A Process Standard for System Security Engineering: Development Experiences and Pilot Results

Rick Hefner, Ph. D.
TRW
One Space Park
Redondo Beach, CA 90278

Abstract

The Systems Security Engineering Capability Maturity Model℠ (SSE-CMM℠) describes the essential characteristics of an organization's security engineering process. The standard was developed by a unique government-industry consortium of leading security providers and acquirers. This paper summarizes the model and presents lessons learned in the model's development and from pilot appraisals.

Introduction

A Capability Maturity Model℠ (CMM℠), is a reference model of mature practices for a given engineering discipline. A project or organization can compare their practices to measure the maturity of their processes and identify potential improvements. Many companies have used CMMs to improve their practices for software [1] and systems engineering [2].

Although the field of security engineering has several well-accepted criteria for evaluating security products, systems, and services [3]-[8], it has lacked a comprehensive framework for evaluating information security engineering practices. The Systems Security Engineering Capability Maturity Model (SSE-CMM) provides such a standard.

Project History

The SSE-CMM project was initiated by the National Security Agency (NSA) to improve security engineering practices and to augment existing assurance methods. In 1995, the project formed a government-industry consortium, with representation from the security engineering acquisition and supplier communities (Figure 1). The project also invites identified experts in the security engineering community to review and provide comments on project materials before public release. All security practitioners are encouraged to provide comments on publicly released products.

- Arca Systems, Inc.
- BDM International, Inc.
- Booz-Allen & Hamilton, Inc.
- Communications Security Establishment (Canada)
- Computer Sciences Canada
- Computer Sciences Corporation
- 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 Corporation
- Hughes Aircraft
- Institute for Computer & Information Sciences
- Institute for Defense Analyses
- Internal Revenue Service
- ITT
- Lockheed Martin
- Merdan Group, Inc.
- MITRE Corporation
- 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 & Evaluation Division
- Northrop Grumman
- Office of the Secretary of Defense
- Oracle Corporation
- pragma Systems Corporation
- San Antonio Air Logistics Center
- Science Applications International Corporation
- SPARTA, Inc.
- Stanford Telecom
- Systems Research & Applications
- Tax Modernization Institute
- The Sachs Groups
- tOmega Engineering
- Trusted Information Systems
- TRW
- Unisys Government Systems

Figure 1. SSE-CMM Project Participants

1082-3670/97 $10.00 © 1997 IEEE

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 CMM [2].

Model Structure

The model is divided into two dimensions, domain and capability. On the domain side (Figure 2), 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:

- Specify Security Needs
- Provide Security Input
- Verify and Validate Security
- Attack Security
- Assess Operational Security Risk
- Build Assurance Argument
- Monitor System Security Posture
- Administer Security Controls
- Coordinate Security
- Determine Security Vulnerabilities

On the capability side (Figure 3), the model identifies capability levels from 0 to 5. Higher levels imply increased organizational support for planning, tracking, training, etc., leading to more consistent performance of the domain activities. This support is captured in a set of Common Features and Generic Practices for each level. Details are in [9] and [10].

Appraisal Method

An assessment against this model determines an organization's capability level in each Process Area, forming a spectrum of capability across the domain. To define desired improvements, the organization decides what capability they desire in each of the process areas, and addresses any deficiencies. An appraisal methodology, termed the System Security Appraisal Method (SSAM), was defined [10].

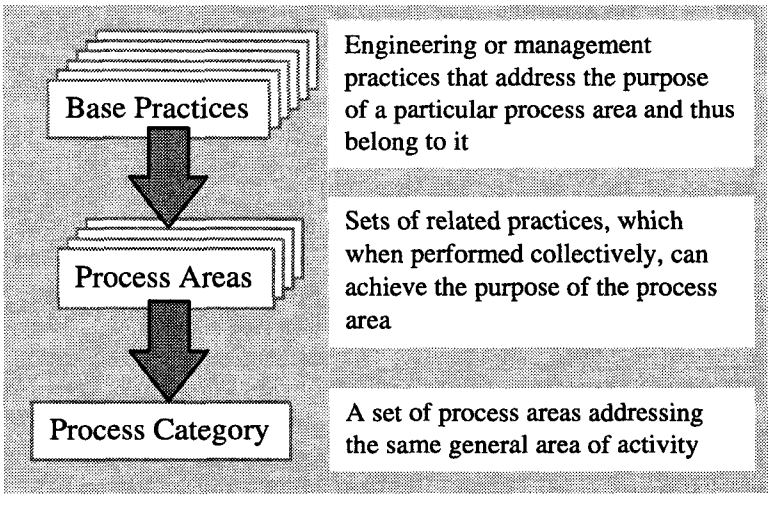

Figure 2. Domain Aspect

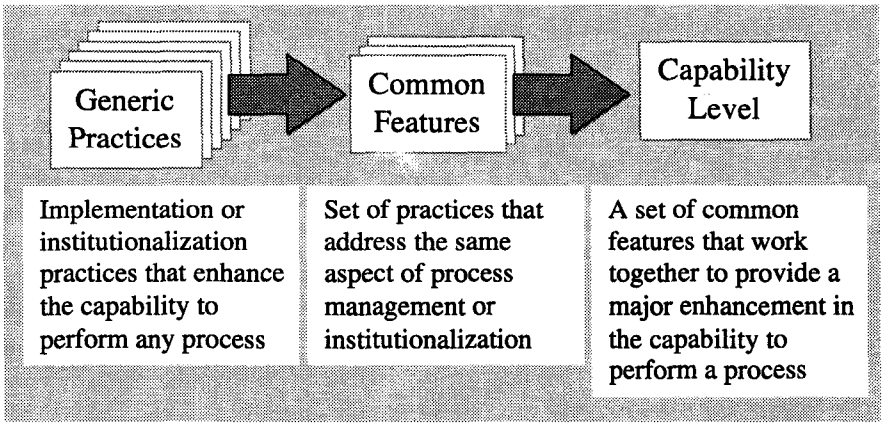

Figure 3. Capability Aspect

Development Issues

Several observations can be made about issues that arose in the development of the SSE-CMM model and appraisal method. These comments may be useful to other groups developing similar maturity models, and to organizations implementing improvement programs.

