Object™ Security
The Security Policy Company

Model Driven Security

Protection of Resources in Complex Distributed Systems

Ulrich Lang, Rudolf Schreiner
ObjectSecurity Ltd.
University of Cambridge

Agenda

- COACH Project
- Model Driven Architecture
- Model Driven Security
  - Architecture
  - Policy Definition Language
  - Policy Repository
  - Policy Evaluation and Enforcement
  - Target Platform: CCM as example
- Conclusion

COACH Project

- Large IST research project partially funded by the European Commission
- Goal: Development of two complete CCM tool chains for mission critical applications
- Focus:Telecom, air traffic control

- Special consideration: Security

COACH Project Participants

T · · Systems ·

CNRS USTL LIFL

HUMBOLDT-UNIVERSITÄT ZU BERLIN

Object Security

THALES

Fraunhofer Institute for Open Communication Systems

LIP6 UNIVERSITÉ PIERRE & MARIE CURIE

INTRACOM

Lucent Technologies
Bell Labs Innovations

Model Driven Security

COACH Project

- Revision and extension of the CCM specification
  - Separation of container and services
  - Streaming, quality-of-service
- Contribution to various OMG specifications:
  - Deployment
  - Modeling (MOF2IDL, UML Model for CCM, UML Model for QoS)
  - Security

COACH Goals

- Implementation of CCM tool chains:
  - Qedo (C++)
  - OpenCCM
- Implementation of security framework
- Integration with state of the art modeling techniques: UML, MDA
- All software will be release as Open Source
- More info: www.ist-coach.org

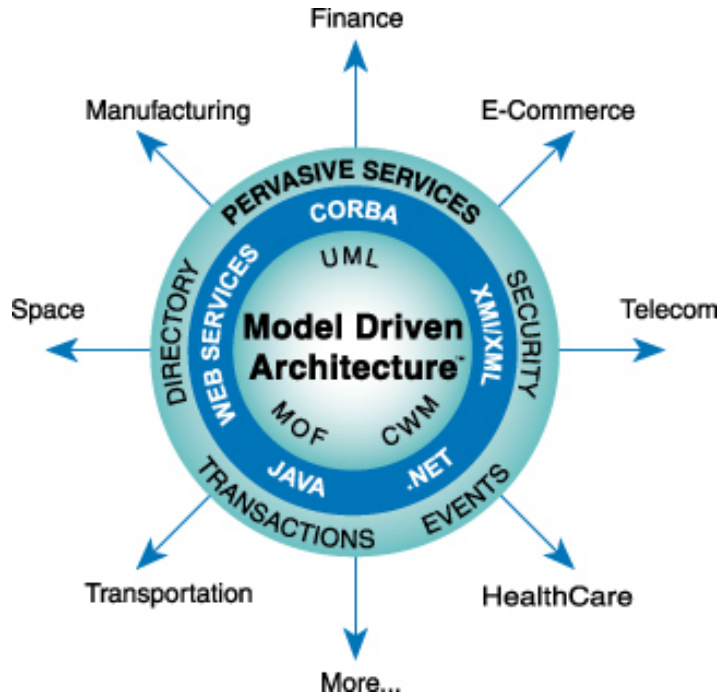
Model Driven Security

Why CCM?

- Motivation of COACH:
  - CORBA is a solid and proven base for mission critical systems
  - For tightly coupled systems no alternatives:
    - Web Services/.NET not suitable
    - EJB fine for simpler systems, and interoperates well with CCM
  - CCM adds required functionality for large scale applications and state-of-the-art software development: From objects to components
  - But there's still some work to do: COACH

Model Driven Architecture (MDA)

- Architecture for software development
- Platform-Independent Model (PIM)
  - Unified Modelling Language (UML) used to model systems
  - Stored in Meta Object Facility (MOF) repository
  - Exchanged via XML Metadata Interchange (XMI)

