DOCsec2001 Workshop

March 26 - 29, 2001 - Annapolis, MD USA

Workshop Program

MONDAY - March 26, 2001

0830 – 1730 - ***CORBA Tutorial***
Dr. Jon Siegel, Object Management Group

This all-day tutorial covers OMG's Object Management Architecture including CORBA, the CORBAservices and CORBAfacilities, the Domain CORBAfacilities, and an afternoon concentrating on the new specifications included in OMG's latest release, CORBA 3. Starting with a brief look at requirements and needs in distributed computing and how UML, the MOF, and XMI fit into the rest of the OMG specifications, the tutorial moves on to cover OMG Interface Definition Language and mappings to various programming languages, structure of the Object Request Broker, interoperability and the standard protocols GIOP and IIOP, and integration with Java and COM/DCOM. The next section of the tutorial covers the CORBAservices and facilities, and the Domain CORBAfacilities.

The afternoon covers the new specifications included in the CORBA 3 release, which fall into three categories: Improved integration with Java and the Internet; Quality of Service Control, and the CORBA Component Model or CCM. The discussion of CCM starts with a closer look at the Portable Object Adapter or POA, on which CCM is based.

1015 – 1045 - Morning Refreshments

1230 – 1330 - Lunch

1515 – 1545 - Afternoon Refreshments

TUESDAY – March 27, 2001

0830 – 1730 - ***Security Engineering Using OMG Specifications***
David Chizmadia, Promia

This all-day tutorial introduces the basic concepts of security engineering in distributed object and component (DOC) systems and then illustrates these concepts with existing and emerging OMG security specifications. The tutorial starts with the general security engineering considerations in DOC system architectures. An abstract model is used to show the security threats to DOC system architectures and the security technologies available to mitigate those threats. A DOC Security Interfaces Framework (DOCSIF) that can be used to identify (and compare) the security technologies exposed in one (or more) DOC system architecture(s) is then introduced.

The tutorial then uses the DOCSIF to present the OMG security specifications in a broader context. First, the OMG CORBA and CORBA Component Model specifications are described in terms of the same abstract model used to describe security threats. Next, adopted OMG security specifications are described in terms of the DOCSIF, followed by an analysis of the security technologies that are absent or under-specified in OMG specifications and a description of the OMG Security SIG roadmap to incorporate those technologies. The tutorial ends with a discussion of how OMG technical specifications relate to other aspects of security engineering, such as evaluation, operation and system evolution.

1015 – 1045 - Morning Refreshments

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

1230 – 1330 - Lunch

1515 – 1545 - Afternoon Refreshments

WEDNESDAY, March 28, 2001

0845 – 0900 - ***Opening Remarks***
Dr. Richard Soley, Object Management Group

0900 – 1030 - ***Case Studies***
Chaired by Carol Burt, 2AB, Inc.

This session will present a series of Case Studies from companies regarding their experiences implementing and testing distributed security solutions based on OMG specifications. The presenters will share experiences implementing solutions in AeroSpace, Finance, and Mobile computing. They will share architectures, problems and lessons learned while attempting to secure diverse technical environments. Each case study will be followed by question and answer time for workshop participants.

"Using CORBAsec to Secure Distributed Aerospace Propulsion Systems"
Tammy M. Blaser, NASA Glenn Research Center

NASA Glenn Research Center and its industry partners are developing a CORBASec test bed to secure their distributed aerospace propulsion simulations. NASA Glenn Research Center is an active domain member of the OMG and has been working with its aerospace propulsion industry partners to deploy the Numerical Propulsion System Simulation (NPSS) object based technology. When the NPSS is deployed, it will assemble a distributed aerospace propulsion simulation scenario from proprietary analytical CORBA servers and execute them with security afforded by the CORBASec implementation.

The NPSS CORBASec test bed will integrate the Hitachi TPBroker Security Service (SS) product, initially using the TPBroker Basic Object Adaptor (BOA) based ORB, with its NPSS software across different firewall products. The test bed will migrate to the Portable Object Adaptor (POA) architecture after Hitachi ports their SS to the VisiBroker 4.x ORB. NASA Glenn Research Center, General Electric Aircraft Engines and Pratt & Whitney Aircraft are the initial industry partner contributors to the PSS CORBASec test bed.

The test bed is expected to demonstrate NPSS CORBASec specific policy functionality, confirm adequate performance and validate the required Internet configuration in a distributed collaborative aerospace propulsion environment.

