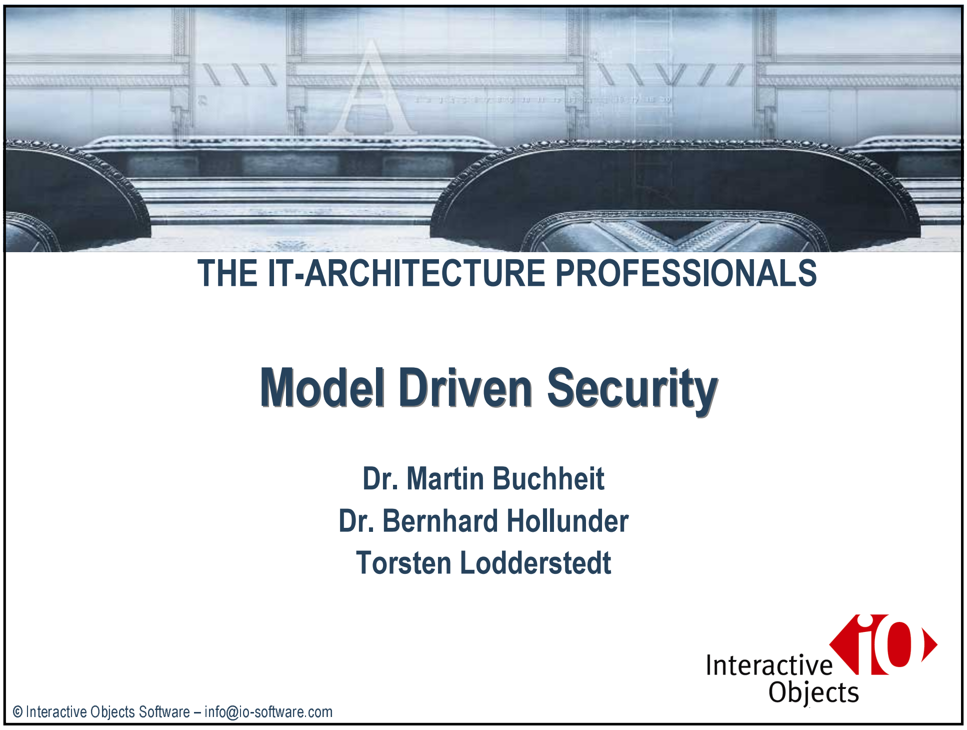
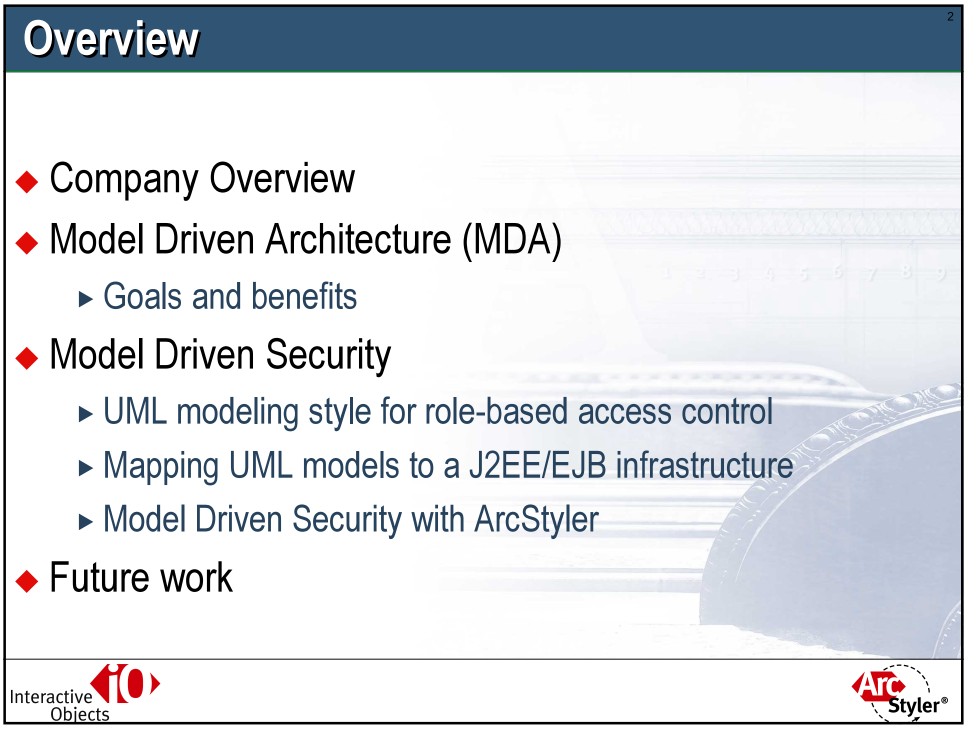