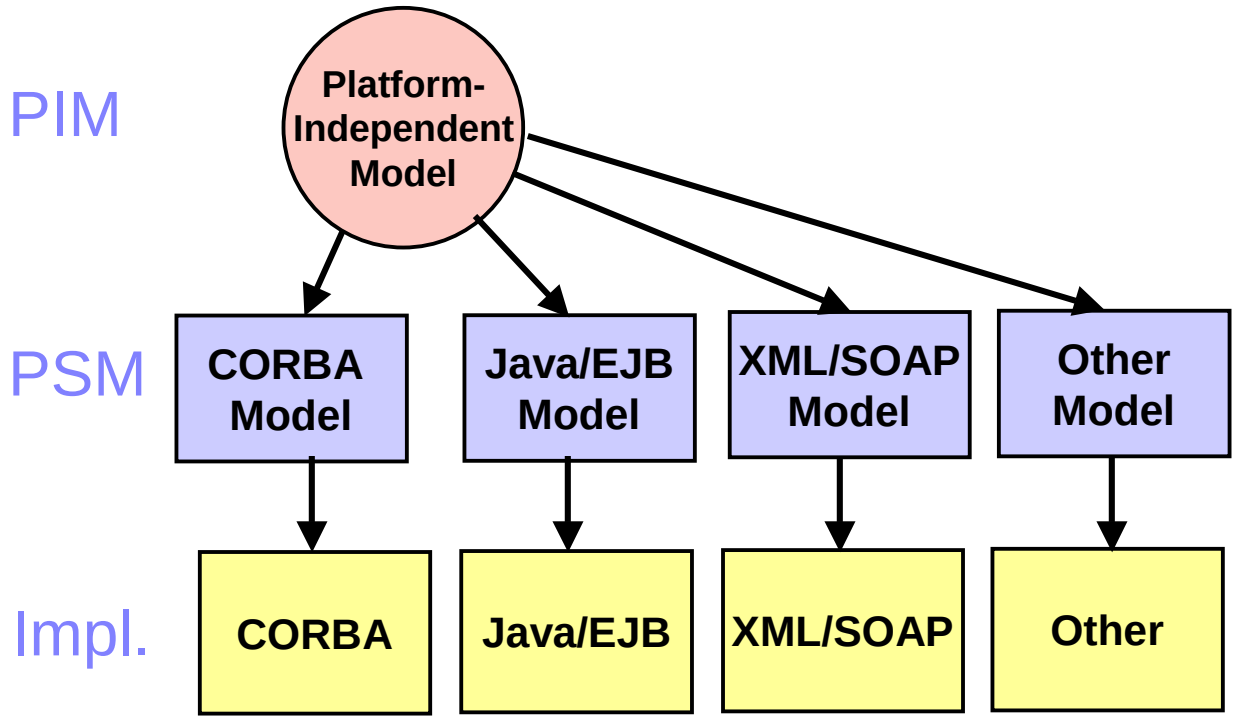


Model Driven Security

Model Driven Architecture (MDA)

- Platform-Specific Model (PSM)
  - Standard mapping from PIM to (multiple) deployment technologies
    - E.g. models for CCM/CORBA, Java/EJB, XML/SOAP
  - Partially generated by MDA tool, partially hand-written
- Implementation (partially or fully) generated by MDA tool

Model Driven Architecture (MDA)



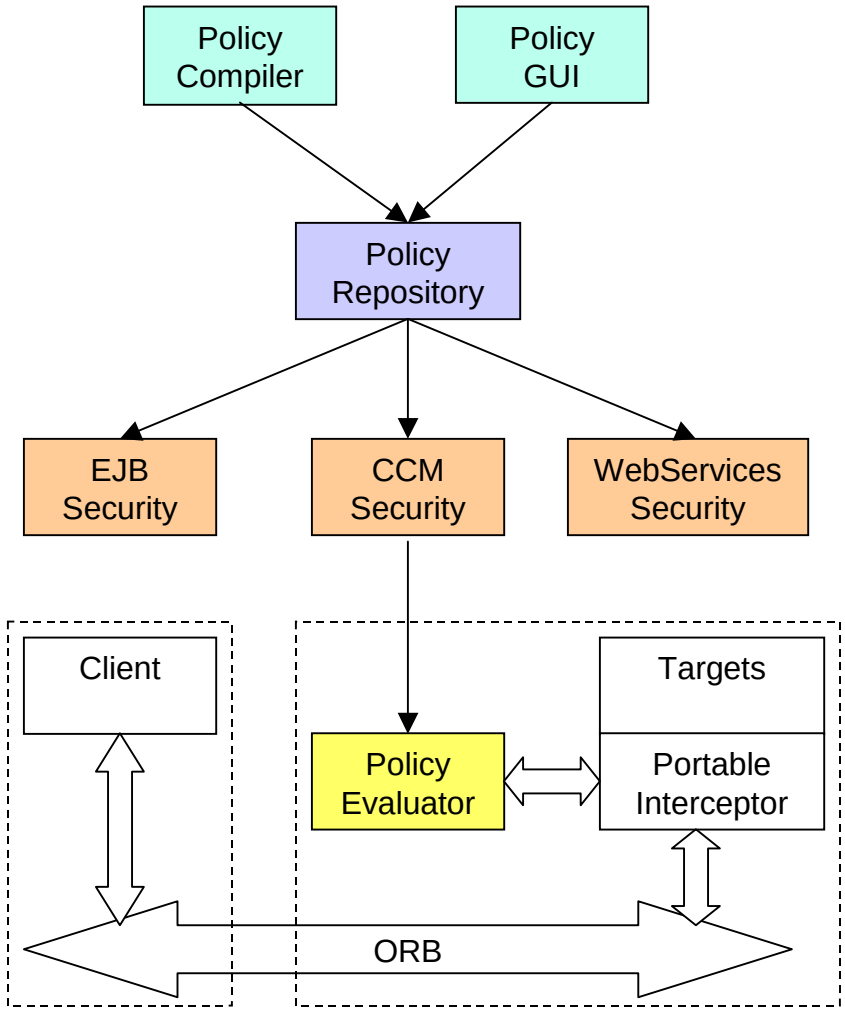
Model Driven Architecture (MDA)

