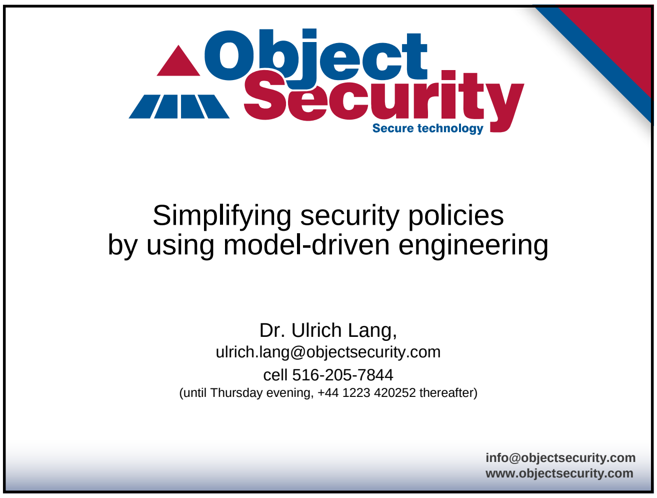
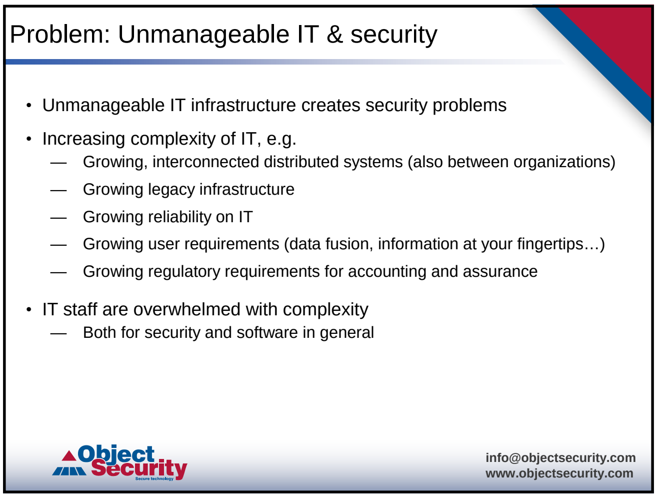


Simplifying security policies by using model-driven engineering

Dr. Ulrich Lang,
ulrich.lang@objectsecurity.com
cell 516-205-7844
(until Thursday evening, +44 1223 420252 thereafter)

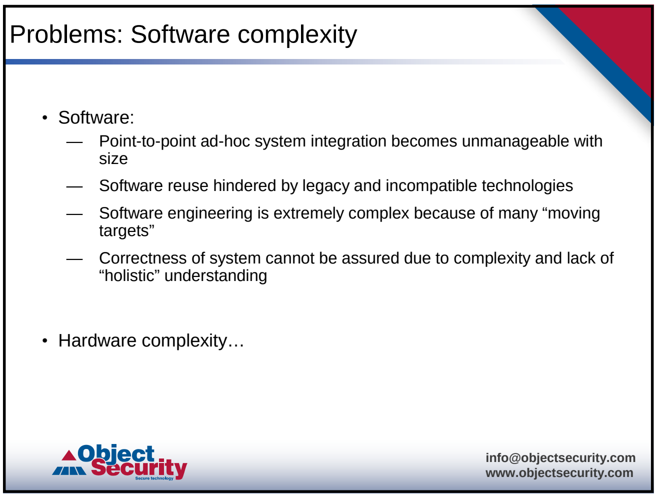
info@objectsecurity.com
www.objectsecurity.com



Problem: Unmanageable IT & security

- 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
- IT staff are overwhelmed with complexity
  - — Both for security and software in general

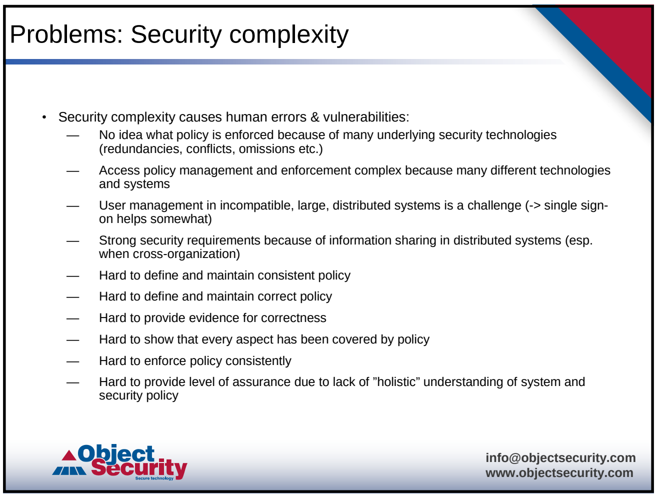
info@objectsecurity.com
www.objectsecurity.com



