

# **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

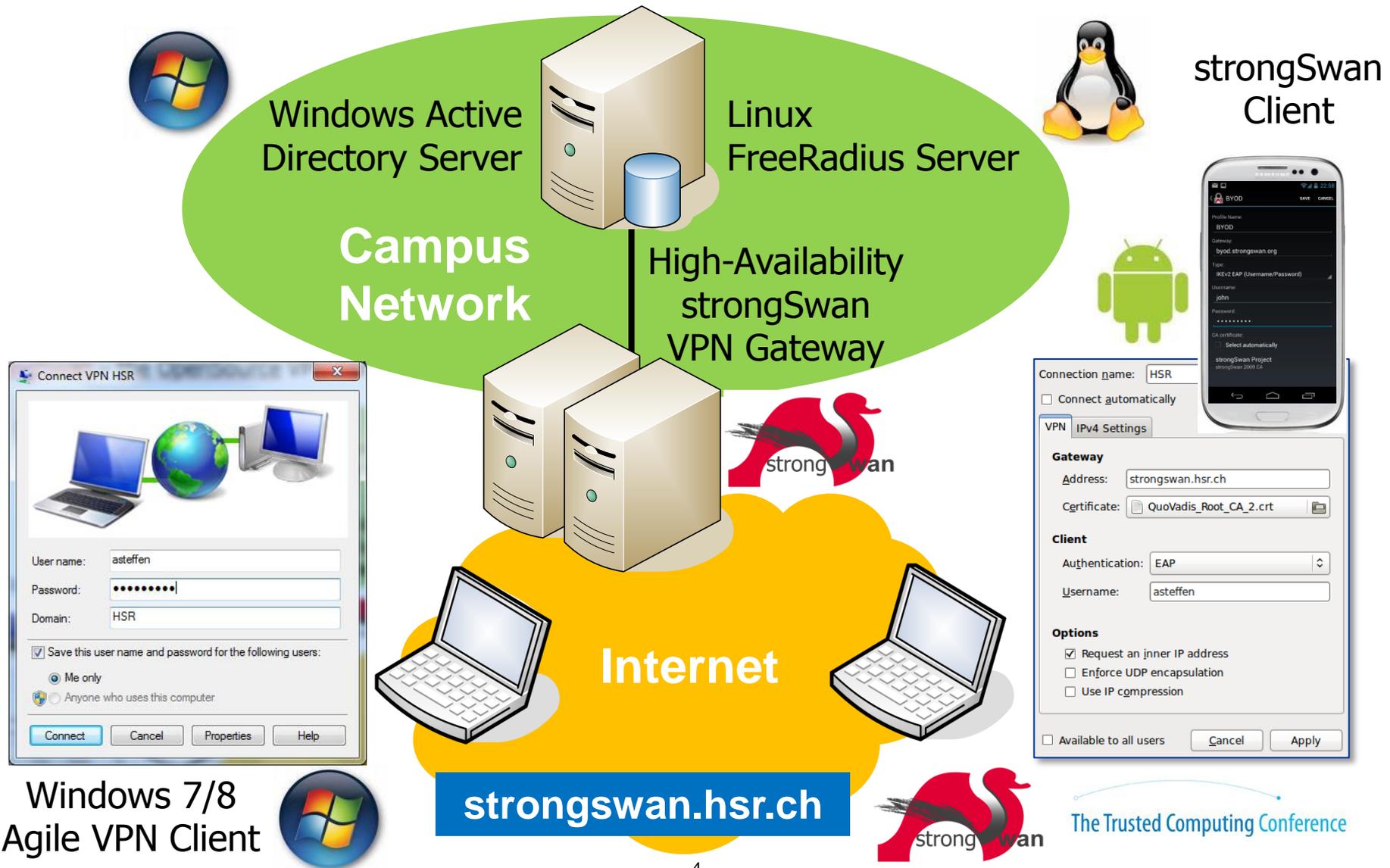
# Where the heck is Rapperswil?



- 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 Open Source VPN Solution

