Assurance Forum: Lessons Learned

Moderator: John Adams, Trusted Information Systems.

Debate has raged over the best way to obtain assurance about information systems. Researchers conduct painstaking analyses of alternative techniques and discover strengths and weaknesses of each. Technical journals are filled with passionate arguments in favor of one technique or another. When the dust settles, what is the user to do? What practical, cost-effective techniques exist for the vendor and user to employ in systems that must protect sensitive information?

The Forum on Assurance presents the work of practitioners who have employed a variety of techniques for identifying, obtaining, measuring, and monitoring assurance in information systems. These are not theoretical studies of what might be done; rather, they are the results of actual implementations. Presenters discuss their assumptions, their accomplishments, and lessons learned in their efforts to solve the most perplexing problems in information security today.

Karen Ferraiolo, Arca Systems.

There are many efforts currently looking at alternative ways of providing assurance with the intent of reducing the time and cost associated with traditional product evaluation and system certification. The Systems Security Engineering Capability Maturity Model (SSE-CMM) Project has as one of its goals to provide a mechanism that would give a measure of process capability-based assurance. Research is currently being conducted to determine the actual contribution of process capability as measured by the SSE-CMM. This presentation will report on this research by discussing answers to the following questions:

--Would demonstration of process capability provide assurance?

--Can SE-CMM organizational ratings for specific types of organizations, products, and systems be formulated for the purpose of building assurance arguments?

Dr. Dixie Baker, SAIC.

Patient Centered Access to Secure Systems Online (PCASSO) is a three-year research project funded by the National Library of Medicine (NLM) of the National Institutes of Health (NIH) to develop, test, and deploy a model system for accessing highly sensitive patient information (including HIV/AIDS, adoption, mental health, genetic, etc.) over the Internet. (The PCASSO project and architecture are described in a separate paper presented at the conference.) The healthcare industry is looking to electronic commerce to provide solutions for securing Internet access to patient information. PCASSO argues that these technologies, while necessary, do not provide a comprehensive solution. PCASSO uses state-of-the-art security technologies and assurance methods, including B2-assurance in the host, role-based access control, SSL encryption, Java, and intrusion detection to provide a level of assured protection that hopefully will be acceptable to both patients and providers.

Jan Filsinger, Trusted Information Systems.

The security community has pondered various aspects of security assurance and concluded that security assurance can be multidimensional -- meaning that security assurance can be derived from different types of analysis and techniques. The employment of new information assurance techniques is required for the development and deployment of systems that are critical in military and commercial environments. To support the growth of complex computer systems and technologies employed to develop and implement these systems, alternatives to assessing and measuring system security are needed. This presentation presents a multidisciplinary approach to maintaining a high standard of information assurance, especially in the domain of distributed systems.

William Dawson, BDM International

The DOCKMASTER II System, which replaces the operational DOCKMASTER I system, is a National Security Agency (NSA)-sponsored information system that provides communications to geographically dispersed users and management of INFOSEC Activities. Strong data, user, and communications security protections are provided while maintaining a user-friendly Web-based interface. Additionally, the system provides reliable and secure management of Unclassified and Proprietary Information and will upon completion of the B2 evaluation also provide this management to Secret Information.
The approach, challenges, and lessons learned in the Certification and Accreditation of the DOCKMASTER II System as the system evolved from a centralized host based architecture to its now operational distributed client/server web based architecture has been unique in that not just the system components but the entire DOCKMASTER II System must meet the B2 level of assurance.