- Main goal is PIM reuse:
  - If the system should be mapped to another technology (the “next best thing”)
- Legacy integration: MDA tool can reverse-engineer existing application into a model
- Bridge generation: MDA tool can bridge different technologies that have a common PIM

Model Driven Security (MDS)

- Apply the same approach to security
  - Describe technology-independent security policy
    - Stored in Policy Repository (MOF)
    - Can express different security models
      - e.g. DAC, MAC, RBAC
  - Map to particular technologies and security mechanisms
    - e.g. CORBASec, CCM security, EJB security, firewalls

MDS Architectural Overview



Generate Policy

Generate Policy Evaluators

Exemplary CCM Integration of Evaluation and Enforcement

Model Driven Security

Policy Definition Language

- Abstract language to describe security policies independent of platforms and security mechanisms
- Inspired by Ponder, but based on *Principal Calculus* (Abadi et alt.)
- PDL supports:
  - Delegation
  - Roles and groups
  - Constraints (Based on OCL)

Policy Repository

- Stores the enterprise security policy
  - Consistent
  - Centralized
  - Optimized
  - Security mechanism independent
  - Automatic mapping to different technologies
  - Can be mapped to future technologies

Model Driven Security

Policy Repository

- Based on Meta Object Facilities (MOF)
  - UML model for security
  - A meta-policy describes how the policy is described
  - Inherit all advantages of MOF:
    - Automatic generation of repository
    - XMI exchange format
- Security Model independent
  - Storage of the logical structure of the policy
  - Supports DAC, RBAC, MAC,…

Policy Evaluation

- Runtime evaluators make decisions based on abstract attributes
- Simple interpreter for security rules
- Policy loaded from repository
- Independent of:
  - Platform: CCM, EJB,…
  - Security mechanisms
- Language specific

