Android in SIEM-Umgebungen

Einbindung des freien Betriebssystems für mobile Geräte in SIEM-Umgebungen

Markus Schölzel[1] Evren Eren[1] Kai-Oliver Detken[2]

[1]Fachhochschule Dortmund, EFS 42, 44227 Dortmund
schoelzel@mailbox.org, evren.eren@fh-dortmund.de

[2]DECOIT GmbH, Fahrenheitstraße 9, 28359 Bremen
detken@decoit.de

D·A·CH Security 2015

Übersicht

1. Motivation
2. F&E-Projekte
3. TNC/IF-MAP
4. Android
   - Datenerhebung
   - Monitoring
5. DECOmap for Android
6. Herausforderungen und Ausblick

Motivation
F&E-Projekte
TNC/IF-MAP
Android
Fragmentierung
Datenerhebung
Monitoring
DECOmap for Android
Herausforderungen und Ausblick

BYOD

Research: 74 percent using or adopting BYOD [1]

Tech Pro Research's latest survey shows that the Bring Your Own Device movement is booming, with 74 percent of organizations either already using or planning to allow employees to bring their own devices to work.

BYOD

Research: 74 percent using or adopting BYOD [1]

Tech Pro Research's latest survey shows that the Bring Your Own Device movement is booming, with 74 percent 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 [2]

The bring your own device (BYOD) movement [...] will continue to grow despite security risk, according to Ernst & Young.

Studie: „Bring Your Own Device“ zwar ratsam, oft aber noch schädlich [3]

Bereits 29 Prozent aller deutschen Unternehmen mit mehr als 1000 Mitarbeitern haben geschäftskritische Daten verloren, nachdem sie Mitarbeitern den Einsatz privater Geräte im Firmennetz gestattet haben.

Android Security

Samsung Swiftkey

CVE-2015-4640 - Insufficient Verification of Data Authenticity

Stagefright (Android 2.2 bis 5.1.1)

CVE-2015-1538 - MP4 Atom Integer Overflow Remote Code Execution
CVE-2015-1539 - MP4 Atom Integer Overflow Remote Code Execution
CVE-2015-3824 - MP4 Atom Integer Overflow Remote Code Execution
CVE-2015-3826 - 3GPP Metadata Buffer Overread
CVE-2015-3827 - MP4 Atom Integer Underflow Remote Code Execution
CVE-2015-3828 - 3GPP Integer Underflow Remote Code Execution
CVE-2015-3829 - MP4 Atom Integer Overflow Remote Code Execution

OpenSSLX509Certificate (Android 4.3 bis 5.1.1)

CVE2015-3825 - „One Class To Rule Them All“ [4]

F&E-Projekte (SIEM-Systeme)

iMonitor: intelligentes Monitoring durch KI-Ereignisverarbeitung [5]

Forschungs- und Entwicklungsprojekt der DECOIT GmbH, dem Technologie-Zentrum Informatik und Informationstechnik (TZI) der Universität Bremen und neusta software development.

F&E-Projekte (SIEM-Systeme)

iMonitor: intelligentes Monitoring durch KI-Ereignisverarbeitung [5]

Forschungs- und Entwicklungsprojekt der DECOIT GmbH, dem Technologie-Zentrum Informatik und Informationstechnik (TZI) der Universität Bremen und neusta software development.

SIMU: Security Information and Event Management (SIEM) für Klein- und Mittelständische Unternehmen (KMU) [6]

Entwicklung eines SIEM-artigen Systems zur signifikanten, mit geringem Aufwand erzielbaren Verbesserung der IT-Sicherheit und von Kontrollmöglichkeiten in einem Unternehmensnetzwerk.

TNC/IF-MAP

Motivation

F&E-Projekte

TNC/IF-MAP

Android
Fragmentierung
Datenerhebung
Monitoring

DECOmap for Android

Herausforderungen und Ausblick

TNC/IF-MAP

- Trusted Network Connect: offene NAC-Architektur der Trusted Computing Group [7]
- Basiert auf IEEE 802.1x (AR, PEP und PDP)