THE IT-ARCHITECTURE PROFESSIONALS

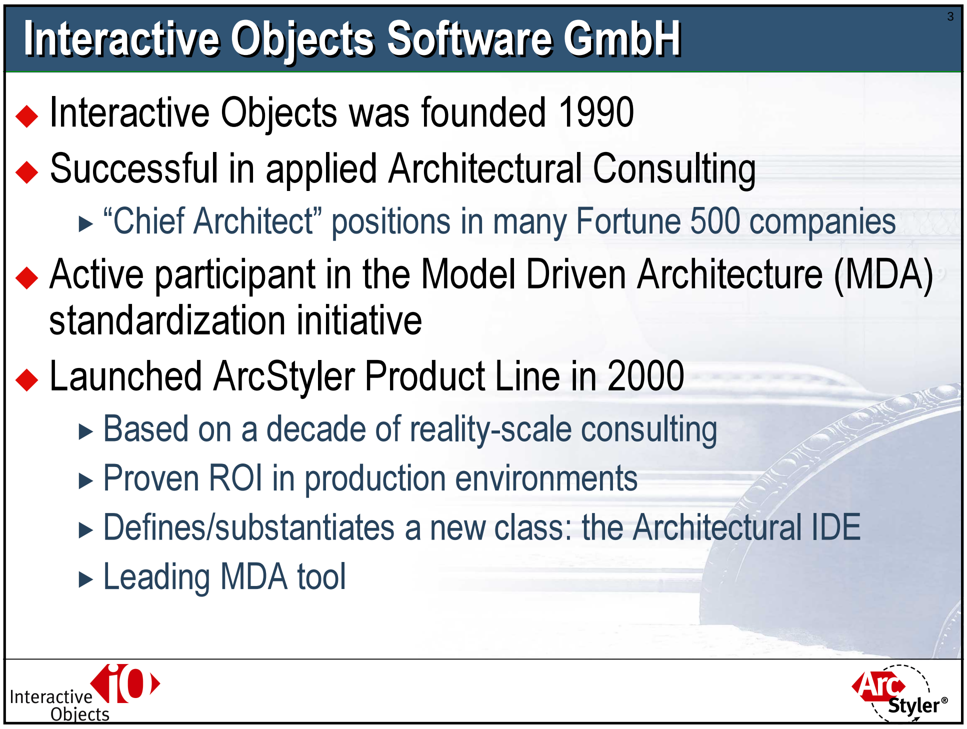
Model Driven Security

Dr. Martin Buchheit
Dr. Bernhard Hollunder
Torsten Lodderstedt



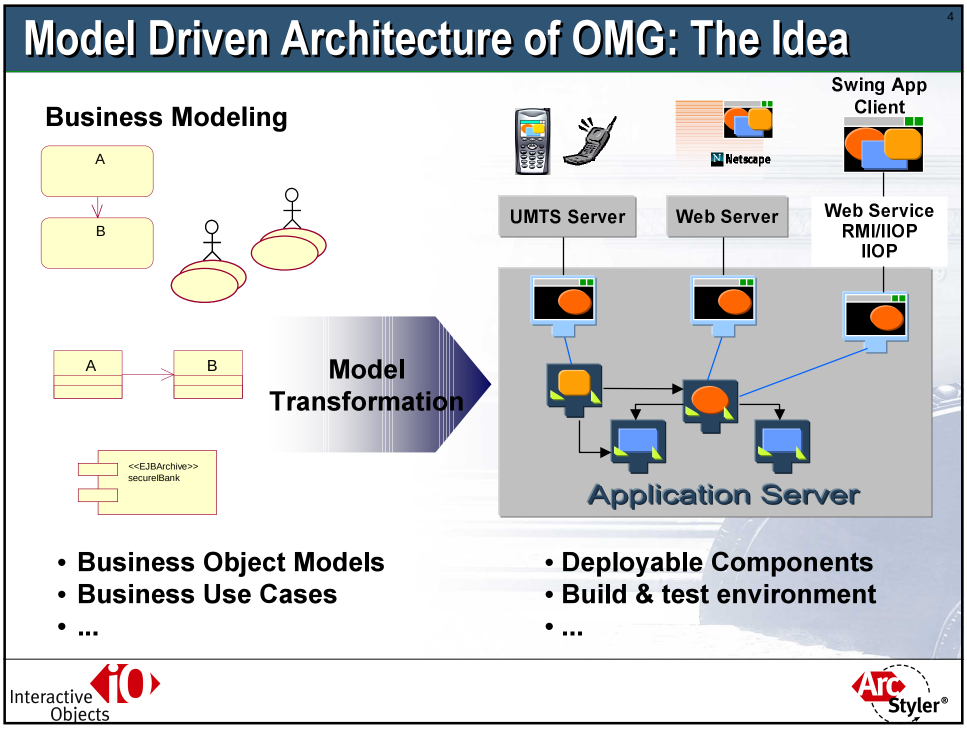
Overview

- Company Overview
- Model Driven Architecture (MDA)
  - Goals and benefits
- Model Driven Security
  - UML modeling style for role-based access control
  - Mapping UML models to a J2EE/EJB infrastructure
  - Model Driven Security with ArcStyler
- Future work



