GSAW 2018 Tutorial I:

Reducing the Software Risk in Ground System Software

Length: Half day

Overview:
Course Outline:

a. Defining what is software in the ground system
    i. Software is custom developed, COTS, GOTS and FOSS
    ii. Metrics from 3 year's worth of SW analysis on ground systems
    iii. Examples of actual ground software vulnerabilities/weakness discovered during code analysis or penetration tests (e.g. Front End Processor)
b. Discuss security requirements or lack thereof for secure software
    i. Can NIST help?
    ii. Continuous Data Monitoring (CDM) saving the day?
c. Describe end to end approach for reducing software risk
    i. Classify the weaknesses and vulnerabilities you want to remove
        1. CWSS, CWEs, CVEs
    ii. Develop or follow coding standards to prevent weaknesses
    iii. Test for adherence to coding standards and presence of weaknesses or vulnerabilities
d. Why securing software doesn't cure all?
    i. Need for Defense in Depth
        1. Discuss enclaves, pivot points and attack depth
e. Things to implement now if securing software is unachievable
    i. Securing existing assets
        1. Network layer
        2. Host layer
    ii. Future Deployments
        1. Implement coding standards/best practices
    iii. Train developers, managers, etc.

Instructor: Brandon Bailey, NASA IV&V

Biography:
Brandon Bailey has over 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:
Have understanding of basic software development. The audience are developers and managers for developers. Will be a mix of detailed technical content as well as concepts for management.

What can Attendees Expect to Learn:
An estimated 84% of all security breaches are application-related, not firewall violations. To what extent is your organization focused on addressing security issues in its software? Software plays a critical role in mission success, and software similarly plays a role in mission security. However, software can introduce vulnerabilities to the system, such as use of a COTS product that has a backdoor, or a hole in the security of the system deliberately left in place by designers or maintainers. The motivations for such holes are not always sinister, but can provide a means for malicious intrusion into the mission. Students will learn an approach to securing ground software within the context of federal information systems. Federal requirements, coding standards, tool usage will be discussed as part of the solution to securing software.