Model Driven Security

Dr. Ulrich Lang
CEO, ObjectSecurity
InfoSec PhD (Cambridge)
& Master’s (RHUL London)

INCOSE Conference, 1 November 2014
The Security Policy Automation Experts
information security specialists: innovative technologies + consulting, R&D

CUSTOMERS
ITS, ATC, Defense & Aerospace, Manufacturing, ICT, Smart Cities

Promia (US Navy)
RTI (US Navy + Air Force)
Agilent
IBM
Smartronix
CHI
FutureTek (Boeing)
US Naval Research Laboratory
General Electric

QinetiQ
UK MoD
BAA
UK TSB
Artechouse
Cyber Security KTN
Intel
ESG
SAP
Royal Bank of Scotland
Twinsoft/HP
BMVIT
European Commission
Deutsche Telekom
European Space Agency
Lufthansa Systems
Eurocontrol
Hornbach
UL VS

"Cool Vendor in Authentication and Application Security 2008"
(Gartner, also on Hype Cycles 2007 + 2008)
Gartner
"thorough and enlightening"
(QinetiQ, SOA best practice analysis for UK Ministry of Defence)
QinetiQ
"in-depth technical knowledge and industrial experience"
(U.S. Naval Research Lab)

"rapid one-to-one support, highly knowledgeable"
(Royal Bank of Scotland)

"well-known security experts"
(Object Management Group)

"significant experience in security management"

2000 ...Middleware Security
2000 ...Middleware Security

Implementing policies too difficult:
- Too many rules (whitelisting) in too many places
- Too many dynamic changes (agility)
- Policy support not expressive enough
- No assurance
- ...
Implementing policies too difficult:
- Still too many rules, now in one place
- Too many dynamic changes (agility)
- Policy support not expressive enough
- Little assurance
2004 ... OpenPMF v2 (MDS)

Model-Driven Security:
✓ cheaper
✓ more secure
✓ faster accreditation/compliance
✓ for agile, complex IT landscapes
✓ standards

Security Models
Other Information Sources
Semantic Gap

Human-intuitive policies
Policy Automation
Compliance Automation
Runtime policy enforcement
Challenges are growing & converging!

- **IT environment**
  - agile, complex, interconnected SoS

- **Policies**
  - numerous, complex, meaningful/feature-rich (e.g. privacy), fine-grained, contextual/dynamic

- **Status quo fails**
  - blacklisting; anomaly/behavior/incident-based; manual policy implementation...

- **Need better policy tools**
  - meaningful, preventive (whitelisting), manageable, supports IT agility, information flow based, repeatable/traceable/verifiable
Model-Driven Security

- Information flow based SoS security (users & devices)
  - IoT/M2M often has system description & well-defined M2M interactions
- Access policies
  - Whitelisting; meaningful access policies; support IT agility
  - Advanced access control approaches (ABAC, PBAC, RAdAC, ZBAC, PHABAC...)
- Model-Driven Security
  - Tool supported process
  - Model “undistorted” security requirements models at a high level of abstraction,
  - Using other information sources (produced by other stakeholders, expressed in DSL),
  - Transform models into enforceable security rules with little/no human intervention;
  - Run-time decisioning enforcement, dynamic policy updates, policy incident monitoring.

**MDS:** Automatic generation of technical security rules for information flow enforcement
Use case: Access control, monitoring

**MDSA:** Automatic generation and update of supporting evidence for information assurance accreditation (→ requires MDS)
Use Case: for Common Criteria
MDS Video Clip

http://www.youtube.com/watch?v=Eiy19v-n-1s
MDSA Video Clip

http://www.youtube.com/watch?v=Eiy19v-n-1s
OpenPMF™

OpenPMF is standards-based (incl. Ecore/MOF, XMI, XACML, ABAC), award-winning, and patented.

OpenPMF Components

- A model-driven policy authoring tool,
- A model-driven rule generation tool,
- An attribute-based authorization policy server,
- Policy decision/enforcement points,
- A model-driven compliance/accreditation evidence generation tool

The OpenPMF Solution is customizable for your particular business and IT landscape. We currently offer pre-developed integration and support for the following technologies:

- XACML Authorization Management
- Eclipse IDE & modeling framework
- BPMN business processes: Intalio BPM
- SOA web app server: BEA Weblogic, Glassfish, Axis2/Tomcat
- Data Distribution Service: RTI DDS
- CORBA Components: Qedo CCM
- CORBA MICO C++ CORBA
- CORBA: JacORB Java CORBA
- Message-oriented middleware: XMLBlast
- Fraunhofer FOKUS AD4 CCM MDA toolchain
- Firewalls: IIOP ObjectWall ('network PEP')
- Promia Raven NIDS
- Public Key Infrastructure (PKI): X.509
- Privilege Management (PMI): OMG ATLAS
- Directory Services: LDAP
- Databases: Secerno (under dev.)
- Databases: PostgreSQL (under dev.)