Problems: Software complexity

- Software:
  - — 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…

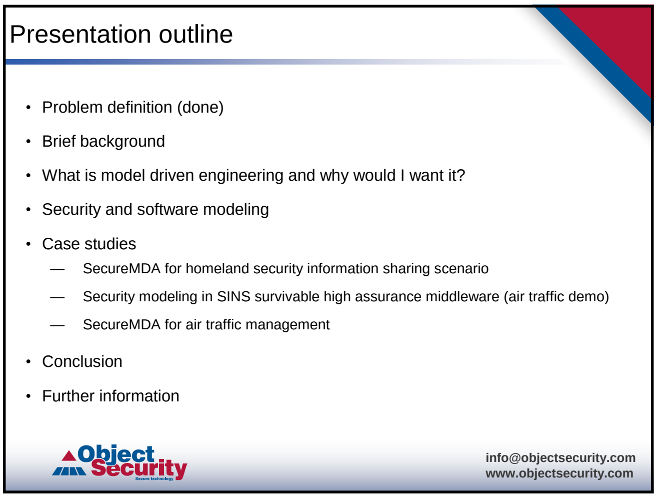
info@objectsecurity.com
www.objectsecurity.com



Problems: Security complexity

- Security complexity causes human errors & vulnerabilities:
  - — No idea what policy is enforced because of many underlying security technologies (redundancies, conflicts, omissions etc.)
  - — Access policy management and enforcement complex because many different technologies 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 (esp. 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

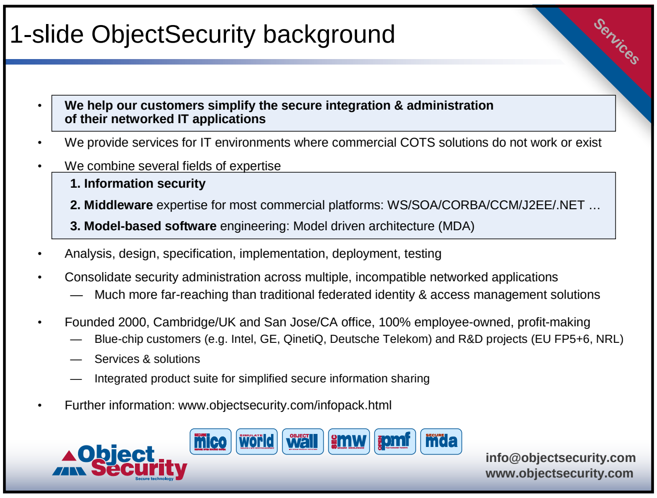
info@objectsecurity.com
www.objectsecurity.com



Presentation outline

- Problem definition (done)
- Brief background
- What is model driven engineering and why would I want it?
- Security and software modeling
- Case studies
  - — SecureMDA for homeland security information sharing scenario
  - — Security modeling in SINS survivable high assurance middleware (air traffic demo)
  - — SecureMDA for air traffic management
- Conclusion
- Further information

info@objectsecurity.com
www.objectsecurity.com



1-slide ObjectSecurity background

- **We help our customers simplify the secure integration & administration of their networked IT applications**
- We provide services for IT environments where commercial COTS solutions do not work or exist
- We combine several fields of expertise
  1. **Information security**
  2. **Middleware** expertise for most commercial platforms: WS/SOA/CORBA/CCM/J2EE/.NET …
  3. **Model-based software** engineering: Model driven architecture (MDA)
- Analysis, design, specification, implementation, deployment, testing
- Consolidate security administration across multiple, incompatible networked applications
  - — Much more far-reaching than traditional federated identity & access management solutions
- Founded 2000, Cambridge/UK and San Jose/CA office, 100% employee-owned, profit-making
  - — Blue-chip customers (e.g. Intel, GE, QinetiQ, Deutsche Telekom) and R&D projects (EU FP5+6, NRL)
  - — Services & solutions
  - — Integrated product suite for simplified secure information sharing
- Further information: www.objectsecurity.com/infopack.html

