Report on the 17^{th} IEEE Symposium on Security and Privacy May 6-8 1996, Oakland, CA

Christoph L. Schuba
COAST Laboratory
Department of Computer Sciences
Purdue University
1398 Department of Computer Sciences
West Lafayette, IN 47907–1398
schuba@cs.purdue.edu

Mary Ellen Zurko
Open Group Research Institute
11 Cambridge Center
Cambridge, MA 02142
zurko@osf.org

1 Introduction

The 17^{th} IEEE Symposium on Security and Privacy was held at the Claremont Resort in Oakland, CA on May 6-8, 1996. This one-track symposium was sponsored by the IEEE Computer Society Technical Committee on Security and Privacy in cooperation with the International Association of Cryptologic Research (IACR).

The symposium was well attended with about 200 registered attendees. Monday consisted of four sessions, two of which were panel discussions that addressed the activities of the object management group's CORBA security standard, and goals for computer security education. The refereed paper session held Monday discussed new results in covert channel analysis. The final session of the day was composed of sixteen five-minute research talks. The official program closed with a reception and poster session.

Tuesday consisted of four sessions, the first was a panel discussion on medical information systems. The other sessions covered topics in security protocols, database security, and biologically inspired topics in computer security. Eight additional presentations focused on modeling and networks.

The focus of the symposium has shifted in the past few years, the emphasis moving from military security in the 80's to commercial security in the 90's. Rich Simon, a conference attendee in the mid-80's, pointed out that there was not a single military uniform to be seen this year (a big change). Conversely, Dan Wallach, a Princeton graduate student and co-author of the Java paper, mentioned he had never seen so many suits in one room. The program addressed application areas such as electronic commerce and medical information systems. Additionally, last year's experiment, with a complete session consisting of five-minute research talks, was so successful that the experience was repeated. Sixty-seven submissions for refereed papers, four panel proposals, and the diligent work of the program chairs and referees resulted in an interesting and diverse symposium program.

2 Monday

2.1 Panel: Object Management Group CORBA Security Standard; moderated by Terry Benzel (TIS)

The participants included Bob Blakley (IBM), Richard Soley (OMG), Bret Hartman (Black Watch Technology), and Roger Shell (Novell). Terry Benzel's current project is exploring the use of CORBA to interoperate between trusted and untrusted systems.

Soley began the presentations with an overview of the OMG. He explained the CORBA architecture and goals of the OMG standards. He emphasized that objects are only the tools to solve problems in information access, particularly in terms of interoperability between users and any information source.

Bob Blakley gave an overview of the CORBA security standard. He reviewed four issues in detail: authorization management scale, object semantics, forms of delegation, and non-repudiation services. The first problem is scale; there are thousands of users and millions of objects. Users have privilege attributes, which are name/value pairs. Some attributes such as groups, roles, and clearances are defined, but attributes are also extensible. There is a defining authority for privilege attributes. The second problem is that objects are not structured any way in advance. Objects must be grouped into domains which have an access policy that maps privilege attributes to granted rights. Domains can be implemented in many different ways. A similar problem had to be addressed with object operations, since objects are heterogeneous and can have many operations. Classes are mapped to required rights. Operations such as 'get', 'set', and 'admin' are defined a priori, and the set is extensible. Finally, a policy maps privilege attributes to required rights, and the access control decision engine compares required and granted rights. Two forms of delegation are supported: a simple impersonation model (delegate all my attributes) and a compound delegation model that allows individual attributes to be delegated. There is a standard non-repudiation interface. Object reuse protection and system integrity are up to implementors. CORBA does produce guidelines for high integrity systems and for auditing. The audit guideline is motivated by auditable events occuring below the object code, e.g., in DCE.

