OMG's Seventh Annual Workshop On
DISTRIBUTED OBJECTS and COMPONENTS SECURITY

April 7-10, 2003
Baltimore, Maryland, USA

Program

Monday, April 7, 2003

0900 - 1230 **Tutorial:** ***Survey of Security of Threats and Countermeasures in Distributed Object, Component, and Service Architectures***
David Chizmadia, Senior Security Architect, Promia, Inc.

The goal of this tutorial is to provide a context within which to understand the motivation for, and compare the appropriateness of, the security features in each of the specific Distributed Object, Component, and Service (DOCS) architectures that will be described in the remaining tutorials. The tutorial will start by describing a notional framework that includes the common features of existing DOCS architectures. This framework will then be used to analyze the security threats to the various DOCS system elements - including the communications paths between those elements. The tutorial will conclude with a survey of the security countermeasures that can be used to mitigate the threats described.

1030 – 1045 Morning Refreshments

1230 – 1330 Lunch

1330 – 1700 **Tutorial:** ***Web Services Security Overview and Implementation***
Jorgen Thelin, CTO, Cape Clear Software, Inc.

This tutorial provides an assessment of the various security concerns and implications for XML Web Services, and the different means to address them. A framework is presented outlining the variety of measures and approaches for achieving end-to-end security for Web Services, leveraging any pre-existing security environments where possible. The various technical security aspects of authentication, authorization, confidentiality and integrity are explored, along with how they affect Web Services and how they relate to the business-driven security concepts of identity, single-sign-on, privacy, trust and non-repudiation. An overview is provided of the emerging XML security standards such as XML Digital Signatures (XML-DSIG), XML Encryption, Security Assertions Markup Language (SAML) and WS-Security, including how they combine to address the fundamental security requirements of line-of-business Web Services. Examples are shown of a common technique for implementing the security requirements for a Web Service application through the use of custom or pre-built client-side and server-side interceptor plug-ins, in a manner similar to existing Aspect-oriented programming concepts. Finally, some lesson from the initial experiences implementing and using Web Services security are provided, along with advice and guidance for future projects.

1500 – 1515 Afternoon Refreshments

Tuesday, April 8, 2003

0900 – 1215 ***Introduction to the OMG's Security Specifications***
David Chizmadia, Senior Security Architect, Promia, Inc.

This tutorial will provide a high-level technical introduction to the security specifications that the OMG has adopted. It will start with a survey of the OMG's security specifications and move on to a technical description of the purpose and object model for each specification.

The tutorial will cover, in order:
- CSIv2 (Common Secure Interoperability version 2)
- CORBAsecurity SecurityLevel2
- RAD (Resource Access Decision)
- ATLAS (Attribute Token Layer Acquisition Service)
- CORBA Firewall Traversal
- PKII (Public Key Infrastructure Interfaces).

1030 – 1045 Morning Refreshments

1200 – 1800 ***Demonstration Area Open***

1215 – 1315 Lunch

1315 - 1330 ***Workshop Welcome and Opening Remarks***
(Program Committee Co-Chair)
Richard Soley, Chairman & CEO, Object Management Group

1330 – 1500 ***Session 1: Case Study – Medical Systems***
Chair: Carol Burt, President, 2AB

This session highlights real results from the deployment of a secure, distributed system in the field of medical records.

Experiences Deploying a Secure, Multi-enterprise Distributed Medical Records System for Medical Surveillance
David Forslund, Jim George & Douglas Wokoun, Los Alamos National Laboratory

As part of the National BioDefense Initiative, we have deployed a medical surveillance system (BSAFER) in Albuquerque, NM, which integrates heterogeneous data from 6 distinct hospital systems. This has required the use of a secure CORBA infrastructure linking multiple secure enterprises. We will discuss the mechanisms we have to provide interoperable security solutions including the ability to identify the end user and restrict their access through the multiple SSL connections required by the firewalls.

1500 – 1530 Afternoon Refreshments

1530 – 1730 *Session 2: Nip it in the Bud: Proactive Secure Application Design*

Chair: Polar Humenn, Principal, Adiron LLC

This session focuses on emerging techniques for integrating security into the early stages of application design and development. Our first presentation recognizes several issues concerning system qualities and threats. The author then looks at the most common reoccurring solutions to those issues, i.e. patterns, and the ways in which early design of applications will benefit from the use of these patterns. Our second presentation concentrates on the formal modeling of secure applications by "Use case oriented development". The authors present a mechanism with which they use a security enhanced form of the Unified Modeling Language (UML), called UMLsec, during the early stages of application design to relate security requirements of the data model with the behavior specification of the application.

Three Design Patterns for Secure Distributed Systems

Alan H. Karp, Principal Scientist & Kevin Smathers, Hewlett-Packard Labs

We present three patterns that can be used in the design of distributed systems to reduce their vulnerability to attack. Mediation makes it easier to see what is going on in the system. Using a proxy makes it easier to control what is done by remote users. Separating the granting of permissions from access control decisions makes it easier to express a security policy and reduces the coordination needed to enforce it. We'll describe these patterns and our experience with them in e-speak.

