GSAW 2016 Tutorial E:

A Proven Methodology for Developing Secure Software and Applying It to Ground Systems

Length: Full day

Overview:

Part One opens with a discussion of current cyber threats facing developers and their applications — who these threats are, what they are doing, and why they are doing it. Next the presentation explores the principle of Defense In-Depth, which defines and outlines the effectiveness of layered security. Participants then learn to apply security within each step of the software development lifecycle. Then the discussion shifts focus to errors, weaknesses, and exploits — diving into why errors happen, how easily they are exploited, and a proven process to prevent errors and subsequent exploitation. As the part one winds down, attendees are shown two proven Threat Model approaches and an exercise on how to use them. Finally, part one discusses static, dynamic, and component testing, and participants learn about available testing tools.

Part Two expands upon Part One in an attempt to translate the methodology for ground system personnel. The goal is to build upon the methodology presented in part one by showing examples and details on how to implement the methodology.

Instructors: Barry Lyons IV, SGT, Inc. and Brandon Bailey, NASA IV&V

Biographies:

Barry Lyons has 23 years of extensive, leading edge Cyber/ Information Assurance (IA) security expertise and systems engineering experience focusing on the architecture, design, implementation, certification and accreditation, management and operations of mission critical enterprise systems, airborne solutions, cross domain information sharing solutions, and comprehensive "Need to Know/Need to Share" On Demand Information Delivery solutions. Highly skilled in all critical disciplines and activities required for management and oversight of enterprise network and application systems. Extensive experience in large scale enterprise applications and leading edge software solutions designed specifically to meet mission critical needs. Dynamic, fun speaker.

Brandon Bailey has 10 years of experience in the test and evaluation field with specialization in cybersecurity. Brandon has experience testing in both the intelligence and civil space arena. Recently Brandon's work at National Aeronautics and Space Administration (NASA)'s Independent Verification and Validation Program involved building and managing a software testing and research laboratory as well as leading the information assurance and cybersecurity activities as they relate to NASA's space and ground missions. These efforts resulted in improving the security for the mission segments within NASA's enterprise which includes: vulnerability assessments, infusing secure coding principles, counteracting the threat landscape by infusing security analyses in the standard IV&V workflow and working within the CCSDS security working group to develop international security standards.

Description of Intended Students and Prerequisites:

With no prerequisites, this seminar is designed to inform and equip software developers and testers along with their managers, program managers and senior management, with the knowledge of how to develop applications securely. This is not a coding session but a methodology tutorial with emphasis on how to apply it to ground systems.

What can Attendees Expect to Learn:

Part 1:

- A proven methodology on how to develop secure code based on a standard SDLC approach
- Why traditional Defense-in-Depth no longer works
- Why & how it is so easy for attackers to exploit code
- SECOPS vs. CONOPS – how they complement each other and why both are needed
- How to use readily available tools to determine common weaknesses and attack patterns
- How to perform successful Threat Modeling
- How to incorporate Abuse cases during the requirements phase
- How to identify & apply application security mechanisms
- The differences and benefits of Static, Dynamic & Component vulnerability testing
- How to determine if there is any “hidden” Open Source code within the application
- Added Bonus: “How to Avoid the Top Ten Software Security Flaws” from the IEEE Center For Secure Design

Part 2:

- Learn how the methodology presented in part one applies to ground systems (see outline for additional details)