Interactive Objects Software GmbH

- Interactive Objects was founded 1990
- Successful in applied Architectural Consulting
  - “Chief Architect” positions in many Fortune 500 companies
- Active participant in the Model Driven Architecture (MDA) standardization initiative
- Launched ArcStyler Product Line in 2000
  - Based on a decade of reality-scale consulting
  - Proven ROI in production environments
  - Defines/substantiates a new class: the Architectural IDE
  - Leading MDA tool



Model Driven Architecture of OMG: The Idea

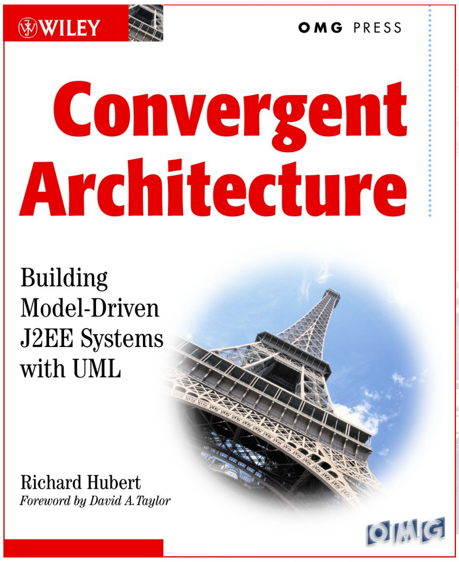
- Business Object Models
- Business Use Cases
- ...

- Deployable Components
- Build & test environment
- ...

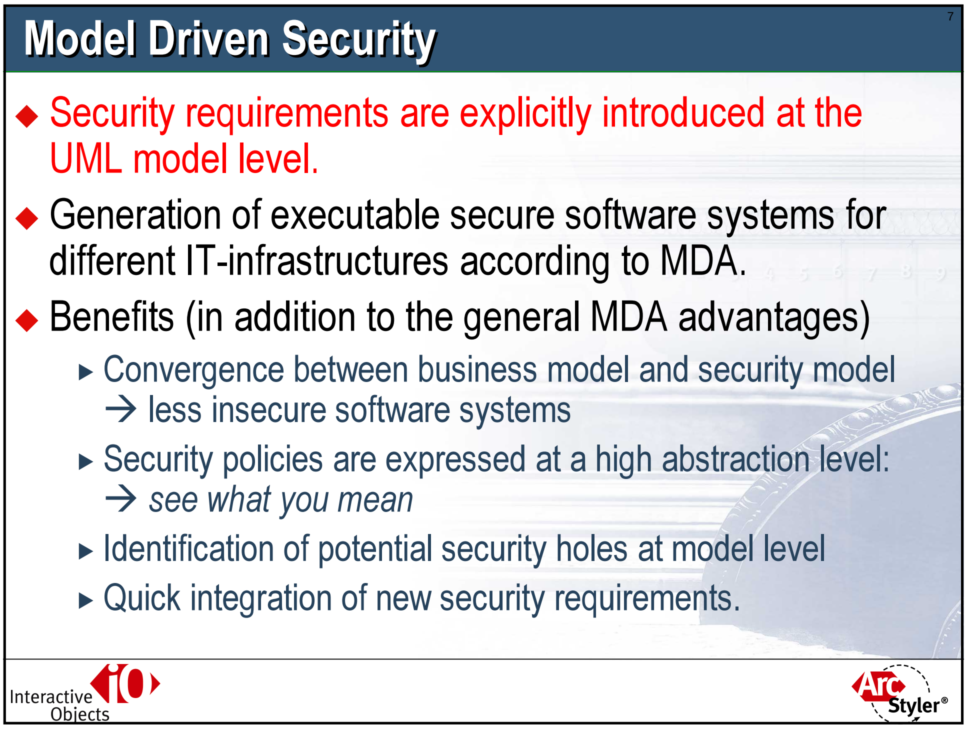
Model Driven Architecture: www.omg.org/mda

- Design goals
  - addresses the complete life cycle of designing, implementing, integrating, testing, deploying, and managing applications
  - separates the fundamental logic behind a specification from the specifics of the particular middleware that implements it
  - built on well-established standards such as Unified Modeling Language (UML) and XML Metadata Interchange (XMI).
- Main benefits
  - reduced cost and complexity of application development
  - improved application quality and validation at model level
  - reuse of business models
  - plattform independence
  - rapid inclusion of emerging technologies

For Details See ...


