The Systems Security Engineering Capability Maturity Model (SSE-CMM)

Karen Ferraiolo
ISSEA Director of Technical Development
karen.ferraiolo@exodus.net
410-309-1780
Topics

- Why define security engineering practices?
- How can they best be defined?
- Who developed and supports the SSE-CMM?
- What is security engineering?
- How does the SSE-CMM* define practices for security engineering?
- What is the relation between the SSE-CMM and other methods of obtaining assurance?

* SSE-CMM = Systems Security Engineering Capability Maturity Model
Where are we now?

- Security needs are changing
  - global interconnection
  - massive complexity
  - release of beta versions of products
  - evolutionary development of systems
Where are we now? (cont.)

- **Security products/systems**
  - come to market through:
    - lengthy and expensive evaluation
    - no evaluation
  - results:
    - technology growth more rapid than its assimilation
    - unsubstantiated security claims

- **Security services**
  - viewed as an art
  - relies on individual expertise

- **Secure system operation and maintenance**
  - everyone has security concerns
  - improved practices are needed today
The Relevance of Competencies

90% of High Technology Projects Undertaken in the USA Fail to Complete On Time and Within Budget

Figure 1

Source: RAND Research Group 1996
What is needed?

• Continuity
• Repeatability
• Efficiency
• Assurance
What tools are currently available to address the problem?

<table>
<thead>
<tr>
<th>Tool</th>
<th>Target</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO-9000</td>
<td>Quality Assurance Process for Software</td>
<td>Defined Software QA Process</td>
</tr>
<tr>
<td>CMMs</td>
<td>Engineering/Organizational Processes</td>
<td>Continuously Improved Processes</td>
</tr>
<tr>
<td>CISSP</td>
<td>Security Engineering Professionals</td>
<td>Individual Certification</td>
</tr>
</tbody>
</table>

CMM = Capability Maturity Model  
CISSP = Certification of Information Systems Security Professionals
Why use the CMM approach to define practices?

• Accepted way of defining practices and improving capability
• Increasing use in acquisition as an indicator of capability
• Return on Investment for software indicates success
  – productivity gains per year: 9 - 67%
  – yearly reduction in time to market: 15 - 23%
  – yearly reduction in post-release defect reports: 10 - 94%
  – value returned on each dollar invested: 4 - 8.8%

Why was the SSE-CMM developed?

- **Objective:**
  - advance security engineering as a defined, mature, and measurable discipline

- **Project Goal:**
  - Develop a mechanism to enable:
    - selection of appropriately qualified security engineering providers
    - focused investments in security engineering practices
    - capability-based assurance
Who developed the SSE-CMM?

- SSE-CMM Project
  - Original work and project infrastructure sponsored by NSA
  - Additional support provided by OSD and Communications Security Establishment (Canada)
  - Collaborative effort by industry and government on their own funding
SSE-CMM Project Participants

44 Pioneers

- Arca Systems, Inc.
- BDM International Inc.
- Booz-Allen and Hamilton, Inc.
- Communications Security Establishment (Canadian)
- Computer Sciences Corporation
- Data Systems Analysts, Inc.
- Defense Information Systems Agency
- E-Systems
- Electronic Warfare Associates - Canada, Ltd.
- Fuentez Systems Concepts
- G-J Consulting
- GRC International, Inc.
- Harris Corp.
- Hughes Aircraft
- Institute for Computer & Information Sciences
- Institute for Defense Analyses
- Internal Revenue Service
- ITT Aerospace
- JOTA System Security Consultants Inc.
- Lockheed Martin
- Merdan Group, Inc.
- MITRE Corporation
- Mitretek Systems
- Motorola
- National Center for Supercomputing Applications
- National Institute for Standards and Technology
- National Security Agency
- Naval Research Laboratory
- Navy Command, Control, Operations Support Center; Research, Development, Testing, and Evaluation Division (NRaD)
- Northrop Grumman
- Office of the Secretary of Defense
- Oracle Corporation
- pragma Systems Corp.
- San Antonio Air Logistics Center
- Science Applications International Corp.
- SPARTA, Inc.
- Stanford Telecom
- Systems Research & Applications Corp.
- Tax Modernization Institute
- The Sachs Groups
- tOmega Engineering
- Trusted Information Systems
- TRW
- Unisys Government Systems
What is ISSEA?

- Selected by SSE-CMM Project to continue support
- Non-profit professional membership organization
- Oversees SSO in furthering development and use of the SSE-CMM
- receives advice and guidance from Advisory Council and Board of Sustaining Members

* ISSEA = International Systems Security Engineering Association"
Membership Options

• Organizations
  – Sustaining Membership
  – Charter Sustaining Membership

• Individuals
  – Individual membership
ISSEA’s Current Activities

• ISO* Standardization
  – ISSEA approved as Publicly Available Standard (PAS) Submitter

• Annual Conference
  – February 28 - March 2, 2001

• Appraiser Certification
  – developing program for appraiser and facilitator certification

• Training
  – 2 and 4 day courses in model and appraisal method

• SSE Textbook

* ISO = International Organization for Standardization
What is Security Engineering?

