VisITMeta

Visualizing the security of modern IT environments by using metadata

Project presentation

Bastian Hellmann

Trust@FHH Research group
Hochschule Hannover

May 30th, 2012
6th ESUKOM Workshop, Nuremberg

Trust@FHH
Fachhochschule Hannover
University of Applied Sciences and Arts

Motivation: Why visualize metadata?

What is metadata?

- Metadata contains information **about** the components in a network, that is transporting or processing raw or payload data
- Metadata has to be created and collected
- Metadata has to be provided
- Metadata can be processed
- Metadata in the remainder of this slides: metadata for network security

Metadata in the real world

How they are used in the real world

- Metadata **can** be gathered → IF-MAP specification [1]
- Metadata **is** beeing gathered and processed → ESUKOM project [2]
- Automatic processing of metadata → e.g. correlation of metadata

Visualization of metadata in the real world

- Plain textual representation of metadata does not allow for easy comprehension by human beeings
- No quick overview of a network possible
- Choose a suitable visualization according to the underlying data → IF-MAP metadata as a graph

[1] `http://www.trustedcomputinggroup.org/resources/tnc_ifmap_binding_for_soap_specification`

[2] `http://www.esukom.de/cms/front_content.php?idcat=10&lang=1`

Necessity for visualizing metadata

Status quo

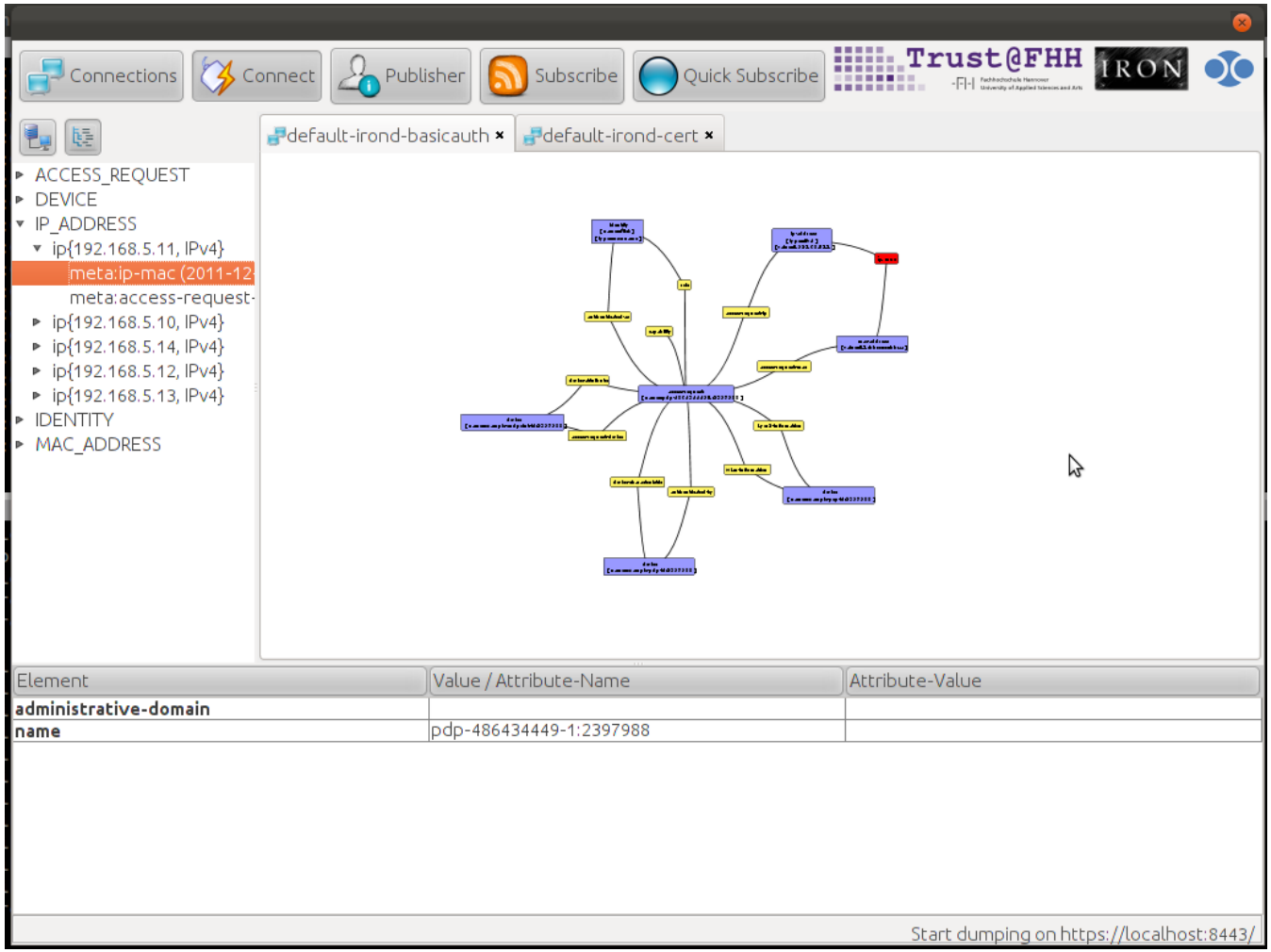
- As a result of ESUKOM, metadata is available in a large amount (directly gathered by IF-MAP clients or as a result of correlation)
- Logging output of MAP server is not sufficient for looking at these large numbers of metadata