Policy Enforcement

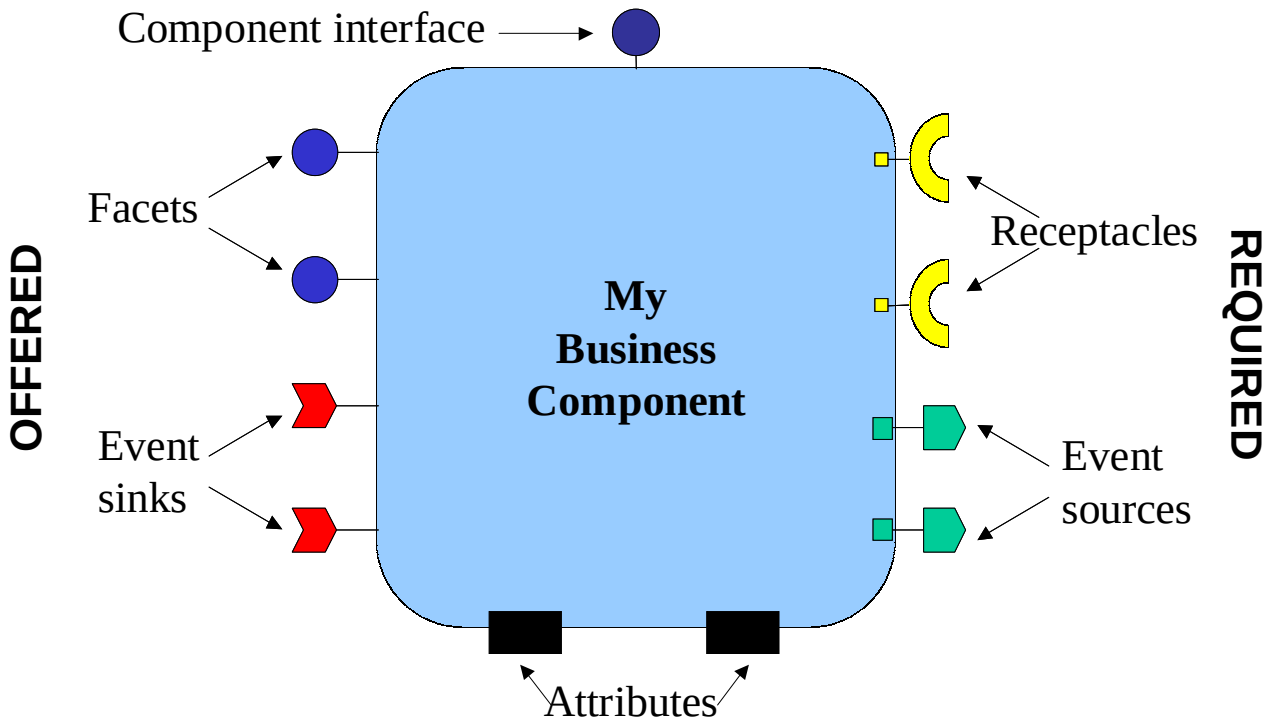
- Integration into call chain platform specific:
  - CCM&CORBA: Portable Interceptors
- Calls policy evaluator which uses:
- Transformers to obtain attributes
  - Translate platform specific identifiers
  - Translate security mechanism identifiers
  - Apply mapping, e.g. identity2role
  - Allow easy integration of security mechanisms

Infrastructure Integration

- The MDS framework integrates:
  - Public Key Infrastructure (implemented by T-Systems)
  - Privilege Management Infrastructure
    - ATLAS for generation of authorization tokens
  - Directory Services for storing user data
- In the future:
  - Domain boundary controllers
  - Distributed intrusion detection

CORBA Component Model

- Component model
  - Interconnections: 4 kinds of interfaces (ports)
  - “Homes”: instance managers (factory & finder)



CORBA Component Model

- Programming model
  - *Component Implementation Definition Language (CIDL) & Framework (CIF)*
    - implementation structure of a component and its (non-functional) system requirements
  - Generates skeleton & XML descriptor
  - Dynamic Introspection

CORBA Component Model

- Deployment model
  - ZIP archives contain component descriptors and implementations
  - Allows architects to easily install an application on various sites

Model Driven Security

CORBA Component Model

- Execution model
  - Container
    - Runtime environment for component instances and their homes
    - Hides complexity, manages services, i.e. no explicit programming of non-functional properties necessary
      - ORB, POA, security, transaction, persistence, notification

CCM Mapping

- An integration simply using Portable Interceptors is possible, but not optimal
- COACH partners are defining a *flexible container* to integrate various services:
  - Minimum container
  - Well defined interfaces for service integration:
    - Context interfaces
    - Interception points
  - Specific security requirements taken into account, e.g. target descriptors
- Secure deployment

CSIv2

- Most standard security mechanisms do not support advanced functionality:
  - Delegation
  - Token transfer
- To address this problem in the CORBA world CSIv2 was developed
- CSIv2 and the upcoming API are based on Principal Calculus
- Common formal model from line level protocol to access control

Model Driven Security

MDS Benefits

- Integration of security policy and business model
- Formally sound security model from abstract policy to line level protocol
- Flexibility & consistency of security policies
- Integrated validation
- Technology independent:
  - Integration of security policies across technologies (“enterprise-wide security policy”)
  - Easy integration of new security technologies

Model Driven Security

Conclusion

- MDA approach can be successfully applied to security
- Model Driven Security integrates business and security models
- The effort for the development of complex secure applications is reduced

Object-Security

Model Driven Security

Object™ Security

The Security Policy Company

www.objectsecurity.com

info@objectsecurity.com