- **Definition:** No precise definition exists today!
- **Goals:**
  - Understand Security Risks
  - Establish Security Needs
  - Develop Security Guidance
  - Determine Acceptable Risks
  - Establish Assurance
Who practices security engineering?

- Developers
- Product vendors
- Integrators
- Buyers
- Security evaluation organizations
- System administrators
- Consulting/service organizations
- Program/project management
When is security engineering practiced?

- Pre-concept
- Concept exploration and definition
- Demonstration and validation
- Engineering, development, and manufacturing
- Production and deployment
- Operations and support
- Disposal
Who needs to know about security?

- Enterprise Engineering
- Systems Engineering
- Software Engineering
- Human Factors Engineering
- Communications Engineering
- Hardware Engineering
- Test Engineering
- Systems Administration
What do security engineering activities encompass?

- Operations Security
- Information Security
- Network Security
- Physical Security
- Personnel Security
- Administrative Security
- Communications Security
- Emanations Security
- Computer Security
How does the SSE-CMM define best practices?

• Domain Aspect
  – process areas
  – base practices

• Organizational Capability Aspect
  – implementation of process areas
  – institutionalization of process areas
SSE-CMM Base Architecture

- Three Domain Process Categories
  - Security Engineering
  - Project
  - Organization

- Five Capability Levels
  - Performed Informally
  - Planned and Tracked
  - Well Defined
  - Quantitatively Controlled
  - Continuously Improving
SSE-CMM Process Categories

- Engineering Processes
- Project Processes
- Organizational Processes
**SSE-CMM Organizational Process Areas**

- Define Organization’s Security Engineering Process
- Improve Organization’s Security Engineering Process
- Manage Security Product Line Evolution
- Manage Security Engineering Support Environment
- Provide Ongoing Skills and Knowledge
- Coordinate with Suppliers
SSE-CMM Project Process Areas

• Ensure Quality
• Manage Configurations
• Manage Program Risk
• Monitor and Control Technical Effort
• Plan Technical Effort
SSE-CMM Engineering
Process Areas

- Administer Security Controls
- Assess Impact
- Assess Security Risk
- Assess Threat
- Assess Vulnerability
- Build Assurance Argument

- Coordinate Security
- Monitor Security Posture
- Provide Security Input
- Specify Security Needs
- Verify and Validate Security
The Security Engineering Process

Product, System, or Service

Engineering Process

Assurance Process

Risk Process

Assurance Argument

Risk Information
The Security Engineering Process

Product, System, or Service

Engineering Process

Assurance Process

Risk Process

Risk Information

Assurance Argument
Security Risk Area

• Purpose:
  – To identify combinations of threat, vulnerability, and impact that deserve further attention

• Goals:
  – Determine Metrics
  – Gather Threat, Vulnerability, and Impact Information
  – Identify and Assess Risks
What is Risk?

• Definition
  – The expected value (likelihood $\times$ consequence) associated with an unwanted event

• Approaches
  – All involve notions of consequence, threat, and vulnerability
Risk Definitions

- **Events**: threat-vulnerability pairs that lead to unwanted outcomes
- **Likelihood**: the probability that an unwanted event will occur

\[
\text{Likelihood} = \text{Threat} \times \text{Vulnerability}
\]
**Risk Definitions**

- **Consequence**: the impact, either harm or loss, associated with an exploited vulnerability
- **Risk**: combines the concepts of likelihood and consequence

\[
\text{Risk} = \text{Likelihood} \times \text{Consequence}
\]
The Model

Assess Threat
Assess Vulnerability
Assess Impact
Assess Security Risk

Threat Information
Vulnerability Information
Impact Information
Risk Information
PA 04: Assess Threat

Goal

• Threats to the security of the system are identified and characterized

BP 04.01 Identify Natural Threats
BP 04.02 Identify Man-made Threats
BP 04.03 Identify Threat Units of Measure
BP 04.04 Assess Threat Agent Capability
BP 04.05 Assess Threat Likelihood
BP 04.06 Monitor Threats and Their Characteristics
PA 05: Assess Vulnerability

Goal

- An understanding of system security vulnerabilities within a defined environment is achieved

BP.05.01 Select Vulnerability Analysis Method
BP.05.02 Identify Vulnerabilities
BP.05.03 Gather Vulnerability Data
BP.05.04 Synthesize System Vulnerability
BP.05.05 Monitor Vulnerabilities and Their Characteristics
Goal

