SIXTH WORKSHOP ON
DISTRIBUTED OBJECTS and COMPONENTS SECURITY

DOC*sec* 2002

March 18-21, 2002

Workshop Program

MONDAY – March 18, 2002

Tutorials

0900 - 1000 ***Survey of Threats and Countermeasures in Distributed Object, Component, and Service Architectures***
David Chizmadia, 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.

1000 – 1015 Morning Refreshments

1015 – 1215 ***UMLsec - Presenting the Profile***
Jan Jurjens, Software & Systems Eng. Department of Informatics, TU Munich

Security requirements are increasingly vital for networked software systems. Ad hoc development has lead to many deployed systems that do not provide relevant security requirements, since these are intrinsically very subtle. To aid the difficult task of developing security-critical systems, we describe a method for secure systems design based on the notation of the Unified Modeling Language. We present UMLsec, an extension of UML in form of a UML profile that allows the expression of security-relevant information within the diagrams in a system specification using the standard UML extension mechanisms. We provide criteria that evaluate the security of the system design, by referring to formal semantics of a simplified fragment of UML. Being able to formulate security concepts in the context of a general-purpose modeling language allows encapsulation of established principles of security engineering to avoid common vulnerabilities introduced by developers without in-depth training in security issues. The formal foundation of the approach allows the discovery of even non-obvious weaknesses that security experts may not detect without use of formal tools. We sketch a design process to be used with the UML extension and discuss applicability of the approach with examples from various application domains (such as Java security and electronic payment schemes).

1215 – 1315 LUNCH

1315 – 1515 ***Overview of .NET Web Services Security***
Konstantin Beznosov, Hitachi Computer Products (Quadrasis Security)

The tutorial provides an overview of the security architecture of Microsoft™s .NET-based web services. First it explains how .NET web services work and describes the main parts of the .NET web services infrastructure: IIS, ASP.NET, .NET CLR, and Windows OS and relationships among them. It proceeds with describing authentication mechanisms used, including IIS and ASP.NET authentication methods, third-party and application-level authentication. Protection of web service request and response messages is described afterwards, which is followed by explanation of the access control mechanisms available for web services developers. The tutorial is concluded with discussion of the audit capabilities available. Throughout the tutorial the relationships between web services and native OS security mechanisms are discussed.

1515 - 1530 Afternoon Refreshments

1530 - 1730 ***J2EE Security Tutorial***
Rakesh Radhakrishnan, Sun Microsystems

TUESDAY, March 19, 2002

Tutorials

0900 - 1200 ***An Overview of Distributed Security Architectures and Integration across CORBA, J2EE and Web Services***
Don Flinn & Ted Burghart, Hitachi Computer Products (Quadrasis Security)

With the rapid pace of product development focused on Web Services and the abundance of security technologies being deployed throughout the enterprise, integration of these disparate products and services becomes increasingly important in order to maintain a manageable level of complexity. This presentation gives an overview of the various security models in use today and illustrates the requirements for and development of an extensible, distributed framework that allows sharing of security components across multiple platforms and middleware technologies. Included are commonalities and differences between security technologies and approaches to mapping between them, as well as their implementation outside of their 'native' platforms.

1200 – 1800 Demonstration Area

1015 – 1030 Morning Refreshments

1200 – 1300 LUNCH

1300 - 1500 ***Security Assertion Markup Language Tutorial***
TBD

1500 – 1530 Afternoon Refreshments

1530 – 1730 ***Enforcement of Enterprise-Wide Security Policies with CORBASec***
Ulrich Lang, ObjectSecurity Ltd. & University of Cambridge

Enforcement of security policies in distributed applications is a complex and often error-prone task, especially if implemented enterprise-wide and for B2B. CORBASec provides a useful toolkit to secure distributed applications, but it has to be used correctly to ensure consistent and effective protection. This tutorial gives an introduction to the fundamental limitations of middleware security. It then explains how CORBASec and other related OMG standards, as well as other security systems, are designed to protect real-world distributed applications, and how they can be integrated into an enterprise-wide security architecture.

