This video and all related information and materials ("materials") are owned by Carnegie Mellon University. These materials are provided on an “as-is” “as available” basis without any warranties and solely for your personal viewing and use.

You agree that Carnegie Mellon is not liable with respect to any materials received by you as a result of viewing the video, or using referenced websites, and/or for any consequences or the use by you of such materials.

By viewing, downloading, and/or using this video and related materials, you agree that you have read and agree to our terms of use ([www.sei.cmu.edu/legal/](http://www.sei.cmu.edu/legal/)).

Distribution Statement A: Approved for Public Release; Distribution is Unlimited

Security Requirements Engineering

Christopher Alberts
CERT® Division

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213
Topics

Background

Security Engineering Risk Analysis (SERA) Method

Summary
Security Requirements Engineering

Background
Software Assurance (SwA)

Definition

• “The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner.”

Key Aspects of SwA

• Trustworthiness – No exploitable weaknesses exist, either maliciously or unintentionally inserted.

• Predictable Execution – When executed, software functions as intended.

1. National Information Assurance Glossary CNSS Instruction No. 4009; DoDi 5200.44 p.12
Software Assurance: Lifecycle Focus

Focus of this module

Mission thread (Business process)
Thread Threat Analysis
Abuse Cases
Architecture and Design Principles
Coding Rules and Guidelines
Testing, Validation and Verification
Monitoring
Breach Awareness
Uncaught Breach

Sustainment

Requirements and Acquisition

Engineering and Development

Deployment and Operations
Software Security Requirements

Features (e.g., controls or constraints) that specify how to preserve the confidentiality, integrity, and availability of critical system data\(^1\)

---

Polling Question

Are you experienced in developing security requirements?

Answers:
• Yes
• No
Security Requirements Engineering: Key Activities

1. Agree on definitions.
2. Identify system assets and security goals.
3. Perform security risk analysis.
4. Elicit security requirements.
5. Categorize security requirements.
6. Prioritize security requirements.
7. Inspect security requirements using a well-defined method (e.g., Fagan inspections).

Focus of this Module

1. Agree on definitions.
2. Identify system assets and security goals.
3. Perform security risk analysis.
4. Elicit security requirements.
5. Categorize security requirements.
6. Prioritize security requirements.
7. Inspect security requirements using a well-defined method (e.g., Fagan inspections).

This module examines the role of risk analysis during security requirements engineering.
Security Requirements Engineering

Security Engineering Risk Analysis (SERA)
Polling Question

Are you experienced in assessing security risk?

Answers:
• Yes
• No
Security Engineering Risk Analysis (SERA)

**What**
- A systematic approach for analyzing complex security risks across the lifecycle

**Why**
- Build security into software-reliant systems
- Address design weaknesses as early as possible (e.g., requirements, architecture, design)

**Benefits**
- Correct design weaknesses before a system is deployed
- Reduce residual cybersecurity risk in deployed systems
- Ensure consistency with risk management standards
SERA Approach: Focus on Mission Impact

SERA analyzes the mission impact of data security breaches.

- Establishes a baseline of operational performance to inform risk identification
- Employs scenario-based structure for documenting cybersecurity risks

Outcomes:
- Disclosure of data (Confidentiality)
- Modification of data (Integrity)
- Insertion of false data (Integrity)
- Destruction of data (Availability)
- Interruption of access to data (Availability)
SERA Method: *Four Tasks*

1. Establish operational context.
2. Identify risk.
3. Analyze risk.
4. Develop control plan.

**Modeling Techniques**

**Risk Identification Worksheet**

**Risk Evaluation Criteria**

**Risk Analysis Worksheet**

**Control Approach Worksheet**

**Control Plan Worksheet**
Pilot Example: *Wireless Emergency Alerts (WEA)*

WEA is a major component of the Federal Emergency Management Agency (FEMA) Integrated Public Alert and Warning System (IPAWS).

- **Initiator** – decides to issue an alert (e.g., weather alert, AMBER alert)
- **Alert originator (AO)** – sends alerts to mobile devices in the targeted area
- **FEMA** – receives and processes alerts
- **Commercial mobile service provider (CMSP)** – receives and processes alerts
- **Recipients** – receive alerts automatically

Establish Operational Context (Task 1)

The operational environment for the system of interest is characterized to establish a baseline of operational performance.