info@objectsecurity.com
www.objectsecurity.com

Model Driven Engineering Background

Model Driven Architecture

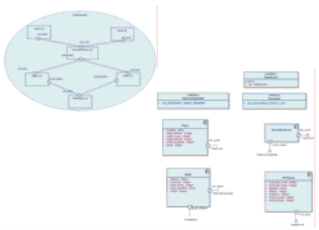
Software modeling helps

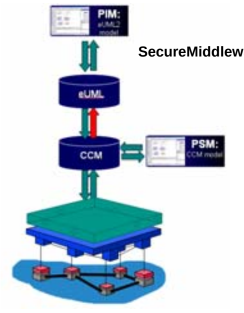
- Model-driven engineering
  - — Software design approach
  - — forward engineering, i.e. producing code from abstract, human-elaborated specifications
  - — Benefits:
    - Better understanding & assurance of software
    - Easier migration and reuse
  - — Various frameworks:
    - OMG Model Driven Archictecture (MDA)
    - Model Integrated Computing
    - Microsoft's DSL Tools

Focus on MDA because leading approach, case study, time constraints

How does MDA work?

- Platform independent model (PIM) in UML
- Generate platform specific model (PSM)
- Generate code
- Toolchain to help do this

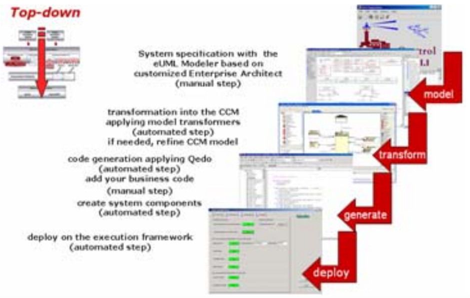




SecureMiddleware™

How does MDA work in practice?

- Toolchain automates much of the process (SecureMiddleware™)



System specification with the eUML Modeler based on customized Enterprise Architect (manual step)

transformation into the CCM applying model transformers (automated step)
if needed, refine CCM model

code generation applying Qedo (automated step)
add your business code (manual step)

create system components (automated step)

deploy on the execution framework (automated step)

Security Policy Modeling

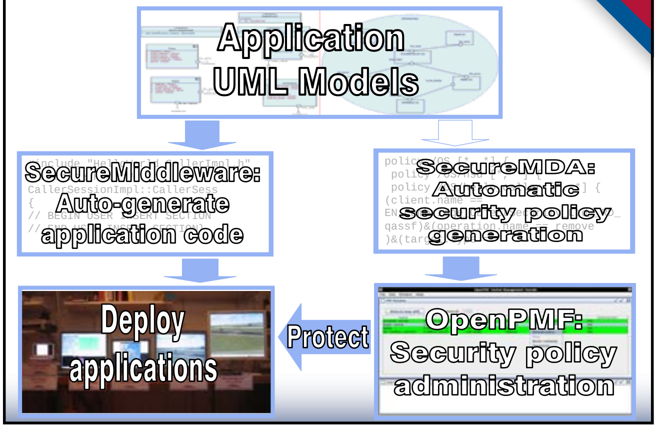
How to leverage the architecture to simplify security

Model driven security training workshops available:
www.objectsecurity.com/en-services-training.html

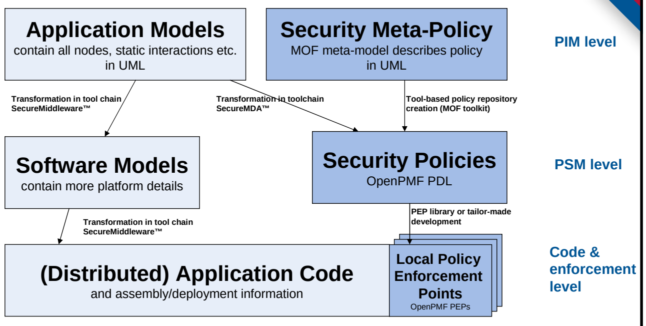
Modeling to simplify security

- Use modeling to also simplify security complexity
- Idea: Generate (most of the) security policies from application models
  - — Deny access except for interactions from the models
- Benefits:
  - — Frees up time & resources
  - — Improved security: Prevents human errors & security holes
  - — Easier to administer
  - — Allows policy reuse & migration together with models
  - — Improved security also because guarantee that entire environment is covered
  - — Easier to provide evidence for assurance
  - — Easier to show link between enterprise policy and enforcement

Basic SecureMDA concept


Application UML Models
SecureMiddleware: Auto-generate application code
SecureMDA: Automatic security policy generation
Deploy applications
Protect
OpenPMF: Security policy administration

Architecture: Software & security modeling


Application Models
contain all nodes, static interactions etc. in UML

Security Meta-Policy
MOF meta-model describes policy in UML

PIM level

Transformation in tool chain SecureMiddleware™

Transformation in toolchain SecureMDA™

Tool-based policy repository creation (MOF toolkit)