Preliminary work: irongui

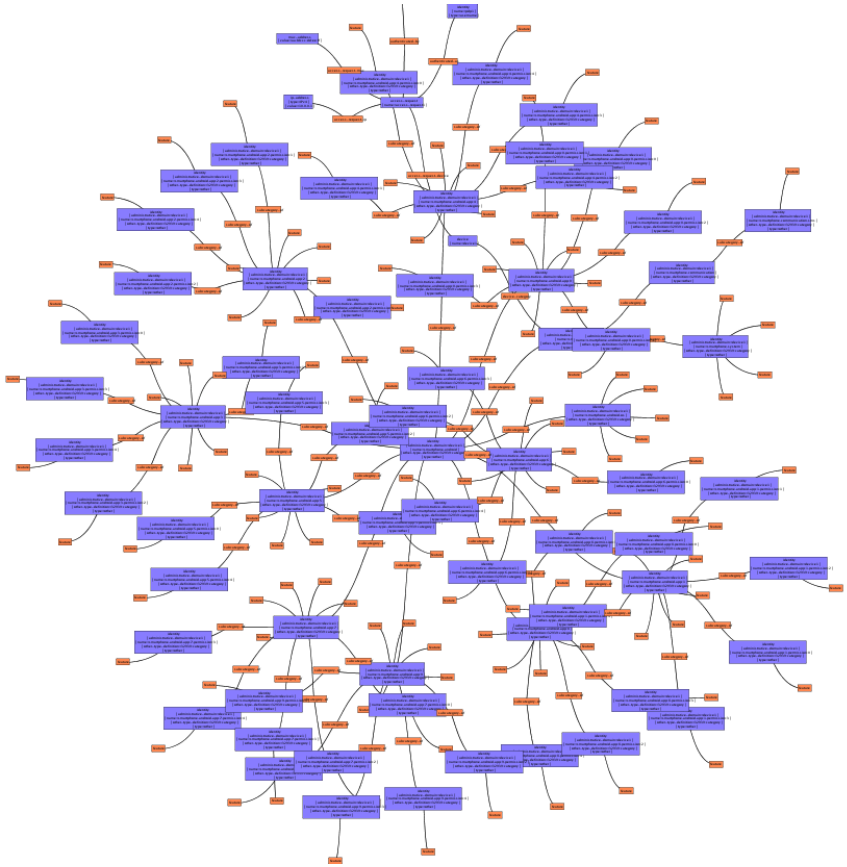
Preliminary work: irongui (1/2)

- First results for visualizing IF-MAP metadata developed available with **irongui** by Tobias Ruhe, B. Sc.
- Result of a bachelor thesis at Hochschule Hannover
- Further development in Trust@FHH research group
- Uses *Prefuse* for layouting and rendering metadata
- Uses *ifmapj* (Java library by Arne Welzel, B.Sc.) for using IF-MAP

Preliminary work: irongui (2/2)



Big metadata graphs



Problems of irongui

Problems

- Problems at meaningful visualization of large data sets
- Implementation is strongly prototypic
- Problems with the used libraries for layouting and rendering

Approach

- Start a new research project to study different techniques to visualize IF-MAP metadata

Research project: VisITMeta

Visualisierung der Sicherheit mobiler **IT**-Infrastrukturen auf der Basis von **Meta**daten

(**Vis**ualizing the security of modern **IT** environments by using **meta**data)

General information

Funding

- Line of funding: ProfilNT (BMBF)
- Project duration: 3 years
  - Starts on April 1st, 2012
  - Ends on March 31st, 2015

Partners/Cooperation

- Internally (Hochschule Hannover): Research group for visualization (Prof. Dr. Volker Ahlers)
- Externally: partners of ESUKOM project
- Cooperation with Universität der Bundeswehr München

Overall goals

- Development of an open source software to visualize IF-MAP metadata
- Regard the results and ideas of **irongui**
- Interoperability with other IF-MAP clients and servers
- Spread the use of IF-MAP in the real world:
  - Contribute to the development of the specifications by the TCG
  - Adoption of VisITMeta software at the ESUKOM members
- $\rightarrow$ Incorporate feedback of the ESUKOM members

Detailed goals 1/3

Render metadata as a graph

- Use nodes, edges and labels for Identifier, Links and metadata
- Layouting of the graph
  - Robust layouting when strong changes occur
  - Level-of-Detail or other methods for abstraction
  - use own layouting for subgraphs (e.g. some parts are more hierarchically ordered)
- Use filter techniques to adjust the visualization

Alternate views

- Concentrate on specific aspects via coloring, different shapes, sizes, ...
- Dashboard

Detailed goals 2/3

Actuality and performance

- Visualize the current state of the network
- High performance of rendering and layouting with great amount of metadata

Display the history of metadata

- Display all chronological states of metadata
- Allows to reproduce and understand events in the network
- Idea: control via timestamp slider
- Use animations to illustrate changes in the graph

Detailed goals 3/3

Navigation within the data

- Support for moving and zooming
- Allow for simple concentration of parts of the whole graph

Search functionality

- Search for specific Identifier respectively metadata
- Search by user defined criteria

Requirements on new software

- Strict separation of software layers; especially between data model/persistence and graphical output
- Easy extensibility
- Easy switching from one library to another (in contrast to *irongui* and *Prefuse*)
- Use *ifmapj* for all IF-MAP related functionality

Outlook

Reference to the results of ESUKOM

Visualization of correlation results

- Correlation of metadata
  - Using anonamlies and signatures, based on *features* of Smartphones
  - Use arbitrary methods for correlation (statistics, clustering, . . .)
- Trust rating for metadata
- Snapshots for storing different states of one information

Possible

- Display the results of correlation
- Display the changes of a single feature
- Display the trust rating of a single information
- Display changes in the trust rating

Further (possible) research questions and ideas

- Visualize the spatial changes of devices in the network $\leftrightarrow$ privacy
- Display information to the *user* of an endpoint
- 3D visualization
- Stereoscopic visualization
- (Software) ergonomy
- Large-format screens
- Control by gestures
- ...