WEDNESDAY, March 20, 2002

0845 - 0900 ***Opening Remarks*** – David Chizmadia, Promia, Inc.
(Co-Chair – Program Committee)

0900 - 1000 ***Emerging Technologies I - Foundations for the Future***
Chair: David Chizmadia, Promia, Inc.

One sign of a robust and healthy technology is the existence of advanced research and development that provides the foundation for future technologies, products, and specifications. This first session on Emerging Technologies includes two presentations. The first is on a formal foundation for agreeing on the time in DOCSec architectures. The second discusses emerging standards and technologies for managing sensitive data in Web Services architectures.

Assured Trusted Time Stamping - Non-repudiation of Timely Interactions

Polar Humenn, Center for Systems Assurance Syracuse University,
Grzegorz Lewandowski, Syracuse University, & Dan Zhou, Florida Atlantic University

We will be presenting research being performed at the Center for Systems Assurance at Syracuse University, an NSA Center of Academic Excellence. This work looks at the formal security properties of time and time stamping documents. We analyze the properties of a time stamp service and provide a formal means with which to reason about the integrity, assurance, and trustworthiness of the electronic time stamp.

Sensitive Data Management in Financial Systems

Mike Gurevich, Inventigo Corporation & Peter Latscha, uGuard Corporation

This presentation identifies problems with current approaches in sensitive data management in financial systems and justifies the need for the following requirements: The subscribers are always in control of their sensitive data; Participating service providers have access to subscribers' data only under their supervision; Each data item is individually encrypted with a unique encryption key using encryption standards, and that key is re-created when access to the data is required.

1000 –1030 Morning Refreshments

1000 – 1800 Demonstration Area

1030 – 1130 ***Emerging Technologies II - Disrupting the Future***

Another sign of a robust and healthy technology is the emergence of entirely new ways to meet existing or emerging needs in more effective, secure, and believable ways. The very best of these technologies are considered disruptive because they change the ground rules for the way a domain does business. This second session on Emerging Technologies includes two presentations of such disruptive technologies. The first is an architecture for securely mobilizing application code. The second is an emerging open source operating system that has been carefully designed to be object-oriented, reliable, responsive, and verifiably secure.

Mobile Agent Security

Chris Rygaard, Aramira Corporation

Mobile agent technology has not been widely adopted primarily because of security concerns.
Recent advances have addressed most of these issues. This presentation will discuss techniques in mobile agent security including code assurance, itinerary assurance, monitoring and intervention, code signing, encrypted computing, and more. In addition, the limitations and risks of these approaches to security will be discussed.

Operating System Support for Secure, Distributed Object Systems

Jonathan S. Shapiro, Systems Research Laboratory, Johns Hopkins University,
Information Security Institute

Secure distributed systems can be built only from secure end systems, and ideally from secure, component-based end systems. This talk will identify some of the key requirements for a secure, component-based operating system. The talk will then briefly discuss the fusion of three pieces of ongoing work within the SRL: CapIDL, EROS, and PARAID. CapIDL is a CORBA-derived IDL for pure object systems. EROS (the Extremely Reliable Operating System) is a persistent, system built from the ground up using secure components and supporting secure, component-based applications. PARAID is a new storage subsystem technology that provides hands free storage administration for arbitrarily scalable stores. All of these technologies are either running now in the lab, or will shortly be deployed.

1130 – 1200 ***Keynote* – Congressman Pete Sessions**

(R- Texas) As a member of the House Republican Cyber Security Team, and a former top-level manager for Southwestern Bell Communications (SBC), Congressman Sessions has become a national leader on issues important to the Internet, cyber-security, telecommunications, and the increasing needs and demands of information technology.

1200 – 1300 LUNCH

1300 – 1330 ***Sponsor Presentation***

John Mullen, President & CEO, Promia, Inc.

"The Importance of Open Standards in Secure Distributed Systems”

1330 – 1500 ***Modeling & Requirements***

Chair: Teresa McLaughlin, NSA

In this session we explore the current approaches for standards based security requirements analysis and modeling. Our experts will present their strategies for developing a comprehensive and effective set of security requirements within the federal government and business domains. These projects are discussed in the context of implementation-independent Protection Profiles and Model Driven Architecture.

NIST/NSA Standards Based Security Requirements

Ron Ross, Director, National Information Assurance Partnership

The National Institute of Standards and Technology and the National Security Agency have recently agreed to cooperate on the development of standards-based security requirements in key technology areas necessary for the protection of Federal information systems and networks, including those comprising the critical infrastructure within the United States. The initiative focuses on developing security requirements for operating systems, database systems, firewalls, biometrics devices, smart cards, public key infrastructure components, network devices, telecommunications devices (including wireless), virtual private networks, web browsers, and intrusion detection systems using the international security standard Common Criteria (ISO/IEC 15408). This presentation will cover the long-term strategy and implementation plan for the NIST-NSA Protection Profile Development Project as well as the impact on the Common Criteria Evaluation and Validation Scheme.

Specifying Security Requirements in Business Domain Models in Model Driven Architecture

Ringo Ling, Hugo Latapie, and Vu Tran

Security requirements are gaining importance in software development and yet there is no formal way to express security requirements in business domain modeling. Very often, security requirements are specified at the wrong level of abstraction and interfere with domain modeling. This presentation presents our work to express security requirements within business domain models without such interference. In particular, our work supports the specification of security requirements, such as confidentiality, data integrity, authentication and auditing, at the computation independent business model level within the OMG's Model Driven Architecture. The security requirements are expressed as attributes and constraints of domain classes.

Model-Driven Security

Martin Buchheit, Bernhard Hollunder, & Torsten Lodderstedt
Interactive Objects Software GmbH

We investigate techniques for specifying security requirements in the context of Model-Driven Architecture (MDA). In particular, the following issues are considered in depth: Specification of an appropriate UML modeling style for role-based access control and authorization constraints; Definition of a projection that maps UML security models to the J2EE/EJB security architecture. We highlight the properties of the UML modeling style such as conciseness, scalability, and technology-independence and illustrate how the model information can be mapped consistently to a J2EE/EJB environment. To demonstrate the practicability of the concepts we show how our approach can be integrated into the MDA tool ArcStyler.

1500 – 1530 Afternoon Refreshments

1530 – 1700 ***Implementation Experiences***
Chair: Carol Burt, 2AB

Although there are a number of security technologies available, the task of constructing a secure solution is tedious. It requires that security technologies be selected and integrated into a framework that is usable by business software developers. It also requires that policies be carefully considered so that they can be maintained and administered with minimal impact. The presentations in this section focus on implementation experiences - how security technologies are being integrated and used in practice. They also provide practical advice for security implementers.

Defense Enabling Using QuO:Experience in Building Survivable CORBA Applications

Chris Jones, Partha Pal, & Franklin Webber, BBN Technologies

The Defense Enabling Using QuO (Quality Objects) presentation will describe a middleware-based technology to make DOC applications more resilient to certain kinds of attacks ('defense enabling') using adaptation and the services of various defense mechanisms. I will briefly describe the QuO middleware, which is at the core of technology and our experience of red-team validation of defense enabling. I will also summarize our experience in developing the defense-enabling technology and applying it to example applications, highlighting certain aspects of current DOC security that would help maximize the benefits of dynamic and adaptive defensive strategies.

Dynamically Authorized Role Based Access Control for Secure Distributed Computation - CORBA Common Secure Interoperability in Action

C. Joncheng Kuo & Polar Humenn, Center for Systems Assurance Syracuse University

We implemented a Role-Based Access Control (RBAC) policy using the OMG's Common Secure Interoperability Version 2 (CSIv2) and Authorization Token Layer Acquisition Service (ATLAS) standards. We use the ATLAS concept of an "authorization domain" to authorize the roles of East, West, North, and South neighbors to computation objects. Clients use CSIv2 and ATLAS to declare a role and transport the authorization for that role. Objects make access decisions based on the role within their authorization domain. One key benefit is that we can use an access control policy that is static leaving the dynamic nature of authorization relationships outside the scope of access control policy specification.