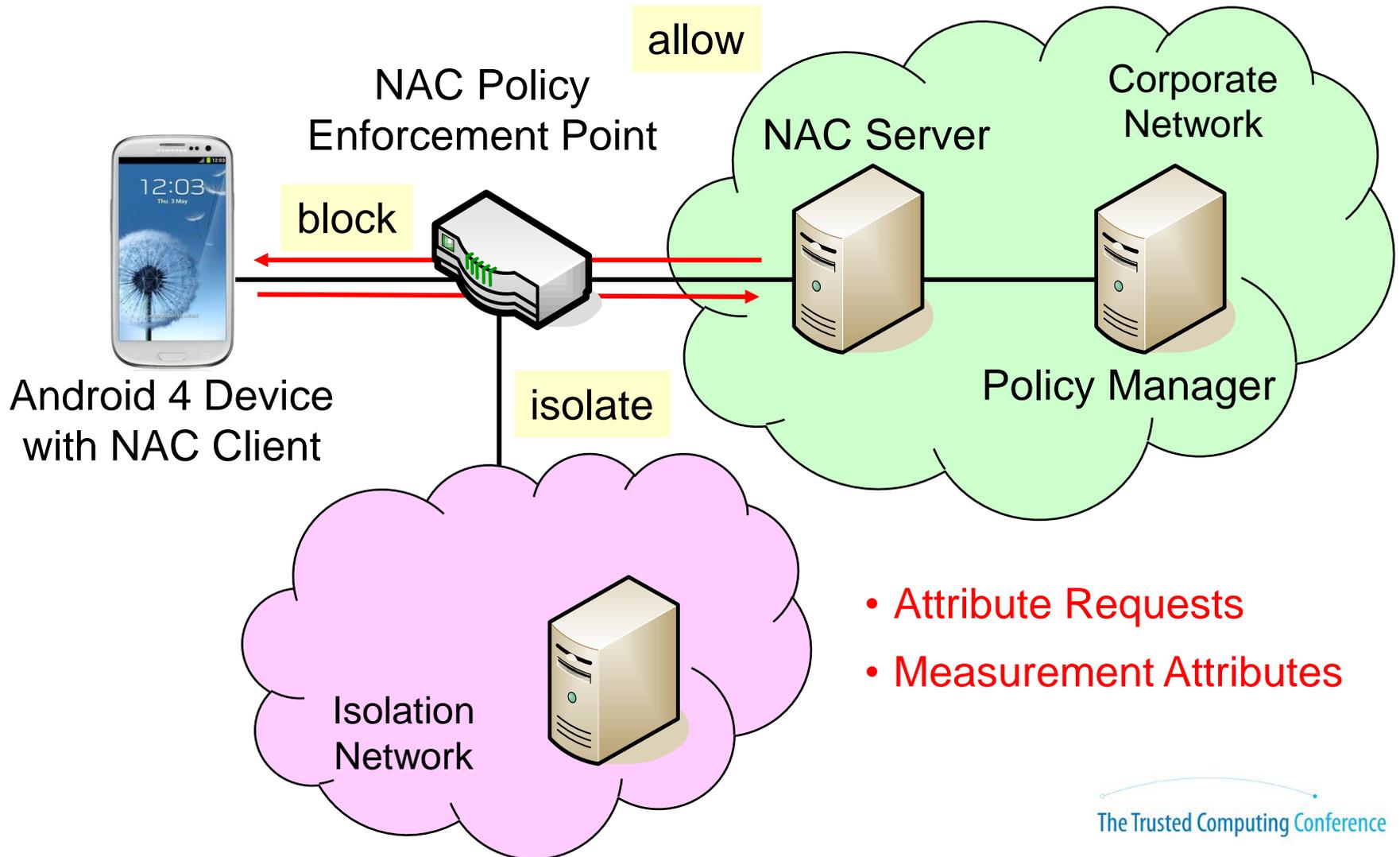


# BYOD – Bring Your Own Device

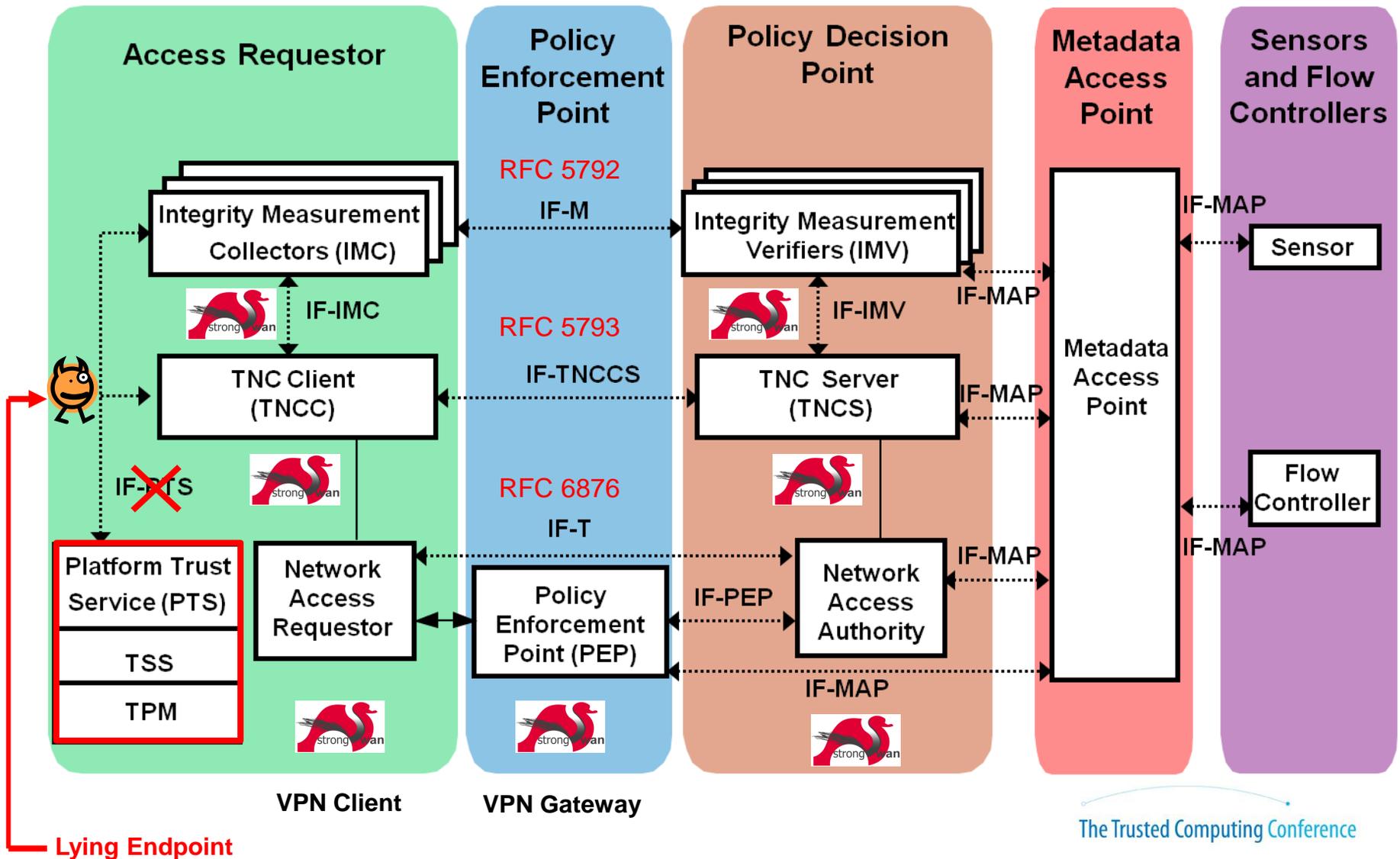
## Security Issues

- 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



# 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'
```