WILEY
OMG PRESS
Convergent Architecture
Building Model-Driven J2EE Systems with UML
Richard Hubert
Foreword by David A. Taylor
OMG

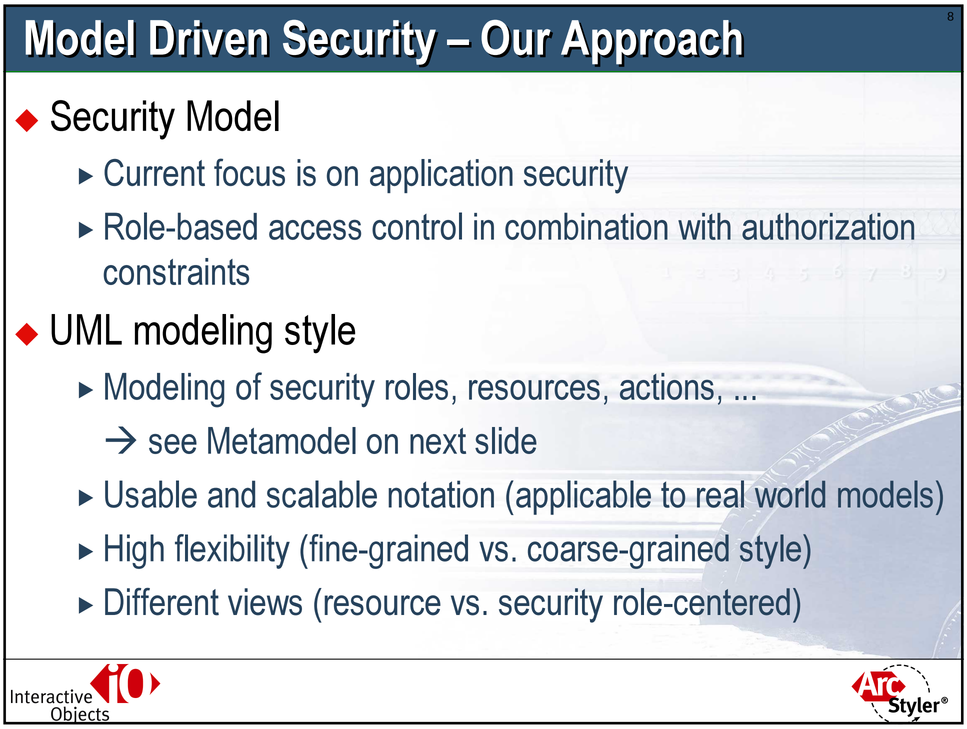
(J. Wiley, New York, 2002, ISBN 0-471-10560-0)



Model Driven Security

7

- Security requirements are explicitly introduced at the UML model level.
- Generation of executable secure software systems for different IT-infrastructures according to MDA.
- Benefits (in addition to the general MDA advantages)
  - Convergence between business model and security model → less insecure software systems
  - Security policies are expressed at a high abstraction level: → *see what you mean*
  - Identification of potential security holes at model level
  - Quick integration of new security requirements.

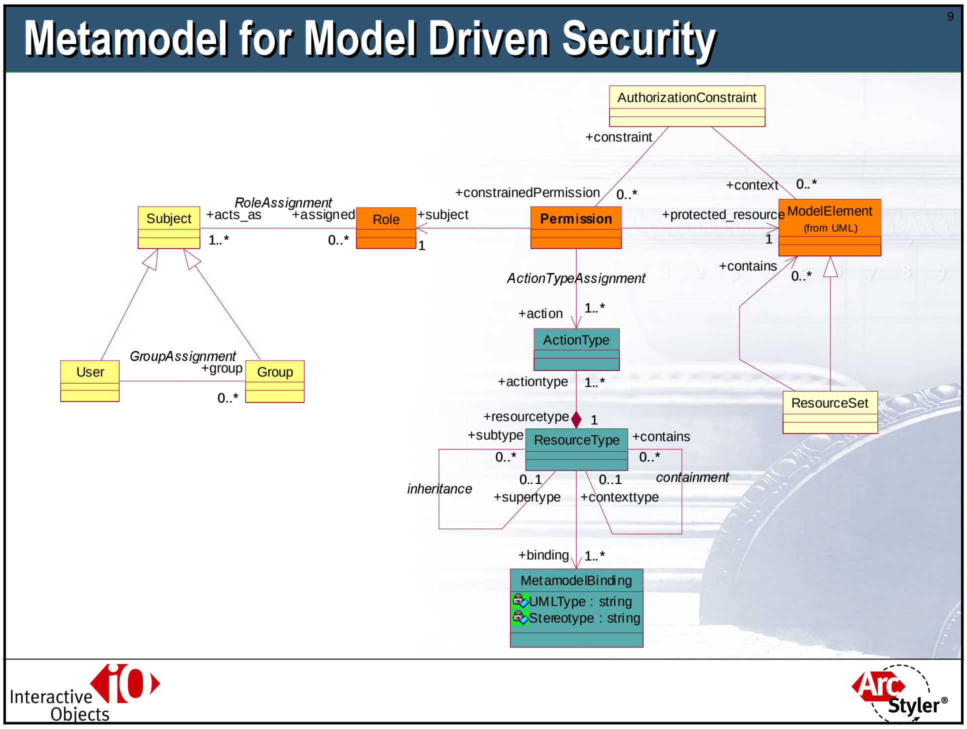


Model Driven Security – Our Approach

8

- Security Model
  - Current focus is on application security
  - Role-based access control in combination with authorization constraints
- UML modeling style
  - Modeling of security roles, resources, actions, ...