Hartman discussed building a trustworthy CORBA system. He concentrated on the question of who wants assurance, what the vulnerability trade-offs in distributed object systems are, and what conformance with the CORBA security standard means. The specification describes how to build a secure ORB, not how to give security services to users. Having a good API alone is not enough, the internal integrity of the system is critical. The security standard guidelines encourage flexibility and offer different levels of assurance. Within CORBA, there is a common security framework. Distributed object systems pose a complex security problem. They are complex to administer, dynamic systems are hard to analyze, diverse environments lead to unjustified trust, disjoint policy domains do not interoperate well, and layered security mechanisms require complex analysis. Hartman pointed out that the importance of key security issues differ across areas: the main concern of healthcare is with the integrity of patient records; the military cares strongly about confidentiality; and electronic commerce is very interested in non-repudiation. Vendors of CORBA security compliant systems have to produce a conformance statement, describing the security relevant features of their product. Hartman claims this procedure allows customers of such systems to make informed decisions about the security of their systems.

Roger Shell criticized the CORBA security standard on several points. First, it is

not clear what the standard is trying to accomplish. It is obviously infeasible to solve all security related problems, but there is no concrete statement in the specification that makes clear what an important subset to be solved is. Shell was concerned that users would have problems understanding what they get when purchasing CORBA security compliant systems. He also pointed out that there was very little reference to the existing body of knowledge in security (a minor theme that would turn into a full chorus at the Java evening discussion). For Shell, the relationship between security services and a more classical view of security as protection against efforts to circumvent controls was not clear. What set of security services and mechanisms is sufficient for protection?

During the following discussion, Blakley pointed out that the OMG had not wanted to exclude any vendor, nor any existing standards. That is why the specification is so large and unfocused. Vendors choose what subset of security services they considered sufficient. In the competition in object-oriented systems, security might not be the determining factor. When questioned about the maturity of the system, the audience was told "not to use this system for air traffic control this year". Another important point raised was that implementations are not interoperable, and the specification does not ensure interoperability.

2.2 Covert Channels; chaired by Sylvan Pinsky (NSA)

The first paper presented by Ira S. Moskowitz (NRL) was "An Analysis of the Timed Z-Channel" (joint work with colleagues Stephen J. Greenwald and Myong H. Kang). This work is one of the first contributions in literature on noisy covert channel analysis. The goal is to devise a closed form for the capacity of noisy covert timing channels.

Todd Fine (Secure Computing Corporation) presented "Defining Noninterference in the Temporal Logic of Actions". His motivation was to provide an intuitive statement of noninterference as well as conditions appropriate for analysis. Noninterference is a technique for analyzing a system model for covert channels.

2.3 Panel: Goals for Computer Security Education; chaired by Cynthia Irvine (Naval Postgraduate School)

Panelists were Stephen F. Barnett (NCSC), Jim Schindler (HP), Leslie Chalmers (Wells Fargo Bank), Karl Levitt (UC Davis), and Roger Shell (Novell). Irvine's motivation, as an educator of individuals trained for security work, was to understand what the employers are looking for.

From an employer's prospective, Stephen Barnett examined the kind of training today's security practitioners require. In particular, Barnett discussed the questions: what are people currently educated to do, what should be included in a security curriculum, and what can industry do to help. He stressed the fact that not only security officers, product designers, and educators need to be educated, but also the consumers and users of computer technology.

Jim Schindler based his analysis of the need for security education on a central theme: Change. Technology is changing, computer paradigms are changing, and security requirements are changing. He considers security education a must for a much larger community than security professionals, e.g., vendors, end-users, managers, and executives. Electronic

commerce was his example for the latest trend in computer technology and the need for strong security.

Leslie Chalmers pointed out that there is a need for credentials for security professionals without special university degrees. At Wells Fargo, junior security people have jobs that require little skill. The more senior and professional employees are assigned higher responsibility projects. Chalmers discussed the need for knowing the business, consulting skills, communication skills, and sales skills. Security is only important and viable as long as it supports the business goals. Chalmer mentioned that the banking security crowd rarely overlaps with the traditional audience of the IEEE symposium.

