.DECOIT®
01110000111010111000100101110000111010111000100

IDAACS 2015, 24.-26.09.15

A viable SIEM approach for Android

Kai-Oliver Detken · Evren Eren · Markus Schölzel

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
https://www.decoit.de
detken@decoit.de

Outline

- Introduction
- Motivation
- TNC IF-MAP
  - Data model
  - MAP graph
- Android
- SIEM without IF-MAP
- DECOmap for Android
- Conclusion and Outlook

Introduction (1)

- The term SIEM is divided into:
  - Security Event Management (SEM)
  - Security Information Management (SIM)
- SEM security management includes:
  - Real-time monitoring
  - Event correlation
  - Event messaging
- Security management of SIM includes:
  - Long-term capturing
  - Analyze of log data
  - Reporting of log data
- Basically SIEM systems are able by collecting sensor information and events to recognize anomalies and prevent threats

Introduction (2)

- iMonitor project (www.imonitor-project.de) of BMWi started in July 2013 and ended in June 2015 successfully
- Partner of the „Bremer" project were:
    - DECOIT GmbH (coordination, development, exploitation)
    - University of Bremen, TZI (development)
    - neusta GmbH (development, exploitation)
- The project developed a new form of event correlation, which recognize new attack variants automatically (with artificial intelligence)
- Exchange rules through a central knowledge server
- An event overview is presented in one SIEM-GUI centrally

Motivation (1)

- Tech Pro Research's latest survey (January 2015) shows that the Bring Your Own Device (BYOD) movement is booming: 74% of organizations either already using or planning to allow employees to bring their own devices to work
- BYOD will drive Android into the enterprise despite security concerns: The bring your own device (BYOD) movement [...] will continue to grow despite security risk, according to Ernst & Young
- In case of a malicious event monitoring systems need to respond immediately!

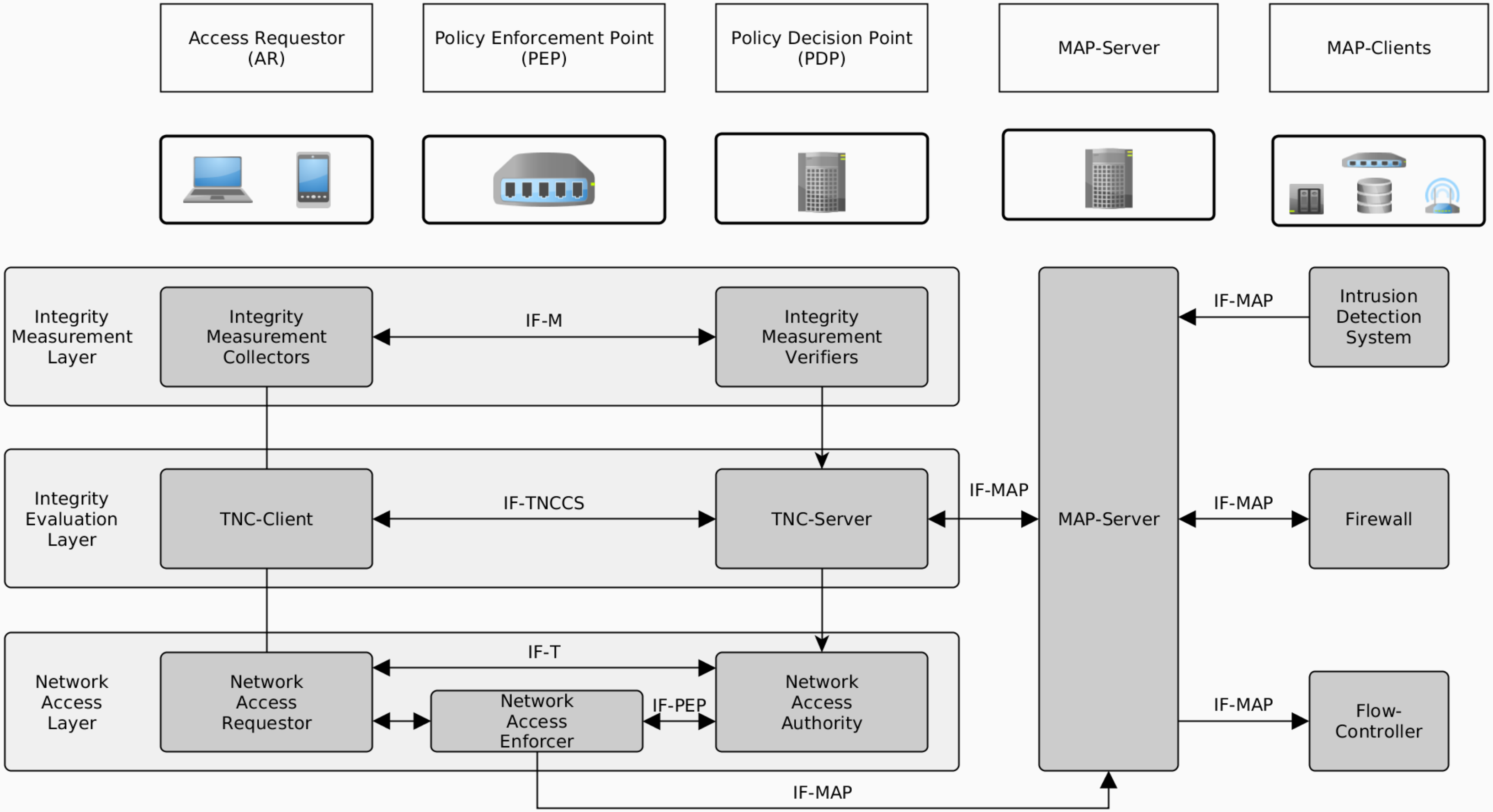
Motivation (2)

