Trust@FHH - IF-MAP Research Projects and Open Source Software

Josef von Helden

Trust@FHH Research Group
Hochschule Hannover
University of Applied Sciences and Arts

June 26, 2013

Trust@FHH

Team

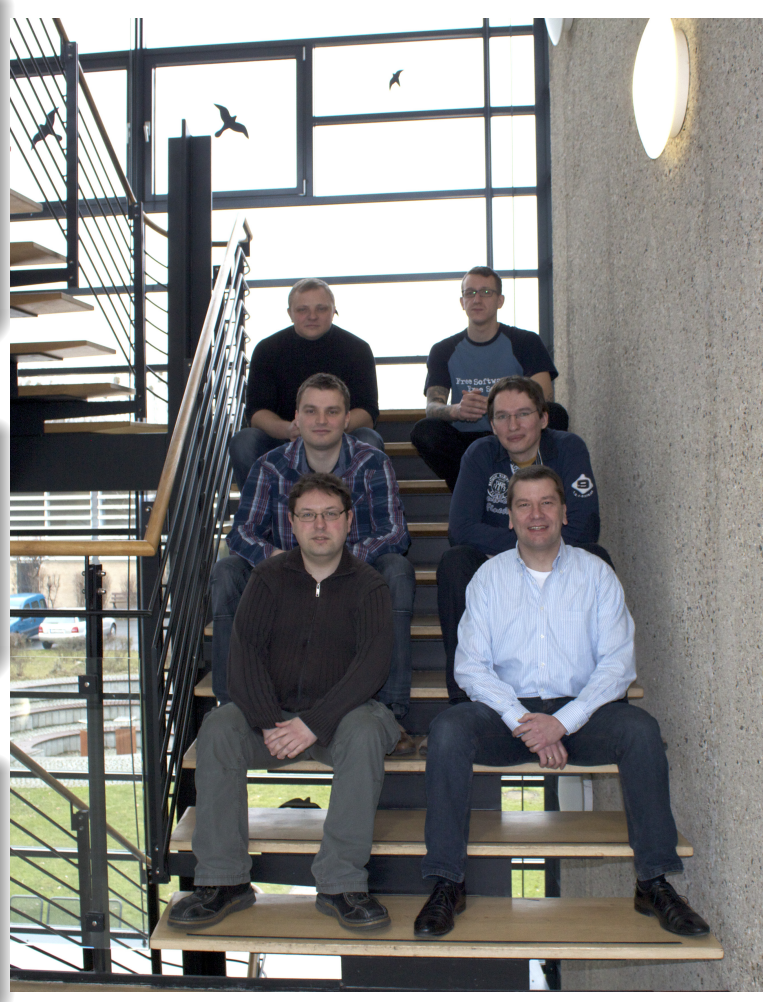
- Prof. Dr. Josef von Helden
- 1 (2,3?) research associates
- 2 (-4) student research assistant

Research Field

- Trusted Computing
- Network & Mobile Security

Research Projects

- TNC@FHH, IRON, ironcontrol
- tNAC, ESUKOM, VisITMeta, (SIMU)



Website: `http://trust.f4.hs-hannover.de/` (**new URL!**)

Agenda

1. Research Projects At A Glance
   - ESUKOM
   - VisITMeta
   - (SIMU)
2. Latest News On iron* Open Source Software
   - General information
   - ifmapj
   - irond
   - irondetect
   - ironvas
   - irondemo
   - VisITMeta
   - ironcontrol
3. Live Demo

Research Projects At A Glance

ESUKOM

General information

- Started 10/2010 - ended 09/2012
- Consortium
  - 2 research institutions (FHH, Fraunhofer SIT)
  - 3 german companies + several international associate partners
- Funded by German Federal Ministry of Education and Research
- `http://www.esukom.de`

Project Goals

... to develop a real-time security solution for enterprise networks that works based upon the correlation of metadata.