Roger Shell stated that he was not impressed with what education provides. He needs people who can think and grow, as well as having a grounding in the fundamentals. Both Shell and Chalmers referred to the problems of people trying to work in security without any background or reading on the subject. There is a phenomenon that people think they know security, but they really do not. This occurs, because failure is not apparent.

Karl Levitt emphasized the need for additional support in security education at the undergraduate level, in particular the need for a good and current textbook. He (together with Ross Anderson) stressed the role of educational institutions as providers of science, not specifics. Particular technical knowledge must come from different sources.

The panel agreed that it is desirable to provide security education to a broader audience than only computer science students. However there was no consensus on the question of the appropriate place for this topic in an already filled undergraduate curriculum, or how to make time for it. Additionally, the ethics of teachers encouraging students to try to break software and systems as part of learning about security was briefly discussed.

2.4 Five-minute Research Talks Session; chaired by John McHugh (Portland State University)

This type of session was introduced last year. During the many presentations one can easily find out about early or on-going research. Like last year, no submission was rejected. The quality varied, though it was up from last year. A listing of the titles and authors follows.

- "SSGP: the Sleepy Security Gateway Protocol for IPSEC" by Shyhtsun F. Wu (NC State University)
- "Security for Mobile Agents" by Vipin Swarup (MITRE)
- "Browsing the Web Safely with Domain and Type Enforcement" by Daniel F. Sterne, Terry V. Benzel, Lee Badger, Kenneth M. Walker, Karen A. Oostendorp, David L. Sherman, Michael J. Petkac (TIS)
- "An Integrated Security Analysis Process with Knowledge-Based Tool Support" by R. Neely, J. Freeman (CTA)
- "A Multimedia Threat in Computer Networks: Subliminal Message" by Yuko Murayama (Hiroshima City University)
- "Genetic Algorithms, a Biologically Inspired Approach for Security Audit Trail Analysis" by Ludovic Me (SUPELEC)

- "Defining an Adaptive Software Security Metric from a Dynamic Software Fault-Tolerance Measure" by Gary McGraw, Anup Ghosh, Jeff Voas (RST Corp.)
- "The Specification of Static Security Policy in the Critical System Logic (CSL)" by Scott Knight (Royal Military College of Canada)
- "A Framework for MLS Interoperability" by Myong H. Kang, Judith N. Froscher, Ira M. Moskowitz (NRL)
- "Subject's Interpretation of Objects on Lower Security Levels" by N. Jukic, S.V. Vrbsky (University of Alabama)
- "A Safety-Progress Composition Principle" by Heather M. Hilton, E. Steward Lee (University of Toronto)
- "Access Control to Multimedia Services based on Trusted Third Parties" by Jose Guimaraes, Jean-Marc Boucqueau, Benoit Macq, Augusto de Albuquerque
- "Building Chinese Walls in BSD UNIX" by Simon Foley (University College Cork)
- "Communicating Security Agents" by Robert Filman, Ted Linden (Lockheed)
- "Towards the expression of security policies at the application level" by Christophe Bidan, Valerie Issarny (IRISA)
- "Server-Supported Signatures: a New Non-repudiation Concept" by N. Asokan, G. Tsudik, M. Waidner (IBM)

3 Tuesday

3.1 Domain Specific Security; moderated by Deborah Cooper (Cooper)

"Security for Medical Information Systems" was the anchor paper by Ross Anderson (University of Cambridge). It was followed by a panel, chaired by Deborah Cooper, with Don Biggar (Unisys), Thomas C. Rindfleisch (Stanford University), and Bruce Sams, a retired MD.