    → see Metamodel on next slide
  - Usable and scalable notation (applicable to real world models)
  - High flexibility (fine-grained vs. coarse-grained style)
  - Different views (resource vs. security role-centered)



Metamodel for Model Driven Security

AuthorizationConstraint

+constraint

+constrainedPermission 0..*

+context 0..*

Subject +acts_as *RoleAssignment* +assigned Role +subject Permission +protected_resource ModelElement (from UML)

1..* 0..* 1 1

ActionTypeAssignment +contains 0..*

+action 1..*

ActionType

+actiontype 1..*

User *GroupAssignment* +group Group 0..*

ResourceSet

+resourcetype 1

+subtype ResourceType +contains

0..* 0..*

inheritance 0..1 0..1 *containment*

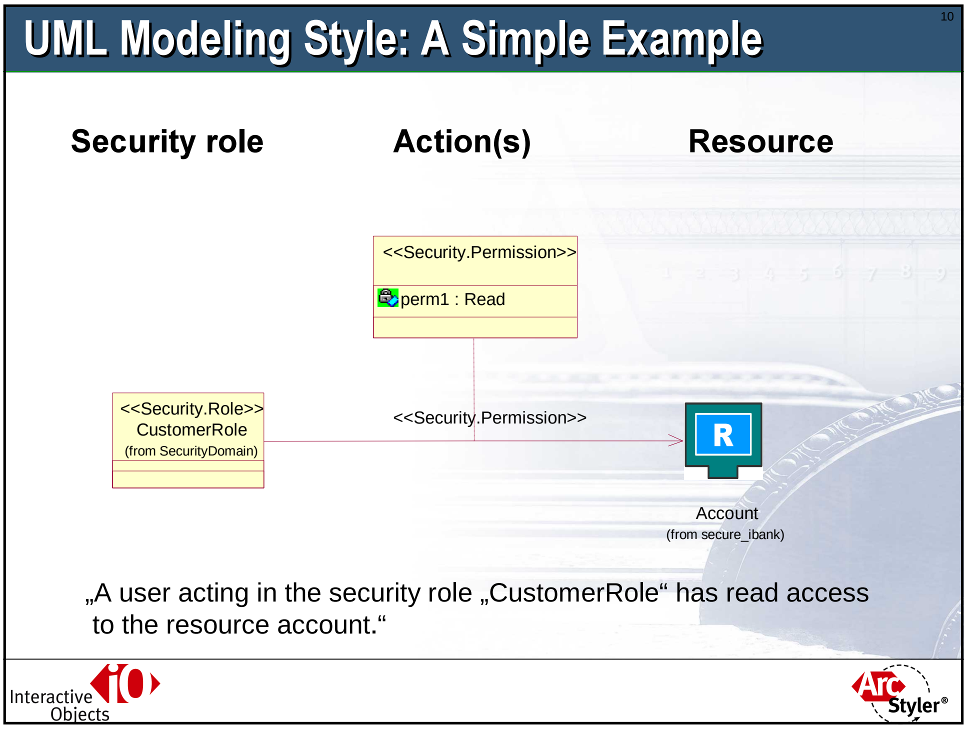
+supertype +contexttype

+binding 1..*

MetamodelBinding

UMLType : string

Stereotype : string



UML Modeling Style: A Simple Example

Security role **Action(s)** **Resource**

<<Security.Permission>>

perm1 : Read

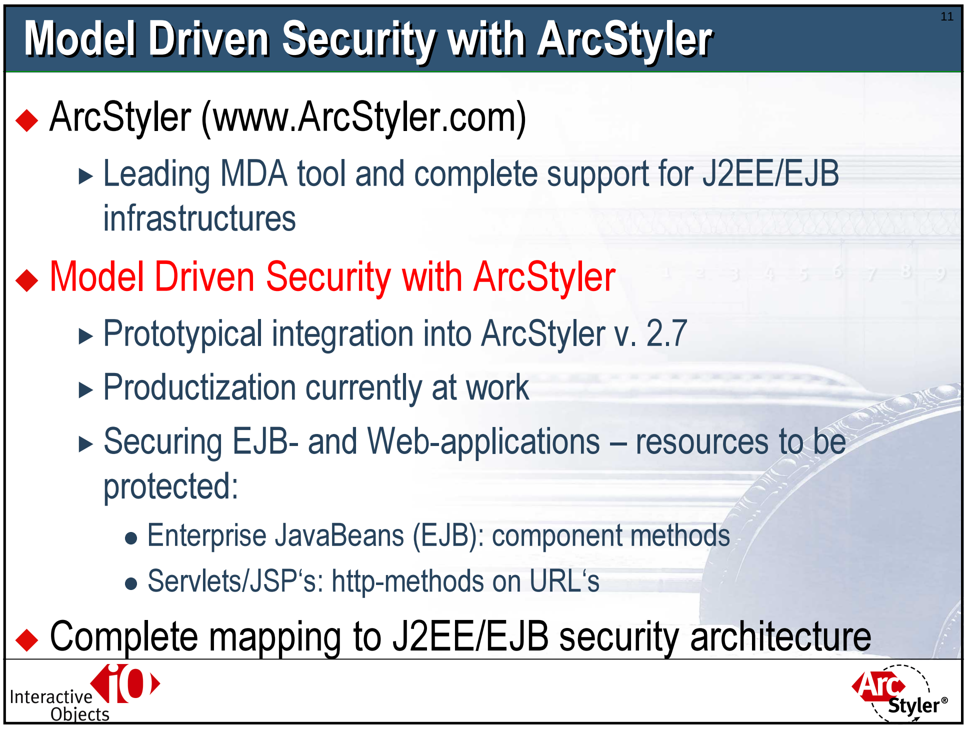
<<Security.Role>>
CustomerRole
(from SecurityDomain)