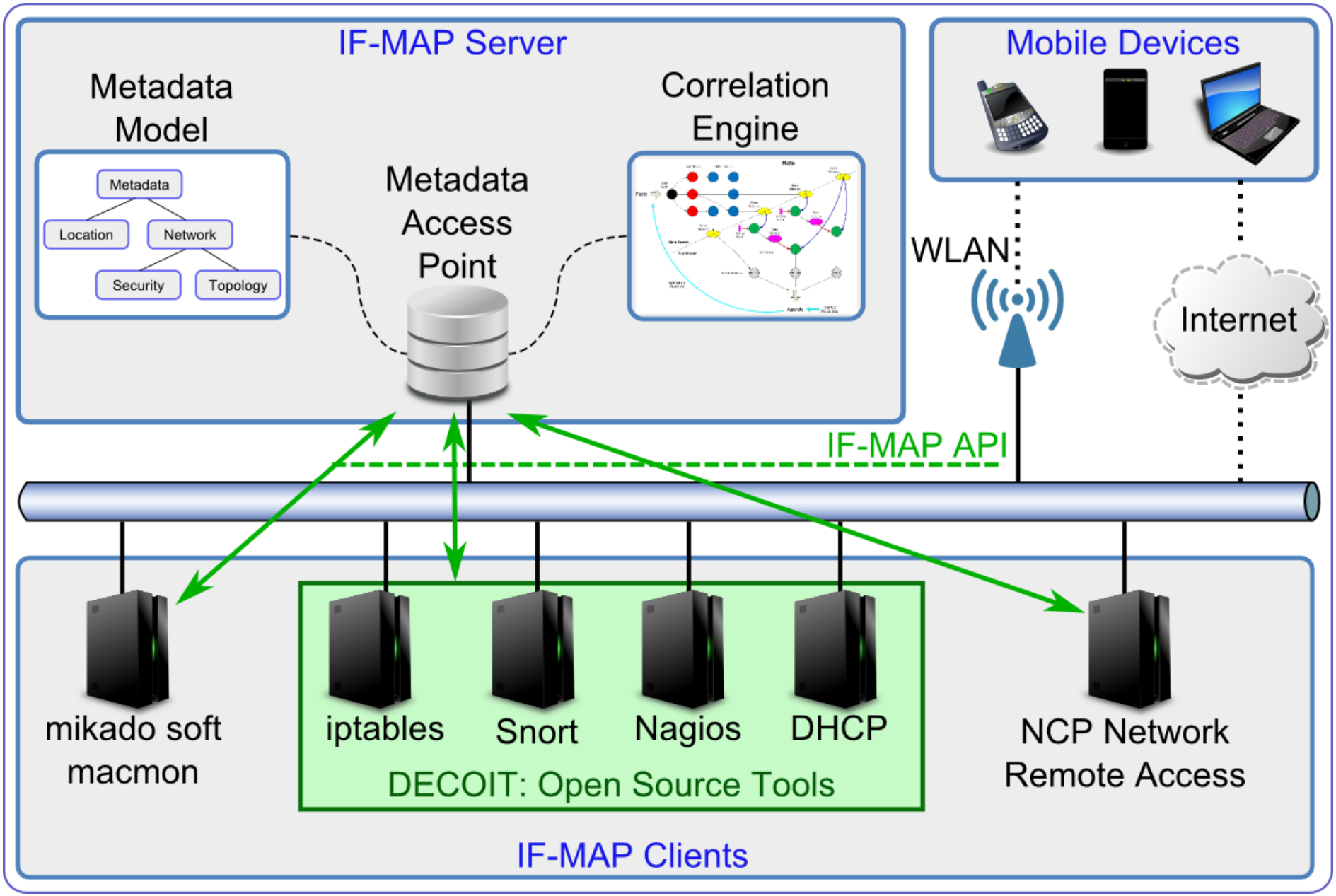
Motivation

- Growing adoption of mobil devices (smartphones)
- Smartphones are special: always-on, apps, sensors, constrained resources ...
- Impact on enterprise security?

