Predictive Security Analysis
Concepts, Implementation, first Results in Industrial Scenario

Roland Rieke\textsuperscript{1}  Romain Giot\textsuperscript{2}  Chrystel Gaber\textsuperscript{2}

\textsuperscript{1}Fraunhofer SIT, Darmstadt, Germany
Email: roland.rieke@sit.fraunhofer.de

\textsuperscript{2}France Télécom-Orange Labs, Caen, France
Email: romain.giot@orange.com, chrystel.gaber@orange.com

CYBER SECURITY & PRIVACY EU FORUM 2013, 19th April 2013

MASSIF
Overview

1. Advanced Security Information & Event Management
2. Predictive Security Analysis @ Runtime
3. Mobile Money Transfer Scenario
4. Conclusions
Advanced Security Information & Event Management
Advanced SIEM - tomorrow

**Requirements**
- High interoperability - heterogeneity of input sources
- High scalability - handle and processing of load peaks of events
- High elasticity - resources coupling the flow of events

**Features/Properties**
- Multi-domain - different application areas
- Cross-layer - logical security, physical security and service layer
- Predictive security analysis
- Countermeasures selection and evaluation - RORI
- Trustworthiness and resilience framework
Example: Mobile Money Transfer

Transactions Monitor (TM): monitors Transactions in the systems

PIN Monitor (PM): monitors the number of PIN attempts

Mobile Location Monitor (MLM): monitors the location of transactions

Possible symptoms of misuse case "Account Takeover":
- excessive number of PIN attempts
- excessive number of transactions
- too many different mobile phone locations starting transactions
Requirements-driven System Design

Business Process
Application
Infrastructure

Requirements Analysis

Design Guidelines

Security

Compiler Technologies

Event Processing

Technical Integration

Fit to problem space
Close information gap
Resilient and affordable

Scalability
Elasticity
Cross-layer
Heterogeneity

A3 - Event and Information Collection

Physical + logical events
Unknown behavior
Failure prediction
Attack/response analysis

A4 – Event, Process Models and Attack Models

Resilient operations
Countermeasure Support
OSSIM/Prelude Integration

A5 – Advanced SIEM Framework

Roland Rieke, Romain Giot
Predictive Security Analysis
CSP’13
Knowledge is built on theory. The theory of knowledge teaches us that a statement, if it conveys knowledge, predicts future outcome, with risk of being wrong, and that it fits without failure observations of the past.
— William Edwards Deming

Predictive Security Analysis @ Runtime
Operational Model of Process

1. Discover process model Petri net, EPC

2. Predict close-future process behaviour
Adapt Process Model

Detect unknown process actions

Belief change w.r.t. process model
Predict Security Violations

Detect missing events

5.

Use process model to predict future events

Predict feasible security violations

6.

Roland Rieke, Romain Giot

Predictive Security Analysis

CSP’13
Mobile Money Transfer Scenario
Illustration of Money Laundering
PSA Configuration for Detection

abnormal transfer detected
PSA Behavior on Real Events - Obtained Transitions

Roland Rieke, Romain Giot

Predictive Security Analysis

CSP'13 16
PSA Behavior on Real Events - Scaling

Roland Rieke, Romain Giot

Predictive Security Analysis

CSP’13 17
PSA Behavior on Real Events - Facts

Simple EPC with alerts
- 4.5 millions of events treated in 6 hours
- 0.5 millions of alerts generated

Complete EPC without alerts
- 4.5 millions of events treated in 33 minutes
- 0 alerts generated

Facts
⇒ Processing time is minimal when no alerts have to be generated
- PSA is able to manage in real time all the logs of an operational system
  ▶ Best case: 2272 events/second without alerts
  ▶ Worst case: 25 events/second with alerts
PSA Behavior on Simulated Events - Simulation

- As we do not have a groundtruth on the real events
  ⇒ it is necessary to work with simulated events
PSA Behavior on Simulated Events - Results
PSA Behavior on Simulated Events - Deeper analysis

Figure: Illustration of the transactions

Roland Rieke, Romain Giot
Predictive Security Analysis
CSP’13 21
Conclusions

- MMTS analysis utilizes alerts generated by the uncertainty reasoning component of PSA to detect money laundering patterns.
- PSA is able to detect irregular events regarding the behavior of the user of the MMTS system.
- It is necessary to cope with False Alarms and make decisions regarding the alerts.

- MASSIF ([http://www.massif-project.eu/](http://www.massif-project.eu/)) will analyse advantages of PSA with respect to “measuring” security and compliance @ runtime.

- Advanced application-aware SIEM requires novel concepts such as PSA.
- Lesson learned: SoS need to be designed for security assessment @ runtime.
Conclusions

• MMTS analysis utilizes alerts generated by the uncertainty reasoning component of PSA to detect money laundering patterns.
• PSA is able to detect irregular events regarding the behavior of the user of the MMTS system.
• It is necessary to cope with False Alarms and make decisions regarding the alerts.

• MASSIF (http://www.massif-project.eu/) will analyse advantages of PSA with respect to “measuring” security and compliance @ runtime.

• Advanced application-aware SIEM requires novel concepts such as PSA.
• Lesson learned: SoS need to be designed for security assessment @ runtime.
Conclusions

- MMTS analysis utilizes alerts generated by the uncertainty reasoning component of PSA to detect money laundering patterns.
- PSA is able to detect irregular events regarding the behavior of the user of the MMTS system.
- It is necessary to cope with False Alarms and make decisions regarding the alerts.

**MASSIF** ([http://www.massif-project.eu/](http://www.massif-project.eu/)) will analyse advantages of PSA with respect to "measuring" security and compliance @ runtime.

- Advanced application-aware SIEM requires novel concepts such as PSA.
- Lesson learned: SoS need to be designed for security assessment @ runtime.
Conclusions

- MMTS analysis utilizes alerts generated by the uncertainty reasoning component of PSA to detect money laundering patterns.
- PSA is able to detect irregular events regarding the behavior of the user of the MMTS system.
- It is necessary to cope with False Alarms and make decisions regarding the alerts.

MASSIF (http://www.massif-project.eu/) will analyse advantages of PSA with respect to “measuring” security and compliance @ runtime.

- Advanced application-aware SIEM requires novel concepts such as PSA.
- Lesson learned: SoS need to be designed for security assessment @ runtime.