<<Security.Permission>>

R

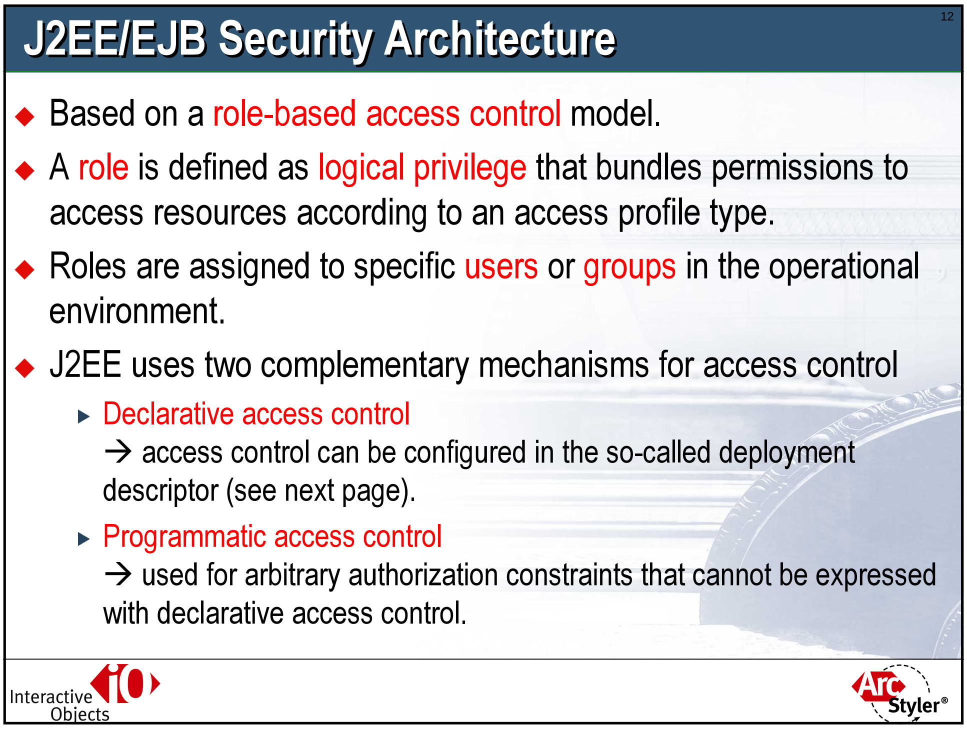
Account
(from secure_ibank)

„A user acting in the security role „CustomerRole“ has read access to the resource account.“