"Real Life Use of CORBA Security and RAD"
Jeffrey P. Cahoon, iWitness.net

Enterprise level records management systems can have difficult security issues:
- protection of extremely sensitive data
- large numbers of ever changing groups of users in various roles
- vast numbers of documents
- few resources for administration
- different security requirements for various portions of records or different records operations
- the need for accurate accounting of accesses or attempted accesses along with convincing proof security was not bypassed

The iWitness records management system (Verimail) implements a portion of the CORBA Resource Access Decision (RAD) specification on top of the CORBA Security Service (CosSec). iWitness is very pleased with these specifications. This presentation offers the iWitness experience regarding:
- The specifications' strengths and weaknesses found during implementation
- Steps for mapping real life security to the CORBA model
- Security extensions the specifications make possible for iWitness
- Traps to avoid

1000 – 1800 - ***Demonstration Area Open***

1030 – 1100 - Morning Refreshments

1100 – 1230 - ***Case Studies Continued***

"MICOSec: CORBAsec Reality Check"
Ulrich Lang, ObjectSecurity Ltd.

This talk will give an overview of the lessons learnt during the development of MICOSec, our proof-of-concept CORBA Security Services implementation. MICOSec is currently used in a variety of contexts to explore the viability of middleware security, in particular as a secure mobile middleware platform, and as a secure application platform for telecommunications environments.

We will present some of the issues which are not obvious from the specification but only surface during the actual implementation. While most of these issues can be solved though minor adjustments, there are also some fundamental limitations to middleware based security enforcement. Wherever possible, we will illustrate how modifications and improvements were applied to MICOSec. Our talk will also focus on CORBA security on mobile platforms, as there is a big emerging market for secure middleware application platforms, which extend onto mobile devices.

1230 – 1330 - Lunch

1330 – 1345 - ***Sponsor Presentation***
Bret Hartman, CTO – Hitachi Software
Software Solutions Division - Hitachi Computer Products (America), Inc.

1345 – 1530 - ***Users' Roundtable***
Moderators: Richard Soley, Object Management Group &
Jishnu Mukerji, Hewlett-Packard Company

In this panel session users who have been through the implementation of distributed object security projects will explore the difficulties they have faced and relate practical experience for people faced with DOC security projects.

Panelists: Konstantin Beznosov, Security Architect, Concept Five Technologies

Tammy M. Blaser, Senior Software Engineer, NASA Glenn Research Center

Jeff Cahoon,, Systems Analyst, iWitness.net

Mary Kratz, Health Sciences Manager, Internet 2

1530 – 1600 - Afternoon Refreshments

1600 – 1730 - ***Authorization and Delegation***
Chaired by Fred Dushin, Hitachi Software

Authorization runs to the heart of distributed security and delegation is generally mentioned in the same breath. Although the specifics can change, security concerned organizations can learn much by inspecting the solutions that other organizations have crafted.

"Supporting Secure and Transparent Delegation in PI-squared"
Zoltan Nochta, Rainer Ruggaber &Taufiq Rochaeli, Institute of Telematics, University of Karlsruhe, Germany

In our talk we will present a solution for securing applications using Pi^2. Pi^2 is a generic CORBA proxy platform that is used to support applications in mobile and wireless environments. Because the CORBA security service does not support the transparent integration of proxies between client and server, we provide a proprietary solution with end-to-end authentication based on a PKI for key exchange and symmetric encryption on the subconnections due to performance.

"Security Lite"
Bob Burt, iLock; 2AB, Inc.

This presentation will discuss how to implement a light weight security service for CORBA using SSL for authentication, LDAP for credential acquisition, CORBA portable interceptors for delegation and OMG Resource Access Decision Facility (RAD) for authorization services. The session will also discuss how the RAD framework can be utilized for the fine-grain access control services required by many application domains.

1800 – 2000 ***Workshop Reception hosted by Hitachi Software***

THURSDAY, March 29, 2001

830 – 1000 - ***Current Status of Security Specifications***
Chaired by Konstantin Beznosov, Concept Five Technologies

The session presentations will update the workshop attendees on the latest state in the standards related to DOCSec. It will feature overviews of the EJBv2 security, as well as recently adopted protocol for Common Secure Interoperability version 2 (CSIv2), which enables the wire interoperability not only of CORBA Security servers, but also EJB and mixed (CORBA and EJB) environments. In addition, the audience will receive updates on the status of ongoing work on the upcoming OMG specifications for passing Internet Inter-ORB Protocol (IIOP) messages through firewalls, and managing security policy domains in CORBA systems.

"Current Status of OMG Firewall Specification"
Brian Niebuhr, Network Associates - NAI Labs

One well-known problem in the CORBA community is how to use IIOP in a networked environment where firewalls have been deployed to protect networked resources. A specification exists to address this problem, but it is widely agreed that the specification does not meet the needs of CORBA vendors or users.

In order to address those needs, a new CORBA Firewall Traversal RFP was submitted. ORB and firewall vendors have responded to the RFP and are attempting to develop a new specification. The purpose of this presentation is to inform the DOCSec attendees of the status of the specification, and to receive feedback from users who would potentially deploy such a system. Additionally, we will present what we know about the current submissions, and outline the features and limitations of those submissions.

