Information Assurance Technologies: 10 Years Past, Present and Future

Chair

- Jack Murphy, Ph.D, Electronic Data Systems

Panelists:

- Gary Moore, Entrust
- Dr. Tom Haigh, Secure Computing Corp.
- Robert Giovagnoni iDEFENSE
- Ronda Henning Harris

In the next decade Information Assurance will dominate the attention of many CIOs. The technologies and service offerings have evolved significantly in the past 10 years. Basic protocol filters and limited proxy servers provided boundary protection. The secure socket layer protocol provided transport security for client/server applications. And operating system provided basic event information for host security monitoring. As concerns for scalability and performance of information assurance increased, the focus shifted. PKI has gained attention as a scalable technology for identification and authentication and firewalls began to introduce performance-enhancing techniques. Still, the threat increases. Simple amateurish e-mail viruses continue to plague CIOs. Professional hackers are becoming more sophisticated every year in identifying and exploiting network, host, and application vulnerabilities. Rapid, effective response to these threats is one of today's biggest problems. No wonder CIOs will spend so much of their time and resources in Information Assurance if the companies they serve are to increase competitiveness in their respective industries. Success over the next 10 years depends upon the results of Research and Development in progress today.

This panel consists of five representatives of the Information Assurance industry who will discuss the evolution of Information Assurance technologies and solutions over the next 10 years. The challenge will be to balance competing demands to enhance organizational mission capability through information technology and enhance security in response to increasing threats. Striving for measurable improvements in both requires new, improved, and integrated approaches.

Dr. Jack Murphy (Electronic Data Systems) is the Chief Architect for the EDS Information Assurances Center of Excellence serving government and commercial clients. He has developed security architectures and designed Information Assurance solutions while integrating best industry practices and products.

Gary Moore (Entrust Technologies, Inc) is the Technical Director for Entrust's Federal Systems Division. He has worked with both Government and Commercial clients over the last six years in architecting comprehensive PKI solutions to address the needs of e-business and e-government. He has also been directly involved in the developing Federal Bridge CA within the civilian and Defense agencies.

Position Statement: The Comprehensive PKI and Privilege Management—As the area of PKI has rapidly developed over the last five years there has been a recognized need to step beyond the authentication and confidentiality aspects offered by the Public Key Infrastructure available today and to step into the realm of authorization. Knowing who is involved in a transaction is a part of the complete need to finalize that transaction. Providing privilege management to the environment becomes the next major step. This developing area will be discussed in terms of capabilities today and those that are developing.

Dr. Tom Haigh (Secure Computing Corp.) As Vice President and Chief Technical Officer for Secure Computing Corporation, Dr. Tom Haigh is responsible for the development of product evolution strategies and technology roadmaps across the company's product and Advanced Technology divisions. Prior to his current position, Haigh was Vice President and Director of Research at Secure, where he focused on developing acquisition plans, and planning and implementing contract and independent research and development programs. Dr. Haigh has written and presented many papers on computer security, most recently at the 1999 Electronic Commerce World and Internet Electronic Commerce (iEC) conferences. He has taught courses on information security at the UCLA Extension, and he has served on the program committees for the IEEE Symposium on Security and Privacy, the IEEE Workshop on the Foundations of Computer Security, and the Workshop of IFIP Working Group 11.3 on database security. He has a Ph.D. in Mathematics from the University of Wisconsin, Madison.

Position Statement: The nature of information assurance has changed with the evolution of information system technology, the role that information systems play within the enterprise, and corresponding changes in vulnerability and threat models. At one time a simple lock on the door to the computer room was adequate assurance. In the days of time-share systems, the emphasis was on careful design and analysis of the underlying operating system. The growth networking led to the enclave model of information assurance, with its strong emphasis on firewalls and perimeter defense. The rapid evolution of e-business is making even that model of information assurance obsolete.

