Volume 102, Number 3, May–June 1997
Journal of Research of the National Institute of Standards and Technology

[J. Res. Natl. Inst. Stand. Technol. **102**, 367 (1997)]

Conference Report

19th NATIONAL INFORMATION SYSTEMS SECURITY CONFERENCE Baltimore, MD October 22-25, 1996

Report prepared by

Ellen Flahavin

Computer Security Division,
Information Technology Laboratory,
National Institute of Standards and Technology,
Gaithersburg, MD 20899-0001

1. Introduction

Since the first computer security conference held at the National Bureau of Standards in 1979, attendance and active participation have grown. This year's conference attracted a diverse national and international audience of more than 1500. The group represented leaders in the security field from government, industry, and academe. The presenters reported on dynamic and complex research activities as well as technical issues which allowed attendees to focus on a broad perspective of trends in information technology security.

The National Institute of Standards and Technology and the National Computer Security Center (NCSC) of the National Security Agency (NSA), jointly sponsored the 19th National Information Systems Security Conference held at the Baltimore Convention Center. This 3 1/2 day conference provides a unique international forum in which to address information technology security issues. The conference program focuses on developing and implementing secure networks, technologies, applications, and testing of products and systems. An important dimension of this conference is that it provides a platform for information sharing and new approaches for solving technical and management issues. A vendor exposition, sponsored by the Armed Forces Communications and Electronics Association (AFCEA), was held in parallel with the conference.

The conference theme, "Policy and Technology, Partners in Solution," provided a forum for technology interchange among the national and international experts. Many reported that the opportunity to network with peers to discuss problems and solutions was one of the most valuable assets of the conference.

2. Conference Program Highlights

2.1 Opening the Conference

Tim Grance, Manager of the Systems and Network Security Group at NIST, welcomed the conference participants. Grance gave an overview of the conference program and encouraged participants to visit the AFCEA exposition. The keynote speaker, August Bequai, presented the opening plenary address featuring his paper on "Rise of the Mobile State: Organized Crime in the 21st Century." Shukri Wakid, Director of NIST's Information Technology Laboratory (ITL), addressed the audience about the role of the ITL and joint efforts with the National Security Agency, the planned NIST Testing Center, and the Common Criteria Testing Program. The presentation of the annual National Computer System Security Awards was made by Stuart Katzke, Chief of the Computer Security Division. An address by two of the award recipients, Whitfield Diffie and Ronald Rivest, followed. The third recipient, Martin Hellman was not available to receive the award. Ellen Flahavin, NIST Conference Program Director, presented the best paper award to Helmut Kurth of IABG, Germany, for his paper on "Integration of Digital Signatures into the European Business

Register," and to Todd Heberlein and Matt Bishop, of the Computer Science Department, University of California, Davis, for their paper on "Attack Class: Address Spoofing."

2.2 Criteria and Assurance Track

In the last few years, the special sessions on the Common Criteria were so well attended that this year a track was dedicated to Criteria and Assurance. The Common Criteria was not the only criteria for which papers were submitted. The papers submitted included subject matter on the Trusted Computer Security Evaluation Criteria (TCSEC) and the European Information Technology Security Evaluation Criteria (ITSEC). A group from the MITRE Corporation submitted a paper titled "Design Analysis in Evaluations Against the TCSEC C2 Criteria." This paper provided an overview of design analysis, which is a key component of product evaluations under NSA's Trusted Product Evaluation Program (TPEP). The paper described activities performed and issues considered for evaluation against the TCSEC C2 criteria.

Another paper discussed the recently completed evaluation of the Processor Resource/System Manager (PR/SM) on the ES/9000 processors (9021 and 9121), performed by a European Commercial License Evaluation Facility, against the ITSEC. PR/SM achieved an E4 rating which certifies its use as a security consolidation platform for combining workloads at different security classifications. The paper covered the configuration and use of PR/SM in a secure mode, including the intended environment for use and the intended method for use. A discussion followed of the security enforcing functions which were certified as part of the evaluation, and why they are important for anyone interested in consolidating workloads while maintaining a high level of isolation and security.

There are other ways to gain assurance than evaluating against criteria. Among these alternatives are Certification and Accreditation of a system, Configuration Management, and the System Security Engineering Capability Maturity Model. Papers and panels enlightened the community on some of the alternatives.

A detailed paper on the Certification and Accreditation of the U.S. Government Key Escrow System (KES) was submitted by Ellen Flahavin and Ray Snouffer of the NIST's Computer Security Division. In order for this effort to be successful, a multi-agency certification of a national system requires coordination, planning, and an established structure. The presentation provided an approach for certifying and accrediting multi-agency systems to newcomers and veterans.

2.3 Electronic Commerce Track

The Electronic Commerce Track provided an international forum in which to address secure electronic commerce issues. One of the two best paper awards was presented in this track by Helmut Kurth of IABG, Germany. This paper, "Integration of Digital Signatures into the European Business Register," reported on a project created by the European Union to demonstrate the feasibility of the use of digital signatures in European Networks. Companies could extract the official business register data from companies of four European countries on-line and authenticate by digital signatures. This is significant because the common way to obtain information on specific business contracts is to get an officially signed copy of the business register data by surface mail. This may take up to 2 weeks, causing time and financial losses as a result of delayed contracts. With the infrastructure established in this project, the official business register data could be obtained digitally signed in a few seconds.

2.4 In Depth Track

Much like the "In Depth" concept on the nightly news, this track presented subjects in greater detail. The paper on cryptographic protocols is a prime example of a subject covered "In Depth." Cryptographic protocols are short sequences of message exchanges intended to establish secure communications over insecure networks; whether they actually do so is a subtle question. "Automated Formal Analyses of Cryptographic Protocols," by Stephen H. Brackin of ARCA, described results produced by a software tool for automatically proving desired properties of protocols using an extension of the Gong, Needham, Yahalom (GNY) belief logic, if possible, and showing exactly what goes wrong otherwise.

2.5 Internet Track

The Internet Track, once again one of the most popular tracks, addressed various aspects of Internet security. What industry needs to look at in the future with regard to security technology was addressed by Dan Federmen of Premonos on "Secure Business on the Internet: Looking Ahead with Electronic Data Interchange." The speaker gave a brief history of Electronic Data Interchange and discussed how today's marketplace on the Internet needs cost effective and secure business solutions to function over the Word Wide Web.

One of the most popular panels of the conference was chaired by Peter Neumann of SRI International. The panel "Webware: Nightmare or Dream Come True?"

considered the risks involved in the open-ended routine security problem introduced by World Wide Web browsers and some programming languages. The ability to execute arbitrary code of unknown trustworthiness from unknown sites (perhaps without your awareness) presents fascinating security challenges. The session explored various approaches to avoiding or living with those risks. The problem has the potential for greatly advancing computer use if it is handled intelligently, and greatly impairing security if it is not.

2.6 Legal Perspectives Track

The Legal Track, new to this year's conference, focused on legal security issues that are evolving to deal with emerging technology in the government and private sectors. Mark Gembicki, WarRoom Research LLC., formed a panel that addressed cybercrime issues and how they affect legal competitive intelligence, the National Information Infrastructure, information warriors, and the commercial business environment. Examples of traditional organized crime elements to individual "cyberterrorists" as well as proposed changes in government strategies were presented.

2.7 Management and Administration Track

The Management and Administrative Track concentrated on subjects in the management and administration of the security functions and the information systems which they support. The papers and panels in this track explored the theme of previous years regarding privacy issues, ethics, the security professional, and the importance of process improvements. A paper submitted by Olin Sibert, Oxford Systems, Inc., was one of the most popular among the conference committee. Sibert pointed out that traditionally, computer security has focused on containing the effects of malicious users or malicious programs. However, as programs become more complex and additional threats arise, malicious data becomes an issue. This threat arises because apparently benign programs can be made malicious, or subverted, by introduction of an attacker's data—data that are interpreted as instructions by the program to perform activities that the computer's operator would find undesirable. A variety of software features, some intentional and some unwitting, combine to create a software environment that is highly vulnerable to malicious data. Sibert's paper catalogs those features, discusses their effects, and examines potential countermeasures. In general, the outlook is depressing. As economic incentives increase, these vulnerabilities are likely to be exploited more frequently. Yet, effective countermeasures are costly and complex.

2.8 Research and Development Track

The other paper chosen for the Best Paper Award, "Attack Class: Address Spoofing," was presented in this track. Matt Bishop of the University of California, Davis, and Todd Heberlein of Net Squad, presented an analysis of a class of attacks called address spoofing. Fundamentals of internetwork routing and communication were presented, followed by a discussion of the address spoofing class. The attack class was made concrete with a discussion of a well-known incident. They concluded by dispelling several myths of purported security solutions, including the security provided by one-time passwords.