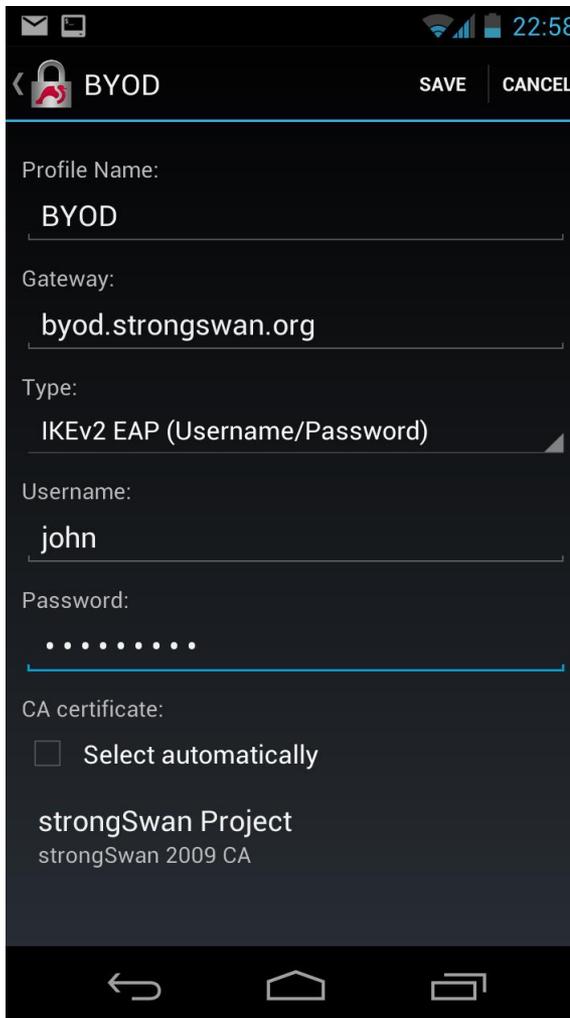
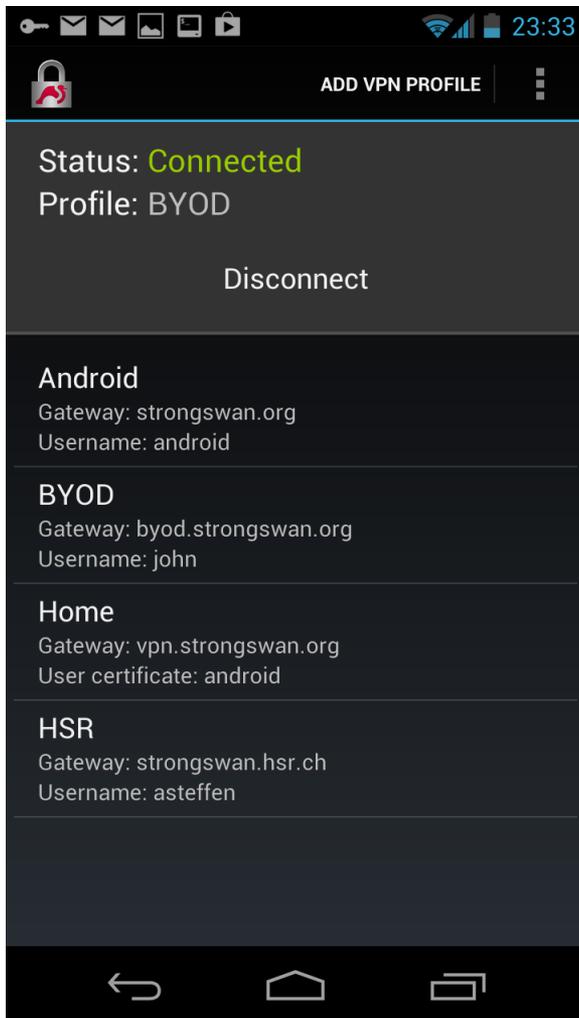
- IF-M Measurement Protocol PA-TNC (RFC 5792)

```
[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
```

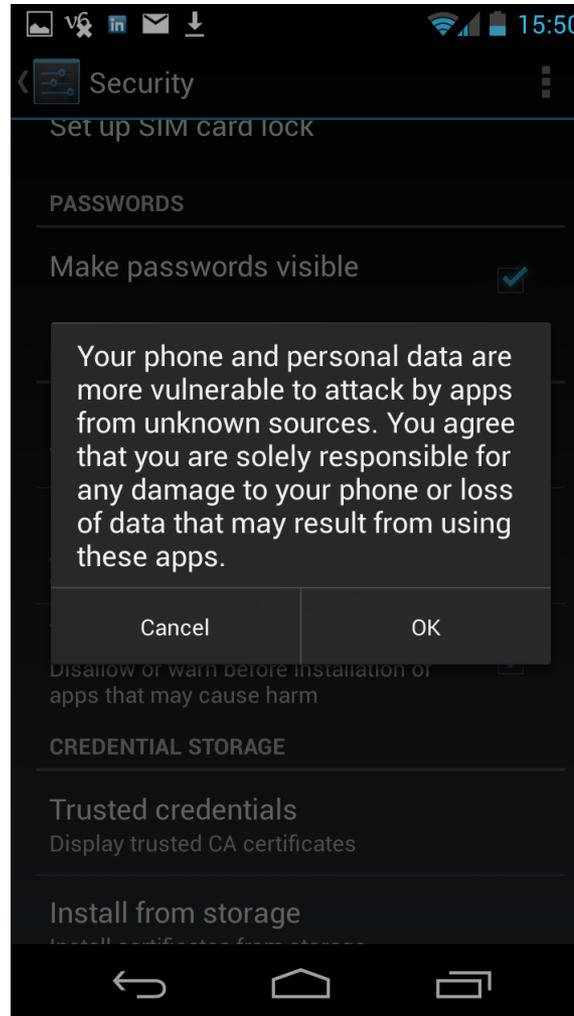