<table>
<thead>
<tr>
<th>Steps</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Determine system of interest.</td>
</tr>
<tr>
<td>1.2</td>
<td>Select workflow/mission thread.</td>
</tr>
<tr>
<td>1.3</td>
<td>Establish operational views.</td>
</tr>
</tbody>
</table>
SERA Task 1: *Operational Views*

Mission thread / workflow

Technology (e.g., system, system of systems, architecture, network)

Use case

Data

Physical

Stakeholder

Others as needed
SERA Task 1: WEA Operational Models

**WEA Workflow/Mission Thread**

- **Alert Originator (AO)**
  - Initiator (e.g., First Responder)
- **FEMA**
- **CMSP**
- **Recipients**
  - AOS Initiator
  - AOS Operator
  - Initiator Computer
  - AO Computer
  - IPAWS-OPEN Aggregator
  - CSMP Infrastructure
  - IPAWS-OPEN Gateway
  - Federal Alert Gateway
  - CMSP Gateway
  - Federal Alert Gateway
  - CSMP Infrastructure

**CMSP Workflow/Mission Thread**

- **IPAWS-OPEN Aggregator**
  - Federal Alert Gateway
  - CMSP Gateway
  - CMSP Infrastructure
  - Mobile Devices
  - Convert CAP-compliant alert message into CMAC format
  - Send CMAC to CMSP Gateway
  - Receive, validate, and process CMAC
  - Send acknowledgment
  - Perform geo-targeting
  - Send CMAM
  - Receive CMAM
  - Broadcast CMAM
  - Receive CMAM
  - End of Scenario
  - If conversion fails
  - If conversion succeeds
  - End of Scenario
  - If validation succeeds
  - If validation fails
  - End of Scenario
  - If WEA not supported in area
  - If no cell sites in area

**CMSP Architecture**

- **Federal, State, and Local Agencies**
  - Generates WEA messages
  - Authenticates and validates alerts
  - Maintains CMSP profiles
  - Maintains multiple alert gateways
  - Pairs of BMC support external CMSP
  - Single point of entry for WEA messages
  - MC function collocated with CMSP Gateway for message delivery to CDMA network
  - CBC function collocated with CMSP Gateway for message delivery to GSM, UMTS, and LTE networks

**WEA System of Systems**

- **User Information System**
  - Generate public information message to CN
  - Send CAP to CN
  - Receive CAP from CN
  - Send CAP to CN
  - Receive CAP from CN
  - Generate public information message to CN

**Note:** Information is transferred between AOS and AO computers by AOS operators using USB drives.

**Note:** Communication of alert information between the initiator and AOS operator can be verbal (i.e., via telecommunications) or electronic (e.g., via email).
## SERA Task 1: Data Security Goals (Excerpt)

<table>
<thead>
<tr>
<th>Data Asset</th>
<th>Form</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert message</td>
<td>Electronic</td>
<td>There are no restrictions on who can view this data asset (public data)</td>
<td>The data asset must be correct and complete (high integrity).</td>
<td>This data asset must be available when needed (high availability).</td>
</tr>
<tr>
<td>Geo-targeting data</td>
<td>Electronic</td>
<td>There are no restrictions on who can view this data asset (public data)</td>
<td>The data asset must be correct and complete (high integrity).</td>
<td>This data asset must be available when needed (high availability).</td>
</tr>
</tbody>
</table>
Identify Risk (SERA Task 2)

Security concerns are transformed into distinct, tangible risk scenarios that can be described and measured.

<table>
<thead>
<tr>
<th>Steps</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Identify threat.</td>
</tr>
<tr>
<td>2.2</td>
<td>Establish consequence.</td>
</tr>
<tr>
<td>2.3</td>
<td>Identify enablers and amplifiers.</td>
</tr>
<tr>
<td>2.4</td>
<td>Develop security risk scenario.</td>
</tr>
</tbody>
</table>
SERA Task 2: Threats Selected for Analysis

R1. Insider Sends False Alerts
R2. Inherited Replay Attack
R3. Malicious Code in the Supply Chain
R4. Denial of Service
SERA Task 2: R1 Threat Sequence

T1. The insider is upset upon learning that he is not receiving a bonus this year and has been passed over for a promotion.