Anderson's work was based on the British medical system. The United Kingdom government's initial approach at a security policy for computerized medical data was similar to multi-level security. This was unworkable since even low level data such as contract data can be sensitive, e.g., if it deals with psychiatric work. Anderson's approach assumes that the main threat is from insiders, i.e., someone with legitimate, but limited access to patient records, and that the inability to locate and access all of the distributed paper records is a good defense. Therefore, aggregation of data must be controlled. Anderson discussed nine principles that define his security policy model. One of the guiding principles is that access to health information is under the control of the patient, or the general physician acting as the patient's advocate. Access control lists are the mechanism of choice. Another interesting principle controls aggregation of medical information. Essentially, the patient must give his consent before a party involved that already has access to a large number of records is allowed access to the patient's records.

Rindfleisch reviewed the flow of personal health information in the United States. He pointed out that in the U.S. the situation is more complex compared to the U.K. This complexity is because of legitimate interactions of direct patient care, social uses, support activities, and commercial uses. There is a patchwork of policies, many of which are contradicting each other. Medical information access is regulated on a state, not federal basis, e.g., 28 of 50 states allow patients to access their own medical records. The stewardship of medical information in the U.S. is quite different from the U.K. and other European countries. There are operational difficulties with managing access control lists.

Don Biggar stated that U.S. medical records are already in an electronic format stored on mainframes. He perceives privacy concerns as a far more global problem than discussed by the previous panelists.

Bruce Sams stressed the importance of the privacy problem for medical records and applauded research done in this area. He pointed out that in spite of the tremendous benefits of electronic storage and transmission to facilitate better healthcare and research, there are great dangers. Even though healthcare costs are often higher on the priority list than privacy, anonymity of medical information for research purposes, and privacy in general must be guaranteed by any technical solution proposed.

There is a pilot experiment conducted by the Department of Defense in Hawaii whereby patients carry their own medical records at all times. The panel recognized that access to medical information as a basis for warfare is a tremendous threat.

Rindfleisch concluded that computer systems are not ready for prime time in the healthcare system, simply because they are less usable than paper. For many, security is an even less important concern than usability. In spite of many years of research at building a usable and secure system himself, he has not yet succeeded.

3.2 Protocols; chaired by Michael Reiter (AT&T)

The first presentation was "Entity Authentication" by Dieter Gollmann (University of London). Gollmann investigated the question why the definition of authentication seems to be such a hard problem. There is a translation problem between "human" meaning of authentication, and the meaning of authentication in cryptographic protocols. He advocated using the language of communications protocols instead of human-to-human authentication when discussing these protocols.

A second paper, "A Fair Non-repudiation Protocol", was also presented by Gollmann. This protocol uses a trusted third party to assure that neither party in the non-repudiation protocol has an advantage over the other.

"Limitations on Design Principles for Public Key Protocols" by Paul Syverson of NRL took a cautionary look at the design principle approach to cryptographic protocols. He examined a handful of design principles and gave apparently secure protocols that contradicted those principles. Syverson recommended checking the design motivations when using guidelines, then checking any violated principles for problems.

3.3 Databases; chaired by Mary Ellen Zurko (OSF)

The session began with "Ensuring Atomicity of Multilevel Transactions", presented by Indrakshi Ray (George Mason University) (joint work with colleagues Paul Amman and Sushil

Jajodia). The technique decomposes multilevel transactions into single level transactions, ordered from low to high. These transactions are then analyzed (for now, by hand) to ensure that interleaving will produce correct results.

"View-Based Access Control with High Assurance", written by Xiaolei Qian (SRI), was presented by Teresa Lunt (ARPA). Specifying a level on a view is very easy and natural, and leads to content-based access control. However, the query processor is the bulk of the code in a database management system. This amount of code is considered too large to be part of the trusted computing base in a high assurance environment. In addition, there are complications from overlapping views and from overclassifying data. The technique described in the paper addresses two problems of multilevel secure databases: safety and assurance. It describes a polynomial-time label compilation algorithm that transforms view-level labeling to tuple-level labeling. A further contribution of the paper are proofs that the lowest classification and minimal upgrade problems are NP-complete.

