# Near Real-time Network Security with Open Source Tools

Josef von Helden, Bastian Hellmann, Thomas Rossow, Ralf Steuerwald

{josef.vonhelden,bastian.hellmann,thomas.rossow,ralf.steuerwald}@hs-hannover.de

Hochschule Hannover - University of Applied Sciences and Arts

Andreas Steffen

andreas.steffen@hsr.ch

University of Applied Sciences in Rapperswil

Kai-Oliver Detken, Dennis Dunekacke

{detken,dunekacke}@decoit.de

DECOIT GmbH

February 24, 2014

The demonstration intends to illustrate how Trusted Network Connect (TNC) Open Source tools of multiple vendors can be combined to smartly address the complex scenario of securing a Bring Your Own Device (BYOD) scenario. The example scenario integrates the strongSwan[1] VPN solution, developed by the University of Applied Sciences in Rapperswil (Switzerland), with several iron*[2] tools by the Trust@HsH research group at the University of Applied Sciences and Arts in Hanover (Germany), and the Android-IF-MAP-Client[3] by DECOIT GmbH, a SME company from Bremen (Germany). The combination of those tools allows to implement a network security solution which responds to security incidents in near real-time. The scenario is set in a Bring Your Own Device (BYOD) environment where employees use their own smartphones for enterprise tasks. Different TNC IF-MAP tools are combined to enforce corporate policies affecting the employees' Android cell phone devices on initial network connection and to continuously monitor policy conformity if behavioral changes of the devices occur.

## 1 Scenario Overview

The scenario for the demonstration is shown in figure 1. The strongSwan VPN gateway enables external devices, such as the smartphone, to access the internal corporate network. In terms of Trusted Network Connect (TNC) the strongSwan VPN gateway acts as Policy Enforcement Point