Other technologies: supported on demand
Advanced Access Control: ABAC

- Attribute-Based Access Control (ABAC):
  - “attributes: subject, object, requested operations, environment conditions
  - policy, rules, or relationships: allowable operations for a given set of attributes.” (NIST 800-162 draft)

- by 2020, 70% of all businesses will use ABAC as the dominant mechanism to protect critical assets, up from less than 5% today (Gartner)

- Very useful concept, but the term itself is a misnomer, imprecise, overlapping

- Challenges: Hard to implement, hard to author policies, hard to get attribute consensus

- Example: OASIS XACML

Also: PBAC, ZBAC, RAdAC, PHABAC/HBAC, RelBAC/VBAC ...
Advanced Access Control: PBAC

- **Proximity-Based Access Control (PBAC)**
  - policies based on relative proximity/distance
  - between one or more proximity attributes associated with an accessor
  - and one or more proximity attribute associated with an accessed resource.
  
  (source: ObjectSecurity)

- **Many PBAC dimensions**
  - Geo-Location/Geospatial Proximity
  - Organizational Proximity
  - Operational Proximity
  - Temporal Proximity
  - Business Process Proximity
  - Security Proximity
  - Risk proximity
  - Social Proximity
  - Information Proximity
  - ...
MDS Example
Functional System Description
MDS Example
OpenPMF™ ABAC Deployment
MDS Example

Metamodel & Metadata Population
MDS Example
Non-PBAC Policy

Requestors working on PII relevant tasks can only access PII resources if requestor not in the EU and PII resource not in EU.

Model-Driven Security
Bridge
Semantic Gap
(attributes)

ASS1: requestor_identity
ASS2: requestor_geolocation_position
ASS3: resource_label_task
ASS3: resource_label_geolocation
MDS Example

PBAC Policy

Requestors can access mission resources if they are in “80% mission proximity” to the resource

Model-Driven Security
Bridge
Semantic Gap
(rule elements)
+ attributes
OpenPMF™ User Experience
User Experience
Push-Button Automation
Questions?

ObjectSecurity LLC
1855 1st Ave, Suite 103
San Diego, CA, 92106
101 The Embarcadero, Suite 200
San Francisco, CA 94105
Tel: 1-650-515-3391
Fax: 1-360-933-9591
www.objectsecurity.com
info@objectsecurity.com

ObjectSecurity Ltd.
St John’s Innovation Centre
Cowley Road
Cambridge CB4 0WS
United Kingdom
Tel: +44 (0) 1223 420252
Fax: +44 (0) 1223 420844
Terms & Conditions

© 2000-2014 ObjectSecurity Ltd. All rights reserved.

This entire document is copyright protected and may not be published in any form in other works without expressly written permission from ObjectSecurity. This document contains commercially protected information, including patents and patent applications. Any distribution or exploitation without permission will be considered infringement.

No re-selling permitted without prior explicit permission. No patenting of any of any of the described aspects permitted.

Intellectual property: This document describes internals of OpenPMF, which are the intellectual property of ObjectSecurity, for which patents are granted and pending. ObjectSecurity is the inventor of several of the described concepts, and any exploitation of these without permission will be considered as infringement of ObjectSecurity’s legal rights.

Copyright, author rights, trademarks and other intellectual property rights: Some names are protected by trademarks which are the property of ObjectSecurity or other third parties whether a specific mention in that respect is made or not. In particular (but not limited to): The ObjectSecurity logo, ObjectSecurity, the OpenPMF logo, OpenPMF, the ObjectWall logo, ObjectWall, TrustWall, the TrustWall logo, SecureMDA, the SecureMDA logo, TrustedSOA, the TrustedSOA logo, SecureMiddleware, the SecureMiddleware logo, Security Management Ecosystem, SimulateWorld, and the SimulateWorld logo are trademarks or registered trademarks of ObjectSecurity.

This document and its contents are protected by copyright, author rights and/or other intellectual property rights which are the property of OBJECTSECURITY or third parties. Reproduction and use of the materials (or any information incorporated thereto such as but not limited to articles, graphical images, pictures, diagrams, video materials…) published in this document are hereby authorized provided that:

(a) reproduction and use are solely for informational and non commercial use within your organisation in support of your better knowledge of Model Driven Security; and
(b) any reproduction retains all original notices including proprietary or copyright notices; and
(c) materials are not modified, in whole or in part, in any way whatsoever.

No other use of the materials and of any information incorporated thereto is hereby authorized.

All concepts described may be protected by one or more patents or pending applications.

No part of this document may be reproduced in any form by any means without prior written authorisation of ObjectSecurity

Disclaimers
This document is provided for general information only and should not be relied upon or used as the basis for making any transactions of any kind whatsoever.

All the information and any part thereof provided in this document are provided « AS IS » without warranty of any kind either expressed or implied including, without limitation, warranties of merchantability, fitness for a particular purpose or non infringement of intellectual property rights.

OBJECTSECURITY makes no representations or warranties as to the accuracy or completeness of any materials and information incorporated thereto and contained in this document.

OBJECTSECURITY makes no representations or warranties that this document will be free of harmful components.

The use of the materials (or any information incorporated thereto), in whole or in part, contained in this document is your sole responsibility. OBJECTSECURITY disclaims any liability for any damages whatsoever including without limitation direct, indirect, incidental and/or consequential damages resulting from access to the document and use of the materials provided therein.

This document may contain links to third party sites. The links are provided to you only as a convenience and the inclusion of any link does not imply neither an endorsement by OBJECTSECURITY of the linked sites nor any warranty from OBJECTSECURITY on said sites. Access to said linked sites is at your own risk.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS.