Panel Title: The Current State of the CORBA Security Market

Panel Chair: Edward A. Feustel, Institute for Defense Analyses
Panelists: Bob Blakley, DASCOM Inc.
David M. Chizmadia, Computer Science Corporation
Bret Hartman, Concept Five Technologies
Polar Humenn, Adiron

Session Abstract

by
Edward A. Feustel
Institute for Defense Analyses

The OMG is a consortium with over 800 members drawn from Industry, Government, and Academia worldwide. Its purpose is to establish specifications that permit the development of object-oriented distributed computing. First OMG developed its CORBA specification in early 1991. Revisions to the service interface specification followed that clarified the specification, making it possible for implementers to begin work on it. The revision version in February 1999 is 2.3. Numerous implementations have been developed. The specification has had substantial influence in Distributed Computing with many adoptions by commercial and government interests.

This specification gave reference to a set of fundamental services including the security service and a set of management services. The OMG promulgated a first version of its specification for security services in 1993. The current version is 1.5 and a revision task force has been chartered to do version 1.6. The current version is quite complex with a specification of over 350 pages.

The security service may be implemented at one of three strengths: Level 0; Level 1; and Level 2 where Level 2 is the most elaborate, containing an extensive set of optional functionality. In February, one firm had implemented Level 1, two were working on Level 2, and one firm was shipping a Level 2 product (although not with all options). It is expected that several implementations of Level 2 security services will be shipping in October of 1999.

Interoperability of security services is paramount in a multi-vendor or heterogeneous environment. The OMG recognized this fact and as an early revision specified the Common Security Interoperability (CSI) Specification that gives a protocol for interoperability between Object Request Brokers. At the time of this writing, no vendor was planning to implement this protocol. Vendors were beginning to plan a second version of CSI that was to be more to their liking.

The panel will provide a snapshot of the products and functionality that are shipping in October 1999. They will indicate what features of the security specification have been well specified and which ones still have ambiguities "left to the implementers". They will describe the way in which their products achieve interoperability and the way in which they may be managed. They will describe the "interesting research topics" that have arisen as they have attempted to achieve efficiency and interoperability and indicate how functionality of the specification must be changed if well designed and efficient security services are to be provided to the general community.

.

Position Paper

By
Bob Blakley, DASCOM Inc.

The CORBAsecurity specification was first issued in February 1996. After a little more than three years and several revisions, the functionality it describes is now available in implementations from several different vendors. Most of the leading ORBs are supported by CORBAsecurity implementations offering most, and in some cases all, of the CORBAsecurity level 2 functionality. Some ORBs are supported by several CORBAsecurity implementations, from several security vendors.

DASCOM's CORBAsecurity implementation is called Intraverse for CORBA, or IVcorba for short. It provides CORBAsecurity level 2 functionality and most of the CORBAsecurity level 2 programming interfaces.

The IVcorba implementation supports ORBIXweb and Visibroker ORBs, and provides secure interoperability between these ORBs. The IVcorba functionality has also been incorporated into IBM's ComponentBroker ORB, in a slightly modified form.

IVcorba is built using components of DASCOM's Intraverse technology, and provides authentication, cryptographic message protection, authorization, and audit functionality.

While many vendors, including DASCOM, offer full-featured CORBAsecurity implementations, challenges remain. DASCOM has demonstrated that it is possible to build a CORBAsecurity implementation which will allow multiple vendors' ORBs to communicate securely, but the challenge of getting different CORBAsecurity implementations to interoperate is still largely unmet.

Manageability of CORBAsecurity policies is still problematic also. While domains provide a nice, scalable management abstraction, management of domain membership has not yet been addressed in any OMG specification.

Furthermore, there are policies, particularly access control policies, which can't be enforced using the traditional subject-object-action model on which the CORBAsecurity DomainAccessPolicy is based. OMG has recently adopted the RAD proposal to address some of these deficiencies.

Finally, implementations of the CORBA Non-Repudiation service have yet to appear. Non-Repudiation is more than just a digital signature, as this panel will explain.

Panel Position

"What, exactly, is CORBAsec?"

by

David M. Chizmadia, Computer Science Corporation

Mr. Chizmadia is the co-chair of the OMG Security Special Interest Group (SecSIG), which is the focal point for security issues within the OMG. He will present a VERY short overview of the CORBA Security Service Specification (CORBAsec). The goal of this overview will be to provide sufficient context for the subsequent presentations, which will describe specific products that conform to one of the CORBAsec compliance points. He will also provide a review of on-going security initiatives within the OMG and the timeframe for completion of those initiatives. This will provide a context for the vendor descriptions of their future product plans.

