Conferences / Events

COMPUTER SECURITY CONFERENCE A Report on the Tenth National Computer Security Conference, Baltimore, MD, September 21–24, 1987

The National Bureau of Standards (NBS) Institute for Computer Sciences and Technology (ICST) and Department of Defense (DOD) National Computer Security Center (NCSC) jointly sponsored the Tenth National Computer Security Conference, September 21–24, 1987. Previously this annual conference was held at the NBS. Over the last several years attendance increased dramatically, and for the first time the conference was held at the Baltimore Convention Center. Attendance exceeded 1,600, making this computer security conference the largest ever held.

About the Conference

The conference program was organized around the theme, "Computer Security—From Principles to Practices." The topics covered included research, new vendor products, technical, management, administrative, and educational aspects of computer security. Many of the papers presented at this conference addressed topics that will support the defense community, yet other issues such as ethics in computer security, privacy, risk management, contingency planning, and education were addressed and were of value to business and the civil sector of the government. Sessions addressing these topics were well attended.

There was a high interest in network security and several technical papers described the work on the Secure Data Network System (SDNS). The SDNS project was initiated last year by the National Security Agency (NSA) with the NBS, the Defense Communications Agency (DCA), and 12 communications and computer companies. Within the framework of the SDNS program, government and industry have joined to make products available that will support security services for distributed data processing networks.

The presentations were organized into two parallel tracks, one of which addressed managerial computer security issues and the other technical issues. A third track with occasional special sessions was also provided. This arrangement allowed participants a wide choice of topics from which to choose. The last day of the conference provided an opportunity for attendees to organize and participate in special interest groups.

For the first time, a unique "Poster Session" was offered. This session provided an opportunity for participants to speak for 2 minutes on any computer security related subject. Many speakers participated enthusiastically. As a result, the poster session will be included in next year's program.

Speakers represented computer industry leaders, computer security practitioners, and researchers from the United States and abroad. Brief summaries of a few specific contributions follow.

Opening the Conference

ICST Director James Burrows and NCSC Director Patrick Gallagher welcomed the conference participants. In his talk Burrows stressed the improving network security as use of networks grows. Burrows spoke of how ICST initiated a program in the late 1970s to meet user needs to interconnect different manufacturers' equipment and systems in distributed data processing networks. The Open Systems Interconnection (OSI) standards development has been carried out by national and international committees with ICST assistance. Burrows further stated that the NBS Workshop for Implementors of OSI was organized in 1983 to start a cooperative effort with industry to build compatible commercial products. Burrows stressed that the improved connectivity brought about by OSI must be accompanied by essential protective measures. He encouraged industry and government to identify their requirements for protocols that will support security services in open systems. Burrows stated that NBS will continue its work with NSA to assure compatibility and proper performance of protocols.

Gallagher also discussed the importance of network security. He announced a recent publication produced by the NCSC, "Trusted Network Interpretation." This document, referred to as the "Red Book," was developed to provide a standard to manufacturers and users on the security features and assurance levels that are needed in commercial network products. Gallagher further discussed how the NCSC works closely with U.S. computer manufacturers encouraging the building of "trust" into the hardware and software of computer systems. He further stated that the "Orange Book" (formally, *Trusted Computer System Evaluation Criteria)*, which established a set of basic requirements and evaluation classes for assessing the effectiveness of security controls built into computer systems, continues to be the cornerstone for the Center's evaluation program. Gallagher called for continued cooperative efforts of the government, industry, and academe to build trust into computer systems.

The keynote speaker was U.S. Representative Dave McCurdy (D-Oklahoma). Rep. McCurdy chairs the House Subcommittee on Transportation, Aviation and Materials, which has jurisdiction for communications research and development. It is from this basis, McCurdy explained, that the Subcommittee began an in-depth examination of the issues in computer and communications security and privacy within the Federal government. Hearings before the Transportation Subcommittee revealed that computer security in the Federal government needed improvement. This led to the introduction of legislation that became known as HR 145, The Computer Security Act of 1987. McCurdy explained that the bill starts not only from the premise that computer security in the Federal government needs improvement but that it can benefit from stronger centralized leadership. The bill assigns responsibility for protecting unclassified government computer information to NBS and the protection of classified information to the NSA. Rep. McCurdy reported that HR 145 passed the House and the next step is consideration by the Senate. He called on industry and Federal agencies to continue building on technology to strengthen computer security in the government. He emphasized that the technical capabilities and assistance of both the NCSC and NBS are essential to meeting national computer security goals.