[1] `http://www.strongswan.org`

[2] `https://github.com/trustathsh`

[3] `https://github.com/decoit/Android-IF-MAP-Client`

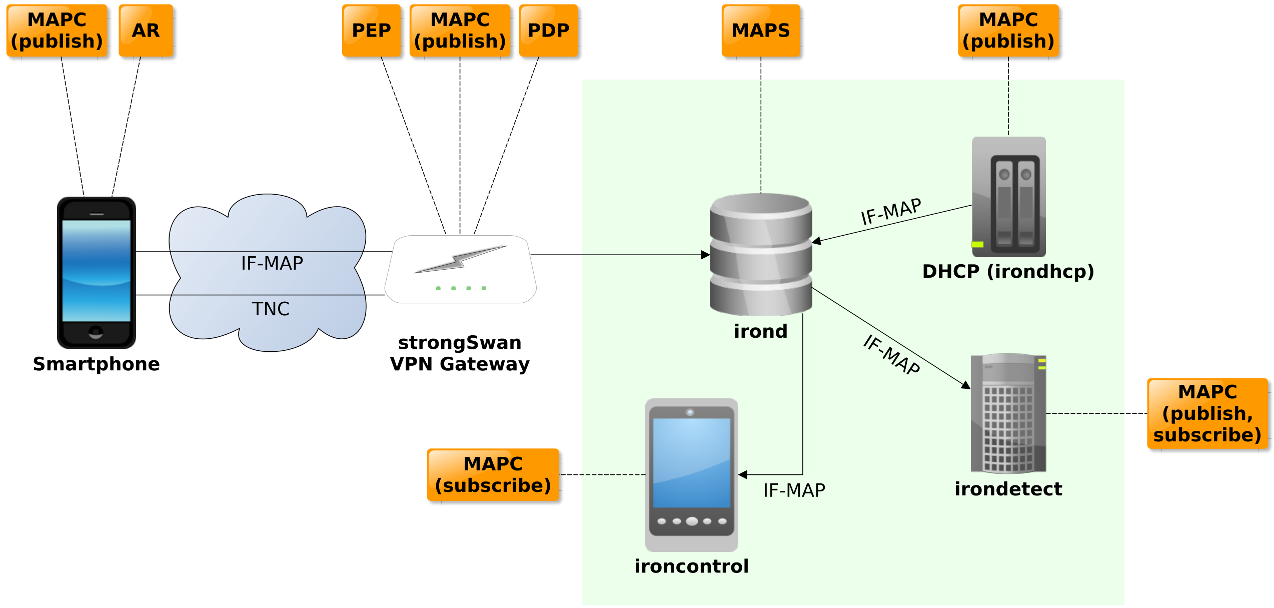


Figure 1: Demonstration scenario

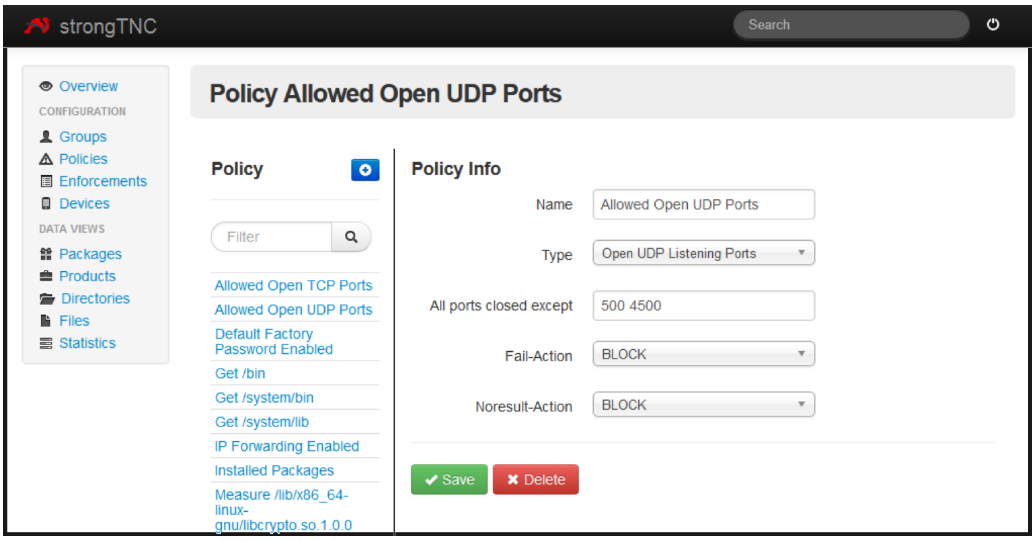
(PEP), Policy Decision Point (PDP) and MAP-Client publishing information about the performed access request to a internal MAP server (irond). The smartphone acts as Access Requestor (AR).

The internal network contains the MAP server irond, a DHCP server that is monitored by irondhcp and irondetect, a detection engine that uses the MAP server as primary data source. Irondhcp publishes the lease data of the DHCP server on irond. Irondetect monitors metadata associated to network clients for evidence of anomalies and predefined signatures of malicious behavior and raises alerts if the corporate policy for mobile devices connecting to the internal network is violated. Part of the required information is gathered from the mobile phone itself, where an application continuously collects feature metadata about the device, such as the installed apps and their permissions and publishes this information on irond. Alerts by irondetect are published as event metadata in irond. Ironcontrol, another mobile IF-MAP client for the Android platform (see figure 3) runs on the security administrator's phone and receives those alerts via subscription and can inform her immediately about policy violations.

## 2 Demonstration Steps

This section describes the individual steps of the demonstration in greater detail. The initial configuration is as follows:

- The strongSwan VPN is equipped with a policy that only grants access to mobile devices connecting to the network, that pass a range of integrity tests (see figure 2).
- Irondetect has been pre-configured with subscriptions for so called "feature metadata" of any device that connects to the network. Android-IF-MAP-Client will publish those "feature metadata" about the device it is running on.