T2. The insider begins to behave aggressively and abusively toward his coworkers.

T3. The insider develops a logic bomb designed to replay a nonsense alert message repeatedly.

T4. The insider uses a colleague’s workstation to check-in the modified code with the logic bomb.

T5. Seven months later, the insider voluntarily leaves the company for a position in another organization.

T6. Twenty-one days after the insider leaves the carrier, the logic bomb is activated automatically.

T7. The malicious code causes the carrier’s WEA service to send a nonsense WEA alert repeatedly to people across the country.
SERA Task 2: Enablers

Threat Step
T7. The malicious code causes the carrier’s WEA service to send a nonsense WEA alert repeatedly to people across the country.

Enabler
Insufficient capability to check message content can allow illegitimate alert messages to be broadcast automatically to designated mobile devices.

An enabler is a condition or circumstance (e.g., weakness, vulnerability) that facilitates a threat’s occurrence.
SERA Task 2: *R1 Stakeholder Consequences*

Recipients of the message quickly become annoyed at receiving the same nonsense message repeatedly. (Recipients)

Many recipients complain to the carrier’s customer service operators. (Recipients)

A large number of recipients turn off the WEA function on their phones. Many will not turn the WEA service back on. (FEMA, Carrier)

The carrier responds to the attack. It removes the malicious code from its infrastructure. The cost to do so is considerable. (Carrier)

People leave the carrier for another carrier because of the incident. (Carrier)

People lose trust in the WEA service. (FEMA, Carrier)
SERA Task 2: Amplifiers

Consequence
Recipients of the message quickly become annoyed at receiving the same nonsense message repeatedly.

Amplifier
Knowledge of the system’s geo-targeting capability can enable the attacker to expand the geographic area being targeted and affect a greater number of recipients.

An amplifier is a condition or circumstance that increases the consequence triggered by the occurrence of a threat.
Analyze Risk (SERA Task 3)

Each risk is analyzed in relation to predefined criteria.

<table>
<thead>
<tr>
<th>Steps</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Establish probability.</td>
</tr>
<tr>
<td>3.2</td>
<td>Establish impact.</td>
</tr>
<tr>
<td>3.3</td>
<td>Determine risk exposure.</td>
</tr>
</tbody>
</table>
### SERA Task 3: R1 Risk Analysis

#### Current Probability: Remote

<table>
<thead>
<tr>
<th>Probability</th>
<th>Rare (1)</th>
<th>Remote (2)</th>
<th>Occasional (3)</th>
<th>Probable (4)</th>
<th>Frequent (5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium (3)</td>
<td>Medium (3)</td>
<td>Medium (3)</td>
<td>Medium (3)</td>
<td>Medium (3)</td>
<td>Medium (3)</td>
</tr>
<tr>
<td>Low (2)</td>
<td>Low (2)</td>
<td>Low (2)</td>
<td>Low (2)</td>
<td>Low (2)</td>
<td>Low (2)</td>
</tr>
<tr>
<td>Minimal (1)</td>
<td>Minimal (1)</td>
<td>Minimal (1)</td>
<td>Minimal (1)</td>
<td>Minimal (1)</td>
<td>Minimal (1)</td>
</tr>
</tbody>
</table>

#### Current Impact: Medium

<table>
<thead>
<tr>
<th>Impact</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Probability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium (3)</td>
<td>Medium (3)</td>
<td>Medium (3)</td>
<td>Medium (3)</td>
<td>Medium (3)</td>
<td>Medium (3)</td>
</tr>
<tr>
<td>Low (2)</td>
<td>Low (2)</td>
<td>Low (2)</td>
<td>Low (2)</td>
<td>Low (2)</td>
<td>Low (2)</td>
</tr>
<tr>
<td>Minimal (1)</td>
<td>Minimal (1)</td>
<td>Minimal (1)</td>
<td>Minimal (1)</td>
<td>Minimal (1)</td>
<td>Minimal (1)</td>
</tr>
</tbody>
</table>

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.
Develop Control Plan (SERA Task 4)

Control plans are developed and documented for all security risks that are not accepted.