- Proposed solution: user authentication (credentials or certificate) + collection of status reports
  - These data could contain traffic, load and usage stats, system, platform and app version information
  - Based on this information mobile devices can be treated differently in real-time to restrict access and scope for devices with known bugs or suspicious behavior
- TNC IF-MAP can be used to allow an integration of multiple tools and an efficient database a SIEM system can rely on

TNC IF-MAP (1)

- Trusted Network Connect (TNC) is an open architecture developed by the Trusted Computing Group (TCG) to enforce policies regarding endpoint integrity
- IF-MAP, as part of TNC, is a client/server protocol for accessing a Metadata Access Point (MAP) and storing/reading information about network-/security-relevant real-time metadata
- Based on IEEE 802.1x (AR, PEP and PDP)
- IF-MAP Clients and a MAP-Server (not TPM required)
- XML/SOAP over HTTPS (CBOR protocol optionally)

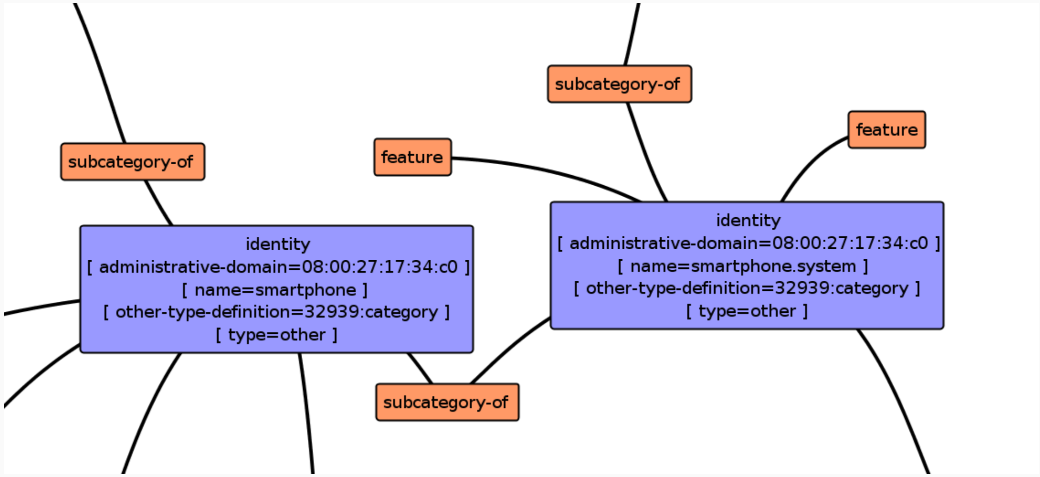
TNC IF-MAP (2)



