Visualization of Network Security Policy Evaluation

Bastian Hellmann  Marcel Reichenbach  Leonard Renners  Volker Ahlers
University of Applied Sciences and Arts Hannover, Germany

Motivation
- Components that use policies to detect attacks and unwanted behaviour in a network do not share their state
- This makes the analysis of why a specific evaluation returns wrong or unexpected results hard.
- Combining both the sensor data as well as the configuration (policy) of a network security tool and its evaluation can help.

The Interface for Metadata Access Points (IF-MAP)
- Specification by the Trusted Computing Group for standardized metadata exchange
- Data model: undirected graph with Identifiers, Metadata and Links
- Communication model: publish/subscribe system, multiple clients and one server
- Data can be adapted to arbitrary domains (in this case: network security)

VisITMeta: Visualising IF-MAP Graphs
- Open-source tool that visualizes IF-MAP graphs
- Result of a 3-year research project in Germany
- Main features: (a) Persistence of history, (b) calculation and visualization of graph deltas, (c) filters and searches and (d) highlighting changes

irondetect: An exemplary policy-based detection engine
- Open-source policy-based tool that performs signature checks and anomaly detection on IF-MAP graphs
- Interchangeable methods to detect anomalies
- Considers the context of data (time, location, ...)

Policy Visualization
- Mapping the policy model of irondetect to IF-MAP entities

VisITMeta: Visualising IF-MAP Graphs
- Open-source tool that visualizes IF-MAP graphs
- Result of a 3-year research project in Germany
- Main features: (a) Persistence of history, (b) calculation and visualization of graph deltas, (c) filters and searches and (d) highlighting changes

VisITMeta: Visualising IF-MAP Graphs
- Open-source tool that visualizes IF-MAP graphs
- Result of a 3-year research project in Germany
- Main features: (a) Persistence of history, (b) calculation and visualization of graph deltas, (c) filters and searches and (d) highlighting changes

Contact information
- Email: trust@f4-i.fh-hannover.de
- Website: http://trust.f4.hs-hannover.de/
- GitHub: https://github.com/trustathsh

http://trust.f4.hs-hannover.de