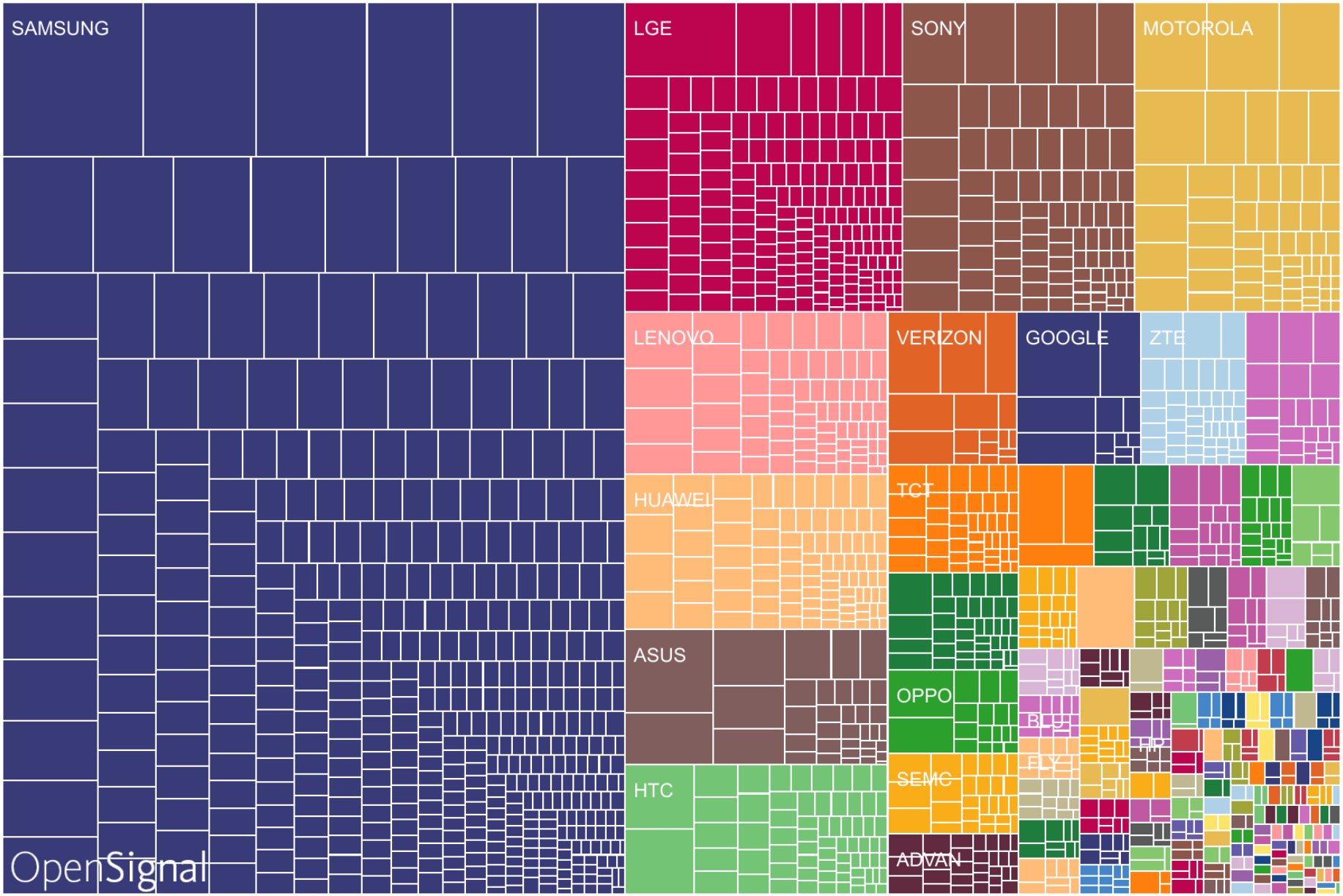
TNC/IF-MAP

- Trusted Network Connect: offene NAC-Architektur der Trusted Computing Group [7]
- Basiert auf IEEE 802.1x (AR, PEP und PDP)
- IF-MAP-Clients und MAP-Server
  (Verzicht auf hardwarebasierte Komponenten)

TNC/IF-MAP

- Trusted Network Connect: offene NAC-Architektur der Trusted Computing Group [7]
- Basiert auf IEEE 802.1x (AR, PEP und PDP)
- IF-MAP-Clients und MAP-Server
  (Verzicht auf hardwarebasierte Komponenten)
- IF-MAP: Protokoll zum Austausch von Metadaten [8]
- MAP-Graph: Identifier, Links, Metadata

Android: Fragmentierung (Hersteller)



Android Fragmentation Visualized: Hersteller [9]