Intrusion Tolerant CORBA: An Update

Brent Whitmore, NAI Labs, Network Associates

At DOCSec 2001, we presented our plan to build a prototype intrusion tolerant CORBA object request broker. These kinds of ORBs go beyond fault tolerance to also handle servers that do not merely fail, but rather, become malicious. Since that presentation, we have been implementing our design. It integrates the work of other researchers - the TAO real-time ORB, a research Byzantine Fault-tolerant multicast protocol, and virtual voting machine technology. Along the way, we have encountered our full measure of challenges, obstacles, and sudden enlightenment. We will present our experiences, and some of what we have learned since last year's talk.

1800 – 2000 ***Workshop Reception** **hosted by*** **NSA & Promia**

THURSDAY, March 21, 2002

0900 - 1030 ***Case Studies in Security Architectures***

Chair: Polar Humenn, Center for Systems Assurance, Syracuse University

This session explores various ways in which security is architected and deployed in commercial environments. Environments where the interaction of applications is distributed and heterogeneous poses special problems. The presenters report on their experience with creating and using existing security technology to get their job done.

Securing a Global CORBA-based Logistics Support System at Volkswagen

Gerald Brose & Jörg Bartholdt, Xtradyne Technologies AG, & Olaf Haase Volkswagen AG

We present the security architecture developed for a CORBA-based logistics application used by Volkswagen to globally track supply items, such as car parts in shipping containers. In order to provide world-wide access at international company sites and logistic service providers, the application is made accessible both over the VW-Intranet and over the Internet. The overall application architecture is a successful combination of a CORBA security product for authentication and firewall traversal with regular packet filters, a commercial application server, databases, security libraries, and an open source CORBA implementation.

CCM based Secure Distributed Telecom Applications

Rudolf Schreiner, ObjectSecurity Ltd.

The presentation gives an overview of the current research on secure telecommunications applications with CORBA components. To motivate the topic, an introduction to typical telecom applications and service platforms, as well as their specific security issues, will be given. The presentation then explains why CCM could be an appropriate base for the development of telecom applications, and describes their security requirements. In addition, first practical experiences of implementing secure components and planned future work are presented.

NIIIP-SPARS: A Case Study in Secure Architectures for e-Business

Paul W. Horstmann, John Laurentiev, & John Schuetz, IBM Corp.

The National Industrial Information Infrastructure Protocols (NIIIP) Consortium has developed a set software protocols and components that enable manufacturers and their suppliers to effectively interoperate as if they were part of the same enterprise. The protocols have been instantiated on IBM hardware and software (WebSphere) as a Virtual Enterprise Server (VES). The NIIIP VES web-enables Business to Business Electronic Commerce. A leading example of the NIIIP VES is in the NIIIP Shipbuilding Partners and Suppliers (SPARS) Project. The SPARS project has focused on meeting the web and business requirements of U.S Shipbuilders that supply ships to the U.S Navy, and has had to deal with the usual security challenges (access control, authentication, encryption, etc.). In the presentation we will discuss how experience and the changing face of technology as well as security requirements have shaped the evolution of security implementation within NIIIP/SPARS.

1030 – 1045 Morning Refreshments

1045 – 1145 ***Web Services Security – Part I***
Chair: Bret Hartman, Hitachi Computer Products (Quadrasis Security)

Web Services use HTTP-compatible protocols to allow interoperation of many different software applications and systems from different vendors. Web Services make it possible for applications to interoperate, but they complicate security by spanning multiple processing domains across corporate or line of business boundaries. Our first talk in this session proposes a security platform for the emerging Web Services environment. Our second talk concentrates on the Security Assertion Markup Language (SAML), an important specification that will be the basis of many new Web Services security products.