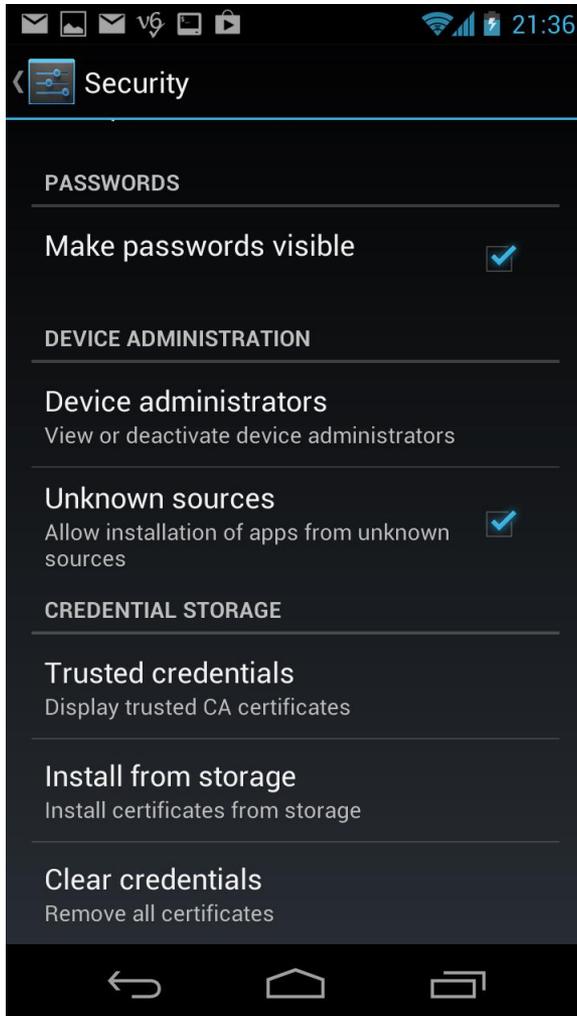
- TNC Measurement Data

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

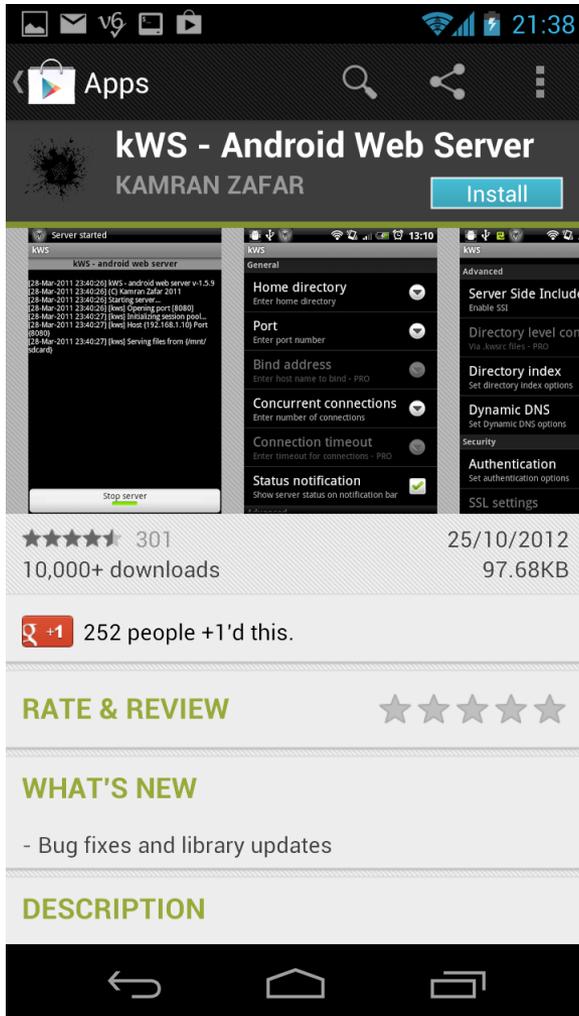
# strongSwan Android VPN Client: Easy to Connect



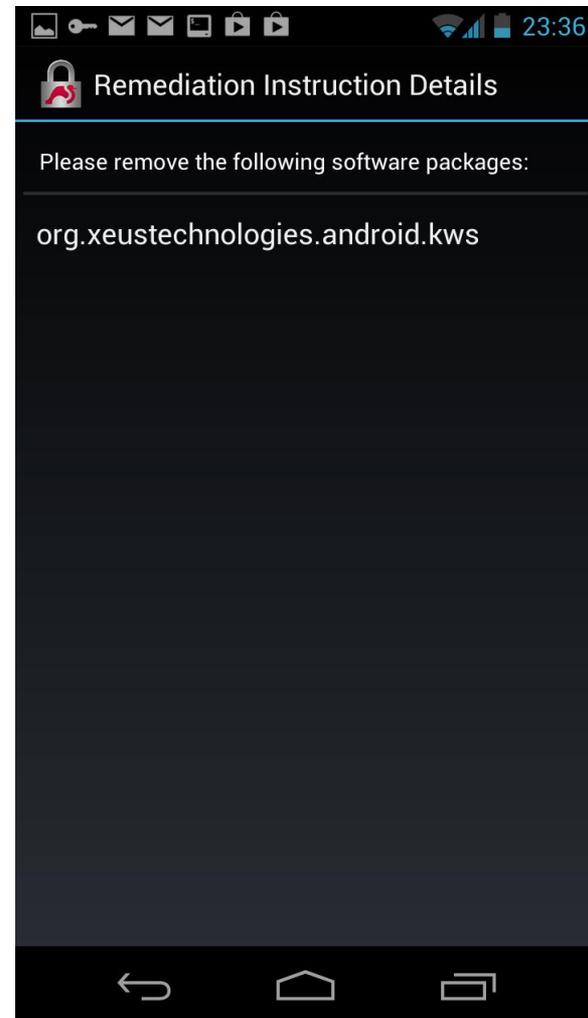