<table>
<thead>
<tr>
<th>Steps</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Prioritize risks.</td>
</tr>
<tr>
<td>4.2</td>
<td>Select control approach.</td>
</tr>
<tr>
<td>4.3</td>
<td>Establish control actions.</td>
</tr>
</tbody>
</table>
## SEI webinar

### 32

Distribution Statement A This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

---

### SERA Task 4: *Prioritized Risk Spreadsheet*

<table>
<thead>
<tr>
<th>ID</th>
<th>Risk Statement</th>
<th>Imp</th>
<th>Prob</th>
<th>RE</th>
</tr>
</thead>
<tbody>
<tr>
<td>R4</td>
<td>Denial of Service</td>
<td>Max</td>
<td>Rare</td>
<td>Med</td>
</tr>
<tr>
<td>R1</td>
<td>Insider Sends False Alerts</td>
<td>Med</td>
<td>Remote</td>
<td>Low</td>
</tr>
<tr>
<td>R2</td>
<td>Inherited Replay Attack</td>
<td>Med</td>
<td>Remote</td>
<td>Low</td>
</tr>
<tr>
<td>R3</td>
<td>Malicious Code in the Supply Chain</td>
<td>Med</td>
<td>Rare</td>
<td>Min</td>
</tr>
</tbody>
</table>

*Note*: A control plan will be developed for all security risk scenarios with an impact of medium or greater.
SERA Task 4: Controls

Threat Step
T7. The malicious code causes the carrier’s WEA service to send a nonsense WEA alert repeatedly to people across the country.

Enabler
Insufficient capability to check message content can allow illegitimate CMAM messages to be broadcast automatically to designated mobile devices.

Control
The carrier monitors messages for suspicious content (e.g., illegitimate messages, duplicate messages) and responds appropriately.

A control is a safeguard or countermeasure to
• Recognize, resist, and recover from security risks
• Counteract identified enablers and amplifiers
SERA Task 4: CMSP Cybersecurity Guidelines

The CMSP Cybersecurity Guidelines comprise 35 high-priority security controls that address the four WEA risk scenarios included in this study.

Controls were identified in the following areas:

- Human Resources
- Training
- Contracting
- Physical Security
- Change Management
- Access Control
- Information Management
- Vulnerability Management
- System Architecture
- System Configuration
- Code Analysis
- Technical Monitoring
- Independent Reviews
- Incident Response
- Disaster Recovery
SERA Task 4: **Controls with Requirements Implications**

**Access Control**
- The carrier controls access to sensitive information based on organizational role.

**System Architecture**
- The carrier’s WEA alerting system has a backup capability that uses a separate communication channel.

**Technical Monitoring**
- The carrier monitors messages for suspicious content (e.g., illegitimate messages, duplicate messages) and responds appropriately.
- The carrier monitors the WEA alerting system for abnormal activity and responds appropriately.
Security Requirements Engineering and SERA

1. Agree on definitions.
2. Identify system assets and security goals.
3. Perform security risk analysis.
4. Elicit security requirements.
5. Categorize security requirements.
6. Prioritize security requirements.
7. Inspect security requirements using a well-defined method (e.g., Fagan inspections).
Polling Question

Are your organization’s security requirements designed to reduce security risk in deployed software or systems?

Answers:

• Yes
• No
• Don’t know
Security Requirements Engineering

Summary
Key Points

Software assurance:
• The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner.

Software security requirements:
• Features (e.g., controls or constraints) that specify how to preserve the confidentiality, integrity, and availability of critical system data

Security Engineering Risk Analysis (SERA) Method:
• A systematic approach for analyzing complex security risks in software-reliant systems and systems of systems across the lifecycle
• Can be integrated with security requirements engineering
http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=427321  
For Additional Information

Christopher Alberts
Principal Engineer
Cyber Security Engineering
CERT® Division, Software Engineering Institute

Email  cja@cert.org
Phone  412-268-3045

WWW  http://www.cert.org/cybersecurity-engineering/
U.S. mail  Software Engineering Institute
           Carnegie Mellon University
           Pittsburgh, PA  15213-3890