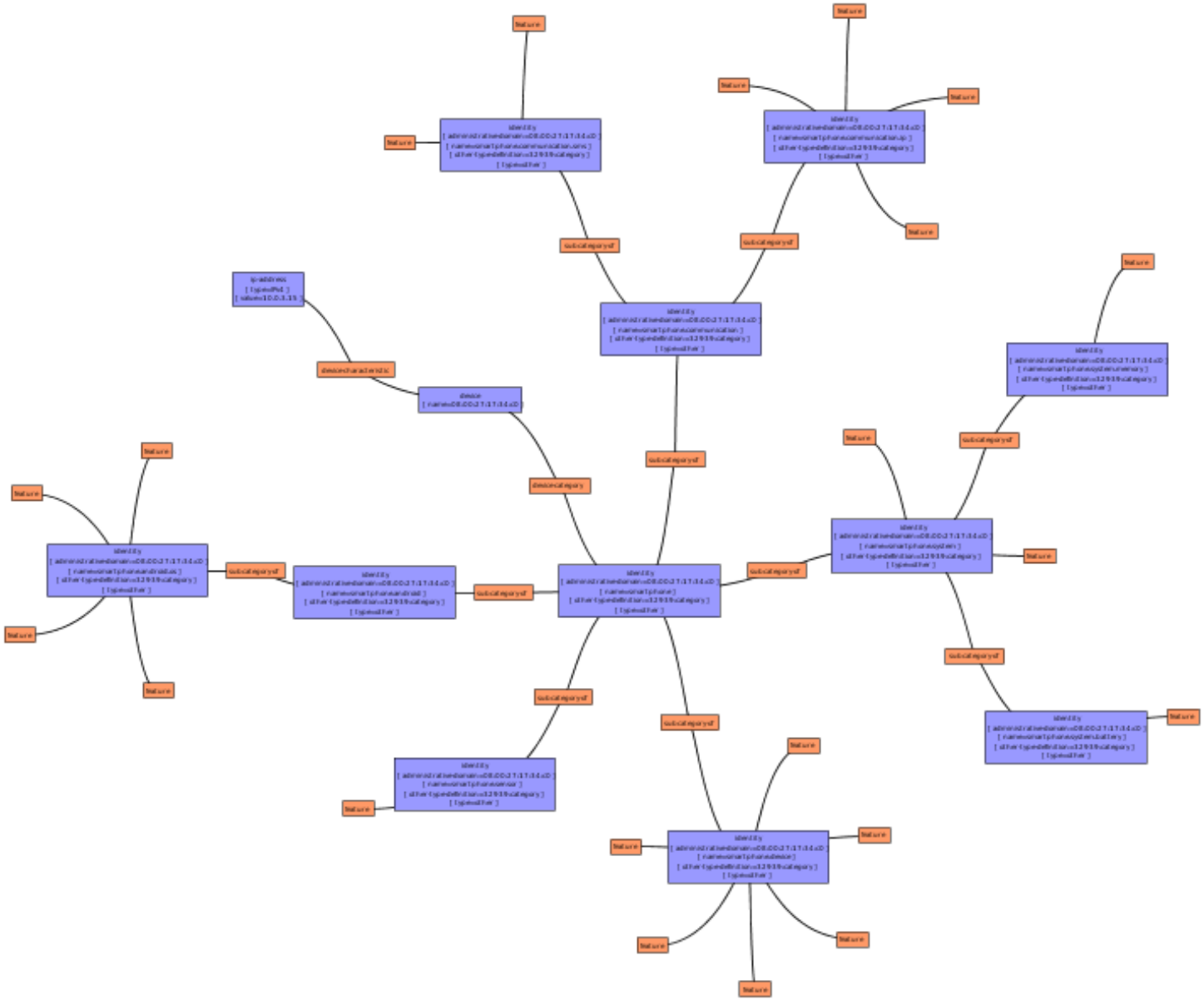
Android: Fragmentierung (Modelle)

Android Fragmentation Visualized: Modelle [9]