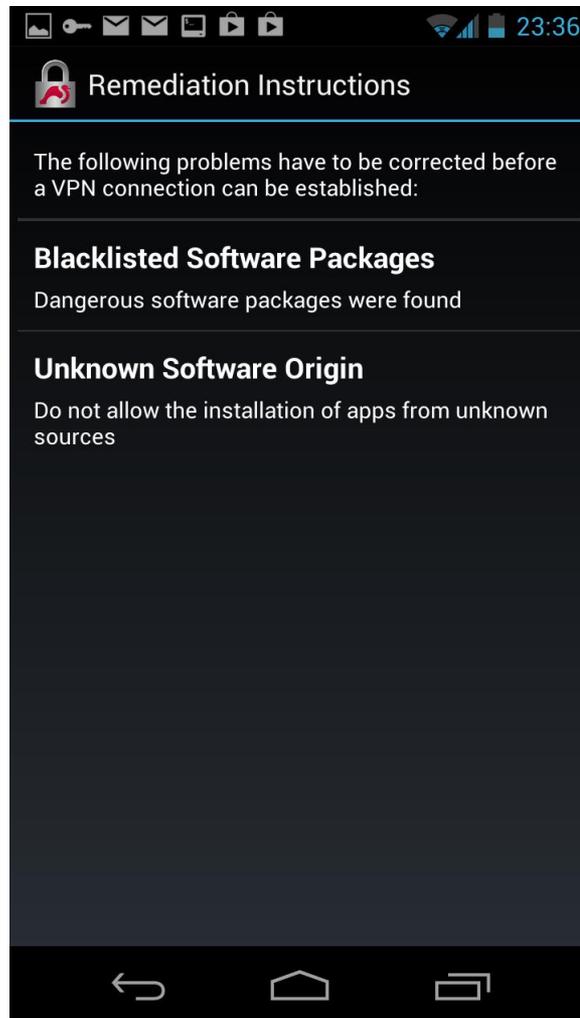
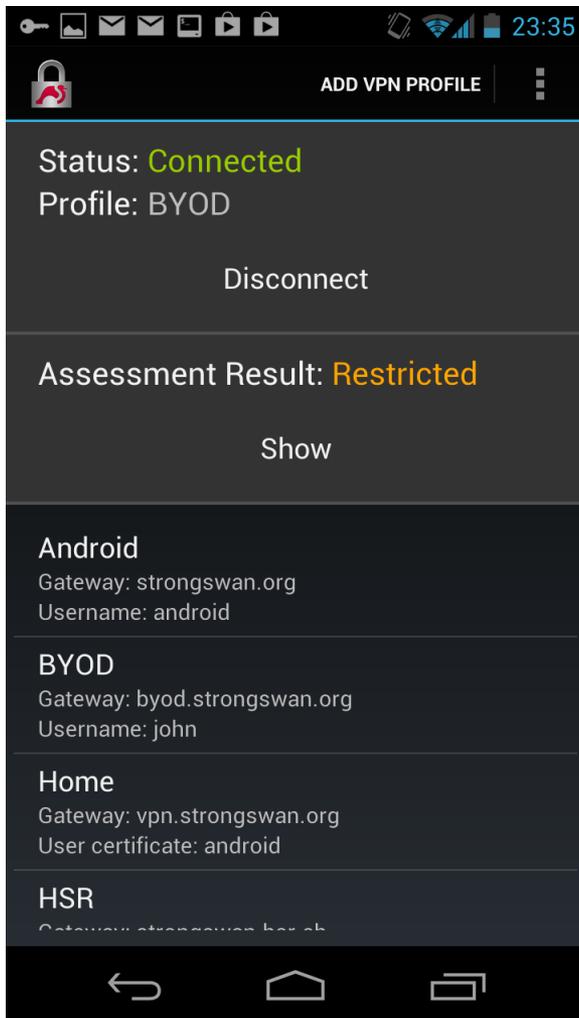
# Dangerous: Allow Download from Unknown Sources



# Install Blacklisted Android Web Server Package



# Minor Non-Compliance: Isolate Client



