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 20, 2012

Trust@FHH
Hochschule Hannover
University of Applied Sciences and Arts

Trust@FHH

Team

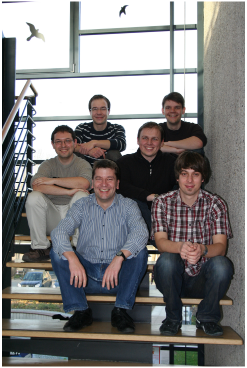
- Prof. Dr. Josef von Helden
- 3 research associates
- 3 student research assistants

Research Field

- Trusted Computing
- Network & Mobile Security

Research Projects

- TNC@FHH, IRON
- tNAC, ESUKOM, VisITMeta



Website: `http://trust.inform.fh-hannover.de`

Agenda

1. Research Projects At A Glance
   - ESUKOM
   - VisITMeta
2. Latest News On iron* Open Source Software
   - ifmapj
   - irond
   - ironvas
3. Live Demo

ESUKOM

General information

- Started 10/2010 - ends 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.

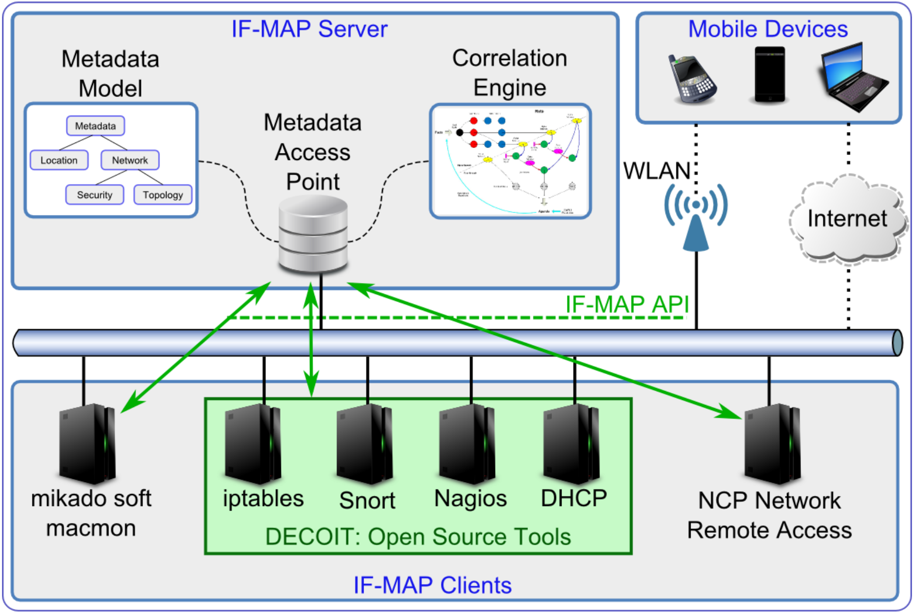
Motivation

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

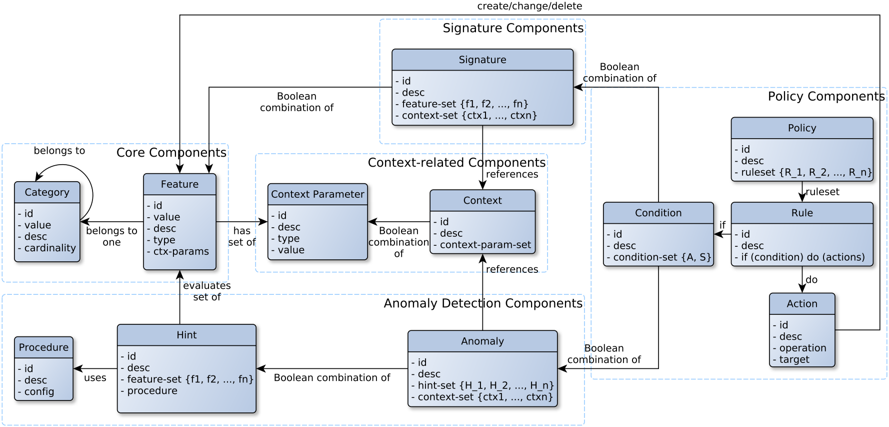
Idea

- 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

Architecture



Correlation Engine - Abstract Model



create/change/delete

Signature Components

Signature
- id
- desc
- feature-set {f1, f2, ..., fn}
- context-set {ctx1, ..., ctxn}

Boolean combination of

Boolean combination of

Policy Components

Policy
- id
- desc
- ruleset {R_1, R_2, ..., R_n}

ruleset

Rule
- id
- desc
- if (condition) do (actions)

if

Condition
- id
- desc
- condition-set {A, S}

do

Action
- id
- desc
- operation
- target

Core Components

belongs to

Category
- id
- value
- desc
- cardinality

belongs to one

Feature
- id
- value
- desc
- type
- ctx-params

has set of

Context-related Components

references

Context Parameter
- id
- desc
- type
- value

Boolean combination of

Context
- id
- desc
- context-param-set

references

evaluates set of

Anomaly Detection Components

Procedure
- id
- desc
- config

uses

Hint
- id
- desc
- feature-set {f1, f2, ..., fn}
- procedure

Boolean combination of

Anomaly
- id
- desc
- hint-set {H_1, H_2, ..., H_n}
- context-set {ctx1, ..., ctxn}

Boolean combination of

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 subscribtions (one for each smartphone that gains network access), continously polls for updates of features

Live Demo

Vendor-specific Metadata I

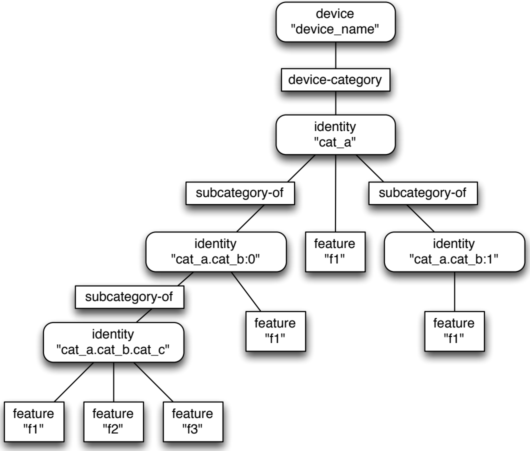
Why not using standard metadata?

- 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

- New research project, started April 1st, 2012, duration 3 years
- 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

ifmapj

About

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

Latest progress

- ifmapj is used by ESUKOM partners to implement their IF-MAP clients

irond

About

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

Latest Progress

- IF-MAP 2.0 server has gotten several improvements
- Performance was drastically improved (now performs 100k updates in less than 30 seconds on commodity hardware ... with enough memory)

ironvas

About

- Brand new 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, ...