Authors' Commentary: The Outstanding Information Technology Security Papers

Ronald C. Dodge, Jr.
Information Technology and Operations Center
United States Military Academy
West Point, NY 10996
ronald.dodge@usma.edu

Daniel J. Ragsdale
Dept. of Electrical Engineering and Computer Science
United States Military Academy
West Point, NY 10996
daniel.ragsdale@usma.edu

Introduction

Information Assurance (IA) education and training in today's world is increasingly important. Several incidents in the past few years, such as data theft, malicious worms and viruses, denial of service attacks, and defacement of corporate and government web pages highlight the need to educate users and administrators of information systems. IA is more than just the simple application of technical measures to secure an information system; it is the combination of defensive technologies; well-conceived policies and procedures, and properly trained users [Maconachy et al. 2001].

Computer networks are ubiquitous, but aside from a relatively small number of network engineering professionals, few understand the fundamentals of information assurance (IA). Many institutions of higher learning that offer degrees in computer science offer courses that address the topic of computer networks. Often these courses focus on network protocols and theory, with little emphasis on the policy and hands-on application that individuals in organizations face every day. The integration of security practices into the business model of an organization is laden with tradeoffs. The implementation of security measures often has both direct costs and productivity costs as affected

The UMAP Journal 25 (2) (2004) 171–174.

information systems become more difficult to use or are degraded with the introduction of enhanced security measures.

Formulation and Intent of the Contest Question

The main goal of this year's interdisciplinary modeling problem was for competitors to reduce the potential costs associated with malicious behaviors in an simulated organization. This reduction results from the implementation of the set of preventative measures that were identified by the contest participants. The problem of how an organization maximizes its IT security posture while considering the overall economics impact on its mission requires an analysis of the known, expected, and potential costs. Organizations must analyze this problem in three primary areas: First, the organization must define the areas of risk in the IT infrastructure. Typically these are data confidentiality, data integrity, and service availability. Next the sources of risk need be identified, for example a malicious outside hacker, a "clumsy" insider, or hardware/software failure. Finally, the costs must be enumerated. This includes both the costs associated with security measure implementation (such as direct costs, training and productivity) and the potential costs if any or all of the areas of risk are compromised.

This is a complex problem that requires a thorough analysis of many variables that have positive impacts in one area and negative impacts in another [Bishop 2002, 17–18; Garfinkel and Spafford 1996, 27–40]. Additionally, an organization might have missions that vary within its structure that require different security measures. The problem of how to design and implement the security architecture of an organization is further complicated by the dynamic nature of the problem. The evaluation conducted in the early stages of an assessment will be modified over time by changes in the organization mission and advances in technology. In building the framework for this year's modeling question, we attempted to generalize many factors to enable the students to build tractable models.

The problem posed to the teams described a generic organization (a university) that consisted of several competing components that in some ways required completely different and competing security measures. The organization required both an open environment for information distribution and student access and a more secure system for grades, tuition, and book store management. Additionally, a hybrid solution was required for a third group made up of staff and faculty. The specific identification of these needs and several others was left to the teams as part of the analysis process.

The teams were then required to examine the efficacy of various technical solutions and security policies in light of the various organization requirements. The solutions were then balanced against the overall potential for loss due to

security failings and the direct costs of the security architecture. This underlines the fundamental premises that: the total cost of a security solution is the sum of the direct financial costs and the indirect costs due to usefulness and productivity and an organization should not spend more on a solution that it is at risk for losing. For example one would not be wise to install a $10,000 alarm system on an item valued at $1,000.

Lastly, the ICM teams were required to analyze their proposed solutions model's ability to withstand technology changes as time passes.

References

Maconachy, V., C. Schou, D. Welch, and D.J. Ragsdale. 2001. A model for information assurance: An integrated approach. In *Proceedings of the 2nd Annual IEEE Systems, Man, and Cybernetics Information Assurance Workshop* (West Point, NY, June 5–6, 2001), 306–310.

Bishop, Matt. 2002. *Computer Security: Art and Science*. Boston, MA: Addison-Wesley.

Garfinkel, Simson, and Gene Spafford. 1996. *Practical Unix and Internet Security*. 2nd ed. Sebastopol, CA: O'Reilly and Associates.

About the Authors

The authors of this year's contest question have been working in the area of Information Assurance for a combined 18 years. The foci of their research include:

- Information assurance simulation development. The problem posed in this year's modeling contest closely mirrors the scenario used to frame simulation being developed under an NSF grant. Various components of the simulation have been under development since 2001 and have been the topic of five conference papers.
- Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) analysis and implementation, including the development and deployment of innovative IDS and IPS solutions, such as honeynets, layer-2 bridges, and attribution technologies.
- Virtual machine technology. The authors have pioneered the use of virtual machines (VMs) to overcome resource constraints encountered by computer science programs enabling each student to manage and administer a robust collection of servers and workstations.

- Information assurance curriculum development. The authors have integrated the use of VMs into a hands-on curriculum consisting of a variety of introductory and technical computer science courses as well as policy-based analysis courses. The development and use of VMs is the topic of six conference and journal publications.
- Competitive cyber defense exercises. The authors developed and implemented the U.S. Military Academy Cyber Defense Exercise. This model is being used as the benchmark for an NSF-funded effort to introduce competitive cyber exercises to civilian universities.

Major Ronald C. Dodge, Jr., has served for more than 16 years as an Aviation officer and is a member of the Army Acquisition Corps in the United States Army. His military assignments range from duties in an attack helicopter battalion during Operation Just Cause in the Republic of Panama to the United States Military Academy. Currently, he is an Assistant Professor and Director of the Information Technology and Operations Center (ITOC) at the United States Military Academy. Ron received his Ph.D. from George Mason University, Fairfax, Virginia in Computer Science. His current research focuses are on information warfare, network deception, security protocols, internet technologies, and performance planning and capacity management. He is a frequent speaker at national and international IA conferences and he has published many papers and articles on IA topics.

Colonel Daniel J. Ragsdale has served for 23 years as an officer in the U.S. Army. He has served in a variety of important operational, and research and development assignments, including participation in Operation Urgent Fury in Grenada and Operation Enduring Freedom in Afghanistan. Currently, he is an Associate Professor and Director of the Information Technology Program, Professor in the Department of Electrical Engineering and Computer Science at the U.S. Military Academy. His current research focuses on information security, Information Assurance (IA), and Information Warfare. He is a frequent speaker and panelist at national and international IA conferences and he has published dozens of papers and articles on IA topics.