The Systems Security Engineering Capability Maturity Model (SSE-CMM) describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering. The model also highlights the relationship between security engineering and systems engineering. This article discusses how the security community is applying the SSE-CMM to help solve today's security issues. These include leading contractors improving their practices, acquisition agencies evaluating potential system security vendors, and potentially using the model as an international standard.

A CMM® is a reference model of mature practices for a specified engineering discipline. A project developer or organization can compare practices to the model to identify potential improvements. Many companies have used CMMs to improve their software and systems engineering practices [1, 2].

The field of security engineering has several well-accepted criteria for evaluating security products, systems, and services [3, 4, 5, 6]. However, it lacks a comprehensive framework for evaluating security engineering practices. The SSE-CMM provides a way to measure and improve capability in applying security engineering principles, and to address capability-based assurance.

Project History
The NSA initiated development of the SSE-CMM to foster improvement in the security engineering process and to augment existing assurance methods. In 1995 the agency formed a government-industry consortium with wide representation from the security engineering acquisition and supplier communities. Organizations that provide or acquire security engineering systems, products, or services were encouraged to participate. The agency also invited identified experts in the security engineering community to review and comment on project materials.

Model and Appraisal Method
The SSE-CMM identifies both the unique characteristics of security engineering, and the integration of security activities into the overall system engineering process. The SSE-CMM uses the same maturity model architecture used in the System Engineering (SE)-CMM [2].

Model Structure
The model is divided into two dimensions: domain and capability. On the domain side (Figure 1), practices are organized in a hierarchy of process categories, process areas, and base practices. The SSE-CMM augments project and organizational process areas from the SE-CMM with security-specific process areas, including:
- 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

On the capability side (Figure 2), the model identifies capability levels from zero to five. Higher levels imply increased organizational support for planning, tracking, training, etc., which leads to more consistent performance of the domain activities. This support is captured in a set of common features and generic practices for each level. Further details are in [7].

SSE-CMM Pilots
The SSE-CMM is structured to support a wide variety of project and organizational needs. This article describes several pilots of the model.

SSE-CMM Project Participants

<table>
<thead>
<tr>
<th>Arca Systems Inc.</th>
<th>National Center for Supercomputing Applications, Univ of Illinois</th>
</tr>
</thead>
<tbody>
<tr>
<td>BDM International Inc.</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>Booz-Allen and Hamilton Inc.</td>
<td>National Institute for Standards and Technology</td>
</tr>
<tr>
<td>Communications Security Establishment (Canada)</td>
<td>Naval Research Laboratory</td>
</tr>
<tr>
<td>Computer Sciences Canada</td>
<td>Navy Command, Control, Operations Support Center</td>
</tr>
<tr>
<td>Computer Sciences Corp.</td>
<td>Research, Development, Testing and Evaluation Division</td>
</tr>
<tr>
<td>Data Systems Analyzers Inc.</td>
<td>Northrop Grumman</td>
</tr>
<tr>
<td>Defense Information Systems Agency</td>
<td>Office of the Secretary of Defense</td>
</tr>
<tr>
<td>E-Systems</td>
<td>Oracle Corporation</td>
</tr>
<tr>
<td>Electronic Warfare Associates - Canada, Ltd.</td>
<td>pragma Systems Corporation</td>
</tr>
<tr>
<td>Fuentez Systems Concepts Inc.</td>
<td>San Antonio Air Logistics Center</td>
</tr>
<tr>
<td>G-J Consulting</td>
<td>Science Applications International Corp.</td>
</tr>
<tr>
<td>GRC International Inc.</td>
<td>SPARTA Inc.</td>
</tr>
<tr>
<td>Harris Corp.</td>
<td>Stanford Telecom</td>
</tr>
<tr>
<td>Hughes Aircraft</td>
<td>Systems Research and Applications</td>
</tr>
<tr>
<td>Institute for Computer and Information Sciences</td>
<td>Tax Modernization Institute</td>
</tr>
<tr>
<td>Institute for Defense Analyses</td>
<td>Tehe Sachs Groups</td>
</tr>
<tr>
<td>Internal Revenue Service</td>
<td>T0mega Engineering</td>
</tr>
<tr>
<td>ITT</td>
<td>Trusted Information Systems</td>
</tr>
<tr>
<td>Lockheed Martin</td>
<td>TRW</td>
</tr>
<tr>
<td>Marden Group Inc.</td>
<td>Unisys Government Systems</td>
</tr>
</tbody>
</table>

The Capability Maturity Model and CMM are registered service marks of the Software Engineering Institute and Carnegie Mellon University.
The appraisal addressed the following Process Areas: requirements, design, analysis, implementation, and testing. A pilot appraisal. The appraisal focused on a single project—a system experience, these changes did not detract in any way from activities. According to pilot participants with SE-CMM assessment duration.