Network Security

Dennis Branstad, NBS Computer Science Fellow, presented a tutorial on the Open Systems Interconnection (OSI) computer network architecture. Branstad explained that the security services being developed for OSI will assure that data being transmitted from one OSI system to another will be protected against modification, disclosure, replay, and undetected loss. He described the seven-layered OSI communications model connecting hosts in star configurations, LANs and LAN bridges, ring configurations, and gateways. Cryptographic procedures were also discussed.

Several technical papers highlighted the work on the SDNS project. This project, as presented by Gary Tater, NCSC, focuses on designing the next generation of secure computer communications network and product specifications to be implemented for applications utilizing both public and private data networks. Tater explained that one of the primary goals of the program is to assist and encourage industry in developing a wide variety of cost-effective communications products and systems that meet OSI standards. Tater reported that the project is advancing well and predicted it would result in data security protocols and products by 1990.

Insider Threat

A panel addressed the issue of "insider threats." Allan Clyde, a Washington businessman, explained that managing the risks arising from insiders on sensitive computer systems is growing in importance.

Clyde reviewed the work being done in the field and proposed a system of analysis to identify suspicious events. This method would perform continuous capture and encryption of all keystrokes for each user. Clyde concluded that full-system surveillance can be achieved cost-effectively with high performance products that do not represent an excessive burden to the system.

James Anderson, a computer security consultant, contends that surveillance is not effective since a user with a high degree of expertise can operate below the surveillance level. He asserted that systems certified at the B2 and B3 levels circumvented the need for surveillance. Another panelist, Priscilla Regan, U.S. Congress Office of Technology Assessment, stated that surveillance could mean an invasion of privacy. She proposed that deterrence mechanisms be used instead of surveillance and that if used, surveillance not be concealed. This panel discussion clearly demonstrated there are no perfect solutions to the insider threat problem.

Computer Viruses

In addition to the insider threat problem, potential solutions to other kinds of threats were discussed. Howard Israel, NCSC, theorized that any protection mechanism used to detect a Trojan Horse threat will work to detect a computer virus as well. Israel pointed out that a virus attack generally causes more damage than a Trojan Horse because more computers or more computer programs are involved in a virus attack. During this presentation, Israel reviewed several virus research activities. He concluded that a well-defined security policy used in conjunction with trusted software can provide reasonable protection against virus and Trojan Horse attacks.

Risk Assessment

Robin Moses, UK Central Computer and Telecommunications Agency (CCTA), and Rodney Clark, BIS Applied Systems LTD, jointly presented a risk analysis methodology, called CRAMM, developed for use in the United Kingdom. CRAMM is designed for the novice risk analyst and combines a baseline "code of good management practices" with a qualitative risk analysis method. CRAMM is threat oriented and emphasizes consequential as well as direct losses. A questionnaire with scales of 1–10 is used to evaluate the vulnerabilities and risks in the system.

Sylvan Pinsky, Senior Scientist for the Office of Research and Development, NCSC, discussed current efforts by the Federal government in the area of computer risk management. Pinsky announced the cooperative efforts of NBS and NCSC in establishing a Risk Management Laboratory. Pinsky highlighted that the primary goal of the laboratory will be to conduct research in risk management techniques and methodologies and to transfer the results of that research to government and private sector organizations. Another related activity being considered is to assist agencies in the selection and use of commercial risk management software. The laboratory, which will be located at NBS, may also provide a clearinghouse for information on risk analysis and management for the Federal government.

Contingency Planning

A special session on contingency planning provided lively discussions on developing computer contingency plans. Ray Pardo, Bechtel Eastern Power Corporation, presented a "fast track" approach (6 months to a year) for implementing a contingency plan. Fast track, as described by Pardo, is targeted toward developing a workable and tested contingency plan for truly critical applications and for a specific range of contingencies. Pardo discussed the advantages of the fast track approach and outlined a method for implementing the plan. Pardo emphasized that unlike other contingency planning methodologies where the benefits of the plan are delayed for 1 to 2 years, "fast track" quickly reaches the crucial testing phase.

