Report on the Internet Society Symposium on Network and Distributed System Security

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

1 Introduction

About three hundred attendees were present for the forth Symposium on Network and Distributed System Security (SNDSS), held at the Princess Hotel in San Diego, CA, February 22-23, 1996. This one-track symposium was sponsored by the Privacy and Security Research Group of the Internet Research Task Force with support from the Internet Society (ISOC).

This symposium brings together builders of software and hardware that provide network and distributed system security services. It focuses on practical aspects, such as actual system design, and implementation and targets researchers, implementors, and users of network and distributed systems facilities. Forty submissions for refereed papers, panels, and BOFs — plus the work of the program committee — resulted in an outstanding symposium program.

Four sessions were held Thursday, including paper sessions on electronic mail security, distributed object systems, and distributed system security and panel sessions on scalability of security in distributed object systems and intellectual property protection. After dinner, Henry Kluepfel (Vice President, SAIC) spoke on "Security and Fraud on the Information Superhighway". The last activity for the day was a Birds of a Feather (BOF) on security in Java.

Four sessions were also held Friday, the last of which was a panel discussion on public-key infrastructure. The other Friday sessions covered aspects of network security, key management, and encryption.

2 Thursday

To open the symposium, James Ellis (general chair, CERT) welcomed attendees and thanked those who had brought the symposium together: Donna Leggett (registration

chair), Thomas Hutton (local arrangement chair), Stephen Welke (publication chair), Clifford Neuman and David Balenson (Program Chairs), session chairs Stephen Kent, Danny Nesset, Michael Roe, Peter Neumann, Matt Bishop, Burt Kaliski, Avi Rubin, and Warwick Ford, the rest of the Program Committee, and several external reviewers.

2.1 Electronic Mail Security; chaired by Stephen Kent (BBN)

Ceki Gulcu (IBM) gave the first talk, "Mixing E-mail with BABEL", which covered work Gulcu performed jointly with Gene Tsudik. Gulcu discussed the goals and desired properties of anonymous e-mail, such as availability of the service to anyone, strong guarantee of anonymity, minimal trust in remailers, and a resistant remailer infrastructure against attack. He then introduced the design and salient features of the BABEL anonymous remailer: basically, the sender repeatedly encrypts the message with the public keys of the remailers that are on the forward path to the destination. Return path information is included in the message to enable replies. This approach has obvious scalability problems but is resistant to a number of active and passive attacks and assumes little trust in intermediate remailers. A prototype implementation is based on freely available software: Perl and PGP.

The next presentation was given by Kazuhiko Yamamoto (Nara IST, Japan), who described and demonstrated a design for the "Integration of PGP and MIME". Combining PGP's privacy services and MIME's capability of exchanging multipart, multimedia documents offers privacy for any non-textual documents. The design allows for the embedding of PGP objects into MIME with a backward compatibility with PGP. It offers confidentiality and authenticity on a whole MIME message or on only selected parts. A prototype was implemented in Emacs LISP and is operational on various Emacs platforms.

2.2 Distributed Object Systems; chaired by Dan Nessett (Sun Microsystems)

Nicholas Yialelis presented the sole paper in this session, "Security Framework Supporting Domain Based Access Control in Distributed Systems", which reviewed work performed by Yialelis and Morris Sloman (both of Imperial College, London, UK). Explicit goals of this work are: to provide a security platform for distributed applications that makes access control and authentication mechanisms transparent to the application level and to support the enforcement of access control policies specified using management domains. The advantage of the latter is that policies can be specified in terms of groups of objects, making it unnecessary to specify policies for potentially millions of individual objects in large scale systems. The architecture provides for a host manager server that is present on all hosts and supports the host manager object, an authentication agent object, and an access control agent object. The provided security is transparent to the applications, and only few modifications are necessary at the application's servers. The components communicate with their remote peers via secure channels. A prototype implementation is underway in the CORBA-compliant Orbix environment.

Bret Hartman (BlackWatch Technology), Dan Nessett, and Nicholas Yialelis served on the panel that discussed "Scalability of Security in Distributed Object Systems". Hartman briefly summarized the problem: to manage a set of objects, rather than the individual

objects separately, is a powerful mechanism. The challenges include how to compose policies that are specified on sets of objects, if compositions can scale in the presence of complex security requirements, and how different solutions to the previous two challenges might interoperate. Nessett provided three examples of applications of large-scale distributed object systems to explore the applicability and advantages of security policy domains. The examples addressed the question of federated domains, federated domains with transitive trust requirements, and security policy updates. The first two examples centered around the insight that technical solutions are necessary but not sufficient to provide good security. The search for higher-level solutions must go on, and a true solution will, in addition to technical aspects, have many other facets, such as nondisclosure agreements, trust, object domains, ...and lots of lawyers.