- The security impacts of risks to the system are identified and characterized

BP.02.01 Prioritize Capabilities
BP.02.02 Identify System Assets
BP 02.03 Select Impact Metrics
BP 02.04 Identify Metric Relationship
BP 02.05 Identify and Characterize Impacts
BP 02.06 Monitor Impacts
**PA 03: Assess Security Risk**

**Goals**

- An understanding of the security risk associated with operating the system within a defined environment is achieved
- Risks are prioritized according to a defined methodology

BP.03.01 Select Risk Analysis Method
BP 03.02 Exposure Identification
BP 03.03 Assess Exposure Risk
BP 03.04 Assess Total Uncertainty
BP 03.05 Prioritize Risks
BP 03.06 Monitor Risks and Their Characteristics
The Security Engineering Process

Product, System, or Service

Engineering Process

Assurance Process

Risk Process

Assurance Argument

Risk Information
What Is Assurance?

Definition:
- “the degree of confidence that security needs are satisfied”
  - What are security needs?
  - What is confidence?
  - How can we measure?
**Assurance Area**

• **Purpose:**
  – To generate and communicate confidence that the enterprise has satisfied its security needs

• **Goals:**
  – Appropriate evidence is collected efficiently
  – Clear and convincing argument establishing confidence is created
The Model

Verify and Validate Security

Verification and Validation Evidence

Build Assurance Argument

Assurance Argument

Many other PAs

Evidence
Assurance Arguments

- Top Level Claim
  - People Argument
  - Process Argument
  - Environment Argument
  - Technology Argument
PA 11: Verify and Validate Security

Goals

- Solutions meet security requirements
- Solutions meet the customer's operational security needs

BP.11.01 Identify Verification and Validation Targets
BP.11.02 Define Verification and Validation Approach
BP.11.03 Perform Verification
BP.11.04 Perform Validation
BP.11.05 Provide Verification and Validation Results
Goal

- The work products and processes clearly provide the evidence that the customer’s security needs have been met

BP.06.01 Identify Assurance Objectives
BP.06.02 Define Assurance Strategy
BP.06.03 Control Assurance Evidence
BP.06.04 Analyze Evidence
BP.06.05 Provide Assurance Argument
The Security Engineering Process

Product, System, or Service

Engineering Process

Assurance Process

Risk Process

Risk Information

Assurance Argument
What is Engineering?

• Solving problems
  – Requirements
  – Identify candidate solutions
  – Tradeoff analyses
  – System configuration

• Part of overall systems processes
  – Not an isolated activity
  – Must balance considerations of performance, safety, human factors, etc…
Security Engineering Area

• **Purpose:**
  – To solve engineering problems involving security

• **Goals:**
  – Determine customer security needs
  – Develop solutions and guidance on security issues
  – Coordinate with other engineering groups
  – Monitor security posture
The Model

Specify Security Needs

Specify Security Needs

Provide Security Input

Coordinate Security

Monitor Security Posture

Administer Security Controls

Risk Information

Configuration Information

Requirements, Policy, etc...

Solutions, Guidance, etc...
**PA 10: Specify Security Needs**

**Goal**

- A common understanding of security needs is reached between all parties, including the customer

**BP.10.01** Gain Understanding of Customer’s Security Needs

**BP.10.02** Identify Applicable Laws, Policies, and Constraints

**BP.10.03** Identify System Security Context

**BP.10.04** Capture Security View of System Operation

**BP.10.05** Capture Security High-Level Goals

**BP.10.06** Define Security Related Requirements

**BP.10.07** Obtain Agreement
**PA 09: Provide Security Input**

**Goals**

- All system issues are reviewed for security implications and are resolved in accordance with security goals
- All members of the project team have an understanding of security so they can perform their functions
- The solution reflects the security input provided

<table>
<thead>
<tr>
<th>BP.09.01</th>
<th>Understand Security Input Needs</th>
</tr>
</thead>
<tbody>
<tr>
<td>BP.09.02</td>
<td>Determine Security Constraints and Considerations</td>
</tr>
<tr>
<td>BP.09.03</td>
<td>Identify Security Alternatives</td>
</tr>
<tr>
<td>BP.09.04</td>
<td>Analyze Security of Engineering Alternatives</td>
</tr>
<tr>
<td>BP.09.05</td>
<td>Provide Security Related Guidance</td>
</tr>
<tr>
<td>BP.09.06</td>
<td>Provide Operational Security Guidance</td>
</tr>
</tbody>
</table>
PA 07: Coordinate Security

Goals

- All members of the project team are aware of and involved with security engineering activities to the extent necessary to perform their functions
- Decisions and recommendations related to security are communicated and coordinated

