Growing regulatory requirements for accounting and assurance

Improved security (consistency, correctness)

ObjectSecurity OpenPMF 2.0

Existing Technology:
- Increased usability (flexibility, intuitiveness etc.)
- Low-maintenance security management for agile systems (e.g. SOA)
- Simplifies security policy (e.g. authorization) management in complex, heterogeneous, connected IT environments

Why use it? Core Benefits
- Hard to define and maintain consistent policy
- Hard to provide evidence for correctness
- Hard to show that every aspect has been covered by policy
- Hard to enforce policy consistently
- Hard to provide level of assurance due to lack of "holistic" understanding of system and security policy

Problem definition

- Unmanageable IT infrastructure creates security problems
- Increasing complexity of IT, e.g.
  - Growing, interconnected distributed systems (also between organizations)
  - Growing legacy infrastructure
  - Growing reliability on IT
  - Growing user requirements (data fusion, information at your fingertips, ...)
  - Growing regulatory requirements for accounting and assurance

- Point-to-point ad-hoc system integration becomes unmanageable with size
- Software reuse hindered by legacy and incompatible technologies
- Software engineering is extremely complex because of many "moving targets"
- Correctness of system cannot be assured due to complexity and lack of "holistic" understanding
- Hardware complexity...
- IT staff are overwhelmed with complexity
- Both for security and software in general

ObjectSecurity Ltd.

Security policy management + secure information sharing in complex, heterogeneous, networked environments

- Products & services/consulting/training/endorsements
- Technology/patents/expertise
- Strong security requirements because of information sharing in distributed systems (e.g. when cross-organization)
- Hard to define and maintain consistent policy
- Hard to provide evidence for correctness
- Hard to show that every aspect has been covered by policy
- Hard to enforce policy consistently
- Hard to provide level of assurance due to lack of "holistic" understanding of system and security policy

Problem definition (2)

Security complexity causes human errors & vulnerabilities:
- No idea what policy is enforced because of many underlying security technologies (conflicts, omissions etc.)
- Access policy management and enforcement complex because many different techniques and systems
- User management in incompatible, large, distributed systems is a challenge (= single sign-on helps somewhat)
- Strong security requirements because of information sharing in distributed systems (e.g. when cross-organization)
- Hard to define and maintain consistent policy
- Hard to define and maintain correct policy
- Hard to provide evidence for correctness
- Hard to show that every aspect has been covered by policy
- Hard to enforce policy consistently
- Hard to provide level of assurance due to lack of "holistic" understanding of system and security policy

ObjectSecurity’s definition, see:
www.modeldrivensecurity.org

“Model driven security (MDS) is the tool supported process of modeling security requirements at a high level of abstraction, and using other information sources available about the system (produced by other stakeholders). These inputs, which are expressed in Domain Specific Languages (DSL), are then transformed into enforceable security rules with as little human intervention as possible. MDS explicitly also includes the run-time enforcement of the policy on the protected IT systems, dynamic policy updates and the monitoring of policy violations.” – ObjectSecurity, OpenPMF 2.0 vendor
Simplified security management for a connected world™

Object Security

Services

Studies/papers, training courses, workshops, R&D, design, roadmap consulting, build assurance systems, technical support

Unique expertise:

• SOA security
• Security management for agile SOA
• Selection of security portfolio
• Model driven security
• World leader in the emerging field, 5 years of experience
• Authorization management (entitlement management)
• Also a world leader, 9 yrs of experience
• Middleware security
• SOA, Web services, J2EE, DDS, CORBA/COM etc.
• Secure information sharing infrastructure
• Sector specific expertise ATM, IAB, HS, ITS etc.
• Application layer firewalls

Ensure low maintenance, maximum flexibility, appropriate security

info@objectsecurity.com
www.objectsecurity.com

Summary

Model Driven Security

Object Security OpenPMF 2.0

What is it? Why buy it?

OpenPMF 2.0 Overview

Object Security OpenPMF 2.0

• Security policy auto-generation within the Model Driven Architecture (MDA) software development process

OpenPMF 2.0 TrustedSOA™

• Low-maintenance security management for agile (e.g. SOA) environments

OpenPMF 2.0 Benefits

• Most flexible, transparent control policies, low maintenance, model driven security management
• Most cost-effective open-source solution
• Most flexible policy management for agile (e.g. SOA) environments
• OpenPMF 2.0 uses existing compliance and regulatory tools
• Increased security (detectability, maintainability, etc.)

Existing Applications

• MDA (OpenPMF 2.0: -th generation model driven open-source security technology)

Opportunities for companies

• Improve security
• Manage security with an MDA environment
• Ubiquitous management model
• Personal approach to OA security management

Terms & Conditions