2.9 Solutions Track

Marianne Swanson of the Computer Security Division of NIST presented a paper describing the many functions that a Federal incident response capability (IRC) would perform and explored the issues that should be addressed prior to the establishment of an IRC. Almost all Federal agencies are now connected to the Internet; they exchange information regularly, and need an incident response capability. The number of Internet-related incidents that have occurred in the past year, along with the increase and complexity of viruses, requires agencies to take seriously their incident handling capability. The Office of Management and Budget has validated this need by requiring in the revisions to OMB Circular A-130, Appendix III, that agencies be able to respond in a manner that both protects its own information and helps to protect the information of others who might be affected by the incident. A government-wide incident response capability (IRC) assists civilian agencies in meeting their requirement.

2.10 Tutorials

As in the past, this year's conference featured a Tutorial Track. This track provided information to newcomers to the security field and a "refresher" for the experienced security professional. From the first day's presentation of "Introduction to Information System Security" to the last tutorial on Friday "Education Technology" the track was well attended. Among the other tutorials, ARCA Systems provided a major portion of the tutorial track. Their "Database Security" focused on issues from the standpoint of using database management systems to meet an organization's security requirements. Topics in this presentation included data security requirements, vulnerabilities, database design considerations, and implementation issues. "OS Security"

focused on security issues for commercial operating systems. The "Trusted Systems Concept," developed by the Institute for Computer and Information Sciences, focused on the fundamental concepts and terminology of trust technology.

2.11 Closing Plenary "Directions and Challenges for the Information Technology Industry"

A distinguished panel addressed some significant issues and engaged in a dialogue on such questions as:

- What challenges do you perceive for your own business or end-user community with respect to information system security?
- What are the security-relevant challenges for your organization? What is security's strategic role in your organization? How are you making tradeoffs?
- What do you see that industry, government, and academia should be doing in computer security? What is each doing well or not so well now?

3. Awards Ceremony

On Thursday, October 24, NIST and NCSC honored those vendors who successfully developed security product lines meeting the standards of the respective organizations. The NCSC recognized vendors who contributed to the availability of trusted products and thus expanded the range of solutions from which customers may select and secure their data. The products are placed on the Evaluated Products Lists (EPL) following a successful evaluation against the Trusted Computer Security Evaluation Criteria.

NIST presented awards to vendors that successfully developed security product lines that have been approved by the NIST Validation Program. The Computer Security Division at NIST provides validation services to test vendor implementation for conformance to security standards. NIST currently maintains validation service for the following Federal Information Processing Standards (FIPS); FIPS 46-2, Data Encryption Standard (DES); FIPS 113, Computer Data Authentication, and FIPS 171, Key Management Using ANSI X9.17. During the awards ceremony, NIST presented "Certificate of Appreciation" awards to vendors who successfully validated their implementation of these standards.

Awards also were presented to companies that participated in Systems Security Engineering Capability Maturity Model (SSE-CMM) pilot appraisals.

4. Other Activities of Interest

For the first time, two free preconference workshops were arranged by Mariannne Swanson and Ellen Flahavin. The Incident Handling and the Common Criteria Protection Profile Workshops were held the day before the conference and were attended by a third of the conference participants. The Common Criteria Protection Profile Workshop was a full-day symposium that provided information and instruction on using the Common Criteria to build Protection Profiles to express information technology security requirements. Community experience in building Protection Profiles was used as a basis for this instruction. Alternative sets of requirements for related technologies were compared and contrasted in the hopes of harmonizing like requirements into generic Protection Profiles for given technologies (i.e., firewalls). In addition, issues arising from attempting to create Protection Profiles representing nonclassic requirement sets were discussed.

The Incident Handling Workshop ran in two half-day sessions. The workshop provided basic concepts and techniques on how to create an incident handling capability. The workshop addressed how to establish and operate a capability using existing services of contracting out, reporting structures, hiring the right people, and other topics. It was designed for security, systems, and network specialists responsible for managing and ensuring the availability and integrity of computer systems.

5. Next Year's Conference

The 20th National Information Systems Security Conference will be held October 6-9, 1997, at the Baltimore Convention Center. For further information, contact Tammie Grice at the NIST Conference Office, (301)975-2775.