2.3 Distributed System Security; chaired by Michael Roe (University of Cambridge, UK)

Jonathan Trostle (CyberSAFE) spoke on "A Flexible Distributed Authorization Protocol", which covered work performed by Trostle and Clifford Neuman (ISI). This work notes that considerable effort has been put into creating interoperability among authentication methods but that authorization methods have received far less attention. Trostle presented a flexible authorization protocol that provides the full generality of restricted proxies while supporting the functionality of and interoperability with existing authorization models, such as OSF DCE and SESAME V2.

Trent Jaeger (University of Michigan) presented "Preserving Integrity in Remote File Location and Retrieval", which covered work performed by Jaeger and Avi Rubin (Bellcore). The work addresses the problems of locating files and the verification of file integrity in the presence of untrusted networks or mobile systems with little memory. Jaeger described a service that provides the capability to automatically locate, retrieve, and verify files specified by a client using a single trusted principal, a certification authority (CA). CAs generate and sign certificates that associate an author with a file and a cryptographic digest of the file. Automated location is possible because all remote files are published with location servers.

Takahiro Kiuchi (University of Tokyo) presented the final talk in this session, "C-HTTP - The Development of a Secure, Closed HTTP-Based Network on the Internet", which covered work performed by Kiuchi and his colleague Shigekoto Kaihara. The components of the system are a client-side proxy, a server-side proxy, and a C-HTTP name server. Client-side proxies and server-side proxies communicate with each other using a secure encrypted protocol while communication between a user agent and its client-side proxy or an origin server and server-side proxy is performed using current HTTP/1.0. The C-HTTP-based secure, encrypted name and certification service is used instead of the DNS. The aim of C-HTTP is to assure institutional level security, in contrast to other secure HTTP protocols currently proposed that are oriented toward secure end-user-to-end-user HTTP communications.

2.4 Intellectual Property Protection; chaired by Peter Neumann (SRI)

The session comprised brief presentations and a question-and-answer session. Olin Sibert (Electronic Publishing Resources) proposed a decentralized approach to electronic pub-

lishing of intellectual property, the components of which would be decentralized servers, 'crypto (un)lock' technology for making documents (in)accessible, and 'local' participation and enforcement of end systems. Sibert also advocated the view that business world security requirements differ from military requirements. Russ Housley (Spyrus) represented a vendor of PCMCIA crypto hardware for metering remote use. Dan Boneh (Princeton University) described a method of using public key cryptography to mark complex documents, such as images, to allow the owner of the document to identify each authorized copy and its owner. The scheme can protect against collusion. It fails if automated tools can be utilized to remove the protecting fingerprints, such as spacing in text documents. During the question-and-answer period, Peter Neumann asked if electronic commerce products can be made secure. Panelists concurred that this is impossible and that the real question is how to make the publishing systems resilient enough that fraud is limited to an acceptable level. Other questions targeted Boneh's work on fingerprinting documents. It was asked if the assumption that products can be associated with the initial purchaser is reasonable, and if so, how much this violates personal privacy issues. The last question discussed if there are methods of fingerprinting that do not affect the artistic contents of the work.

3 Friday

3.1 Network Security; chaired by Matt Bishop (UC Davis)

Jonathan Stone (Stanford University) described "Designing an Academic Firewall: Policy, Practice, and Experiences with SURF", which covered work performed by Stone and his colleagues Michael Greenwald, Sandeep Singhal, and David Cheriton. The interesting premise of this work was that corporate firewall designs are neither effective nor appropriate for academic and corporate research environments. The research group built the Stanford University Research Firewall (SURF). The policy implemented by this firewall allows less restrictive outward information flow than the traditional model. Services such as e-mail, WWW, and anonymous FTP work transparently for internal users. SURF was constructed using off-the-shelf software and hardware components.

Sandra Murphy (TIS) presented "Digital Signature Protection of the OSPF Routing Protocol", which covered work performed with colleague Madelyn Badger. The talk reported on work-in-progress to protect the OSPF routing protocol through the use of cryptography, specifically, digital signatures. The routing information is signed with an asymmetric cryptographic algorithm, allowing each router recipient to check the source and integrity of the information. Murphy discussed fundamental issues in security of routing protocols, reviewed the basics of OSPF operation, the proposed design, and remaining vulnerabilities (such as the age field not being protected by the keyed hash).

Michael Roe (University of Cambridge, UK) concluded the session with a "Case Study of Secure ATM Switch Booting" in the context of the Fairisle ATM switch environment; the work was performed with his colleague Shaw-Cheng Chuang. Roe examined a few techniques for booting Asynchronous Transfer Mode (ATM) switches securely over an insecure network. Each of the techniques assumed a different trust model. The work assumes an open multi-service network wherein ATM switches are booted with third-party software, possibly even using a third-party booting service. In that environment, it is important to ensure that the switches are booted with authorized and authenticated boot code. Michael examined the threats and presented schemes of countering the threats.

