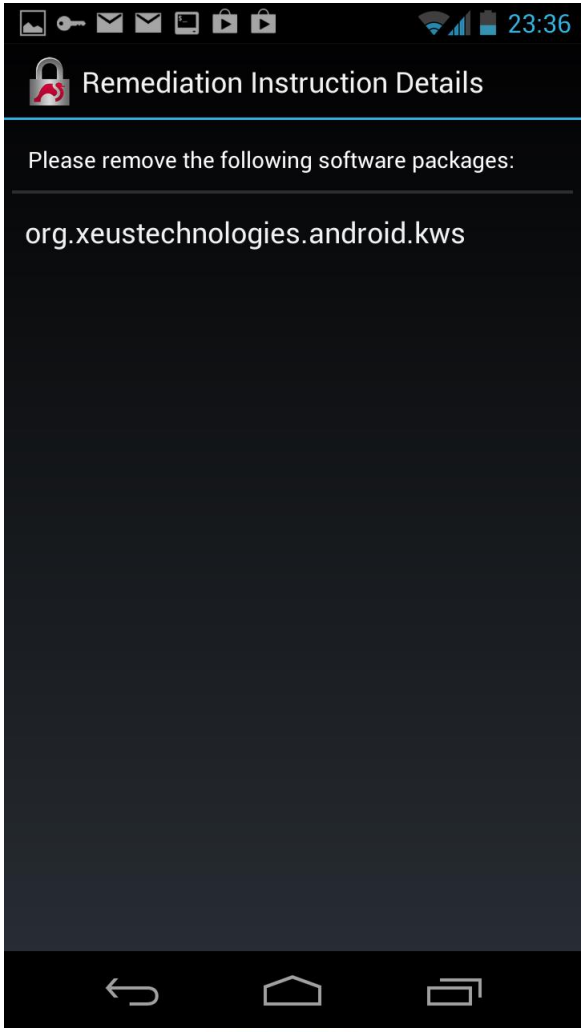


The Trusted Computing Conference

Minor Non-Compliance: Isolate Client

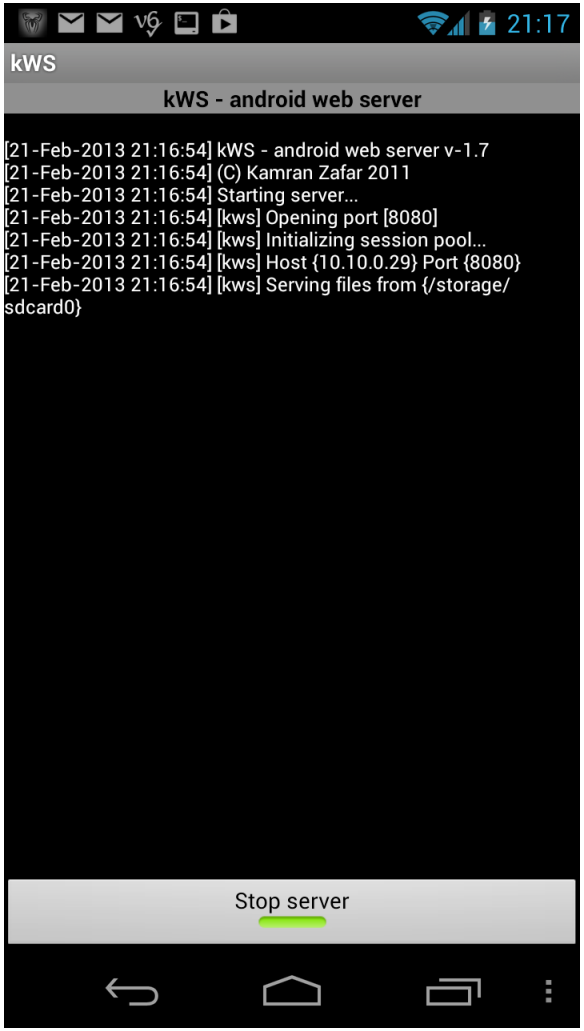




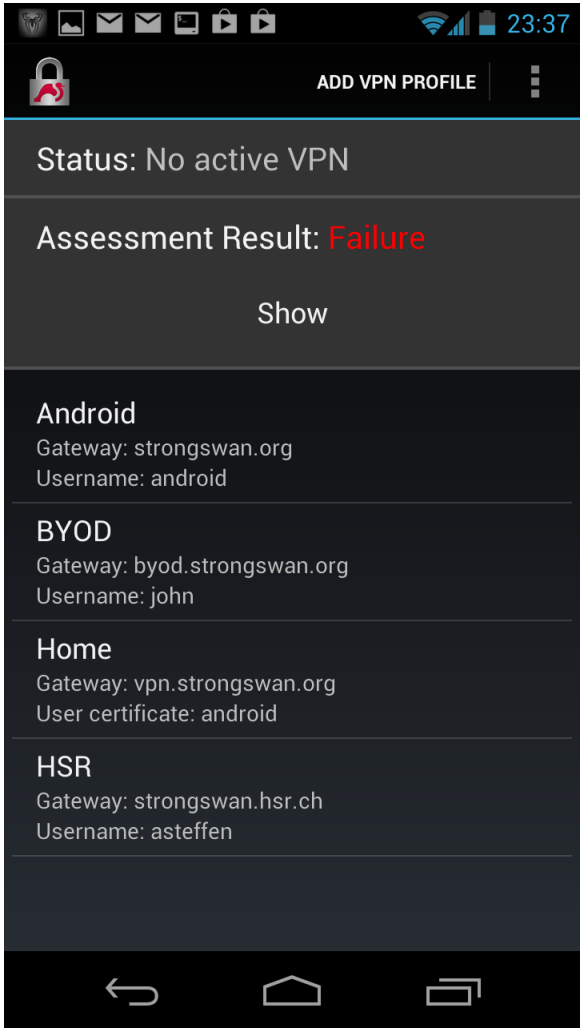


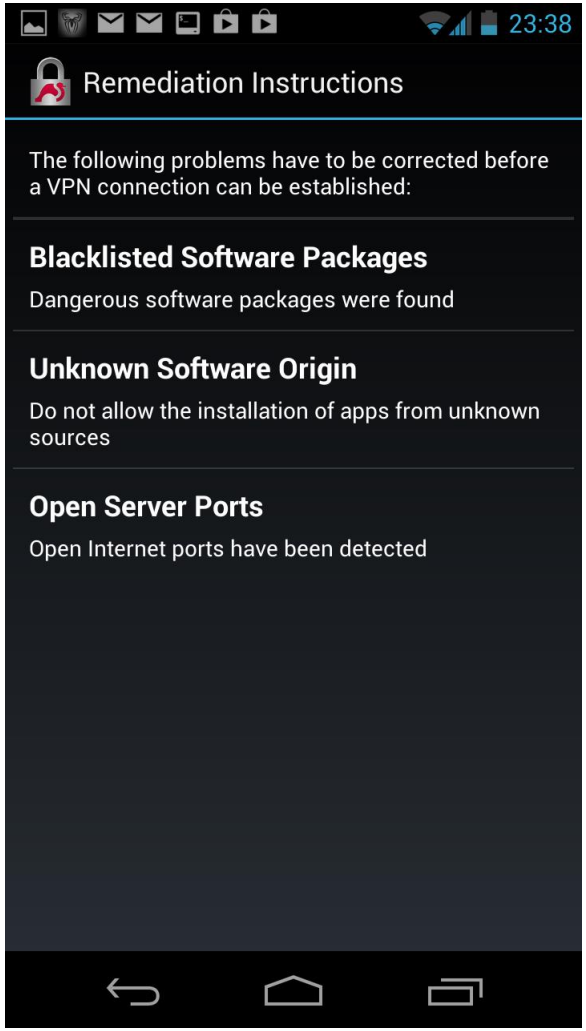
The Trusted Computing Conference

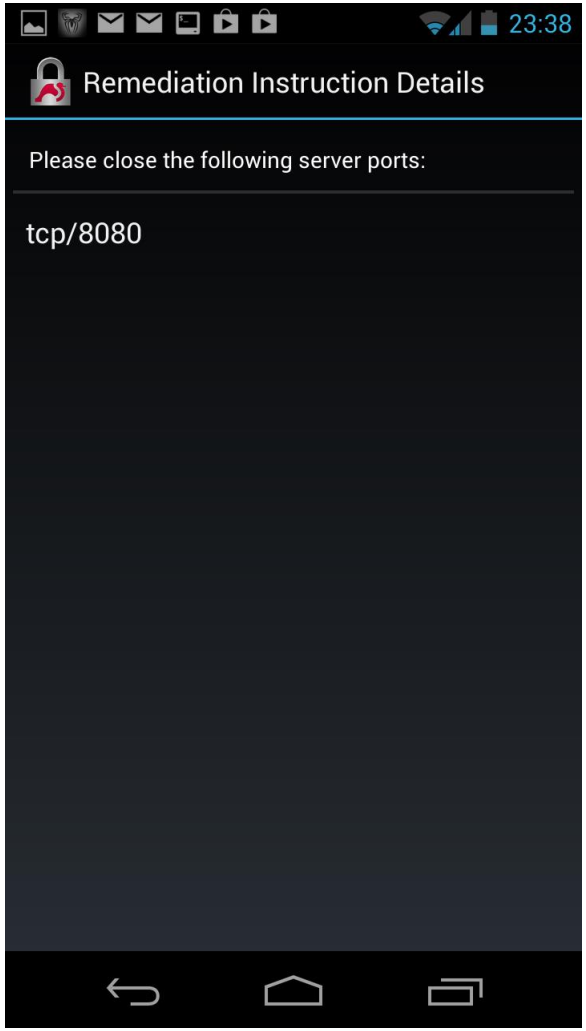
