Object™ Security

CORBASec Reality Check

MICOSec: CORBA Security Reality Check

Ulrich Lang

Rudolf Schreiner

Object Security™

CORBASec Reality Check

CORBASec Reality Check

- The Business Promise
- Design Goals
- MICOSec
  - Implementation
  - Evaluation
  - Wireless CORBA Security
- Challenges and Workarounds
- Upcoming Standards
- Conclusion

Object Security™

CORBASec Reality Check

CORBA Business Promise

Large enterprises use
many incompatible components

Specific Application

Web Server

Legacy Backend Data Store

Contractor Data Access

Firewall

Data Mining Machine

Customer Data

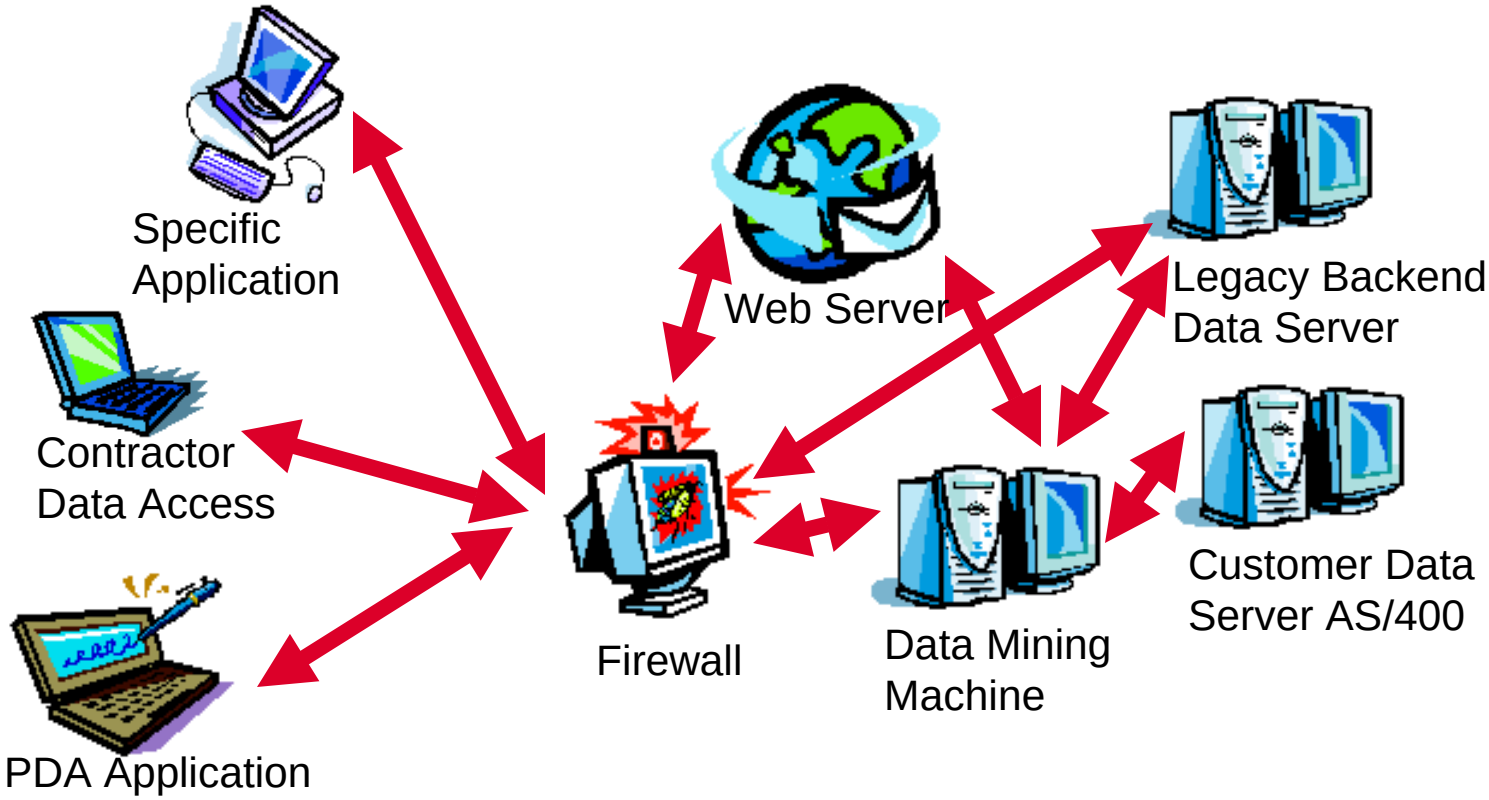
PDA Application

Object Security™

CORBASec Reality Check

CORBA Business Promise

CORBA gives seamless, enterprise-wide integration of services and data



Object Security™

CORBASec Reality Check

CORBA Business Promise

- With minimal extra impact on:
  - Installation, configuration, administration
  - Application development
  - Existing Systems (legacy Integration)
  - Training
  - Performance

Object Security™

CORBASec Reality Check

CORBASec Business Promise

- Add security without sacrificing the purpose of CORBA
- With as little extra impact as possible on existing:
  - Applications
  - Security infrastructure
  - Business processes
- Make security manageable

Object Security™

CORBASec Reality Check

Design Goals

- Preserve main CORBA design goals:
  - Interoperability
  - Flexibility
  - Automation
  - Portability
  - Abstraction
  - Scalability

Object Security™

CORBASec Reality Check

Functionality

- CORBASec specifies:
  - Authentication
  - Message Protection
  - Access Control
  - Audit
  - (Non-Repudiation)
- ORB layer & application layer security enforcement

Object Security™

CORBASec Reality Check

Reality Check

Can CORBASec be used to secure real-world CORBA applications?