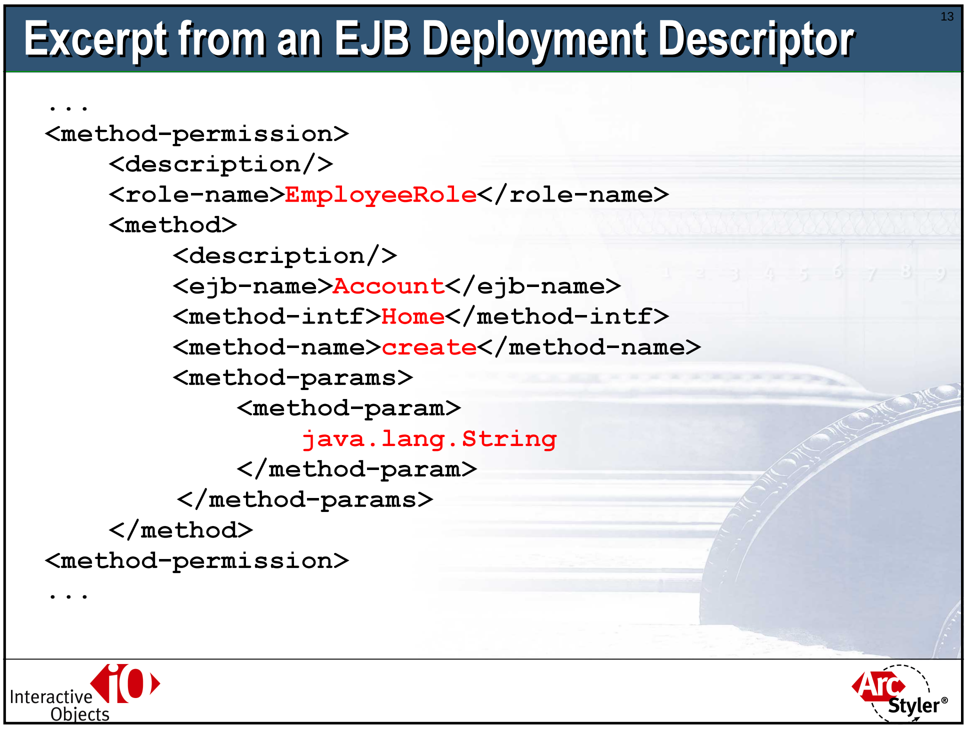
Model Driven Security with ArcStyler

- ArcStyler (www.ArcStyler.com)
  - Leading MDA tool and complete support for J2EE/EJB infrastructures
- Model Driven Security with ArcStyler
  - Prototypical integration into ArcStyler v. 2.7
  - Productization currently at work
  - Securing EJB- and Web-applications – resources to be protected:
    - Enterprise JavaBeans (EJB): component methods
    - Servlets/JSP's: http-methods on URL's
- Complete mapping to J2EE/EJB security architecture



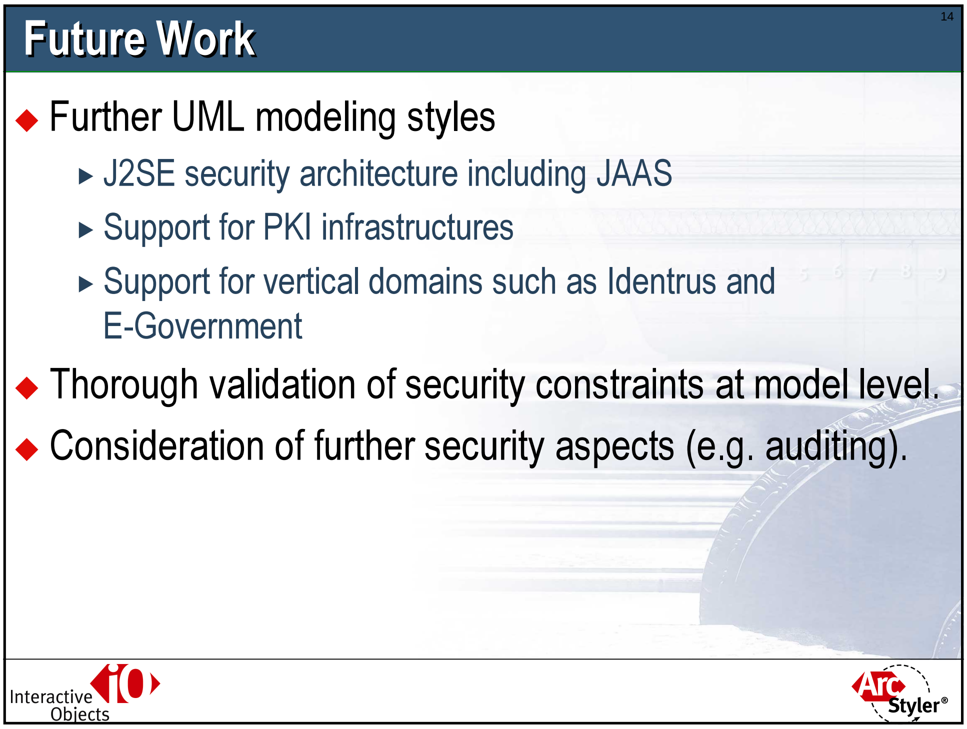
J2EE/EJB Security Architecture

- Based on a role-based access control model.
- A role is defined as logical privilege that bundles permissions to access resources according to an access profile type.
- Roles are assigned to specific users or groups in the operational environment.
- J2EE uses two complementary mechanisms for access control
  - Declarative access control
    → access control can be configured in the so-called deployment descriptor (see next page).
  - Programmatic access control
    → used for arbitrary authorization constraints that cannot be expressed with declarative access control.