Policy Allowed Open UDP Ports

Policy Info

Name: Allowed Open UDP Ports

Type: Open UDP Listening Ports

All ports closed except: 500 4500

Fail-Action: BLOCK

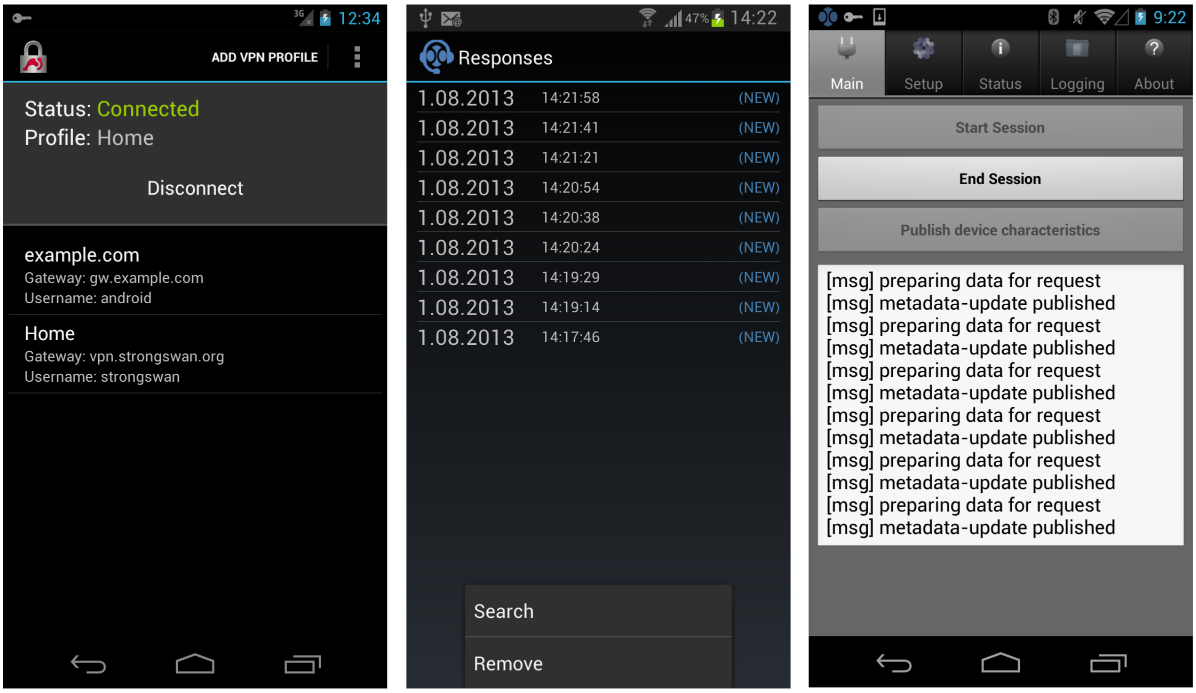
Noresult-Action: BLOCK

Figure 2: The strongSwan policy manager strongTNC

- Irondetect is equipped with a policy that detects mobile malware in terms of "feature metadata" (e.g. by detecting suspicious combinations of apps' permissions).
- The mobile device connecting to the strongSwan VPN is equipped with the strongSwan Android VPN Client (see figure 3) and the appropriate IMC. The device's configuration is compliant to both strongSwan's and irondetect's policies.
- The administrator's smartphone holds subscriptions to event type metadata published by irondetect using the ironcontrol app for Android. The event type metadata will be used to signal warning messages in case irondetect detects suspicious behavior.

The demonstration itself consists of the following activities:

1. At first the smartphone tries to establish a VPN connection to the internal network. In order to make a policy decision, the strongSwan VPN gateway uses various integrity information (scan of open server ports, list of user-installed software packages, hash values of Android system programs and libraries as well as checks on some system security settings) about the smartphone. This integrity information is collected by the IMC provided by the strongSwan Android VPN Client. The results of the integrity measurements are transmitted to the VPN gateway via standard TCG protocols such as IF-M, IF-TNCCS and IF-T over Tuneled EAP Methods. The smartphone reports data that is policy-conform and therefore is granted access to the internal network. The strong swan VPN gateway publishes the access request information on the MAP server.
2. The DHCP server assigns an IP address to the new IPSec tunnel end-point of the smartphone. Irondhcp publishes the lease information on the MAP server.
3. Establishing a connection to the internal network triggers the feature collector application on the smartphone. The feature collector application starts to gather information about the smartphone (e.g. permissions of installed applications) and publishes this data on the MAP server.



Status: Connected
Profile: Home

example.com
Gateway: gw.example.com
Username: android

Home
Gateway: vpn.strongswan.org
Username: strongswan

```
1.08.2013   14:21:58   (NEW)
1.08.2013   14:21:41   (NEW)
1.08.2013   14:21:21   (NEW)
1.08.2013   14:20:54   (NEW)
1.08.2013   14:20:38   (NEW)
1.08.2013   14:20:24   (NEW)
1.08.2013   14:19:29   (NEW)
1.08.2013   14:19:14   (NEW)
1.08.2013   14:17:46   (NEW)
```

```
[msg] preparing data for request
[msg] metadata-update published
[msg] preparing data for request
[msg] metadata-update published
[msg] preparing data for request
[msg] metadata-update published
[msg] preparing data for request
[msg] metadata-update published
[msg] preparing data for request
[msg] metadata-update published
[msg] preparing data for request
[msg] metadata-update published
```

Figure 3: strongSwan VPN Client, ironcontrol, DECOIT IF-MAP-Client

4. Irondetect evaluates the new feature metadata for policy compliance and finds the phone policy compliant.
5. The smartphone changes its behavior/state in a way that breaks policy conformity. For example, the smartphone would install an application that uses a combination of permissions that is considered harmful (e.g. audio/video recording and Internet connection).
6. The feature collector on the smartphone publishes the updated information about the smartphone's apps on the MAP server.
7. Irondetect receives the updated information and re-evaluates the policy conformity of the device. Irondetect recognizes a harmful configuration of the smartphone and publishes this information contained event metadata on the MAP server.
8. The ironcontrol app on the administrator's mobile phone receives message about the event metadata and notifies the administrator.

## 3 Summary

The demonstration shows how different Open Source tools can be used to build a system which detects policy violations in near real-time. It also shows how Open Source Tools developed by different vendors collaborate by leveraging various TNC technologies. Especially the combination of IF-MAP and TNC shows how static access decision can be supported and enhanced by supplementary metadata analysis.