"Supporting Multiple Access Control Policies in Database Systems" was presented by Pierangela Samarati of the University of Milan (joint work with colleague Elisa Bertino and Sushil Jajodia, George Mason University). Their work uses a Directed Acyclic Graph of group memberships to determine authorization based on explicit positive and negative authorizations. An authorization can be strong or weak. Conflicting strong authorizations are not allowed, strong authorizations override weak ones, weak authorizations lower on a single group path override those higher up, and conflicting authorizations deny access.

3.4 Biologically Inspired Topics In Computer Security; chaired by Lee Benzinger (Lockheed)

Stephanie Forrest (University of New Mexico) presented the first paper titled "A Sense of Self for UNIX Processes" (joint work with colleagues Steven A. Hofmeyr and Anil Somayaji, and Thomas A. Longstaff, CERT). Forrest proposed a simple method for anomaly detection. The method is based on a preliminary definition of self for UNIX processes (statistical collection of short sequences of system calls) and the detection of previously unseen behavior (a sequence of unseen system calls). This approach inherits all the well understood shortcomings of anomaly intrusion detection. Forrest presented encouraging first results of this work in progress.

Secondly, Patrik D'Haeseleer (University of New Mexico) described "An Immunological Approach to Change Detection: Algorithms, Analysis, and Implications", (joint work with colleagues Stephanie Forrest and Paul Helman). D'Haeseleer's work also addresses the question of how to detect changes. His work takes an immunological approach by generating a set of detectors as the complement of detectors that detect "self". The generation of detectors is more efficient than previously published algorithms and runs in linear time. A further advantage of this approach is the fact that the detectors are in fact distributable.

"Cryptovirology: Extortion Based Security Threats and Countermeasures" Adam Young (Columbia University), (joint work with Moti Yung, IBM) The approach uses encryption to hide information, and then to extort money or goods from the victims. The point was that encryption could be used as a force for evil as well as good. Good backups are the best defense.

3.5 IEEE Technical Committee Meeting

Debbie Cooper mentioned that the IEEE web site can now be used to add and change membership information (http://www.computer.org/). The Cipher security newsletter recently began a research project registry. After discussion about whether Cipher could support information on job hunting, the group settled on researching if a registry would be enough help to college students looking for a job. Carl Landwehr requested assistance to put together a reader's guide (list of security-related publications).

A discussion of alliances with other conferences developed. The Oakland conference attendance averaged 200 attendees over the last 3 years. The break even point is about 176. At the peak it got over 300 attendees ('89). The number of submissions has been going down, and this caused concern. Many people postulated that the growing number of security conferences has begun to dillute their quality. An alliance with the ISOC symposium on network and distributed system security will be discussed at future meetings.

Sushil Jajodia suggested the addition of tutorials. Several people liked the idea of advanced tutorials in areas to cross-fertilize their research. (Jajodia also suggested a vendor track, for which he received strong criticism). Hilarie Orman brought up the issue of electronic publishing. It is highly likely that next year's proceedings will be available online.

3.6 Secure Mobile Agents (BOF)

The final event of the evening was a discussion session on Secure Mobile Agents. It was primarily about Java, with a Telescript person in attendance. Sun representatives gave an outline on Java. Sun believes that the problem of secure mobile agents is full of subtle difficulties, but that it is a a reasonable thing to try to do. The Princeton authors presented their recommendations on how Java should proceed. There was concern during the meeting that there was no defined policy, and that putting assurance before policy is unworkable. George Dinolt implied that users do not set security policies, systems set security policies. Telescript never looked so good. For any issue, the panelists were able to discuss their approach to a problem, even if they did not have all the answers. In discussing authentication, it was pointed out that the Microsoft model was to emulate COTS software with digital signatures. John McHugh pointed out that the number of applets will be substantially larger than the number of COTS software packages, and what would that imply about level of testing? Dan Wallach brought up points concerning the user interface design of security features. He wished to use "Do not bother the user" as a guiding principle, which would be a refreshing change. Telescript is exploring having every regional server apply digital signatures to endorse mobile agents, but considers it a heavyweight mechanism.