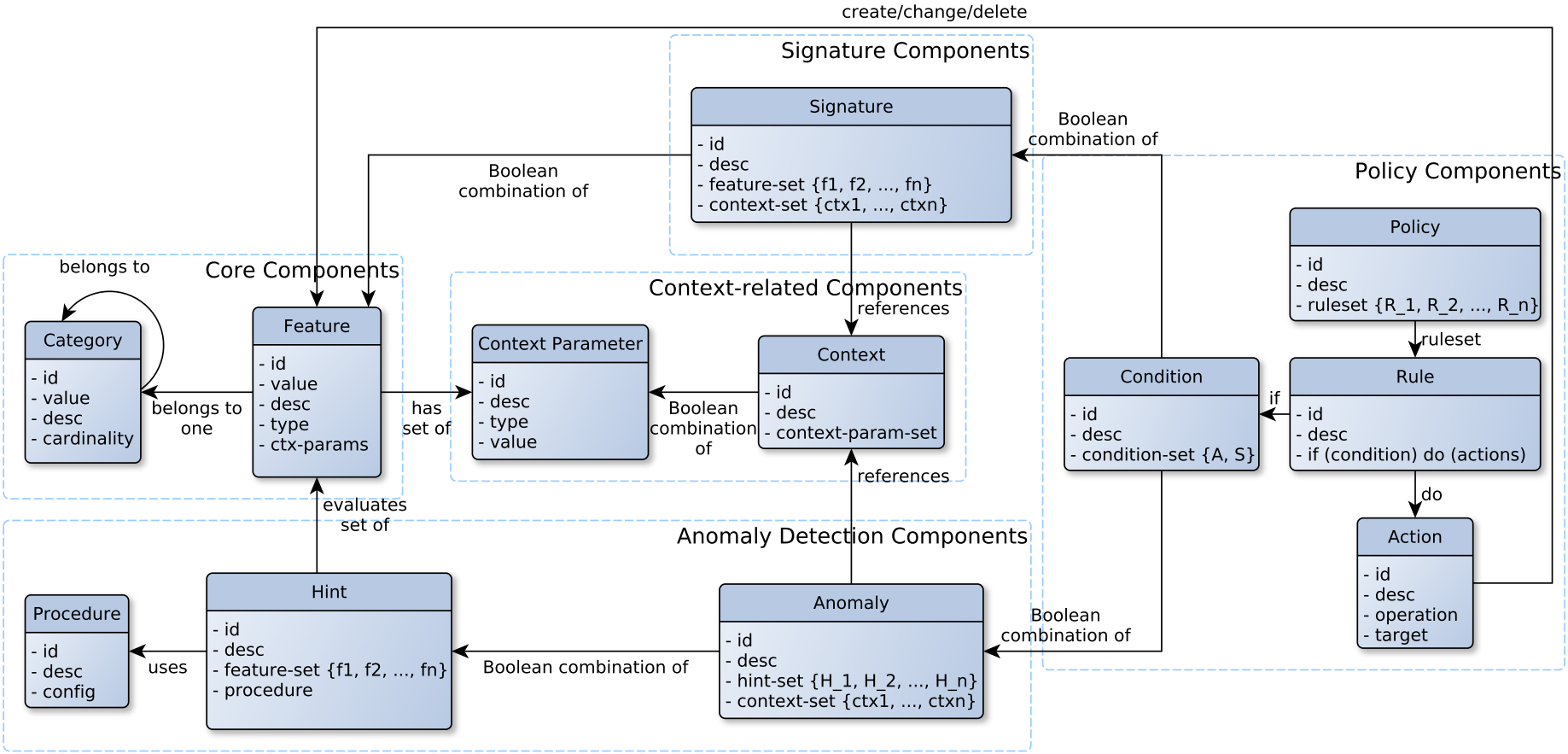
Idea

- Develop a network-based security system for monitoring smartphones
- Gain benefits from collaboration of already deployed security tools
- IF-MAP as technological basis for sharing security related metadata