Use Case Oriented Development of Security-Critical Systems

Gerhard Popp, Jan Jurjens and Guido Wimmel
Department of Computer Science, Munich University of Technology

Computers distributed over the Internet are susceptible to attacks. To address this situation, we have to consider security requirements from the beginning of the system development. In early phases of system development, it is common to use a two-part process for the elaboration of the application core and the functional specification in use cases. We demonstrate an extension of this process for security-critical systems in a methodical concept and the modeling of security aspects in the application core with an extension of the UML for security-critical systems (UMLsec). Furthermore, we introduce security use cases in conjunction with behavioral modeling.

Wednesday, April 9, 2003

0900 – 1130 *Session 3: Authentication and System Level Identity*

Chair: Bill Beckwith, CEO, Objective Interface Systems, Inc.

This session includes two distributed security presentations: one on validating identity for web services and the other on a single sign on for a CORBA environment. The first presentation will discuss how a Network Identity Platform can address the identity of users, applications, and nodes within a web services environment. Related specifications and technologies are discussed in relation to this topic. The second presentation describes single sign on for CORBA applications using an approach based on a security integration platform. Deployment patterns for CORBA-only, mixed CORBA and Kerberos, and generic cross security domain deployment are also discussed.

Validating Identity of Web Sites, Web Applications, Web Services and Users with the Network Identity Platform
Rakesh Radhakrishnan, Sun Microsystems

This presentation covers the topics around validating Identity of web users, web applications, web services and web sites and how end-to-end security is addressed with a Network Identity Platform. The material discusses security mechanisms and techniques leveraged with the Liberty Spec based ID Servers, Directory Servers, in conjunction with PKI/X-KMS based Certificate Management Servers. Several J2EE(tm) Technology Security features are discussed such as JCE, JAAS, JSSE, Java Message ID validation/encryption, support for SAML, x-KMS, etc. Deployment/Network (physical) Architectures of the Sun ONE Network Identity Platform are also covered in the presentation, both current and with respect to the next generation Storage/Network/Server Virtualization solutions (Sun ONE on N1). The presentation also covers how to address perceived tradeoffs associated with Scalability and Availability when extensive security techniques are used.

Single Sign On In A CORBA-Based Distributed System
Igor Balabine, Security Architect, IONA Technologies

A security integration platform based approach to extending single sign on to CORBA applications is presented and a number of deployment patterns are studied. The deployment patterns include single sign on in a pure CORBA environment, in a mixed Kerberos – based environment and a generic cross security domain deployment.

1000 – 1800 *Demonstration Area Open*

1000 – 1030 Morning Refreshments

1130 – 1200 *Co-Sponsor Presentation* - **Promia**

1200 – 1300 Lunch

1300 – 1330 *Co-Sponsor Presentation* - **NSA**

1330 – 1430 *Session 4: Model Driven Security*

Chair: Richard Soley, Chairman & CEO, Object Management Group

Model-driven techniques to define systems, in particular OMG's Model Driven Architecture, promise to abstract away the details of implementation infrastructure choice from the application development process. This is particularly important for "horizontal" pervasive services that are found in any distributed system infrastructure, especially those services that are complicated to implement such as security. This session will explore abstraction of security models away from specific implementation technologies (such as .NET, CORBA and J2EE).

Model Driven Security: Protection of Resources in Complex Distributed Systems
Ulrich Lang, CEO & Rudolf Schreiner, CTO, ObjectSecurity Ltd.

In OMG's model driven architecture, the functional properties of an application are first modeled and then translated into a particular system. In line with this, it would be useful to also model and implement the security policy in a similar fashion. Moreover, in order to integrate the security of a whole organisation, a central security policy should be mapped automatically onto different platforms and applications. This talk will present our new security framework, which consists of the policy repository, a code generator, and platform adapters. We will illustrate our approach using our prototype implementation for the CORBA Component Model.

1430 – 1500 Afternoon Refreshments

1500 – 1700 *Session 5: CORBASec Technologies for Internet and Real-time Environments*

Chair: Tammy Blaser, Sr. Computer Engineer, NASA Glenn Research Center

This session includes two CORBA Security presentations in support of two different operating environments: a large Internet object system and a real-time mission critical environment. The first presentation will discuss a fine grain access, large object system, architecture using the CORBA Security Service and a developed administration GUI. The implementation utilizes a domain based security model applying a single security policy to all objects in the domain, resulting in a minimum number of access control rules providing administration scaling. The second presentation describes an initiative to integrate and standardize Real-time CORBA middleware implementation with several MILS (Multiple Interacting Levels of Security) security separation kernels. The Real-time CORBA 1.0 standard is the foundation of many mission critical systems in the defense, telecommunications, consumer electronics, medical, manufacturing, and vehicle automation industries. Real-time MILS CORBA represents an infrastructure that addresses mission critical distributed object communication requirements including: high-assurance, real-time and high performance.

