The Systems Security Engineering CMM

Rick Hefner
TRW

Ron Knode
Computer Sciences Corp.

Mary Schanken
National Security Agency (NSA)

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].

SSE-CMM Project Participants

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

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:

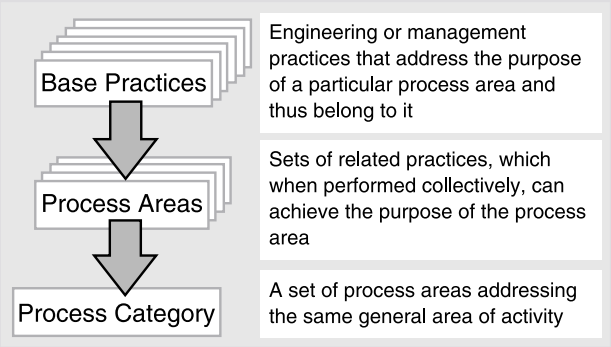
- Administer Security Controls.
- Assess Impact.
- Assess Security Risk.
- Assess Threat.
- Assess Vulnerability.
- Build Assurance Argument.
- Coordinate Security.
- Monitor Security Posture.
- Provide Security Input.
- Specify Security Needs.
- Verify and Validate Security.

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

Figure 1. *Domain Aspect*



® The Capability Maturity Model and CMM are registered service marks of the Software Engineering Instutute and Carnegie Mellon University.

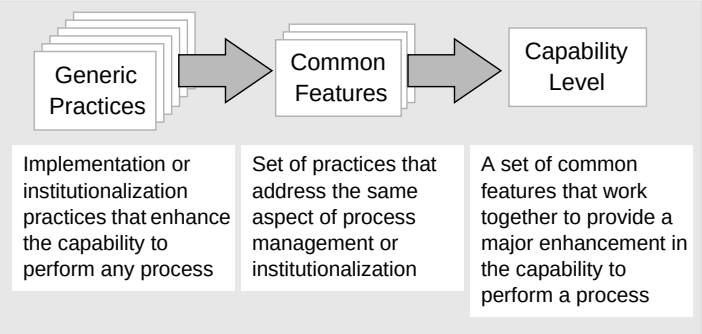


Figure 2. *Capability Aspect*

improvement activities, including self-administered appraisals or internal appraisals augmented by expert facilitators from inside or outside the organization. Although it is primarily intended for internal process improvement, it can also be used to evaluate a potential vendor's capability to perform its systems security engineering process.

An assessment against this model involves determining the appropriate capability level for each process area. To determine appropriate improvement actions, the organization must decide what capability they desire in each of the process areas, and address any deficiencies. An appraisal methodology, termed the System Security Appraisal Method (SSAM), was defined [8].

The purpose of the SSE-CMM pilot program [9], conducted during 1996, was to validate the model and appraisal method, focusing on the Security Engineering Process Areas (PAs). The pilots were performed under nondisclosure agreements with the host organizations, covering proprietary process information and assessment results.

Because the SSAM is based on the SE-CMM Assessment Method, pilot team members received training on the SE-CMM assessment method and adapted it for the SSE-CMM. Since some organizations will want to perform a SSE-CMM assessment in conjunction with a SE-CMM assessment, the Security Appraisal Method was revised to shorten the typical 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.
- Specify Security Needs.
- Verify and Validate Security.

The second pilot focused on security service projects, specifically risk analyses and assessments at Computer Sciences Corp. The appraisal covered two projects: a system in development and an operational system. The engineering PAs addressed were the same as the first pilot with the addition of Adminster Security Controls and the deletion of Provide Security Input.

The remaining three pilots were hosted by Hughes (another system integrator), GTIS (a certification authority), and Data General (a product vendor). The pilots uncovered some potential improvement areas, and the model and appraisal method were updated.

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. NSA, 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-

tribute to the scoring of information security service delivery in accordance with the SLAs. It will ultimately help determine the payment for services rendered.

NSA used the SSE-CMM in the development of an Industrial Information Systems Security Engineering (ISSE) Certification Program to help customers of ISSE services identify qualified ISSE Service Providers and to raise the quality of the service provided throughout the community.

NSA is currently using two tailored versions of the SSE-CMM: the Information Security (INFOSEC) Assessment CMM (IACMM) and the Business CMM (BCMM). The IACMM was designed to measure the capability of an INFOSEC assessment organization. The purpose is to help build a cadre of INFOSEC assessor organizations that are well equipped to provide valid site assessments to their customer base. This will help alleviate the huge demand for NSA resources to conduct such assessments by providing a standardized metric that customers can use to measure the capabilities of suppliers to address the specific INFOSEC assessment needs.

The BCMM was developed in order to measure the Information Systems Security Organization's Business Health. The focus is on the supporting business processes that any organization relies upon to ensure appropriate and timely execution of its mission objectives (i.e. Product and/or Service-based.) At the time of this writing, three pilot appraisals and eight BETA appraisals have been conducted.

Under the National Information Assurance Partnership, NSA has used the SSE-CMM to capture process-related security awareness activities that are included in the National Institute of Standards and Technology National Voluntary Laboratory Accreditation Program Handbook 150-20: *Information Technology Security Testing—Common Criteria.* The inclusion of this set of queries closes the gap between product and process assurance issues in the Common Criteria lab accreditation program.

The SSE-CMM has been submitted to the International Organization for Standardization as a Publicly Available Specification. NSA is also working to have the security Process Areas of the SSE-CMM included in the SEI CMM Integration (CMMI[SM]) initiative.

The Canadian Security Establishment (CSE) stated it is considering using the SSE-CMM to:

- Perform an internal appraisal within Computer and System Security Section of CSE.
- Encourage product vendors to use it to become more mature, helping them to develop better products and facilitate evaluation process.

Conclusion

This paper summarizes the development, piloting, and use of the SSE-CMM. Obviously, there is much to do before the SSE-CMM is fully integrated and in widespread use throughout the security community.

The SSE-CMM must further explore the relationship among current approaches to assurance. The current product-based approach relies on identifying a series of criteria that are evaluated for each intended product or system, based on the intended operating environment and the perceived threats therein.

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., organizaional 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

1. Paulk, Mark; Curtis, William; and Chrissis, Mary Beth, *Capability Maturity Model for Software, Version 1.1*, Software Engineering Institute, CMU/SEI-93-TR-24, DTIC # ADA263403, February 1993.
2. Bates, Roger, et al, *A Systems Engineering Capability Maturity Model, Version 1.1*. CMU/SEI-95-MM-003, November 1995.
3. *Department of Defense Trusted System Evaluation Criteria,* DOD 5200.28-STD, December 1985.
4. *Common Criteria for Information Technology Security Evaluation,* Version 2.1, CCIMB-99-031, August 1999.
5. *The Specification for Information Security Management Systems,* BS 7799: Part 2, February 1998.
6. *DoD Information Technology Security Certification and Accreditation Process (DITSCAP),* DoDI 5200.40, Dec. 30, 1997.
7. SSE-CMM Project, *Systems Security Engineering Capability Maturity Model, Version 1.0*, Apr. 1, 1999.
8. SSE-CMM Project, *Systems Security Appraisal Method, Version 1.0,* Oct. 21 1996.
9. Hefner, Rick; Monroe, Warren; and Hsaio, David, *Experience with the Systems Security Engineering Capability Maturity Model,* Proceedings of the Sixth Annual International Symposium of the National Council of Systems Engineering, Boston, Mass., July 7-11, 1996.

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: 310-8121251
E-mail: rick.hefner@trw.com

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