Tutorial Title: Security Design of Mission-Critical Embedded Systems

Instructor: Dr. Michael Vai, Secure Resilient Systems and Technology Group, MIT Lincoln Laboratory, (mvai@ll.mit.edu);

Michael Vai is a senior staff member in the Secure Resilient Systems and Technology Group, Lincoln Laboratory, Massachusetts Institute of Technology. From 2012 to 2015, he served as an assistant leader of the same group. Previously, he was an assistant leader of the Embedded and Open Systems Group in the Intelligence, Surveillance, and Reconnaissance and Tactical Systems Division. He has worked in the area of embedded systems and technology for more than 25 years, leading the development of advanced embedded systems and publishing his research extensively. Prior to joining Lincoln Laboratory in 1999, he was on the faculty of the Department of Electrical and Computer Engineering at Northeastern University. During his tenure, he conducted multiple research programs funded by the National Science Foundation, Defense Advanced Research Projects Agency, and industry. His current research interests include secure and resilient embedded systems and technology, particularly systems involved in tactical operations. He received his master's and doctoral degrees from Michigan State University, in 1985 and 1987, respectively, in electrical engineering.

Summary:

This tutorial explains a systematic approach of co-designing functionality and security into mission-critical embedded systems.

The tutorial starts by reviewing common issues in embedded applications to define mission objectives, threat models, and security/resilience goals. We then introduce an overview of security technologies to achieve goals of confidentiality, integrity, and availability given design criteria and a realistic threat model. The technologies range from practical cryptography and key management, protection of data at rest, data in transit, and data in use, and tamper resistance.

A major portion of the tutorial is dedicated to exploring the mission critical embedded system solution space. We discuss the search for security vulnerabilities (red teaming) and the search for solutions (blue teaming). Besides the lecture, attendees, under instructor guidance, will perform realistic and meaningful hands-on exercises of defining mission and security objectives, assessing principal issues, applying technologies, and understanding their interactions. The instructor will provide an example application (distributed sensing, communicating, and computing) to be used in these exercises. Attendees could also bring their own applications for the exercises.

Attendees are encouraged to work collaboratively throughout the development process, thus creating opportunities to learn from each other. During the exercise, attendees will consider the use of various security/resilience features, articulate and justify the use of resources, and assess the system's suitability for mission assurance. Attendees can expect to gain valuable insight and experience in the subject after completing the lecture and exercises.

The instructor, who is an expert and practitioner in the field, will offer insight, advice, and concrete examples and discussions. The tutorial draws from the instructor's decades of experience in secure, resilient systems and technology.

Target Audience:

This tutorial is designed for embedded system designers, hardware and software engineers, and project managers interested in an overview and introduction to cyber security with emphasis on embedded computing.

Prerequisite:

We expect the audience to have general knowledge of embedded systems. The use of a laptop for the exercises is optional but helpful.

Tutorial Organization:

1. Introduction (15 mins)
    a. Embedded system definition
    b. Embedded system design methodology
    c. Security, resilience, and mission assurance
    d. Overview of the tutorial
2. Embedded system development (60 mins)
    a. Mission
    b. Platform
    c. Life cycle threats (supply chain, manufacturing, deployment, etc.)
    d. Technologies for security and resilience
3. Solution Exercise (60 mins)
    a. Design and assessment
    b. Metrics and return-on-investment
    c. Residual vulnerabilities and mitigations
4. Summary and further studies (15 mins)

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported under Air Force Contract No. FA8721-05-C-0002 and/or FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the U.S. Air Force.