3.2 Key Management; chaired by Burt Kaliski (RSA)

Hugo Krawczyk (IBM T.J. Watson) began with "SKEME, A Versatile Secure Key Exchange Mechanism for Internet". SKEME constitutes a compact protocol that supports a variety of realistic scenarios and security models over the Internet. It provides clear tradeoffs between security and performance as required by the different scenarios without incurring unnecessary system complexity. The protocol supports key exchange based on public keys, key distribution centers, or manual installation, and provides for fast and secure key refreshment. Additionally, SKEME selectively provides perfect forward secrecy, allows for replaceability and negotiation of the underlying cryptographic primitives, and addresses privacy issues as anonymity and repudiatability.

Carlisle Adams (BNR, Canada) spoke on "IDUP and SPKM: Developing Public-Key Based APIs and Mechanisms for Communication Security Services". Carlisle discussed the progress in the development of APIs and mechanisms that provide a comprehensive set of security services to application developers. Existing APIs, though similar, are developed for distinct environments: the session API (GSS) is aimed at the on-line real-time messaging environment; the store-and-forward API (IDUP) is particularly suited for electronic-mail types of environments. Both APIs were designed to be easy to use yet with appropriate public-key-based mechanisms include many necessary services for communication security, such as data origin authentication, data confidentiality, data integrity, and support for non-repudiation. A full key management and certification infrastructure can be provided by implementations of these APIs/mechanisms in a manner completely transparent to the calling application, thus ensuring maximum flexibility and scalability to future environments.

3.3 Encryption; chaired by Avi Rubin (Bellcore)

Iskender Agi (SRI) presented "An Empirical Study of Secure MPEG Video Transmissions", which covered work performed by Agi and colleague Li Gong. MPEG is an industrial-strength standard for video processing and is widely used in multimedia applications in the Internet. No security provision is specified in the standard. The speakers conducted an experimental study of previously proposed selective encryption schemes for MPEG video security. This study showed that these methods are inadequate for sensitive applications. Agi also discussed the tradeoffs between levels of security and computational and compression efficiency.

The presentation "Parallelized Network Security Protocols" described collaborative work by Erich Nahum, David J. Yates (both with the University of Massachusetts), Sean O'Malley, Hillarie Orman, and Richard Schroeppel (all with the University of Arizona). The premise is that shared-memory multiprocessors make attractive server platforms. The paper is an experimental performance study that examines how encryption protocol performance can be improved using parallelism. The authors show linear speedup for several different Internet-based cryptographic protocol stacks running on a symmetric shared-memory multiprocessor using two different approaches to parallelism.

David A. Wagner (UC Berkeley) discussed a TCP/IP security extension for MS-DOS systems, "A 'Bump in the Stack' Encryptor for MS_DOS Systems", covering work performed by Wagner and Steven Bellovin (AT&T Bell Labs). Because source code is not readily available for MS-DOS systems, Wagner implemented the IP security extensions using the

packet driver interface. The IPSEC module sits between the generic Ethernet driver and the hardware driver; it emulates each to the other. The work showed that it is possible to add IP security features by exploiting open interfaces. However, the implementation has several problems, such as the duplication of functionality (IP fragmentation).

3.4 Public-Key Infrastructure; chaired by Warwick Ford (BNR)

Chair and moderator Warwick Ford introduced the panel members and noted the importance of the topic. He also proposed that this broad subject would be restricted to the question of how many credentials are needed. Panelists gave short presentations and answered audience questions.

John Wankmueller (MasterCard International) stressed one point in his presentation: MasterCard and VISA take a different approach to certification than do most other systems; they try to establish that a valid account is used, not the identity of the user. Authenticating account numbers is in a sense obscuring the identity of users. Wankmueller then presented the architecture of a certification hierarchy that was developed to secure MasterCard electronic commerce transactions.

Taher ElGamal (Netscape) focussed on the importance of user friendly and transparent security features. The number of certificates needed would not matter, if the user has only to click on an icon to commit to a transaction and the software beneath it will determine which certificate is needed. A multitude of certificates is likely: identity type, authorization type, and special purpose certificates. Universal certificates are possible to design, but complicated. Different countries have different styles (e.g., phone cards). ElGamal speculated that one may come to have about as many important certificates as plastic cards in one's wallet.

Michael Baum (Verisign) represented the commercial public-key infrastructure service provider perspective. He questioned if the lack of a single certificate is really a problem and focussed on the practices and the legal side.

During subsequent discussion, Steve Kent observed that there is no need for multiple credentials, not only because of different types of identity but also because of context of identity. Bob Abbott challenged the trust in the system by asking what recourse customers have against fraudulent merchants.

4 Conclusion

The two-day symposium featured many high quality, insightful, and some thought-provoking presentations. The panel sessions were very interactive and touched on a wide variety of aspects of the issues on hand. The symposium gave plenty of opportunity to discuss current issues with experts, catch up with colleagues, and make new acquaintances. It provided encouragement that the information systems and communications security communities can contribute high quality technical solutions addressing security threats. However, it also clearly showed that technical solutions can be only part of any comprehensive approach to computer security.