Thomas Judd, Federal Reserve System Contingency Processing Center, discussed innovative strategies for returning to "business as usual" for those critical organizations that affect the entire society, i.e., utilities, securities firms, and military command and control. Judd suggested that contingency planning be extended beyond the "cook book" approach. His fundamental belief is that the ability to return to normalcy lies in the commitment of senior management, and that the planning, testing, and training remain dynamic to the degree that it matches the changing business environment.

Training and Awareness

Several papers addressed the importance of computer security training and awareness. Elizabeth Markey, U.S. Department of State, described the approach her organization has taken to train their personnel to counter risks that threaten the organization's computer systems. Markey explained that a series of carefully structured systems security seminars and briefings are held for all levels of personnel, including managers, line security personnel, and users. Markey described a 2-hour briefing that is presented to Executive Directors; a 4-day seminar for Regional Security Officers; and a 1- to 2-hour briefing for all new employees.

Eliot Sohmer, NCSC, described the computer security curriculum being developed there. The course is modular and addresses both non-technical and technical issues. Not unlike the training and awareness program developed by Department of State, NCSC's training plan is designed to meet the needs of various categories of personnel ranging from product evaluators to research and development specialists to clerical and administrative assistants. It is planned that each training module will be videotaped and will be available to other government agencies, universities, and vendors.

DOD Computer Security Research and Development Programs

A panel summarized the progress and plans for research and development in the Federal government in the areas of secure architectures, data base management systems (DBMS), networks, modeling and verification, and aids to evaluation.

Data Base Management Security

A joint paper "Data Integrity vs Data Security," by Rhonda Henning and Swen Walker, NCSC, summarized past and current thoughts on these two subjects. Henning pointed out that the presence of a trusted operating system does not guarantee that the DBMS can be used to share information in a trusted way. She stated that the integrity concerns were not sufficiently addressed by conventional secrecy policies. Henning reviewed several integrity policy alternatives concluding that few have actually proven successful in operational environments. She recommended that each application be examined to determine which integrity policy best fits its requirements. Henning further suggested that a combination of integrity policies may be more appropriate.

Social Issues and Ethics

Two papers addressed social issues and ethics in computer security. Dorothy Denning presented a joint paper she wrote with Peter Neumann and Donn Parker, SRI International. Denning examined the social aspects of computer security with respect to the computerized monitoring technologies being developed. She spoke of how many users respond negatively to computer security because they view it as interfering with their productivity and in some cases a violation of their rights. She said these problems stem from a misalignment of the concerns and values of management with those of their employees on the effects of security policies and mechanisms. She believes that the use of security surveillance of computer users could increase this misalignment. Denning recommended that threat monitoring techniques be carefully applied to preserve the rights of privacy and freedom from intrusion and should avoid creating an atmosphere that leads to employee suspicion and dissatisfaction. She further stated that while monitoring user's activities is necessary for accountability and detection of irregularities, threat monitoring must be done with informed consent. Denning also suggested that organizations align their security policies with computer users outside the organization. She suggested setting up a computer system somewhere in the world which offered programming games with prizes and recognition of winners. The purpose is to provide more healthy outlets for the non-malicious hacker. Denning concluded that it is vital that the technological and social considerations be balanced so that serious problems may be avoided.

Marlene Campbell, Murray State University, discussed the need to bring ethics into the classroom and the workplace. Campbell emphasized the need to train our young people in the ethics of protecting our computer systems. She illustrated through several examples that a lack of ethics is a cause of computer crime. Campbell concluded that while security mechanisms and laws are provided to temper the activities of computer users, the truly binding controls rest with the professional ethics of each user.

Hacker Problem

Ken McLeod, a former Arizona sheriff who was involved in numerous computer fraud cases and is now a consultant on computer crime issues, provided a dramatic finale to the conference. McLeod presented videos of criminal interrogations and a "hacker" at work. His presentation provided a vivid understanding of the malicious hacker problem.

For More Information

Proceedings from this conference are available upon request. You may write or call Irene Isaac, NBS, ICST, Building 225, Room B266, Gaithersburg, MD 20899; (301) 975-3360.

The following documents may be ordered from the NCSC:

1. *Proceedings, 10th National Computer Security Conference*, 21–24 September 1987.
2. *Department of Defense Trusted Computer System Evaluation Criteria*, DOD 5200.28-STD, December 1985.
3. *Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria*, NCSC-TG-005, Version 1, 31 July 1987.

Irene E. Isaac
Institute for Computer Sciences and Technology
National Bureau of Standards
Gaithersburg, MD 20899