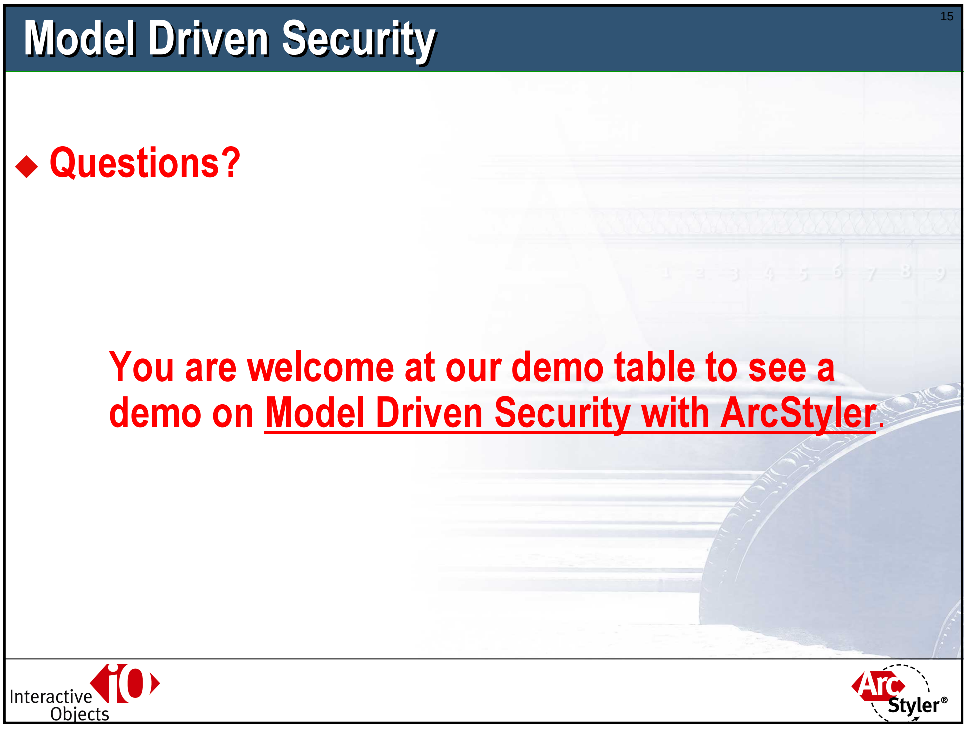
Excerpt from an EJB Deployment Descriptor

```
...
<method-permission>
    <description/>
    <role-name>EmployeeRole</role-name>
    <method>
        <description/>
        <ejb-name>Account</ejb-name>
        <method-intf>Home</method-intf>
        <method-name>create</method-name>
        <method-params>
            <method-param>
                java.lang.String
            </method-param>
        </method-params>
    </method>
<method-permission>
...
```



Future Work

- Further UML modeling styles
  - J2SE security architecture including JAAS
  - Support for PKI infrastructures
  - Support for vertical domains such as Identrus and E-Government
- Thorough validation of security constraints at model level.
- Consideration of further security aspects (e.g. auditing).

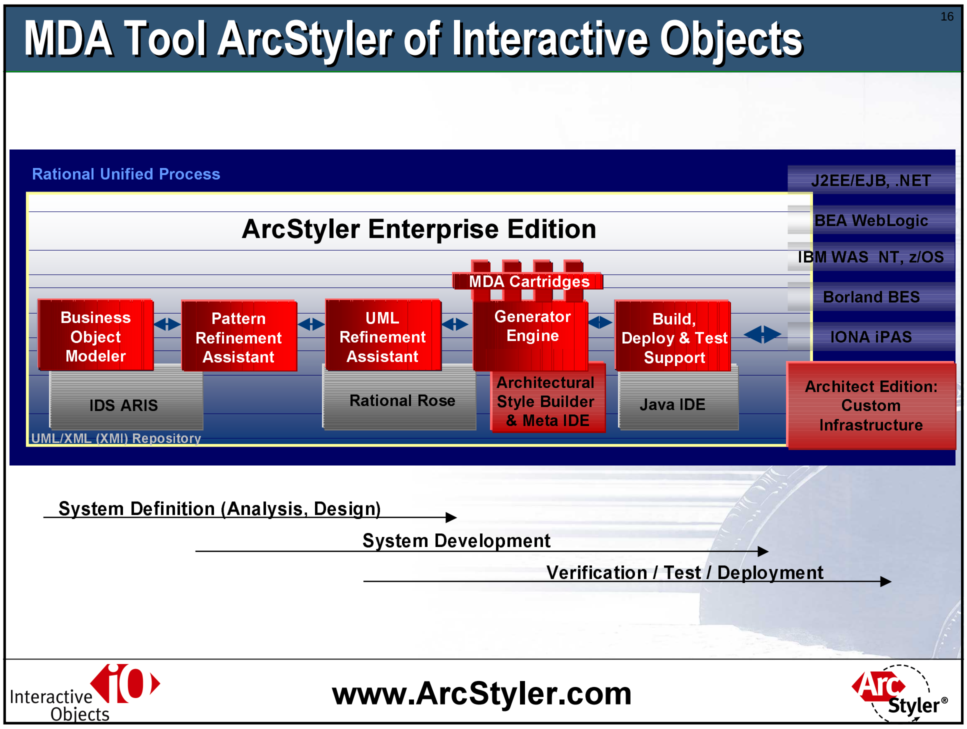


15

Model Driven Security

- Questions?

You are welcome at our demo table to see a demo on Model Driven Security with ArcStyler.



16

MDA Tool ArcStyler of Interactive Objects

Rational Unified Process

ArcStyler Enterprise Edition

MDA Cartridges

Business Object Modeler

Pattern Refinement Assistant

UML Refinement Assistant

Generator Engine

Build, Deploy & Test Support

IDS ARIS

Rational Rose

Architectural Style Builder & Meta IDE

Java IDE

UML/XML (XMI) Repository

J2EE/EJB, .NET

BEA WebLogic

IBM WAS NT, z/OS

Borland BES

IONA iPAS

Architect Edition: Custom Infrastructure

System Definition (Analysis, Design)

System Development

Verification / Test / Deployment

www.ArcStyler.com