Over the next ten years, the challenge for information assurance practitioners will be to allow large numbers of partners into the enterprise while controlling and monitoring their activity. Moreover, the phenomenon of Internet time requires that we do this with less than perfect products that are used in ways they were not designed to be used. Information assurance for e-business environments is both a local problem and a global problem. Locally it requires a much deeper layering of protection mechanisms within the enterprise. Globally it requires significant enhancements to the underlying information infrastructure as well as expanded cooperation across enterprises and national boundaries.

Robert Giovagnoni (iDEFENSE) is Executive Vice President for Strategic Relations. He has been intimately involved in the government's efforts on critical infrastructure protection for several years and is recognized at the highest levels of the federal government as a legal expert on computer crime and cyberspace law. He came to iDEFENSE from the Critical Infrastructure Assurance Office (CIAO), where he served as General Counsel and Assistant Director. He helped organize the President's Commission on Critical Infrastructure Protection and served as General Counsel to the PCCIP and its Transition Office, both predecessors to the CIAO. He was a key author of Presidential Decision Directive 63, Protecting America's Critical Infrastructures. He has also authored numerous articles on Information protection and assurance as well as the private sector’s role in protecting critical infrastructures. Mr. Giovagnoni holds a Bachelor of

Arts degree from Manhattan College, a Juris Doctorate from St. John's School of Law, and a Master's of Law degree from the University of Missouri at Kansas City.

Position Statement: Viewing information as the most significant security tool of the next millennium, he will be addressing the need for a realistic assessment of the threat environment as key to protecting systems and avoiding both corporate and individual corporate leadership liability – an issue that is particularly relevant in light of the proposed Treasury rules/guidelines under Gramm-Leach-Bliley (Public Law 106-102), which places upon the financial services industry an obligation to ensure the security and confidentiality of customer records and information, to protect against any unanticipated threats or hazards to security or integrity of such records, and to protect against unauthorized access to or use.

Under the proposed Treasury rules, current and timely threat and threat assessment information will be essential to boards of directors and managers, whose responsibility it will be to oversee efforts to develop, implement, and maintain an effective information security program. The responsibilities of management will include 1) evaluating the impact of changing business arrangements on the institution's security program and 2) reporting on the overall status of the information security program, including material matters related to the following: risk assessment; risk management and control decisions; results of testing; attempted or actual security breaches or violations and responsive actions taken by management; and any recommendations for improvements to the information security program."

Ronda Henning (Harris) is the senior Secure Systems Engineer for Harris Corporation, Government Communications Systems Division; a Melbourne, Florida based international communications and electronics company. Ms. Henning currently leads the Information Assurance center of excellence, an interdisciplinary engineering group responsible for information assurance technology research and development as well as assurance technology insertion for large-scale systems integration opportunities. Prior to her employment at Harris, Ms. Henning worked in information security research and development at the National Security Agency. A Certified Information Systems Security Professional (CISSP), she holds an M.B.A. from the Florida Institute of Technology, an M.S. in Computer Science from Johns Hopkins University, and a B.A. from the University of Pittsburgh.

Position Statement: What does the future hold for Information Assurance Solutions? As communications technology becomes ubiquitous, assurance technologies will also be more pervasive. The "wired world" of today will evolve to the wireless, miniaturized world of tomorrow. Concurrent with the continuing communications evolution will come an information assurance revolution. Assurance technologies today focus on confidentiality and prevention of denial of service. Tomorrow, we will focus more on personal protection and data management. The medical and credit histories, even the very genomes that comprise a person, will be inherently safeguarded. Biometrics will be taken beyond fingerprints and retina scans to nonintrusive technologies, and self-healing networks will be able to restore themselves to a known state.

That's the best possible picture of tomorrow. In actuality, we will still be searching for the pervasive PKI infrastructure, reductions in false positives in intrusion detection systems, and enterprise level security management that can adapt to an organization's security policies. While information assurance will be an integrated component of systems development, that is not the primary issue. The real question is whether the economics of information assurance can bear the

development and deployment of higher assurance technologies without sacrificing product time to market or cost advantages.