4 Wednesday

4.1 Modeling; chaired by Richard Neely (CTA)

The first paper was "A Security Model of Dynamic Labeling Providing a Tiered Approach to Verification", presented by Simon Foley (University College, Cork), (joint work with Li

Gong and Xiaolei Qian, both SRI). Foley described a verified TCB with security requirements specified on top of it. The tired system has the advantage that for a new application only the security requirements need to be reverified.

Martin Roescheisen of Stanford presented "A Communication Agreement Framework of Access Control" (joint work with colleague Terry Winograd). This model uses communication agreements to establish peer-to-peer relationships, called commpacts. These agreements are the focus of a framework for access/action control. The primary concerns are usability and social acceptability. Commpacts manage relationships providing trusted shareability.

Matt Blaze (AT&T Research) presented "Decentralized Trust Management" (joint work with colleagues Joan Feigenbaum and Jack Lacy). The paper identifies trust management as an important component of security in large distributed systems. The authors argue that it is important not to confuse the questions of "Whose public key was verified" with the question of "For what purpose is this public key issued?" This approach provides an architectural framework that separates generic mechanism and application-specific policies. The concrete system is called PolicyMaker and appears to applications much like a database query engine. The generic mechanism can be utilized from any application with different policies. That provides the decentralized aspect of the architecture. The approach purposefully conflates the specification of security policies and security credentials, the policy decision process, and the deferring of trust to third parties.

The final paper was given by Steve Schneider (University of London) entitled "Security Properties and CSP". Schneider's work is part of a larger project dealing with problems of modeling and analysis of security protocols. The basis is that security protocols can be viewed as communicating sequential processes. CSL can be used to check safety properties (which are viewed as security properties) of protocols described as processes that interact over a medium.

4.2 Networks; chaired by Paul Karger (IBM)

Drew Dean (Princeton University) presented "Security Flaws in the HotJava Web Browser" (joint work with colleagues Ed Felton and Dan S. Wallach). The paper outlines a number of attacks, both potential and verified, on the HotJava Web browser. In Java, local file system applets are trusted. A security manager module needs to be called to approve dangerous operations, but there is nothing architecturally which ensures that the module is always called appropriately. Applets could contact any host (contrary to the stated security policy) through DNS, and could degrade or deny service while other applets were being run. The authors also exploited a vulnerability based on the difference between what code would compile with a legal Java compiler and how byte codes are checked. This vulnerability allowed them to run arbitrary machine code. In Java there is only a single line of defense; the class loader. Most of the vulnerabilities exposed have since been patched, however, some have not.

The next paper was presented by Wenbo Mao (HP Labs, Bristol) "On Two Proposals for On-line Credit-card Payments using Open Networks: Problems and Solutions". He pointed out some missing services in the areas of protocol integrity, non-repudiation, message receipt, and message timeliness, and some misused services where non-repudiation is used where authentication would work, and real-time replay detection is done when batch would be sufficient.

"Secure Network Objects" was presented by Leendert van Doorn (University in Amsterdam) (joint work with Martin Abadi, Mike Burrows, and Edward Wobber, all DEC SRC). Van Doorn described their approach to provide security for object-oriented network communication. The design takes advantage of subtyping and achieves object-level granularity. Both access control lists and capabilities are supported.

The last paper of the conference was "Run-Time Security Evaluation (RTSE) for Distributed Applications" presented by Cristina Serban (University of Missouri-Rolla) (joint work with colleague Bruce McMillin). The central idea of this paper was that formal security specifications for distributed applications can be checked at runtime. This is done through executable security assertions.

The symposium formally adjourned after closing remarks from Dale Johnson and the new program chair George Dinolt.