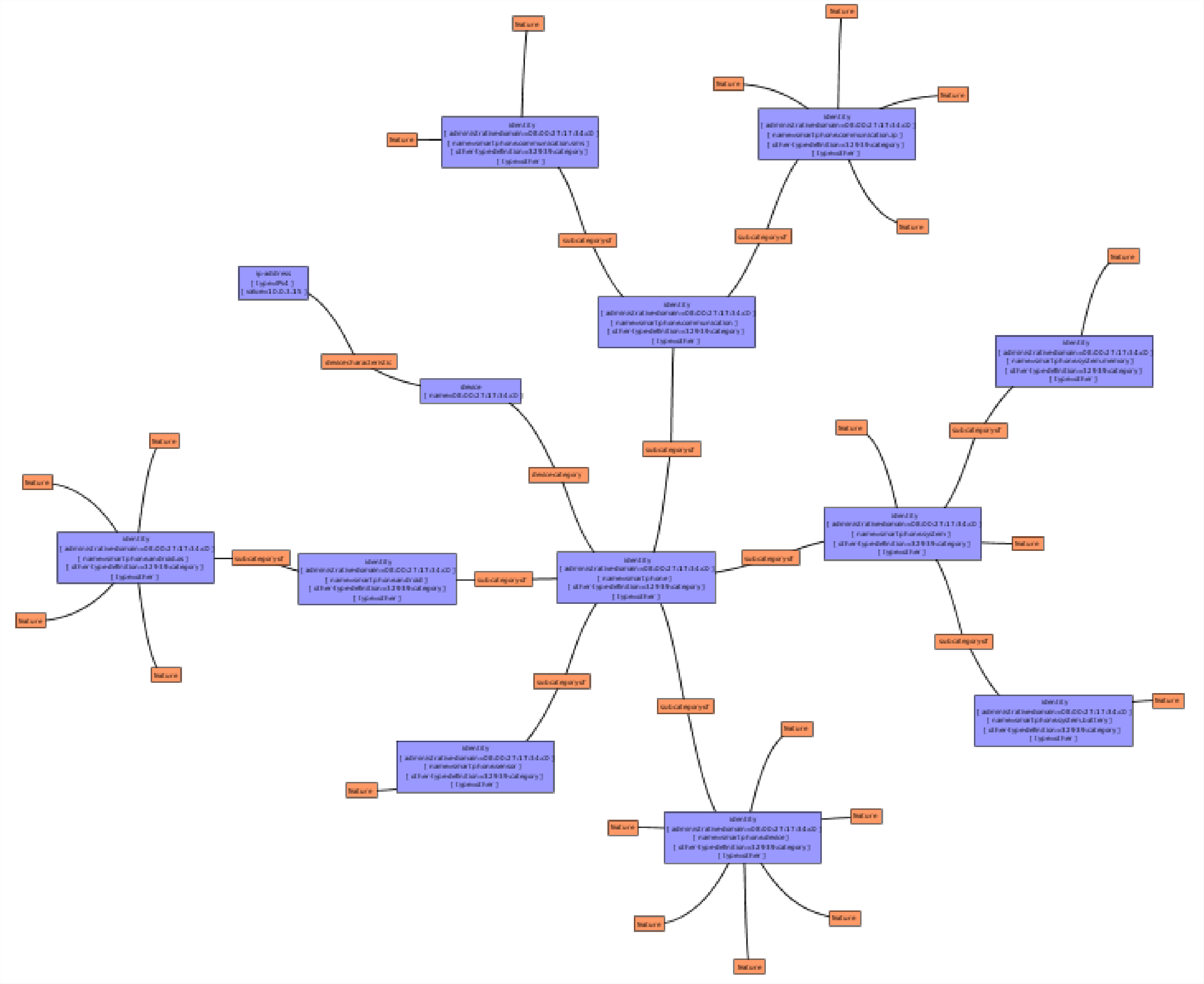
Access Requestor (AR)
Policy Enforcement Point (PEP)
Policy Decision Point (PDP)
MAP-Server
MAP-Clients
Integrity Measurement Layer
Integrity Measurement Collectors
IF-M
Integrity Measurement Verifiers
Integrity Evaluation Layer
TNC-Client
IF-TNCCS
TNC-Server
IF-MAP
MAP-Server
Intrusion Detection System
IF-MAP
Firewall
IF-MAP
Flow-Controller
IF-MAP
Network Access Layer
Network Access Requestor
IF-T
Network Access Enforcer
IF-PEP
Network Access Authority
IF-MAP