Datenerhebung

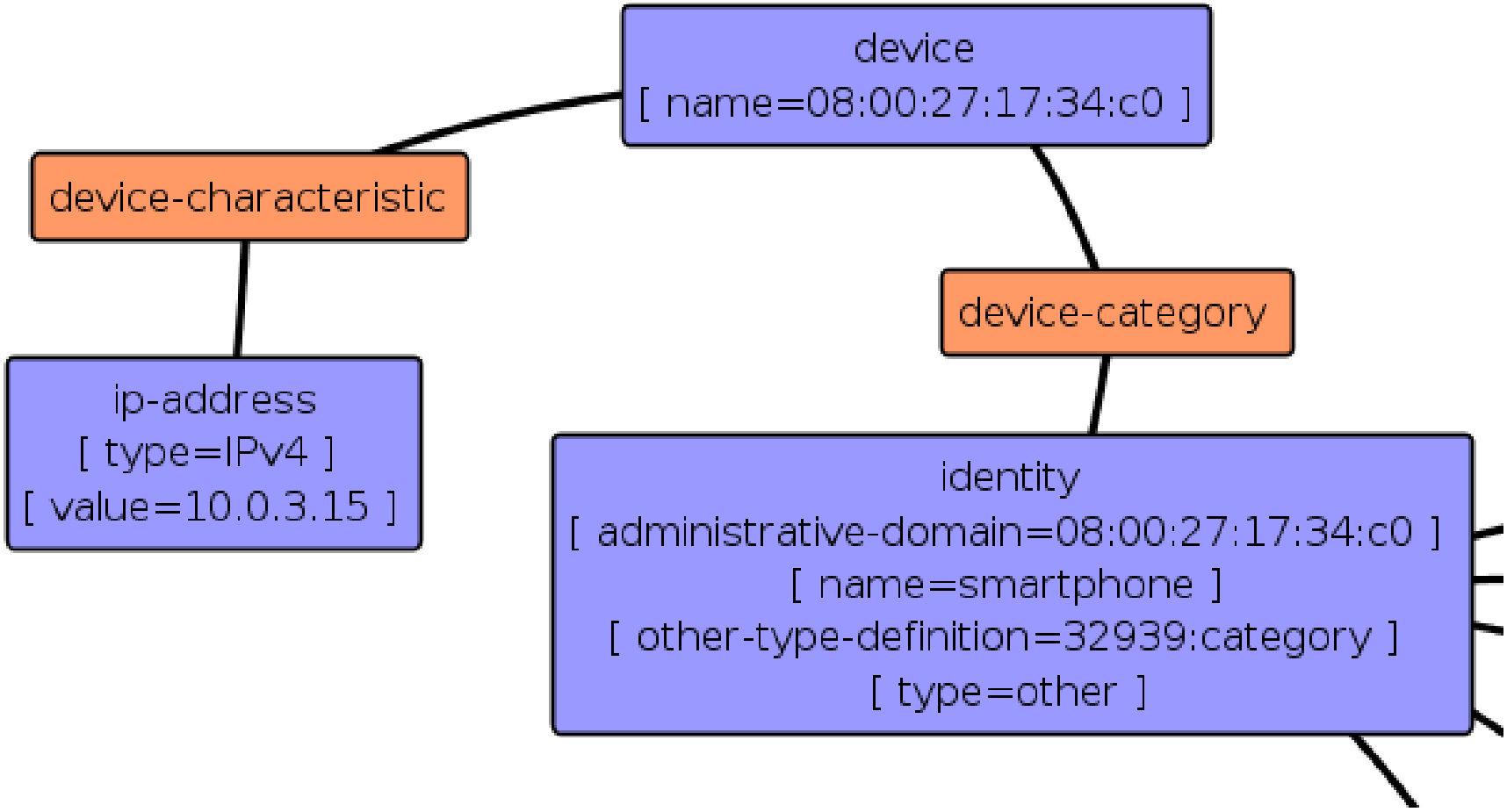
- IMEI (IMSI, MAC, ...)
- Plattform: Firmware-, Kernel-Version, Buildnumber, Baseband
- Hardware: Mikrofon, Bluetooth, GPS
- Zustand: Load, Traffic, Prozesse
- Apps: Version und Berechtigungen

SIMU: MAP-Graph



Android-Daten innerhalb eines IF-MAP-Graphen (Rendering: irongui)

SIMU: MAP-Graph



Android-Daten innerhalb eines IF-MAP-Graphen (Rendering: irongui)

iMonitor: InfoEvent

```
{
    "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>"
    }
}
```

