GSAW 2020 Tutorial E:

Reducing the Software Risk in Ground System Software

Length: Half day

Overview:
Tutorial Outline:

- Getting on the Same Page with Ground Systems
  - Defining ground systems @ NASA and in DoD
- Threat Landscape
- What is SW in a Ground System?
- SW Security is Required but Barriers Exist
- What is FISMA / NIST's role in SW security
- Approach for Secure and Resilient Software
  - System Threat Modeling
  - Sample Process for Developing Secure Software
    - System Security Threat Understanding
    - Develop Security Strategy
    - System Security Plan
    - Secure SW Development (COTS/FOSS/Supply Chain)
  - Alphabet Soup – VA, SCA, OA, CWE, CVE, CWSS
- SW Assurance without Source Code (Binary Analysis)
- Ground Software Examples and Metrics
- Near Team Goals and What to do Now for Legacy?
- Trends and Lessons Learned
- Future: DevSecOps and Cloud

Instructor: Brandon Bailey, The Aerospace Corporation

Biography:
Brandon Bailey, Cybersecurity Senior Project Leader

- Graduated Summa Cum Laude with a bachelor's degree in Electrical Engineering from West Virginia University and currently holds multiple certifications in the cybersecurity field
- While at NASA Brandon was responsible for building and maintaining a software testing and research laboratory to include a robust cybersecurity range as well as spearheading innovative cybersecurity assessments of ground infrastructure that support NASA's mission operations
- Joined Aerospace in June 2019 but he has spent his entire 14-year career supporting the intelligence and civil space arena (NRO, NGA, NASA)
- While at NASA Brandon was responsible for building and maintaining a software testing and research laboratory to include a robust cybersecurity range as well as spearheading innovative cybersecurity assessments of ground infrastructure that support NASA's mission operations
- Brandon's specialties include vulnerability assessments / penetration testing of ground infrastructure for space systems and infusing secure coding principles within the software supply chain.
- While at NASA he was honored with several group and individual awards to include NASA's Exceptional Service Medal for his landmark cybersecurity work (2019), NASA's Early Career Achievement Award (2016) as well as a NASA Agency Honor Awards for Information Assurance/Cybersecurity (2015). Brandon has also contributed to teams who have received honorable mention in the 2012 and 2016 NASA's Software of the Year competition. mention in the 2012 and 2016 NASA's Software of the Year competition.

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.