# Start the Android Web Server

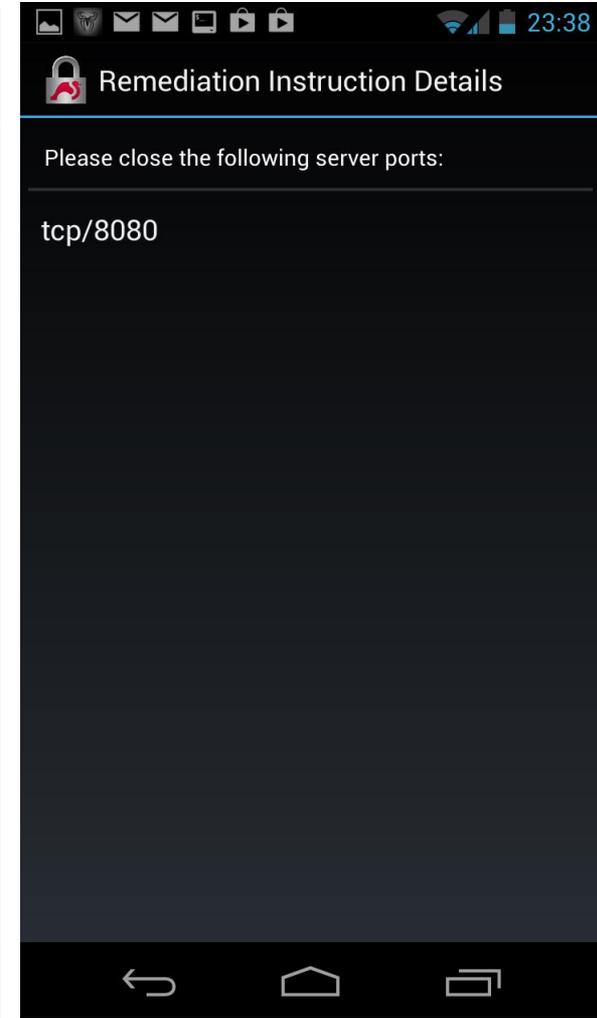
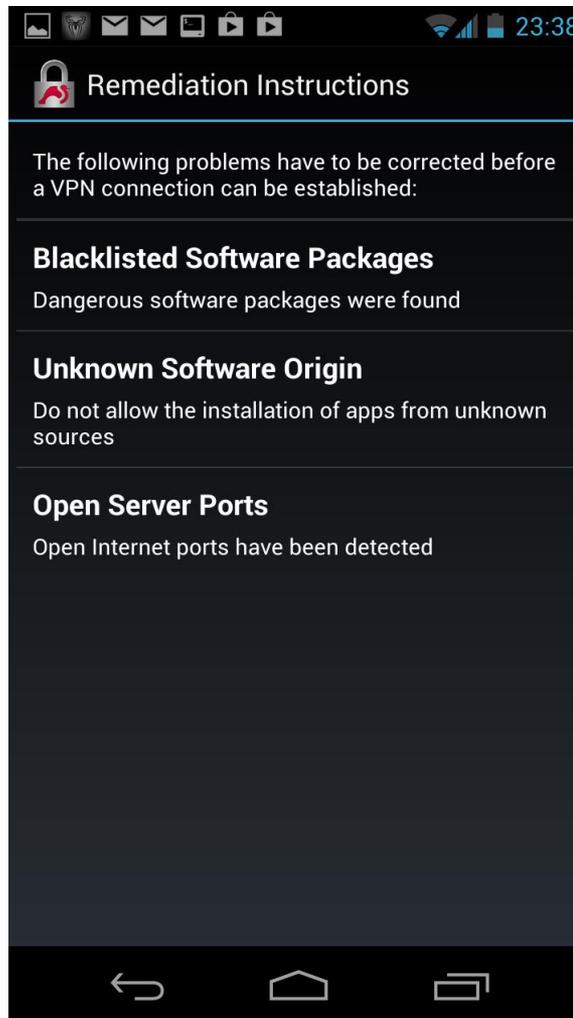
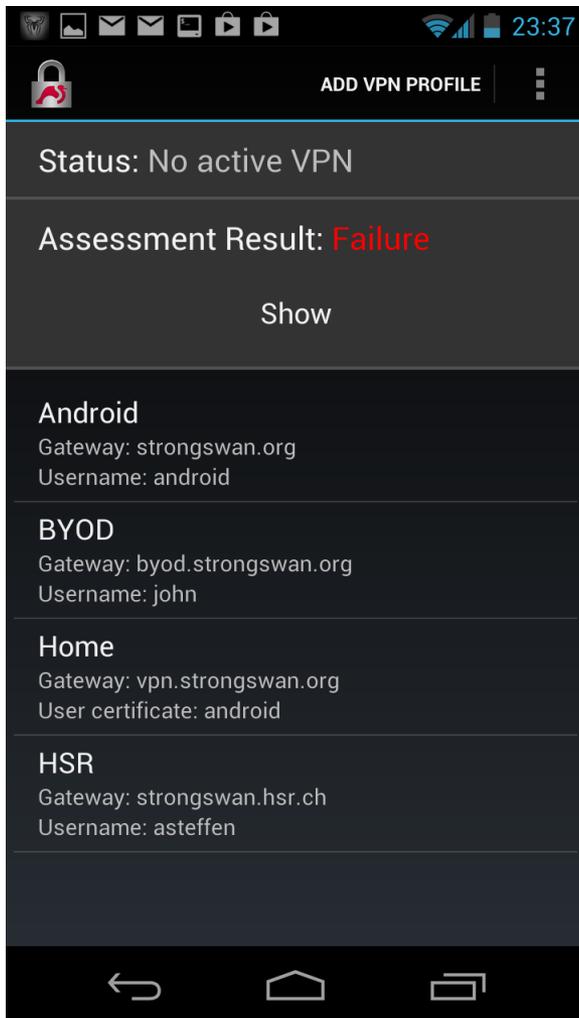


The screenshot shows an Android application window titled "kWS" with a subtitle "kWS - android web server". The main content area displays a log of system messages:

```
[21-Feb-2013 21:16:54] kWS - android web server v-1.7  
[21-Feb-2013 21:16:54] (C) Kamran Zafar 2011  
[21-Feb-2013 21:16:54] Starting server...  