BP.07.01 Define Coordination Objectives
BP.07.02 Identify Coordination Mechanisms
BP.07.03 Facilitate coordination
BP.07.04 Coordinate Security Decisions and Recommendations
PA 01: Administer Security Controls

Goal

- Security controls are properly configured and used

BP.01.01 Establish Security Responsibilities
BP.01.02 Manage Security Configuration
BP.01.03 Manage Security Awareness, Training, and Education Programs
BP.01.04 Manage Security Services and Control Mechanisms
PA 08: Monitor Security Posture

Goals

• Both internal and external security-related events are detected and tracked
• Incident responses are in accordance with policy
• Changes to the operational security posture are identified and handled in accordance with the security objectives

BP 08.01 Analyze Event Records
BP 08.02 Monitor Changes
BP 08.03 Identify Security Incidents
BP 08.04 Monitor Security Safeguards
BP 08.05 Review Security Posture
BP 08.06 Manage Security Incident Response
BP 08.07 Protect Security Monitoring Artifacts
How does the SSE-CMM define best practices?

• Domain Aspect
  – process areas
  – base practices

• Organizational Capability Aspect
  – implementation of process areas
  – institutionalization of process areas
SSE-CMM Base Architecture

• Three Domain Process Categories
  – Security Engineering
  – Project
  – Organization

• Five Capability Levels
  – Performed Informally
  – Planned and Tracked
  – Well Defined
  – Quantitatively Controlled
  – Continuously Improving
Organizational Capability Measures

1. Performed Informally
   - Base Practices Performed

2. Planned and Tracked
   - Plan Performance
   - Disciplined Performance
   - Verify Performance
   - Track Performance

3. Well-Defined
   - Define a standard process
   - Perform the defined process
   - Coordinate practices

4. Quantitatively Controlled
   - Establish measurable quality goals
   - Objectively manage performance

5. Continuously Improving
   - Improve organizational capability
   - Improve process effectiveness

Incremental Improvement
SSE-CMM Model Architecture

**Domain**
- Base Practices
- Process Areas
- Process Category

**Capability**
- Generic Practices
- Common Features
- Capability Level

![Diagram of SSE-CMM Model Architecture](image)
Applying Capability Measures to Base Practices: the Rating Profile

Capability Level

Process Area

<table>
<thead>
<tr>
<th>Process Area</th>
<th>Capability Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>PA01</td>
<td>1</td>
</tr>
<tr>
<td>PA02</td>
<td>2</td>
</tr>
<tr>
<td>PA03</td>
<td>4</td>
</tr>
<tr>
<td>PA04</td>
<td>3</td>
</tr>
<tr>
<td>PA05</td>
<td>2</td>
</tr>
</tbody>
</table>
The SSE-CMM Appraisal Process

Planning Phase
- Scope Appraisal
- Collect Preliminary Evidence
- Plan Appraisal

Preparation Phase
- Prepare Appraisal Team
- Administer Questionnaire
- Consolidate Evidence
- Analyze Evidence/Questionnaire

On-Site Phase
- Executive Brief/Opening Meeting
- Interview Leads/Practitioners
- Analyze Data
- Establish Findings
- Develop Rating Profile
- Manage Records
- Conduct Wrap Up

Reporting Phase
- Develop Final Report
- Report Appraisal Outcomes to Sponsor
- Manage Appraisal Artifacts
- Report Lessons Learned
Using the SSE-CMM

Acquisition Decisions

System Development

Product Vendors

Service Providers

Compliance

SSE-CMM

Critical Business Operations
Where is it taking hold?

- US National Security Agency (NSA)
  - evaluating INFOSEC assessors’ capability
  - trusted product evaluation support
  - applying within to improve
- Canadian Communications Security Establishment (CSE)
  - evaluating contractors’ capability
  - trusted product evaluation support
  - best practices for Canadian CERTs
- United States Agency for International Development
  - framework for model security program
  - component of best practices framework
- Internal Revenue Service Information Systems
  - pilot program for improving security practices
- SSE-CMM Project Pilot Program
  - organizations used results to improve practices
Contributors to Product/Project Success

Product/Project Cost/Quality/Timeliness

Process

People

Technology
Determining the right combination

Reference:
Williams, Jeffrey; Jelen, George, “A Framework for Reasoning about Assurance,” April 23, 1998
Summary

• Why define best practices?
  – Focus investments in security engineering practices

• How can they best be defined?
  – Use an accepted and proven mechanism

• What is security engineering?
  – No precise definition, but can discuss goals

• How does the SSE-CMM define best practices?
  – Domain base practices
  – Capability measures

• What is the relation between the SSE-CMM and other methods of obtaining assurance?
  – SSE-CMM guides effectiveness of process
  – all contribute to assurance
For More Information

International Systems Security Engineering Association:
www.issea.org

Systems Security Engineering Capability Maturity Model
www.sse-cmm.org