This was accomplished by redesigning the questionnaire, streamlining the questionnaire analysis process, eliminating redundant data entry, and increasing the emphasis on pre-onsite activities. According to pilot participants with SE-CMM assessment experience, these changes did not detract in any way from the quality and accuracy of the assessment.

TRW, a major integrator of secure systems, hosted the first pilot appraisal. The appraisal focused on a single project—a system integration effort covering the life cycle from concept to system delivery, including concept definition, definition and analysis of requirements, design, analysis, implementation, and testing. The appraisal addressed the following Process Areas:

- Assess Operational Security Risk.
- Attack Security.
- Build Assurance Argument.
- Coordinate Security.
- Determine Security Vulnerabilities.
- Provide Security Input.
- Verify and Validate Security.

Model Applications Best Operational Practice

One interesting application of the SSE-CMM involves the selection of base practices as identified within selected PAs and forming them into policy statements, process handbooks, or procedural instructions for a specific organization. One of the most notable uses of the SSE-CMM in this manner is the generation of a Model Information System Security Program (MISSP) under the U.S. Agency for International Development (USAID).

The MISSP consists of a framework that links and categorizes collections of best practices that cover an entire information security program. It is intended to be used by any civil government agency that needs to generate a comprehensive information security program, but which may not have the time or resources to start from scratch. The Critical Infrastructure Assurance Office, and the Federal Chief Information Officer Council endorse the MISSP concept.

In late 1999, the U.S. Federal Chief Information Officer Council adopted the USAID MISSP as the foundation for a collection of Best Security Practices.

Standard for Performance

The SSE-CMM is increasingly being viewed as the process analog to the product metric presented by the Common Criteria and the National Information Assurance Partnership. For example, the Common Criteria is being used to generate protection profiles for the components of a Public Key Infrastructure (PKI) to be deployed throughout the Department of Defense (DoD). The protection profiles will then represent the security requirements that need to be present—and evaluated—in vendor equipment being used within this DoD PKI.

The SSE-CMM is being researched as the source for the process equivalent of protection profiles for this same purpose. That is, the SSE-CMM will be used to prepare capability profiles that will describe the organizational security capability requirements for the design, development, deployment, and operation of this PKI within the DoD. If such capability profiles emerge, then the SSE-CMM appraisal method would also be used to verify the existence of such capabilities. This works in the same way a Common Criteria evaluation under the National Information Assurance Partnership verifies the existence of security features and assurances in the products being used.

Another use of capability profiles is to include them as a portion of the metrics identified within Service Level Agreements (SLAs) in outsourcing contracts. In this circumstance, periodic appraisals of performing organizations will con-
As the number and variety of secure systems and products increases, and operating environments and security threats become increasingly diverse, this approach is becoming costlier. Customers are looking to developmental assurance methods, such as the SSE-CMM, to reduce the extent that product-based criteria are used, and to reduce the evaluation and accreditation time. This highlights three aspects of security protection:

- Product (e.g., common criteria).
- Process (e.g., organizational capability via the SSE-CMM).
- Pedigree (e.g., personal capability via the Certified Information Systems Security Professional exam).

Based on the successful results to date and the current initiatives, we expect that use of the SSE-CMM will increase dramatically in the next few years, until the model becomes an industry standard. Only then will the benefits of this model be fully seen.

References


About the Authors

Rick Hefner, Ph.D., is the manager of Process Technology for TRW. He has more than 25 years of experience in software development, research, and management, and has worked in industrial, academic, and government positions. He is co-chairman of the Assessment Methodology Team on the CMM integration project. He is an SEI-authorized lead assessor, and has published more than 30 papers. He received his bachelor of science degree and master of science degree from Purdue University and his doctorate degree from UCLA.

One Space Park
Redondo Beach, Calif. 90278
Voice: 310-812-7290
Fax: 310-812-1251
E-mail: rick.hefner@trw.com

See page 25 for biographies of Ron Knode, Mary Schanken.