ESUKOM architecture



Correlation Engine - Abstract Model



Correlation Engine - irondetect

Overview

- IF-MAP 2.0 client
- Context-related Pattern Matching and Anomaly Detection
- Decision making based on simple policies: if (a and b and c) do x

Approach

- ESUKOM tools publish vendor-specific metadata for smartphones - so called features
- irondetect holds appropriate subscriptions (one for each smartphone that gains network access), continously polls for updates of features

Vendor-specific Metadata I

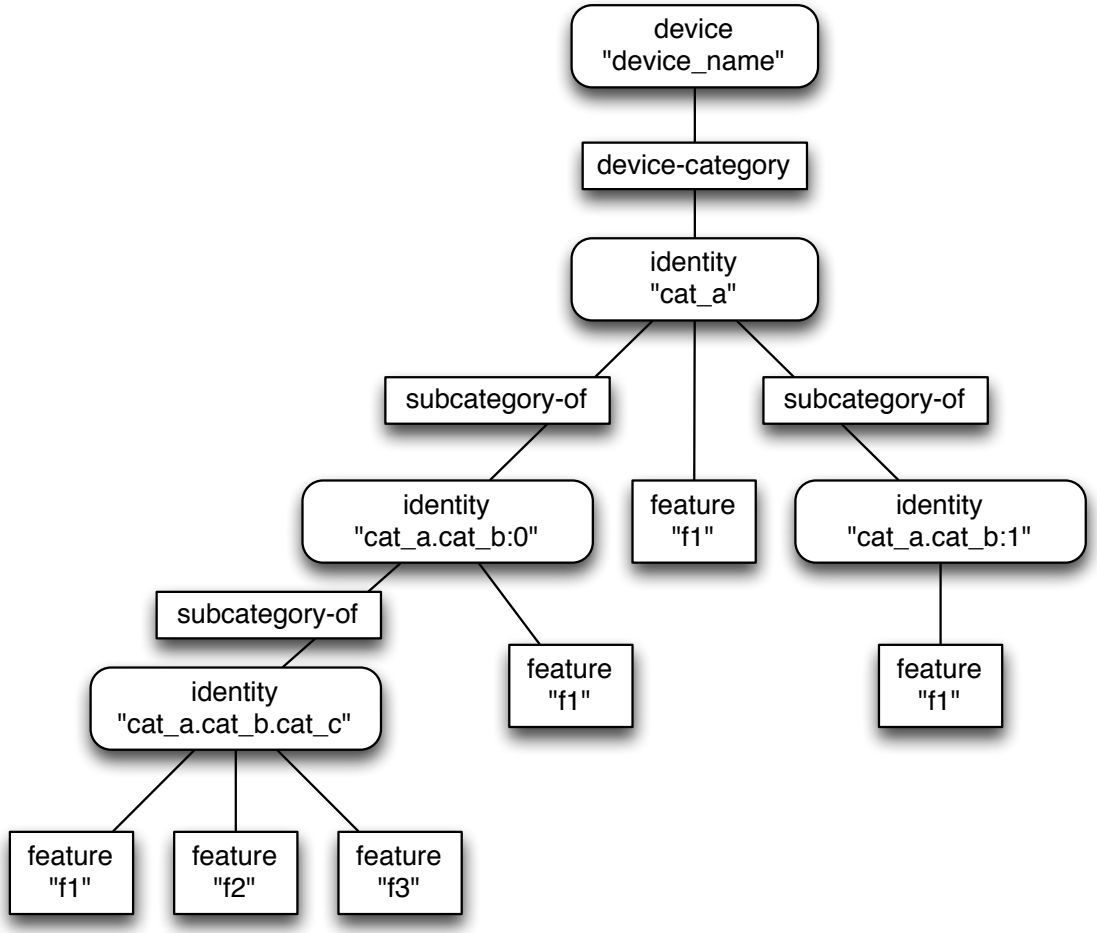
Why not using standard metadata?