TNC IF-MAP data model

- The data model includes:
  - Original and extended identifiers
  - Links
  - Standard metadata and vendor-specific metadata
- Android device in a MAP graph:


subcategory-of
subcategory-of
feature
feature
subcategory-of
identity
[administrative-domain=08:00:27:17:34:c0]
[name=smartphone]
[other-type-definition=32939:category]
[type=other]
identity
[administrative-domain=08:00:27:17:34:c0]
[name=smartphone.system]
[other-type-definition=32939:category]
[type=other]

TNC IF-MAP graph

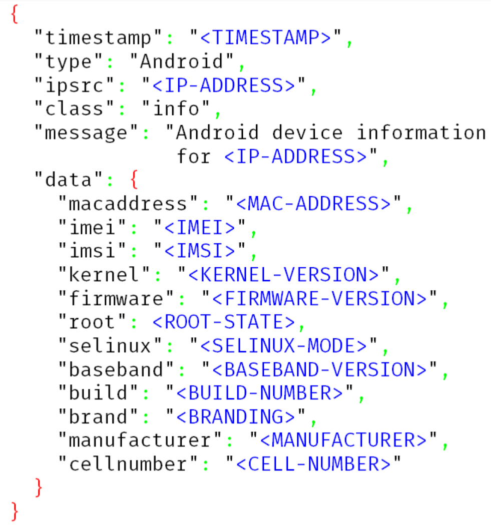


Android platform

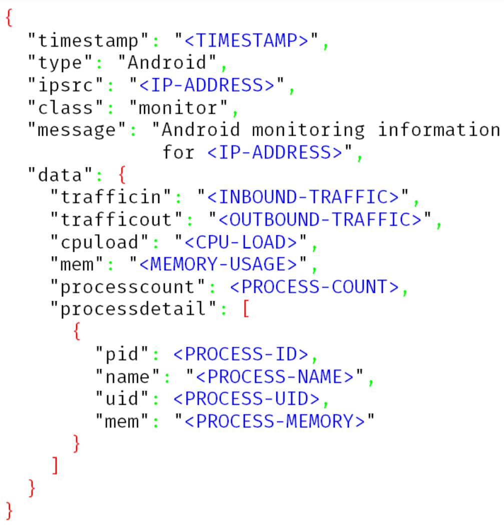
- Metadata used to identify devices and their state:
  - Device specific data (IMEI, IMSI, …)
  - Platform (build number, firmware version, …)
  - System state (cpu load, traffic, …)
  - Communication (bluetooth, sms, nfc, …)
  - Apps (installed, permissions)

SIEM without IF-MAP

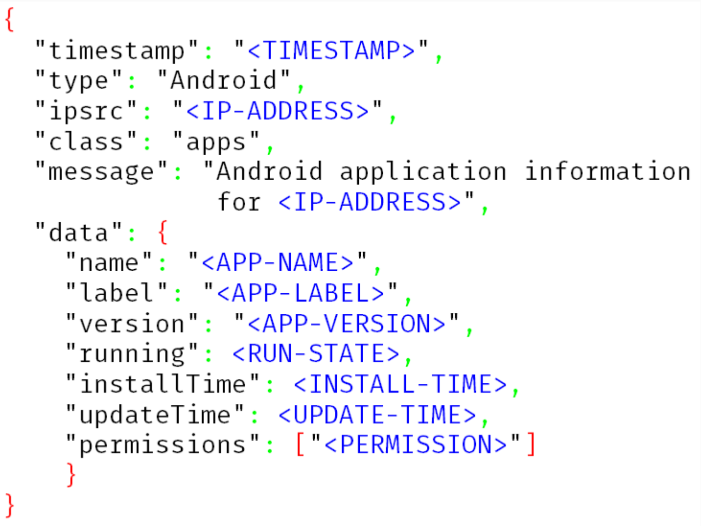
- Data collected by IF-MAP Clients can be re-used to generate events for various types of monitoring systems and statistics
  - Icinga-based approach accepting Android events via NSCA
  - InfoEvent, MonitorEvent and AppEvent:



```
{
  "timestamp": "<TIMESTAMP>",
  "type": "Android",
  "ipsrc": "<IP-ADDRESS>",
  "class": "info",
  "message": "Android device information
              for <IP-ADDRESS>",
  "data": {
    "macaddress": "<MAC-ADDRESS>",
    "imei": "<IMEI>",
    "imsi": "<IMSI>",
    "kernel": "<KERNEL-VERSION>",
    "firmware": "<FIRMWARE-VERSION>",
    "root": <ROOT-STATE>,
    "selinux": "<SELINUX-MODE>",
    "baseband": "<BASEBAND-VERSION>",
    "build": "<BUILD-NUMBER>",
    "brand": "<BRANDING>",
    "manufacturer": "<MANUFACTURER>",
    "cellnumber": "<CELL-NUMBER>"
  }
}
```