Start the Android Web Server



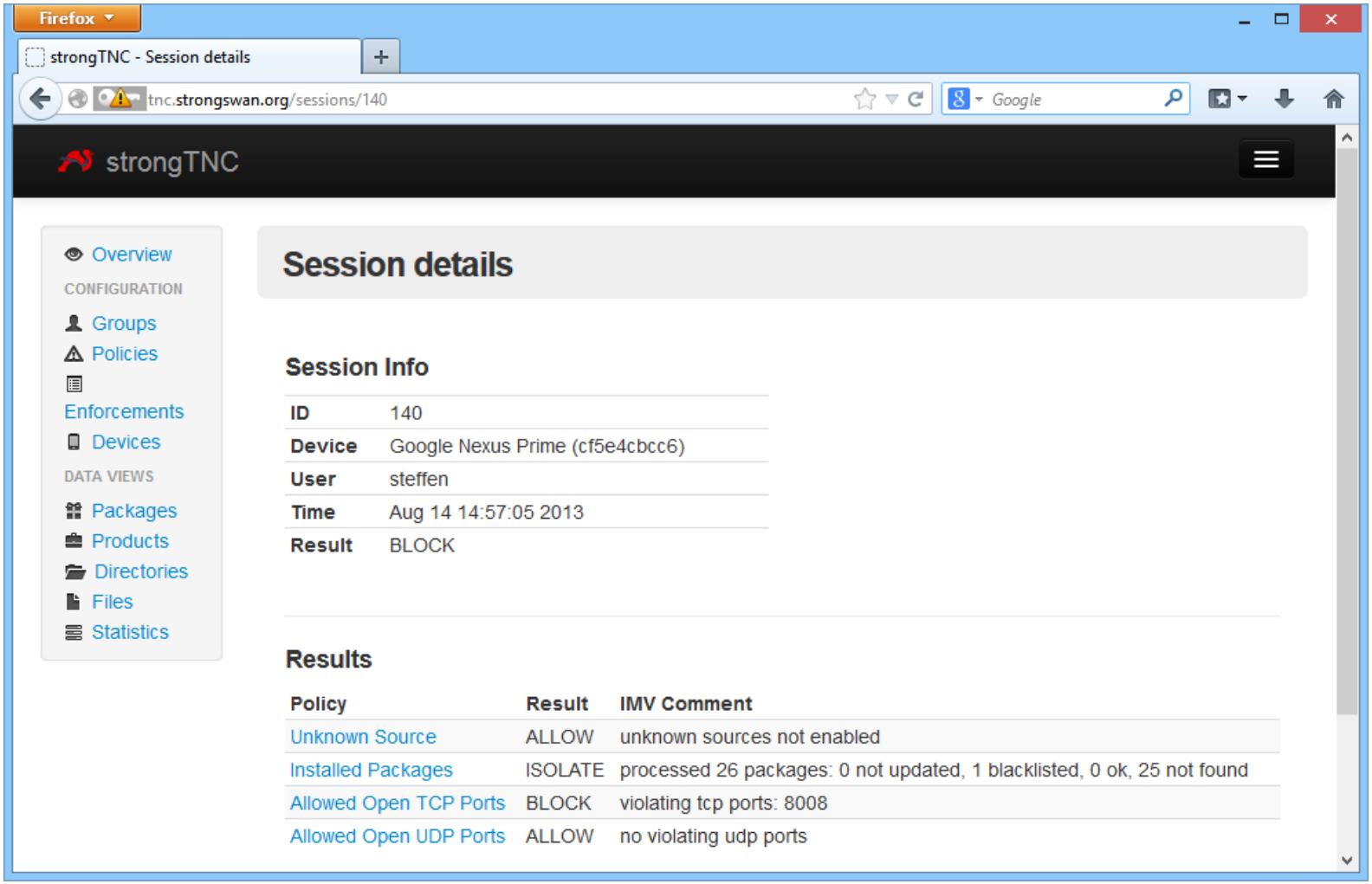
Major Non-Compliance: Block Client







strongTNC Policy Manager

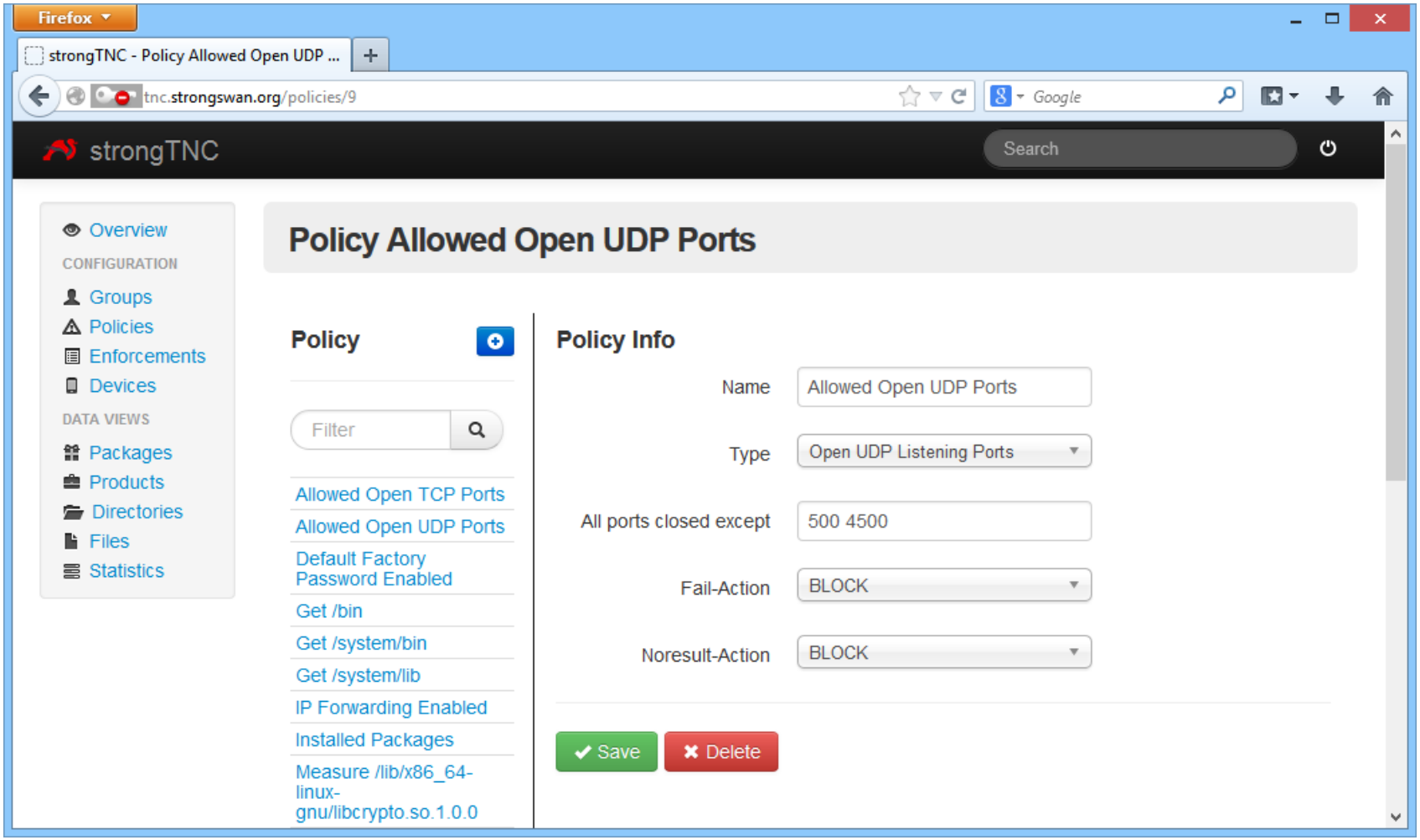


Defining Measurement Policies and Enforcements

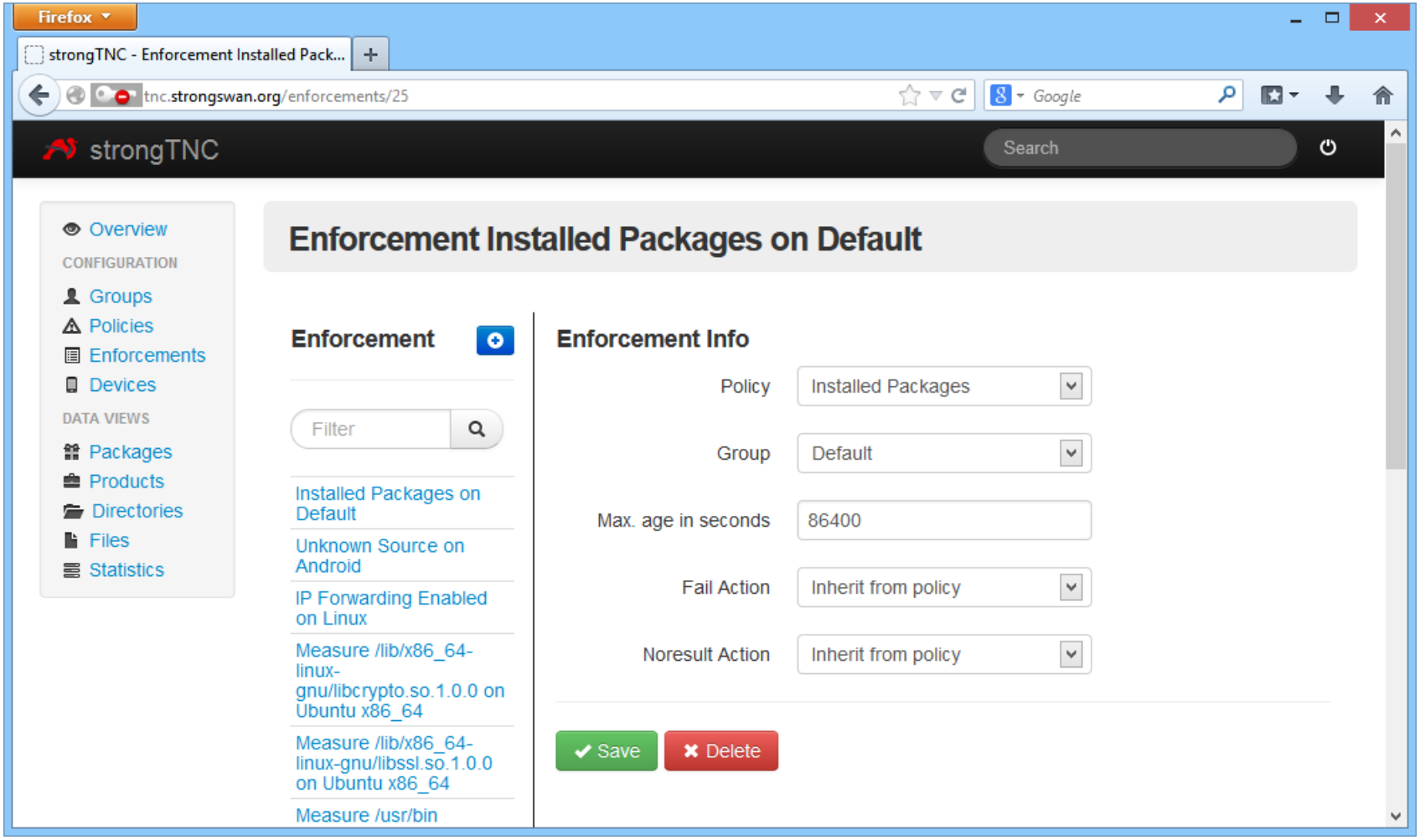