- Context-related detection is based on context-parameters (time, location, other-devices, ...)
- Context-parameters are needed on a per feature basis (i.e. per metadata)
- Standard metadata should not be extended by vendor-specific attributes

Approach

- ESUKOM specific metadata for features
- "Abuse" of identity identifiers to model feature hierarchies

Vendor-specific Metadata II



VisITMeta

VisITMeta

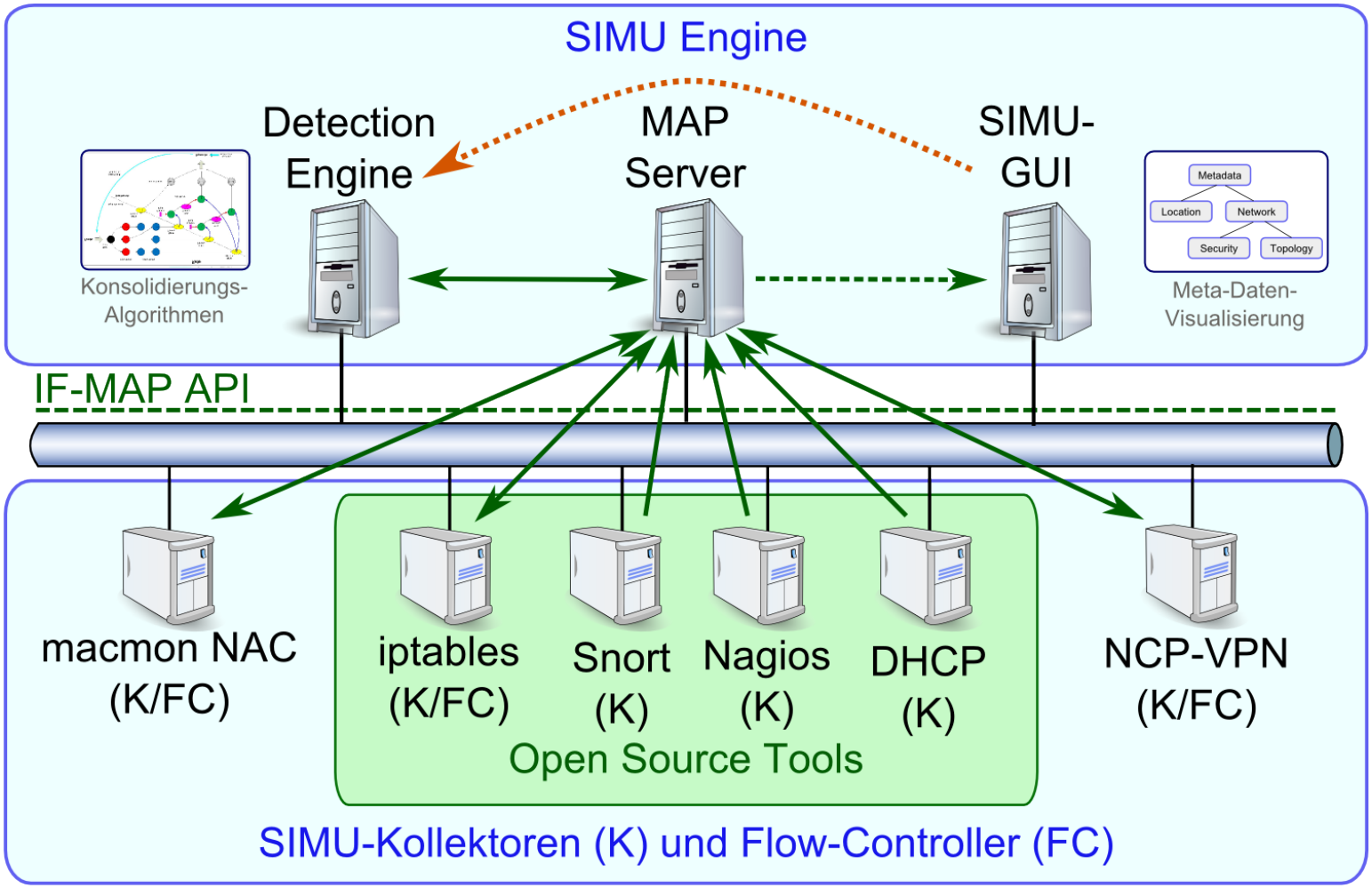
- Started 04/2012 - ends 03/2015
- Funded by German Federal Ministry of Education and Research
- Focused on visualization of IF-MAP metadata
- Based on the experiences gained with irongui
- Will provide features like:
  - View of history
  - Animation of changes within the metadata
  - Support for large graphs with methods for easy navigation