Software Models
contain more platform details

Security Policies
OpenPMF PDL

PSM level

PEP library or tailor-made development

Transformation in tool chain SecureMiddleware™

(Distributed) Application Code
and assembly/deployment information

Local Policy Enforcement Points
OpenPMF PEPs

Code & enforcement level

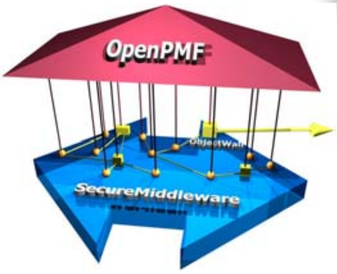
Model driven security training workshops available:
www.objectsecurity.com/en-services-training.html

SecureMDA
Model Driven Engineering Toolchain

Collaborative Decision Making Demo

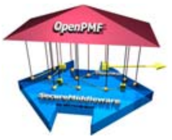
Modeling and security

- What do I generate my policies for?
  - Security toolchain could generate policies for particular target system, e.g. Java RBAC, CORBA rights
  - Better: use central policy administration tool:
    - OpenPMF policy management framework



Modeling and security

- OpenPMF policy management framework
  - Consistent, unified policy language
    - Flexible
    - Extensible
    - Technology-neutral
    - PDL based on Ponder, Principal calc etc.
  - Policy enforcement points
    - Plug-in architecture
    - Modular
    - Can be built for practically any underlying system
  - Central, real-time security admin and monitoring



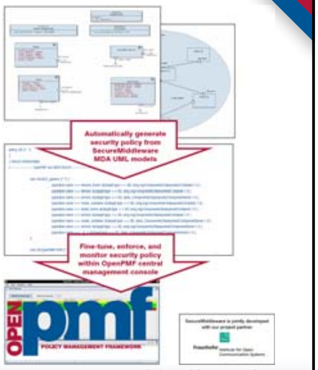
```
policy /OS [*, *]
{
// ROLES DEFINITIONS:
// ------------------ OpenPMF and QEDO ROLES ------------------
                    role /OS/QCS_generic [*,*] {
                                    (operation.name == remove_home )&(target.type == IDL:o
                                    (operation.name == remove )&(target.type == IDL:omg.org
                                    (operation.name == remove )&(target.type == IDL:Qedo_C
                                    (operation.name == create_container )&(target.type == IDL
                                    (operation.name == install_home )&(target.type == IDL:om
                                    (operation.name == remove )&(target.type == IDL:omg.org
                                    (operation.name == create_container )&(target.type == IDL
                                    (operation.name == remove )&(target.type == IDL:omg.org
                                    (operation.name == _is_a )&(target.type == IDL:Qedo_Con
                    };

                    role /OS/OpenPMF/CPM [*,*] {
```

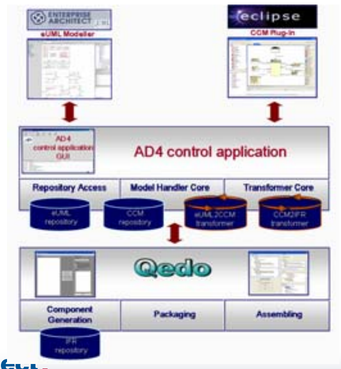
Video clip:
http://www.objectsecurity.com/
en-resources-video-openpmf.html

Modeling and security toolchain

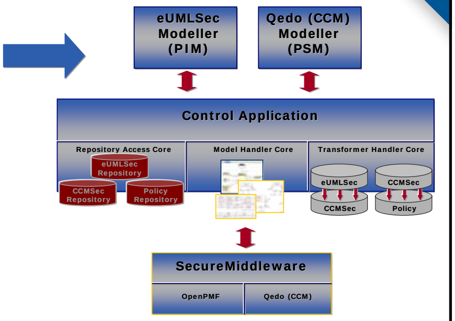
- Automatically generate OpenPMF security policies from application models
- Fine-tune policy in OpenPMF GUI
- Automatically enforce policy using OpenPMF
- OpenPMF to monitor & administer policy
- SecureMDA ™ www.securemda.com
  - Generic toolchain product
  - These pictures for OpenPMF and SecureMiddleware


Automatically generate security policy from SecureMiddleware MDA UML models
Fine-tune, enforce, and monitor security policy within OpenPMF central management console
OPEN pmf
POLICY MANAGEMENT FRAMEWORK
SecureMiddleware is jointly developed with our project partner
Fraunhofer
Institute for Open Communication Systems