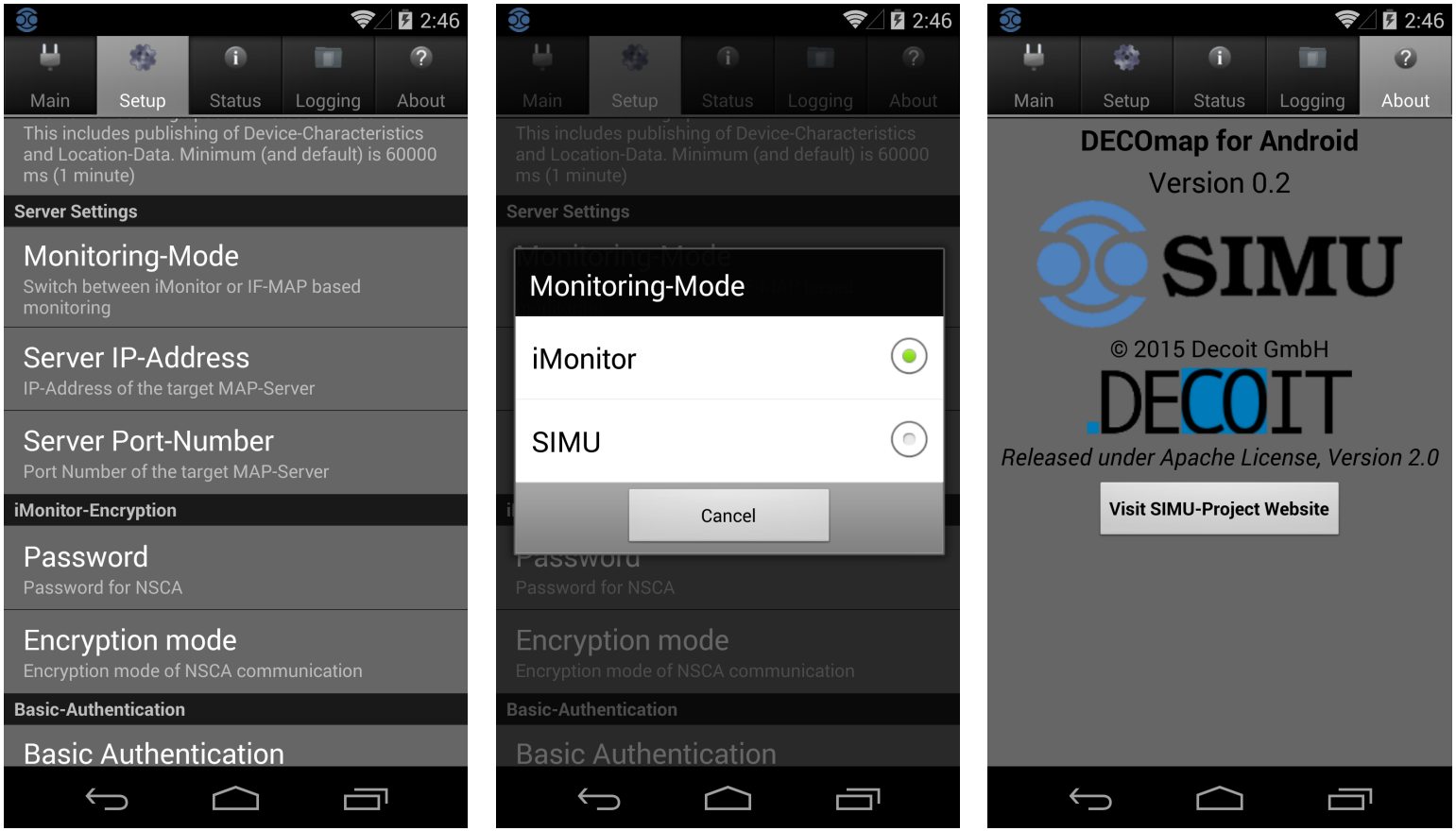
iMonitor: MonitorEvent

```
{
    "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>"
          }
        ]
    }
}
```

iMonitor: AppEvent

```
{
    "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 (Screenshots)

https://github.com/decoit/Android-IF-MAP-Client

Herausforderungen

- Schnittstellen in SIEM-Systemen
- Datenerhebung
- Auswertung und Bewertung von Daten
- Integrität: TPM, SecureBoot

Ausblick

Erweiterung des Konzepts auf weitere Plattformen:

- iOS
- Windows Phone
- Blackberry
- andere

Integration mobiler Geräte in weiteren SIEM-Systemen

Vielen Dank für Ihre Aufmerksamkeit!

Markus Schölzel - schoelzel@mailbox.org

Quellen

[1] http://www.zdnet.com/article/research-74-percent-using-or-adopting-byod/ (letzter Abruf: 19.08.2015)

[2] http://www.v3.co.uk/2396457 (letzter Abruf: 19.08.2015)

[3] http://heise.de/-2035084 (letzter Abruf: 19.08.2015)

[4] One Class to Rule Them All: 0-Day Deserialization Vulnerabilities in Android.
In 9th USENIX Workshop on Offensive Technologies (WOOT 15), Aug. 2015

[5] http://www.imonitor-project.de (letzter Abruf: 19.08.2015)

[6] http://simu-project.de (letzter Abruf: 19.08.2015)

[7] TCG Trusted Network Connect. TNC IF-MAP Binding for SOAP 2.2r9. Mar. 2014

[8] TCG Trusted Network Connect. TNC IF-MAP Metadata for Network Security 1.1r8. May 2012

[9] http://opensignal.com/reports/2015/08/android-fragmentation/ (letzter Abruf: 19.08.2015)