IONA Enterprise Security Platform
Igor Balabine IONA

This presentation will describe the IONA Security Platform (iSP). The purpose of the security platform is to provide authentication, authorization and Public Key Infrastructure (PKI) services implemented by specialized systems (e.g. Netegrity Site Minder, Windows Domain, Active Directory, Entrust Authority, etc.) to applications and services. In general all legacy applications can use iSP as a medium for integrating with enterprise-wide authentication, authorization and PKI services.

Distributed Services Security using the SAML
Krishna Sankar, Cisco Systems

Security Assertions Markup Language initiative by OASIS has developed a set of XML vocabulary, request-response and bindings (SOAP & Browser) for exchanging assertions across distributed services. The assertions include Authentication Assertion, Authorization Decision Assertion and Attribute Assertion. This paper describes the various authorities and the assertions that flow between them. The paper also will describe a few end-to-end use cases, which show the assertion exchange interactions between distributed web services - inside security domains (for example inside a corporate firewall) and intra-security domains (for example between trading partners in a dynamic trading partner network across the Internet)

1145 – 1245 LUNCH

1245 – 1345 ***Web Services Security – Part II***

Our session exploring Web Services security continues with discussions on two supporting technologies: GSS-API and Enterprise Portals. The first talk discusses how Web Services may be built on top of a GSS-API infrastructure, which provides cryptographic-based support for secure sessions. The second talk describes the concept of an Enterprise Portal, a popular approach for integrating applications, and discusses the security challenges of this environment.

Using GSS-API to Secure Web Services
Jan Alexander, Systinet

In this presentation we will summarize our experience using the GSS-API security infrastructure to build a security framework for Web Services in Systinet's Web Applications and Services Platform (WASP) product line. We will describe the integration of the WASP Security API with two GSS-API mechanisms (Kerberos and SPKM) and also with other authentication systems, including SSL, HTTP Basic Authentication, and SOAP Digest Authentication. We will demonstrate the advantages of using GSS-API over these other systems

Securing Your Enterprise Portals
Tushar K. Hazra, EpitomiOne

An Enterprise Portal (EP) offers the most efficient and effective way of integrating existing and new business applications to the Internet. Since the Internet is the foundation for portals, the need for security has become paramount to the continued existence of the enterprise. Without effective security measures, there will be a potential for breach of contract, intrusion, or theft of intellectual property. In this session, we first review the challenges, issues, risks, and concerns faced in developing a secure EP environment. We then explore the available options of using security technologies and how most solution providers handle the situation. Finally, we present a component-based approach in integrating security measures or solutions with the other components of the EP.

1345 – 1400 Afternoon Refreshments

1400 – 1600 ***Vendors Panel***
Chairs: Richard Soley, Object Management Group
Jishnu Mukerji, Hewlett-Packard

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

Panelists:
Igor Balabine, IONA
Carol Burt, 2AB
Bret Hartman, Hitachi Computer Products (Quadrasis Security)
Bernhard Hollunder, Interactive Objects Software GmbH
Anne Thomas Manes, Systinet
Rudolf Schreiner, ObjectSecurity, Ltd.

SIXTH WORKSHOP ON DISTRIBUTED OBJECTS and COMPONENTS SECURITY

PROGRAM COMMITTEE

Co-chairs:
Richard Soley, Object Management Group
David Chizmadia, Promia, Inc.

Members:
Ted Burghart, Hitachi Computer Products (Quadrasis Security)
Carol Burt, 2AB
Janice Gilman, Object Management Group
Bret Hartman, Hitachi Computer Products (Quadrasis Security)
Polar Humenn, Adiron
Gene Jarboe, Promia, Inc.
Ulrich Lang, ObjectSecurity Ltd. & University of Cambridge
Kevin Loughry, Object Management Group
Teresa McLaughlin, National Security Agency
Jishnu Mukerji, Hewlett-Packard
Jon Siegel, Object Management Group
Andrew Watson, Object Management Group