Some details



Some details



- eUML Modeller
  - Security Profile
- CCM Plug-In to security
  - Plug-In extension
- SecureMiddleware
  - already available

SecureMDA+ SecureMiddleware Toolchain in Action:
Automatic Code + Security Policy Generation

Video Clip:
http://www.objectsecurity.com/
en-resources-video-securemda.html

(more: http://www.objectsecurity.com/en-resources-video.html)

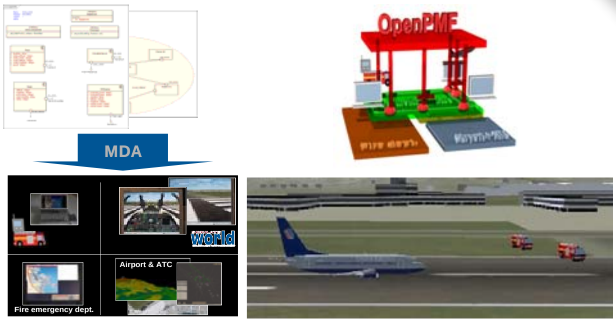
SimulateWorld™

Case Study 1:
The generated application in action

Video clip:
http://www.objectsecurity.com/
en-resources-video-simworld.html
(more: http://www.objectsecurity.com/en-resources-video.html)

MDA case study: SimulateWorld™ demo

Distributed aircraft emergency response scenario



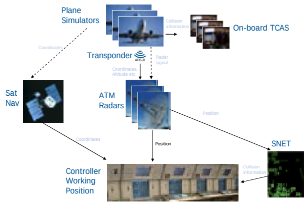
Animated video clips: www.simulateworld.com

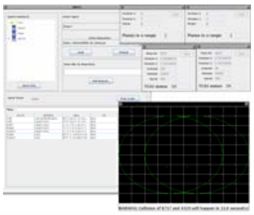
SINS: Case Study 2

Survivable middleware with model driven engineering & security,
U.S. Naval Research Lab air traffic control demo

U.S. Naval Research Lab SINS demo

- Global safety & security constraints in model transformed into code and enforced with high assurance (not based on MDA!)
- Designed for tactical C4ISTAR/CDM style NCW environments





SINS Demo

Video Clip:

http://www.objectsecurity.com/ en-resources-video-sins.html

(more: http://www.objectsecurity.com/en-resources-video.html)

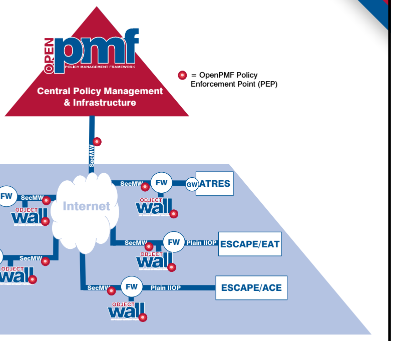
SecureMDA Case Study 3: Generated distributed applications

Secure information sharing platform for air traffic management

EU FP6 R&D Project: Secure ATC integration

Case Study

- Air traffic management simulation data feed integration across the internet



Conclusion

Summary

- Automatic generation of security policies from software models may sound futuristic, but it:
  - — Works!!! -> see www.securemda.com
  - — Frees up time & resources
    - Both for policy specification & management
  - — Improves security
    - Consistency, completeness, correcness, prevents human errors
    - Easier to justify assurance (software & security)
    - Easier to justify correct enforcement of enterprise policy
  - — We are looking for partners who want to:
    - License this technology
    - Collaborate to enhance & use it
    - We invite you to our model driven security workshops

Further Information & Contact Details

Further information

- NRL SINS paper download:
  www.objectsecurity.com/en-projects-sins.html
- EU FP6 Air Traffic Management Project:
  www.ad4-project.com
- SecureMDA page:
  www.securemda.com
- OMG Model Driven Architecture Page:
  mda.omg.org
- ObjectSecurity Information Pack:
  www.objectsecurity.com/infopack.html

Contact details

- Dr. Ulrich Lang:
  ulrich.lang@objectsecurity.com
- 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
- ObjectSecurity LLC
  2910 Stevens Creek Boulevard
  Suite 109-764
  San Jose, CA 95128-2015
  USA
  Tel: 1-800-898-9148
  Fax: 1-360-933-9591

Model driven security workshops:
www.objectsecurity.com/
en-services-training.html

Object Security
Secure technology

info@objectsecurity.com
www.objectsecurity.com