Learning by Doing
implement
and test the
specification

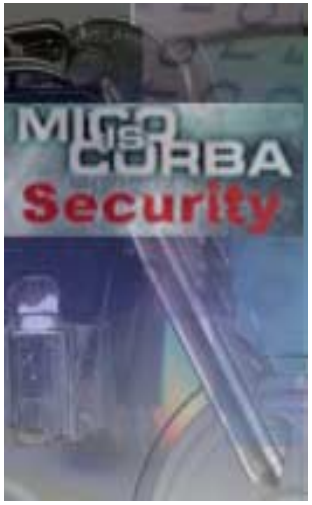
+

Conceptual work
technical flaw
or fundamental
challenge/trade-off?

Object Security ™

CORBASec Reality Check

MICOSec Implementation



- CORBASec level 2
- Based on:
  - MICO ORB
  - OpenSSL library
  - PostgreSQL database
- Originally developed for research
- Work in progress (like CORBASec)

Object Security

CORBASec Reality Check

Wireless MICOSec

- Proof of concept: test CORBASec in a specific environment
- Full MICOSec was ported to a Compaq iPAQ 3630 PocketPC under Linux
  - Performance is adequate
  - Porting of existing applications is easy (except GUI)

Object Security™

CORBASec Reality Check

MICOSec Evaluation

- Lots of pitfalls (esp. for non specialists)
  - Difficult to design
  - Difficult to implement
- Does not meet all requirements:
  - Does not provide simple and automatic security enforcement
  - Does not always integrate well
  - Identity based access control hard to administer
  - Assurance?
  - …

Object Security™

CORBASec Reality Check

MICOSec Evaluation

- Some modifications of the spec necessary:
  - Domain based object names
  - SSL needs simple PKI support
  - …
- Does CORBASec work?
  - Some conceptual challenges
  - But real-world workarounds are possible
  - Fits to wireless systems

Object Security™

CORBASec Reality Check

Challenges & Workarounds

- Example challenges:
  - Conflicting goals
  - Object identifiers
  - Underlying security infrastructure
- Real-world workarounds

Object Security™

CORBASec Reality Check

Challenge 1: Conflicting Goals

- Interoperability requires common mechanisms, data formats etc.
- Flexibility allows many differing mechanisms, data formats

- Assurance requires evaluation of the whole (static) system
- Flexibility results in dynamically changing system

- Workarounds: identify sensible trade-offs

Object Security ™

CORBASec Reality Check

Challenge 2: Object Identifiers

- Challenge: How to represent client and target object in the security policy:
  - Access Control Policy
  - Audit Policy
  - (Authentication)
  - (Non-Repudiation)
- Goal: find an interoperable identifier on the middleware layer – must be:
  - Fined-grained
  - Security mechanism unspecific
  - Static
  - Precise and trustworthy

Object Security™

CORBASec Reality Check

Challenge 2: Object Identifiers

- Reality: CORBASec uses target interface
  - Not precise enough because of object inheritance etc.
- Other options?
  - Abstract from security mechanism
    - Semantics and granularity not clear
  - Target identifier [Host|POA|ObjectID]
    - Changes dynamically
- Workarounds:
  - Target Identifier:
    Object Domain Mapping (ODM)
  - Client Identifier:
    Only security mechanism identifier available, use it.

Object Security™

CORBASec Reality Check

Challenge 3: Infrastructure

- CORBASec runs on top of existing security infrastructure:
  - Security Mechanism
  - Public Key Infrastructure
  - Firewalls
- Often not good enough for CORBASec
- Often do not fit with the architecture

- Workaround: Do it yourself
  - Use own security mechanism
  - Mappings, e.g.directory services for roles, domains

Object Security™

CORBASec Reality Check

CORBASec is Work in Progress

- Upcoming Standards
  - Security Domain Membership Management Service
  - Common Secure Interoperability version 2 (CSIv2)
  - Authorization Token Acquisition Layer Server (ATLAS)

Object Security™

CORBASec Reality Check

Conclusion

- CORBASec is a useful tool for securing today's CORBA applications

- But:
  - Some "wishes" are unrealistic
    - No out-of-the-box security
    - No idiot proof security
    - Cannot solve fundamental difficulties
  - Some technical issues need to be fixed

Object™ Security

CORBASec Reality Check

Object™ Security

www.objectsecurity.com

info@objectsecurity.com

Object Security™

CORBASec Reality Check

MICOSec Main Features

- Security level 2 version 1.7
- security aware and security unaware applications
- All features of MICO 2.3.1, including POA
- SSLIOP based on SSL v 3 with different ciphers
- Extended attributes for X.509 and environment information
- Plain IIOP
- Authentication
- Message protection
- Policies for secure associations
- Extended level 1 interfaces
- Auditing into file/syslog/RDBMS
- Secure interoperability with other ORBs
- Object Domain Mapping
- Domain based access control and auditing
- Domain Membership Management