GSAW 2010 Tutorial J:

Cybersecurity in the Ground System

Length: Half Day

Overview:

National Security Space (NSS) systems have always faced threats from attackers who seek to acquire secrets, corrupt data, interfere with processing of data, or impede access to mission critical information. As technology has advanced, the challenges to NSS systems have grown. The cyber threats have become more advanced and more persistent, the commercial software on which NSS systems rely are riddled with vulnerabilities, and our global supply chain offers many points at which software or hardware could be compromised. Potential mission consequences have become increasingly serious, especially where net-centricity increases interdependencies and where topics such as resilience and continuity may not have been adequately addressed. In addition, because NSS systems often provide truly unique products and services, these systems are often at higher risk than other systems that face many of the same threats. Therefore, it is no longer sufficient to design an accreditable system; our NSS systems must also be engineered to withstand sophisticated cyber attacks. This tutorial delivers 4 modules addressing technical challenges in cybersecurity relevant to NSS and describes concerns for the future.

SOA Security Challenges and Solution Patterns
Summarizes the challenges of SOA-based systems and describes enterprise-level design patterns, derived from existing systems that enable the construction of SOA-based information systems that meet security objectives.

Network Security Challenges in Net-centric Computing
This module will cover common network security issues in NSS systems and will describe classes of attacks and approaches to mitigating risk.

Cloud Computing: Overview and Issues
Describes the various IT capabilities referred to as cloud computing and explain why Clouds are being widely embraced. With any new IT “silver bullet” come interesting and challenging security problems that must be understood and addressed. This module will explore both the security weaknesses and the security strengths hidden in the cloud.

Test Strategies for NSS programs
Information system security testing is performed at several points in the development cycle, both for components and the system, and requiring multiple certifications. Yet, even with extensive testing, numerous vulnerabilities continue to be identified and exploited by attackers. This module will look at current testing approaches and explore new approaches that may be applicable to National Security Space systems.

Instructors: Marion Michaud, Russ Reopell, MITRE Corporation; Robert Lindell, Mikhael Felker, The Aerospace Corporation

Biographies:

Dr. Marion Michaud is an Executive Director of the Information Security Division at the MITRE Corporation. Marion is responsibility for directing MITRE's information security engineering and information assurance efforts for MITRE's sponsors and for protecting the MITRE infrastructure and information. She has been providing information security and systems engineering for various government agencies for 27 years. She holds an M.S. and Ph.D. in Applied Mathematics from Brown University, Providence, RI and a B.S. in Mathematics and Education from Syracuse University, Syracuse, NY.

Mr. Russ Reopell is a Principal Information Security Engineer at the MITRE Corporation. Russ has been providing security engineering support to the Department of Defense for over 20 years. His efforts have included large-scale systems for the U.S. Air Force and U.S. Navy where his focus was on authentication, authorization and access controls. He has spent the last few years focused on service-oriented architecture (SOA) and the role identity and access management have in that area. Prior to becoming a security engineer, Russ worked as a software developer on a major radar program for the U.S. Air Force. He holds a B.S. in Computer Science from North Adams State College in North Adams, MA.

Mr. Robert Lindell is a Senior Project Leader at The Aerospace Corporation in the Computers and Software Division. Recently, he provides engineering support to National Security Space programs in the areas of networking and information assurance. He has supported TSAT, AEHF, AFSCN, GBS, and DMSP. Bob previously worked at Information Sciences Institute (ISI) in their networking division. At ISI, he worked on various DARPA and NSF programs including the RSVP protocol, active networks, application layer multicast, and DDoS detection and prevention systems. Mr. Lindell has a B.S and M.S degree in Computer Science from UCLA.

Mr. Mikhael Felker is a Member of the Technical Staff at the The Aerospace Corporation in the Information Assurance Technology Department. He provides information assurance support for satellite systems. Mr. Felker is also an Instructor within the Computer & Information Systems Division at UCLA Extension and is actively involved in the Los Angeles information security community. He is the Education Director for the Information Systems Security Association (ISSA) and speaker at various security groups including Information Systems Audit and Control Association (ISACA), and Open Web Application Security Project (OWASP). Mr. Felker has published articles on information security in IEEE Security & Privacy, the ISSA Journal, Information Systems Control Journal, and SecurityFocus. He has a B.S. degree in Computer Science from UCLA and an M.S. in Information Security Policy & Management from Carnegie Mellon University.

Ms. Emily Hawthorn is a Principal Information Security Engineer at the MITRE Corporation. She is part of the team researching Cloud Computing security. Since joining MITRE, Ms. Hawthorn has performed vulnerability assessments, led intrusion detection teams, and deployed Public Key Infrastructure systems for various customer organizations. She has over 30 years of information security experience in multiple operating system environments. She holds a B.A. in Mathematics from Rice University, Houston, TX.

What Participants Should Expect to Learn

Gain familiarity with Cybersecurity technologies that are critical to NSS programs.

Who Should Attend:

Familiarity with ground systems engineering, information assurance, information technology.