SIMU

SIMU

- SIEM for SMEs
- expected to be started 10/2013 (duration: 2 years)
- Funded by German Federal Ministry of Education and Research
- Consortium: same as ESUKOM
- Project goals:
  - easy integration in IT infrastructures of SMEs
  - easy traceability of security relevant network events
  - low costs for deployment, operating, maintenance

SIMU architecture



Legende:
- IF-MAP-Publish
- IF-MAP-Subscribe
- Publish / Subscribe
- Regelgenerierung

Latest News On iron* Open Source Software

General information

Move to Github

- Software by Trust@FHH is now available at Github (`https://github.com/trustatfhh`)
- Future software will only be made available via Github
- All projects now use the same build process (Maven)

ifmapj

About

- Lightweight IF-MAP client library written in Java
- Works on a wide range of platforms, including Android

Latest progress

- Version 0.1.5 released with experimental IF-MAP 2.1 support

irond

About

- Open-source IF-MAP 2.0 server
- Written in Java

Latest Progress

- Release 0.3.4 is TNC Certified as being IF-MAP 2.0 compliant
- Release 0.4.0 has experimental support for IF-MAP 2.1
- Prototype of MAP Content Authorization implementation will be available soon (as a branch)

irondetect

About

- IF-MAP 2.0 client
- Written in Java, uses ifmapj

Features

- Correlates on IF-MAP metadata
- Supports both signature matching and anomaly detection
- Uses vendor specific metadata
- Is controlled via user-defined policies

ironvas

About

- IF-MAP 2.0 client
- Integrates vulnerability scanner OpenVAS into a MAP environment
- Provides Publisher and Subscriber functionality
- Written in Java and Scala, uses ifmapj

Subscriber

- ironvas subscribes to `request-for-investigation` metadata
- Creates scan config, targets and tasks for new devices in OpenVAS via OMP

Publisher

- ironvas publishes vulnerability reports from OpenVAS to a MAPS
- Each vulnerability is published as `event` metadata element, with entries like CVE information, significance, ...

irondemo

About

- Set of scripts to build a demo environment (from scratch) with all iron software components
- Also available via Github
- Comes with some example scenarios
- (Will be updated and extended)
- Was used to create the following live demo

VisITMeta

Latest progress

- Will be released as a prototype in June/July
- Prototype supports recording a history of metadata on a MAPS
- Also supports separation between recording and visualizing via a REST-like interface
- Uses highlighting to show changes in the data

ironcontrol

About

- IF-MAP 2.0 client for the Android platform
- Written in Java, uses ifmapj
- administering / controlling IF-MAP from your smartphone graphs

Features

- connect to different MAP server
- publish, search, subscribe (incl. storing lists)
- saving poll results
- notification (vibration / sound) on poll results