[21-Feb-2013 21:16:54] [kws] Opening port [8080]  
[21-Feb-2013 21:16:54] [kws] Initializing session pool...  
[21-Feb-2013 21:16:54] [kws] Host {10.10.0.29} Port {8080}  
[21-Feb-2013 21:16:54] [kws] Serving files from {/storage/  
sdcard0}
```

At the bottom of the application window, there is a button labeled "Stop server" with a green underline. The Android navigation bar is visible at the very bottom, showing the back, home, and recent apps icons.

# Major Non-Compliance: Block Client



# strongTNC Policy Manager

The screenshot shows the strongTNC web interface in a Firefox browser window. The address bar displays `tnc.strongswan.org/sessions/140`. The page title is "strongTNC - Session details". The interface features a navigation sidebar on the left with sections for "CONFIGURATION" (Groups, Policies, Enforcements, Devices) and "DATA VIEWS" (Packages, Products, Directories, Files, Statistics). The main content area is titled "Session details" and contains a "Session Info" section with the following data:

<b>ID</b>	140
<b>Device</b>	Google Nexus Prime (cf5e4cbcc6)
<b>User</b>	steffen
<b>Time</b>	Aug 14 14:57:05 2013
<b>Result</b>	BLOCK

Below the session info is a "Results" section with a table of policy violations:

Policy	Result	IMV Comment
<a href="#">Unknown Source</a>	ALLOW	unknown sources not enabled
<a href="#">Installed Packages</a>	ISOLATE	processed 26 packages: 0 not updated, 1 blacklisted, 0 ok, 25 not found
<a href="#">Allowed Open TCP Ports</a>	BLOCK	violating tcp ports: 8008
<a href="#">Allowed Open UDP Ports</a>	ALLOW	no violating udp ports

# 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

The screenshot shows the strongTNC web interface in a Firefox browser window. The address bar displays `tnc.strongswan.org/policies/9`. The page title is "Policy Allowed Open UDP Ports".

**Navigation Menu:**

- Overview
- CONFIGURATION
  - Groups
  - Policies
  - Enforcements
  - Devices
- DATA VIEWS
  - Packages
  - Products
  - Directories
  - Files
  - Statistics

**Policy Configuration:**

- Policy:** Allowed Open UDP Ports (with a plus icon)
- Filter:** [Filter] [Search]
- [Allowed Open TCP Ports](#)
- [Allowed Open UDP Ports](#)
- [Default Factory Password Enabled](#)
- [Get /bin](#)
- [Get /system/bin](#)
- [Get /system/lib](#)
- [IP Forwarding Enabled](#)
- [Installed Packages](#)
- [Measure /lib/x86\\_64-linux-gnu/libcrypto.so.1.0.0](#)

**Policy Info:**

- Name:** Allowed Open UDP Ports
- Type:** Open UDP Listening Ports
- All ports closed except:** 500 4500
- Fail-Action:** BLOCK
- Noresult-Action:** BLOCK

**Actions:** [Save] [Delete]

# Define Enforcements

The screenshot shows the strongTNC web interface in a Firefox browser. The page title is "Enforcement Installed Packages on Default". The interface is divided into a left sidebar and a main content area.

**Left Sidebar:**

- Overview
- CONFIGURATION
  - Groups
  - Policies
  - Enforcements
  - Devices
- DATA VIEWS
  - Packages
  - Products
  - Directories
  - Files
  - Statistics

**Main Content Area:**

**Enforcement** [Add icon]

Filter [Search icon]

- [Installed Packages on Default](#)
- [Unknown Source on Android](#)
- [IP Forwarding Enabled on Linux](#)
- [Measure /lib/x86\\_64-linux-gnu/libcrypto.so.1.0.0 on Ubuntu x86\\_64](#)
- [Measure /lib/x86\\_64-linux-gnu/libssl.so.1.0.0 on Ubuntu x86\\_64](#)
- [Measure /usr/bin](#)

**Enforcement Info**

- Policy: Installed Packages
- Group: Default
- Max. age in seconds: 86400
- Fail Action: Inherit from policy
- Noresult Action: Inherit from policy

[Save] [Delete]

# 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