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

Windows 7/8 Agile VPN Client

strongSwan Linux Client

strongSwan – the OpenSource VPN Solution

Windows Active Directory Server

Linux FreeRadius Server

Campus Network

High-Availability strongSwan VPN Gateway

Internet

strongswan.hsr.ch

Windows 7/8 Agile VPN Client

strongSwan Linux Client
Trusted Network Connect (TNC) Framework

Source: Trusted Computing Group (TCG)
strongSwan TNC Activities Update

TCG Members Meeting Juni 2013 Dublin

strongSwan IMC/IMV Pairs
OS IMC/IMV Pair

- **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
Attestation IMC/IMV Pair

- **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/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)
Linux Integrity Measurement Architecture

- **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.

## Linux IMA - BIOS Measurements

- 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_bio_measurements`
  - BIOS measurements are extended into PCRs #0..7

<table>
<thead>
<tr>
<th>PCR</th>
<th>SHA-1 Measurement Hash</th>
<th>Comment</th>
<th>PCR</th>
<th>SHA-1 Measurement Hash</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>4d894efe0ae7cb124740df4f6c5c35aa0fe7dae8 08</td>
<td>[S-CRTM Version]</td>
<td>4</td>
<td>67a0a98bc4d6321142895a4d938b342f6959c1a9 05</td>
<td>[Booting BCV Device 80h, - Hitachi HTS723216L9A360]</td>
</tr>
<tr>
<td>0</td>
<td>f2c846e7f335f7b9e9dd0a44f48c48e1986750c7 01</td>
<td>[POST CODE]</td>
<td>4</td>
<td>06d60b3a0dee9bb9beb2f0b04aff2e75bd1d2860 0d</td>
<td>[IPL]</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td>5</td>
<td>1b87003b6c7d90483713c90100cca3e62392b9bc 0e</td>
<td>[IPL Partition Data]</td>
</tr>
</tbody>
</table>
**Linux IMA - Runtime Measurements**

- 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

<table>
<thead>
<tr>
<th>PCR</th>
<th>SHA-1 Measurement Hash</th>
<th>SHA-1 File Data Hash</th>
<th>Filename</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>d0bb59e83c371ba6f3adad491619524786124f9a ima</td>
<td>365a7adf8fa89608d381d9775ec2f29563c2d0b8</td>
<td>boot_aggregate</td>
</tr>
<tr>
<td>10</td>
<td>76188748450a5c456124c908c36bf9e398c08d11 ima</td>
<td>f39e77957b909f3f81f891c478333160ef3ac2ca</td>
<td>/bin/sleep</td>
</tr>
<tr>
<td>10</td>
<td>df27e645963911df0d5b43400ad71cc28f7f898e ima</td>
<td>78a85b50138c481679fe4100ef2b3a0e6e53b50</td>
<td>ld-2.15.so</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>10</td>
<td>30fa7707af01a670fc353386fcc95440e011b08b ima</td>
<td>72ebd589aa9555910ff3764c27dbda4296575fe</td>
<td>parport.ko</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
strongSwan TNC Activities Update

TCG Members Meeting Juni 2013 Dublin

strongSwan PDP as an IF-MAP Client
Open Source TNC IF-MAP Products

IRON Project FH Hannover (MAP-Server)
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

Policy Decision Point (PDP)  Policy Enforcement Point (PEP)  Access Requestor (AR)

- IMVs
- TNC-Server
- Network Access Authority
- Policy Enforcement Point
- IMCs
- TNC-Client
- Network Access Requestor

Integrity Access Layer

Integrity Evaluation Layer

Integrity Measurement Layer

CYGNET

SGLite

IPSec Config DB

Client WebBrowser

StrongSwan Client

27.06.2013, tcg_dublin_2013.pptx 19
Device Google Nexus Prime

ID: cf5e4cbcc6e6a2db
Description: Google Nexus Prime
Product: Android 4.2.1

Groups: Android • Ref. Android
Defining Policies

- **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

```
packages
  - id : Integer
  - name : Text
  - blacklist : Integer

versions
  - id : Integer
  - package : Integer
  - product : Integer
  - release : Text
  - security : Integer
  - time : Integer
  - blacklist : Integer

products
  - id : Integer
  - name : Text
  - version : Integer

files
  - id : Integer
  - path : Text

directories
  - id : Integer
  - path : Text

algorithms
  - id : Integer
  - name : Text

files hashes
  - file : Integer
  - product : Integer
  - key : Integer
  - algorithm : Integer
  - hash : Blob

identities
  - data : Text
  - id : Integer

measurement
  - id : Integer
  - time : DateTime
  - connectionID : Integer
  - recommendation : Action
  - identity : Integer

workitems
  - type : Integer
  - measurement : Integer
  - enforcement : Integer
  - argument : Text
  - id : Integer
  - fail : Action
  - noresult : Action
  - result : String
  - recommendation : Action

results
  - id : Integer
  - policy : Integer
  - result : String
  - recommendation : Action

enforcements
  - policy : Integer
  - group : Integer
  - max-age : Integer
  - noresult : Action
  - fail : Action
  - id : Integer
```

device Infos
  - device : Integer
  - time : Integer
  - count : Integer
  - count_update : Integer
  - count_blacklist : Integer
  - flags : Integer
  - ar_id : Integer

product_file
  - product : Integer
  - file : Integer
  - measurement : Integer
  - metadata : Integer

27.06.2013, tcg_dublin_2013.pptx 22