GSAW 2015 Tutorial G:

Security Risk Management using the Security Engineering Risk Analysis (SERA) Method

Length: Half day

Overview:

Module Overview:

- Introduction
  - This module helps students to understand basic risk management concepts in a software assurance context. It also establishes the value proposition for the SERA method. The primary focus of this module is security risk. Students are also provided a brief introduction to the SERA method and its four tasks.
- Establish Operational Context (Task 1)
  - This module provides an overview of Task 1 of the SERA method. The emphasis of Task 1 is on establishing the operational context for the system being analyzed.
- Identify Risk (Task 2)
  - This module provides an overview of Task 2 of the SERA method. The basic elements of risk are introduced in module 1 of this course; module 3 builds on this foundation by presenting the concept of a risk scenario.
- Analyze Risk (Task 3)
  - This module provides an overview of Task 3 of the SERA method. Here, the risk scenarios identified during Task 2 are prioritized based on their probability and impact values.
- Develop Control Plan (Task 4)
  - This module provides an overview of Task 4 of the SERA method. A control plan is defined and documented for all cybersecurity risks that are not accepted. Risk-mitigation plans typically include actions from the following categories: (1) recognize and respond, (2) resist, and (3) recover.
- Summary
  - This module summarizes key concepts presented in the course, shows how well the course met students' expectations, and answers any final questions the students might have.

Module Details

Program Risks. Provide students with a short scenario about early life-cycle security risk analysis. Present background on the Wireless Emergency Alerts (WEA) service. The scenario should focus on an Alert Originator that is acquiring an Alert Originating System (AOS) for the WEA service. Alert Originator stakeholders in the scenario are concerned about security. Several security concerns are highlighted in the text. Without any guidance regarding content or format, ask them to document the security risks from the scenario.

Early Life-Cycle Security Value Proposition. Provide an overview of the benefits of addressing security early in the life cycle. Be sure to note than many security issues are the result of design weaknesses. Static analysis tools will not find design weaknesses. Also not the cost benefits of addressing security early in the life cycle. Cite numbers from Microsoft to emphasize the cost benefits.

Risk Management Concepts. Provide an overview of key concepts that will be covered in the course, including the following:

- definition of risk; components of risk
- basic risk measures: probability, impact, risk exposure
- definition of risk management
- risk management activities
- definition of issue/problem; components of issue/problem
- definition of opportunity; components of opportunity
- definition of strength; components of strength
- the causal chain of conditions and events
- definition of interactively complex software-reliant systems
- the differences between tactical risk analysis and mission risk
- analysis in relation to the causal chain of conditions and events

Overview of the SERA Method. Provide a brief overview of the SERA method. Show how the method is intended to address design weaknesses early in the life cycle. Also emphasize that the SERA method is designed to address the complexity of modern security risks. Finally, provide a quick introduction to the four SERA tasks:

- Establish operational context. (Task 1)
- Identify risk. (Task 2)
- Analyze risk. (Task 3)
- Develop control plan. (Task 4)

Each of these tasks is addressed in subsequent modules.

Instructor: Carol Woody, Software Engineering Institute

Biography:

Dr. Carol Woody has been a senior member of the technical staff at the Software Engineering Institute since 2001. Currently she is the technical manager of the CERT Cybersecurity Engineering team which addresses security and survivability throughout the development and acquisition lifecycles, especially in the early stages. Her publications focus on building capabilities for measuring, managing, and sustaining cybersecurity for highly complex networked systems and systems of systems and include a recent CrossTalk article “Evaluating Security Risk Using Mission Threads.” Dr. Woody holds a B.S. in mathematics from the College of William & Mary, an M.B.A. from Wake Forest University, and a Ph.D. in information systems from NOVA Southeastern University.

Description of Intended Students and Prerequisites:

Acquisition, program management and system/software engineers will benefit from attending. Attendees of this course will need some general background of security and software to understand the content and examples provided for this course.

What can Attendees Expect to Learn:

Upon completion of this course, students will:

- understand basic risk management concepts in a software assurance context (focusing primarily on security risk)
- understand why it is important to address security risk early in the life cycle
- understand the importance of looking at security risk from a system-of-systems perspective
- understand the core elements of a security risk
- understand how to incorporate the elements of security risk in complex risk scenarios
- understand the four tasks of the SERA method