Live Demo

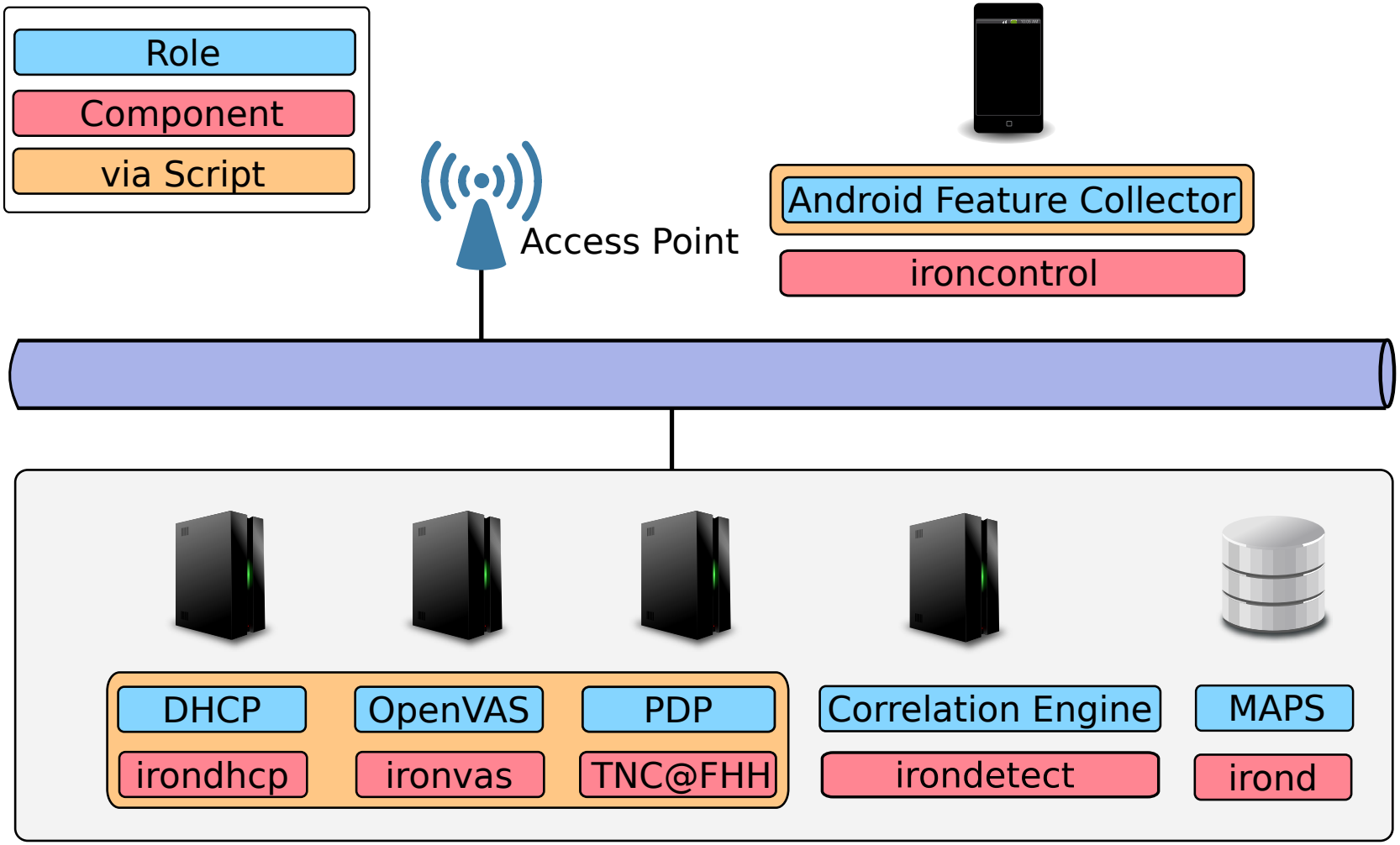


Figure: Demo environment