Software Engineering Institute | Carnegie Mellon

Software Assurance Engineering Workshop

Providing program management, system engineers, and software engineers with the latest methods, tools, and practices

***Software assurance** - implementing software with a "level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software, throughout the life cycle…"* *Section 933 of National Defense Appropriation Act 2013*

This workshop focuses on the decisions made early in the acquisition and engineering lifecycles that influence software assurance. The purpose of this course is to expose participants to the concepts and resources available to address software security assurance across the acquisition and development lifecycles. Tailored to address your organization's specific needs, this workshop combines lecture material with exercises and discussions.

The introduction establishes the importance of focusing on software assurance within the current development and acquisition environment. Assurance methods relevant to each of the four critical software assurance areas are presented and participants are encouraged to discuss ways that adoption into the existing acquisition and development lifecycles would improve their organizational software assurance.

Why attend?

While traditional security principles are still usable today for the security within an individual piece of technology, these principles are no longer sufficient to address the complexity and sophistication of the environment within which that component must operate. It is now important to consider the large-scale, highly networked, software-dependent systems upon which our critical infrastructure, from phones to power and water and industries such as banking, medicine, and retail, depend.

Who should attend?

The target audience includes software managers and technical leads, software and lead engineers, software and system acquisition experts, and program/project managers who are concerned with software security assurance across the acquisition and development lifecycles.

Topics

The following topics are covered in the workshop:

In **Introduction to Software Assurance (SwA)**, we define software assurance and describe the current operational landscape where software assurance is needed. The challenges identified to date for addressing software assurance are described:

- security principles are not sufficient for software assurance
- systems engineering does not effectively address software
- software's role in systems is increasing

Software assurance principles are introduced and additional issues with software that affect software assurance are described.

Software Assurance Engineering Workshop

Providing program management, system engineers, and software engineers with the latest methods, tools, and practices

In **SwA for Development**, we review the range of resources available for building security in as well as provide a brief overview of the Microsoft Secure Development Life Cycle (MS SDL) and a mapping of SEI practices to various MS SDL activities. Three useful process models for requirements engineering are described:

- Comprehensive Lightweight Application security Process (CLASP)
- Security Quality Requirements Engineering (SQUARE)
- Security Requirements Engineering Process (SREP)

Threat modeling is described using the STRIDE process developed by Microsoft and an industry case study in which threat modeling was applied across the organization to address software assurance.

In **Mission Assurance**, the relationship of a system to an operational mission is described. An example of mission failure (2003 Power Blackout of Northeastern U.S.) and the lessons to learn from such failures for software assurance are described. A process for mission thread analysis for assurance is introduced with examples of applicability to software assurance.

In **SwA for Acquisition**, the challenge of "What happens when we don't know who, where, when, and how creates our software or hardware" is explored. The current state of commercially available software and existing limits of available risk mitigations are presented.

A framework for product supply chain risk mitigation, which covers supplier capability, product security, product distribution, and operational use, is described. Extensions for system assurance are introduced and current standards in supply chain risk management are described.

Objectives

- Attendees will develop awareness of the value for software assurance and the challenges of integrating it into the software lifecycle.
- Attendees will develop an understanding of practices and methodologies available for addressing key areas of software assurance across the lifecycle.
- Attendees will begin planning how they will address software assurance for acquisition and development programs
- Attendees will recognize the need and be aware of what to do to address critical areas of software assurance, including security requirements, mission thread analysis, and supply chain risk management.

Schedule

We recommend using two days for this workshop because there is a huge amount of new material to absorb. However, we have and can deliver the workshop in one very long day if required.

For More Information

To learn more, see
www.cert.sei.cmu.edu/cybersecurity-engineering
cybersecurity-engineering/engage-with-us.cfm
Software Engineering Institute
The CERT Division
Carnegie Mellon University
Pittsburgh, PA 15313-2612

For General Information

For information about the SEI and its products and services, contact
Customer Relations
Phone: 412-268-5800
FAX: 412-268-6257
info@sei.cmu.edu
www.sei.cmu.edu

9/20/2013

The Software Engineering Institute (SEI) is a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University.