Panel Position

The Status of OMG CORBA Security Implementations

by

Bret Hartman, Concept Five Technologies

The Concept Five *C5Sec* product implements a suite of security services based on the Level 2 security functionality specified in the *OMG CORBA Security Specification.* C5Sec was developed from the ground up to be portable across different middleware platforms, to be independent of the underlying security infrastructure, and to provide cross-ORB interoperable security.

C5Sec is available already integrated with Iona's Orbix (as Orbix Security 3.0), Hitachi's TPBroker, and Inprise's Visibroker ORBs. C5Sec provides full cross language functionality for both C++ and Java applications. Supported operating systems are NT, Solaris, and HP-UX.

C5Sec implements a facility to secure CORBA applications providing identification and authentication, authorization/access control, security of communication, delegation, and auditing capabilities. C5Sec automatically enforces the security policies "behind the scenes" for each object invocation. C5Sec can be used to provide security for both security-unaware and security-aware applications.

C5Sec provides Level 2 APIs that permit fine-grain access control, audit, and delegation policies. All security policies are stored in an LDAP directory server to support large-scale deployments, replication, and performance. Level 2 APIs allow developers to define user security attributes such as roles and groups, extensible rights, and security policy domains. The Level 2 APIs provide the ability to define and manage CORBA security services down to the object instance level. A system administration GUI along with batch policy definition tools build on the Level 2 administrative interfaces. The administration tools walk administrators through the complex process of setting up and testing the validity of CORBA security policies.

C5Sec provides interoperability via the SSL protocol. C5Sec relies on the SSL implementation provided by the ORB, i.e., SSLeay in Orbix and the SSL Pack in Visibroker and TPBroker. C5Sec provides CSI Level 2 features (i.e., identity and privilege based policies with controlled delegation) by using a public-key privilege attribute certificate (PAC) on top of the SSL implementation. CSI Level 2 interoperability based on a PAC and SSL is not yet an OMG standard. Concept Five is working with other vendors on an improved interoperability standard for the CSI Version 2 RFP that includes CSI Level 2 features based on a standard PAC and SSL.

Panel Position

Toward an Interoperable *and* Portable CORBA Security Specification

by

Polar Humenn, Adiron

The CORBA Security Specification started as a framework on how to build a security service for a CORBA compliant ORB. Interoperability was limited to the wire protocol (SECIOP) and varying GSS-API defined mechanisms. The Security Level 1 and Security Level 2 interfaces gave applications the ability to create their own access and auditing controls. However, the interfaces were found to have many interpretations, which leads to non-portable code and a coherent system was limited to the same implementation and therefore interoperability was not achieved.

Over the past year, speed has picked up on revisions to the Security Specification toward portable code and interoperability. The portable code requirement is driven by companies wanting to supply third party (i.e., non-ORB vendor) security policy tools for the CORBA Security Service. The interoperability angle is just necessary. Major inroads have been made in the last and current revisions of the security specification to achieve both goals, but we are not there yet. An RFP, known as CSIv2 is currently in the works at the OMG to provide a separation of the concepts of authentication mechanisms and authorization mechanisms to yield a better hope for interoperability. This RFP will also give a more stringent semantics to the Security API yielding more portable code that uses the security service.

Adiron provides a Java library based ORB called "ORBAsec SL2" that uses the SECIOP-GSS-Kerberos and SSLIOP standards underneath the Security Level 2 API. It also supports Security Replaceable module, in which third party replacements for any GSS based authentication and cryptographic mechanism can be added to the SECIOP protocol. The programmer is free to write access control code in the application using the Security Level 2 API. It is Adiron's hope to have ORBAsec SL2 be the 'interoperable' secure ORB.

Biographies

Edward Feustel, Panel Chair, has S.B. and S.M. degrees from Massachusetts Institute of Technology, Cambridge, Massachusetts and M.A. and Ph.D. degrees from Princeton University, Princeton, N.J., all in Electrical Engineering. He was a Research Fellow at California Institute of Technology, Pasadena, California. He was an Assistant and Associate Professor of Computer Science at Rice University, Houston, Texas. He was a Senior and Principal Consultant at Prime Computer, Framingham, Massachusetts. He is a Research Staff Member at the Institute or Defense Analyses in Alexandria, Virginia where his current interests include security and distributed object computing, He has been Technical Liaison to the OMG for IDA since 1992.