Currently supported policy types:

• PWDEN	Factory Default Password Enabled	
• FWDEN	Forwarding Enabled	
• TCPOP	TCP Ports allowed to be Open	Closed Port Default Policy
• TCPBL	TCP Ports to be Blocked	Open Port Default Policy
• UDPOP	UDP Ports allowed to be Open	Closed Port Default Policy
• UDPBL	UDP Ports to be Blocked	Open Port Default Policy
• PCKGS	Installed Packages	
• UNSRC	Unknown Sources	
• SWIDT	SWID (Software ID) Tag Inventory	Visit Demo at TCG Booth!
• FREFM	File Reference Measurement	SHA1/SHA256 Hash
• FMEAS	File Measurement	SHA1/SHA256 Hash
• FMETA	File Metadata	Create, Modify, Access Times
• DREFM	Directory Reference Measurement	SHA1/SHA256 Hashes
• DMEAS	Directory Measurement	SHA1/SHA256 Hashes
• DMETA	Directory Metadata	

Add/Edit Policies



Define Enforcements



Summary

- The TNC protocols have become Internet Standards
- The TNC protocols are platform-independent and allow interoperability
- The TNC protocols support trustworthy TPM-based remote attestation
- The strongSwan BYOD Showcase demonstrates that TNC is ready for use
- The strongTNC policy manager bases measurements on past client behaviour

Thank You

The Trusted Computing Conference

AWARENESS IMAGINATION COLLABORATION AND SECURITY