“Overview of Security Domain Membership Management RFP Submission”
Konstantin Beznosov, Concept Five Technologies

The current version of CORBA Security specification uses the notion of security policy domains and alludes to inder-domain relations that require policy composition. However, it does not define mechanisms for managing the domain life cycles and domain hierarchies, nor it specifies how policies assigned to different domains should be composed in the case of domain hierarchies. The specification also lacks the provision of mechanisms for retrieving the information about domain membership in regards to target objects. In order to resolve the listed issues the OMG has issued "Security Domain Membership Management" RFP.

This presentation will describe the RFP requirements, and discuss the architecture of the RFP submission, which is on its track to become a new standard in the arena of CORBA Security.

1000 – 1030 - Morning Refreshments

1030 – 1200 - ***Current Status of Security Specifications Continued***

“CSI V2”
Don Flinn, IONA Technologies

Common Secure Interoperability Version 2 (CSIv2) is an important new specification that supports CORBA to CORBA and CORBA - EJB secure interoperability. Now that CSIv2 has reached the final stages in becoming an OMG Specification you will soon see implementations of interoperable security products at you neighborhood software store.

This presentation will discuss CSIv2 from a users point of view, i.e. what it is and what new capabilities it will give your enterprise applications. For some time now users have been lamenting the inability of their CORBA application to securely interoperate between different vendors'. CSIv2 will change all that. In addition CSIv2 enabled applications and EJB container will also be able to securely able to interoperate.

1200 – 1300 - Lunch

1300 – 1500 - ***Vendors' Roundtable***
Moderators: Richard Soley, Object Management Group &
Jishnu Mukerji,, Hewlett-Packard Company

In this panel session will focus on implementation issues as addressed by the vendors. Representatives of major DOC security products will relate the specification/implementation issues they have faced and discuss their future product plans with relation to this technology.

Panelists: Don Flinn, Principle Engineer, Iona Technologies

Steve Fritzinger, Sun Microsystems

Bret Hartman, CTO, Hitachi Software

Vijaykumar Natarajan, Senior Software Engineer, Borland Software Corporation

Rudolf Schreiner, Object Security

Brent Whitmore, Senior Computer Scientist, NAI Labs@Network Associates

1500 – 1530 - Afternoon Refreshments

1530 – 1700 - ***Emerging Technologies***
Chaired by David Chizmadia, Promia

The best sign of a robust and healthy technology is the existence of advanced research and development that the foundation for future technologies, products, and specifications. This session consists of two presentations. The first describes ongoing research at NAI Labs into making the CORBA infrastructure more resistant to hostile intrusion attempts. The second offers ideas from Hitachi Computer Products for extending the existing CORBAsec policy management architecture to accommodate federation of security policies across administrative boundaries. At the conclusion of both presentations and the question and answer period, the session will be opened to feedback from members of the audience on the DOCSec issues that are emerging or anticipated in their environments over the next 1-3 years.

"Intrusion Tolerant CORBA: Beyond Fault Tolerance"
Brent Whitmore, Network Associates - NAI Labs

Fault tolerant distributed object systems maintain minimal levels of functioning when some of their constituent objects fail. Typically, these systems replicate their operating objects and "fail-over" to spare objects when original objects break. Fault tolerant systems address accidental failures – not failures due to malicious attacks. Consider the situation where an intruder infiltrates a host and changes one of the system's object replicas, or a group of colluding replicas, so that the replicas start behaving in subtly incorrect ways. Many fault tolerant systems fail to detect these sorts of faults and continue to operate without warning. Some systems, termed "fault tolerant", do detect such attacks while continuing to operate correctly. NAI Labs, under contract to DARPA, is extending a CORBA object request broker to transparently replicate objects in a fashion that provides intrusion tolerant service to those objects. At DOCSec, we will present our work to date.

"Approaches to Addressing Federation of Security Policy"
Fred Dushin, Hitachi Software

Today's large organizations typically require centralized management of their user and policy databases, allowing security administrators within organizations to be in sole control of their own "authorization domains." On the other hand, many organizations today deploy distributed application components between organizations, where components of the same application are under control by separate administrative authorities. This distribution may involve invocations from authenticated clients in one authorization domain to targets in another, where these invocations may carry verifiable identity and privilege information about the client. A target's trust of the identity and privileges of a client from outside of the target's authorization domain may require federation agreements between these domains, under which identity and privilege information about a client is mapped into privileges under administrative control of the target's authorization domain. In this paper, we describe approaches to this sort of federation between authorization domains. Attention is paid to security and scalability issues, as well as sovereignty concerns that must be addressed in order to achieve assurance between organizations.

DOCsec 2001 PROGRAM COMMITTEE

Co-chairs: Richard Soley, Object Management Group

David Chizmadia, Promia

Members: Konstantin Beznosov, Concept Five Technologies

Carol Burt, 2AB

Bob Blakley, Tivoli

Janice Gilman, Object Management Group

Polar Humenn, Adiron

Gene Jarboe, Promia.

Carl Koebler, Object Management Group

Kevin Loughry, Object Management Group

Jishnu Mukerji, Hewlett-Packard

Jon Siegel, Object Management Group

David Warren, Hitachi Software