Bob Blakley, Panelist, is Chief Scientist at DASCOM. Before joining DASCOM, he was IBM's Lead Security Architect. He worked at IBM for 9 years; during that time he had security architecture and design responsibility for OS/2, the IBM OS/2 LAN Server, IBM's OS/2 and AIX DCE offerings, the LAN Distance remote LAN access product, and IBM's ORB technologies, including Distributed SOM and Component Broker. In addition to his product design responsibilities, Bob led the IBM Security Architecture Board and was the IBM representative to the Open Group Security Program Group where he served for two years as the chair of the OSF DME/DCE security working group, and edited that group's security requirements document (OSF RFC 8.1). Bob also served as IBM's security representative to the Object Management Group (OMG). He was the principal designer of IBM's proposal to OMG for an Object-Oriented Security Service. He represented IBM in the OMG CORBA Security standardization effort, and co-edited the CORBA Security standard adopted by OMG in 1996. Bob was the original editor of the Open Group PKI working group's "Architecture for Public Key Infrastructure" document, which was originally published as an Internet draft and is now being revised by the Open Group. Bob is a frequent speaker at software industry and software security conferences. He has delivered invited addresses at the RSA Conference, Networld+Interop, GUIDE, the Burton Group Catalyst Conference, the Open Systems Security Symposium, and the Mergent Users' Conference. He has participated in panel discussions at several of these conferences, and has been an invited participant in panel sessions at GUIDE, The National Information Systems Security Conference, and the IEEE Security and Privacy Conference. Bob co-chaired the ACM New Security Paradigms Workshop in 1997 and 1998, and served on the Program Committees for several industry and academic conferences, including the NSA/OMG Distributed Object Computing Workshop, IEEE Security and Privacy, and ISOC Network and Distributed Systems Security (NDSS). Bob has performed software security consulting engagements for several of IBM's customers. Bob has been involved in Cryptography and Data Security design work since 1979 and has authored or co-authored 7 papers on cryptography, secret-sharing schemes, access control, and other aspects of computer security. He holds 8 patents on security-related technologies. He received an A.B. in Classics from Princeton University, and M.S. and Ph.D. degrees in Computer and Communications Sciences from the University of Michigan.

David Chizmadia, Panelist, joined the US NSA as a PC help desk technician after receiving his BS in Computer Science and Mathematics from Towson University in 1984. He then moved into the National Computer Security Center (NCSC), where he was a member of the team that pioneered commercial product evaluations to the Trusted Network Interpretation of the US TCSEC. His next position was in the Standards and Guidelines division of the NCSC, where he authored the "Guide to Writing the Security Features User's Guide" and later served as the technical editor of the US Federal Criteria for IT Security. He went on to become the US Technical Liaison to the UK ITSEC Scheme, where he had the opportunity to compare the US and UK approaches to the conduct and control of commercial computer security product evaluations. In June of 1996, he returned to the US and his current position as technical architect of the

Distributed Object Computing Security (DOCSec) research program in NSA's Office of INFOSEC Computer Security Research. In this position, he has been a member of the OMG since September 1996, originator and co-chair of three DOCSec Workshops, and co-chair of the OMG Security Special Interest Group since June 1998.

Bret Hartman, Panelist, is Chief Security Architect for Concept Five Technologies, Inc. He is responsible for defining the overall security architecture for the Concept Five product line, and works closely with Concept Five partners, including Hitachi and Iona. Mr. Hartman has over 20 years of experience in a variety of security technology positions in industry and government. He has been a long-time participant in Object Management Group (OMG) activities, and is a co-author of the Common Object Request Broker Architecture (CORBA) Security specification along with representatives from several major computer vendors. He has provided security architecture consulting to a number of commercial clients, including JavaSoft (Sun Microsystems), Tandem, 3Com, State Street Bank, General Motors, British Telecom, and DHL. Prior to Concept Five, Mr. Hartman co-founded a venture for building security policy management tools and providing distributed object security consulting services. Mr. Hartman received a Bachelor of Science degree from the Massachusetts Institute of Technology and a Master of Science degree from the University of Maryland

Polar Humenn, Panelist, is founder and principal owner of Adiron, a CORBA Security company. He is Adiron's chief representative to the OMG. He is currently the chair of the OMG's Security Revision Task Force, the body that performs revisions to the current CORBA security specification. His research interests lie in formal methods and security policy for distributed systems and is heavily involved with the Network Security Research Group at Syracuse University. He is also Syracuse University's representative to the OMG.

Audience Background

The audience should be familiar with security concepts. Ideally they should understand the difficulties encountered in specifying and designing portable and interoperable specifications and products. The panel sessions will describe how these two features are being addressed in an object-oriented, distributed computing environment.