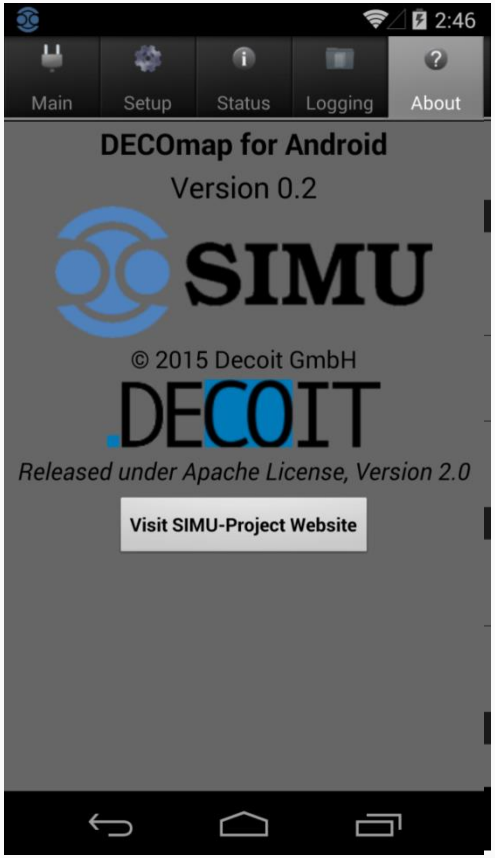
```
{
  "timestamp": "<TIMESTAMP>",
  "type": "Android",
  "ipsrc": "<IP-ADDRESS>",
  "class": "monitor",
  "message": "Android monitoring information
              for <IP-ADDRESS>",
  "data": {
    "trafficin": "<INBOUND-TRAFFIC>",
    "trafficout": "<OUTBOUND-TRAFFIC>",
    "cpuload": "<CPU-LOAD>",
    "mem": "<MEMORY-USAGE>",
    "processcount": <PROCESS-COUNT>,
    "processdetail": [
      {
        "pid": <PROCESS-ID>,
        "name": "<PROCESS-NAME>",
        "uid": <PROCESS-UID>,
        "mem": "<PROCESS-MEMORY>"
      }
    ]
  }
}
```



```
{
  "timestamp": "<TIMESTAMP>",
  "type": "Android",
  "ipsrc": "<IP-ADDRESS>",
  "class": "apps",
  "message": "Android application information
              for <IP-ADDRESS>",
  "data": {
    "name": "<APP-NAME>",
    "label": "<APP-LABEL>",
    "version": "<APP-VERSION>",
    "running": <RUN-STATE>,
    "installTime": <INSTALL-TIME>,
    "updateTime": <UPDATE-TIME>,
    "permissions": ["<PERMISSION>"]
  }
}
```

DECOmap for Android

- DECOmap for Android is an Open Source tool which has been developed by DECOIT GmbH in two research projects
- The App Version 0.2 has been extended in co-operation with the University of Applied Science of Dortmund
- It can be used without license costs with or without IF-MAP protocol
- Currently an integrity check is not available, because of missing TPM modules on mobile platforms
- Download is available at project websites:
  - www.imonitor-project.de
  - www.simu-project.de



DECOmap for Android
Version 0.2

© 2015 Decoit GmbH

Released under Apache License, Version 2.0

Conclusion and Outlook

- Collecting data of Android for SIEM environments with and without IF-MAP protocol has been working out
- Concept to treat mobile devices depending on their status (not only authenticating of the user)
- DECOmap allows real-time actions on specific events
- Future work can be:
  - Developing more clients for multiple platforms using the same or an extended data model (e.g. iOS)
  - Provide usable interfaces for communication between monitoring systems and mobile devices
  - Evaluation and incorporation of metadata to allow an assessment of mobile devices
  - Implement an integrity check on mobile devices with TPM support

Thank you for your attention!

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen

https://www.decoit.de
info@decoit.de