Providing Fine Grained Access Control in CORBA Distributed Object System
Atul Kumar, Dept. of Computer Science and Engineering, Indian Institute of Technology

CORBA Security Service provides a domain based access control mechanism. Same access control rules apply to all the objects in a domain. In some situations, a user may need to assign a different access control policy for different objects (and different methods within the objects). We propose a fine grained access control mechanism that works on the top of existing domain based CORBA Security Service. This can be used to define object and method level access control rules.

Real-time MILS CORBA: High Assurance Security for Real-time, Distributed Systems
Bill Beckwith, CEO, Objective Interface Systems, Inc.

This presentation will describe an initiative to integrate and standardize Real-time CORBA with MILS (Multiple Interacting Levels of Security.

1800 – 2000 *WORKSHOP RECEPTION hosted by Promia & NSA*

Thursday, April 10, 2003

0900 – 1145 ***Session 6: Testing***
Chair: Richard Soley, Chairman & CEO, Object Management Group

Assessment, assurance and testing are critical in systems in which security is not just a checklist item, but an absolute requirement. This session highlights several approaches to testing supposedly secure systems against requirements.

Model-based Automated Security Functional Testing
Ramaswamy Chandramouli, Computer Security Division, NIST
Mark Blackburn, T-VEC Technologies

Independent security functional testing on a product occupies a backseat in traditional security evaluation because of the cost and stringent coverage requirements. In this presentation we discuss the details of an approach we have developed to automate key aspects of security functional testing. The underlying framework is called TAF (Test Automation Framework) and the toolkit we have developed based on TAF is the TAF-SFT toolkit. We illustrate the application of TAF-SFT toolkit for security functional testing of a commercial DBMS product. We also discuss the advantages and disadvantages of using TAF-SFT toolkit for security functional testing and the scenarios under which the impact of disadvantages can be minimized.

Testing Security In Systems Of Distributed Components
David Chizmadia, Senior Security Architect, Promia, Inc.

This presentation will present the preliminary results of an assessment of the full range of security issues that must be considered during security testing of systems of distributed components. It will also include our preliminary proposal for the requirements and architecture of the tools needed to support testing the security of systems of distributed components.

1000 – 1015 Morning Refreshments

1145 – 1245 Lunch

1245 – 1415 ***Session 7: Case Study – Telecom Systems***
Chair: Ulrich Lang, CEO, ObjectSecurity Ltd.

Telecoms are building so-called "service platforms" (e.g., Parlay) on top of traditional middleware such as CORBA. Service platforms give service providers standardised interfaces to functions of the underlying network infrastructure, such as the 3G mobile network. Service platforms can not only be used by the network operator, but also by 3rd party service providers to implement telecommunications services. Users, service providers, network providers, and regulators all have differing security requirements, which will be the focus of this session.

SecureParlay: A Secure Service Platform
Gerald Lorang, Research Scientist, T-Systems Nova GmbH & Rudolf Schreiner, CTO, ObjectSecurity Ltd.

The authors are implementing a secure Parlay platform for the development of secure telecommunications applications. This experimental platform is based on the CORBA security services. The first results showed that there are several issues, mainly gaps and mismatches between Parlay and CORBASec, which make the goal, security enforcement at the abstraction level of the platform, hard to achieve. In the IST- Project COACH, a secure component framework is currently under development. The Secure Parlay platform will use this secure component framework based on the OpenSource ORB Mico to implement its security features. The presentation describes the architecture of the platform and the security concept.

1415 – 1430 Afternoon Refreshments

1430 – 1630 *Session 8: Emerging Security Technology*

Chair: David Chizmadia, Senior Security Architect, Promia, Inc.

Strong indicators of a robust and healthy technology include the existence of advanced research and development that provides the foundation for future technologies, products, and specifications. This year's Emerging Technologies presentations show how two inter-object invocation protocols are demonstrably and believably effective and secure

Secure Interoperation Using a Capability Messaging Protocol
Tyler Close, CEO, Waterken Inc.

This presentation will discuss a messaging protocol designed to facilitate inter-operation both between capability systems and with existing applications. The presentation will introduce the core concepts of capability security and show how this security paradigm is enforced in the messaging protocol. A methodology for adapting existing applications to the capability messaging paradigm will then be presented. The methodology will be demonstrated by showing how it is applied using the Waterken(TM) RDB Webizer. This product is a middle-ware tool for integrating existing relational databases into the capability messaging paradigm.

Formal Aspects of the CORBA CSIv2 Protocol
Polar Humenn, Principal, Adiron, LLC

The Common Secure Interoperability Version 2 (CSIv2) Protocol is the new protocol used by secure CORBA and EJB programs. It is a complex protocol that handles delegation and delivery of authorization information. The CSIv2 Protocol has been developed with some foundations of mathematics behind it. This presentation explains a calculus used to reason about the CSIv2 protocol and gives the formal interpretations of the CSIv2 protocol components using that calculus. Further, it explains some emerging work concerning the formal aspects of authorization information within the CSIv2 protocol, the Security Attribute Markup Language (SAML), the Extensible Access Control Markup Language (XACML), and the way in which analysis using these formal methods can lead to verified systems.

1630 – 1645 *Closing Remarks*

Program Committee Co-Chair:
David Chizmadia, Senior Security Architect, Promia, Inc.