The first issue was the establishment of the government-industry consortium. Project participants felt that a community-wide consensus approach was critical to project success, and was consistent with recent initiatives in the reduction of government standards. There exist many examples of standards developed by a single agency, without industry participation, which are difficult to interpret, costly to maintain, and lead to expensive government processes inconsistent with commercial best-practices. The project adopted an open, consensus approach; all security customers and providers were encouraged to participate as equals. The SSE-CMM project maintains a public web site (http://www.ssecmm.org) to promote participation and distribute information.

Developing the model required a background in both security engineering and maturity model concepts. The typical project member had a background in one, but not the other, and there was tremendous need for education and experience sharing at project start-up. Early discussions focused on the manner in which maturity models and appraisal methods have been used in industry and government, and the advantages and disadvantages of commonly used models and methods.

The concept of process-based assurance is new to the assurance community. Although project participants are confident that improved processes can be used to improve the assurance of security products, there is no universal agreement of exactly how process maturity results will be used with the present product assurance criteria. This remains an area of study.

Determining the proper scope of the model was difficult. The security community has a wide variety of providers, encompassing products, systems, and services. Some providers are part of a separate department within a larger organization, some are integrated into another department, and some are wholly dedicated organizations. Some providers focus on particular portions of the life-cycle, such as maintenance or decommissioning of the system. A wider model addresses more of the providers, but is more time consuming to develop, and requires a broader set of domain experts. The project decided to initially focus on those activities that the majority of providers performed and expand the model over time.

Selecting the maturity model architecture required a choice between a continuous model, such as the SPICE and SSE-CMM architectures, and a discrete model, such the CMM for Software. Both have advantages and disadvantages. The project determined that ease of model integration, especially with the SE-CMM, was a critical factor, and this favored a continuous model. To some extent, the continuous model also simplified development because the domain and capability dimensions are separate. This allowed the security domain experts to focus on defining Process Areas and Base Practices. Due to the recent proliferation of maturity models, maturity model integration is currently receiving increasing attention in the community, and further standardization is expected.

SSE-CMM Pilots

The purpose of the SSE-CMM pilot program, conducted during 1996, was to validate the model and appraisal method, focusing on the Security Engineering Process Areas (PAs). The pilots were performed under non-disclosure 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 an SSE-CMM assessment in conjunction with an SE-CMM assessment, the SAM 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 preparatory 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.

Several issues arose concerning piloting of the model and appraisal method. Since the project is composed of various security providers, who often compete with each other for business, there was concern about the proprietary nature of appraisal materials. The pilot appraisal team will be composed of project members from competing organizations and the government. Allowing your competitors and customers to evaluate your current projects and organizational artifacts in depth requires confidence that the material will be properly safeguarded. The current plan calls for strict control of all information concerning a

particular appraisal; appraisals results will only be made public in the aggregate.

Pilot Descriptions

The first pilot appraisal was hosted by TRW, who is a major integrator of secure systems. The appraisal focused on a single project, a system integration effort covering the life-cycle from concept to system delivery, including concept definition, requirements definition and analysis, design, analysis, implementation, and testing.

The focus of the second pilot was security service projects at Computer Science Corporation, specifically, risk analyses and assessments. The appraisal covered two projects, a system in development and an operational system.

The third pilot was hosted by Hughes, another system integrator, and also examined the security engineering Process Areas in detail.

The fourth pilot was performed on a certification authority, a trusted third-party that distributes the electronic keys used to encrypt and decrypt user and server information and the electronic certificates used to authenticate user and server identities. This pilot covered all Process Areas: Engineering, Project, and Organizational.

Pilot Observations - Model

The pilot participants observed the following concerning the SSE-CMM model:

The SSE-CMM adequately addressed the security engineering processes of the organizations involved in the pilots. The security engineering process areas defined in the model reflected the services and activities of the pilot organizations, and none of the organizations reported performing security engineering activities that were not addressed by the model.

The SSE-CMM was applicable to different organizational approaches to the practice of security engineering. Security engineering practices are highly integrated into the systems engineering practices of one pilot organization, while security engineering is practiced as a separate specialty discipline (albeit with extensive systems engineering interfaces) at the other. Despite these differences, both organizations indicated that the SSE-CMM PAs were recognizable and germane to their particular approaches.

The structure of the model lent itself to tailoring by the pilot organizations. They were easily able to recognize and select for assessment the PAs appropriate to the projects. Because the projects were dissimilar, different sets of PAs were used in each pilot.

The pilots did uncover some potential improvement areas. Some of the Generic Practices were difficult to interpret, and appear to overlap with Base Practices in Project Process Areas. For example, planning for individual process activities is strongly related to overall project planning. This is a difficulty in the maturity model architecture that will be examined.

Pilot Observations - Assessment Method

The following were observed regarding the SSE-CMM assessment method used in the pilots:

The assessment method was effective in both pilots, despite the organizational and project differences noted above. Pilot participants in the organizations being assessed reported that the assessments produced accurate findings. They noted that the findings were appropriate for the focus projects, but practices might vary significantly from other projects in the same organization. An actual appraisal would need to address a wider range of projects to get an overall picture of organizational capability.

The assessment method produced useful results. Participating organizations felt that the assessment findings would help them motivate management interest and focus process improvement efforts. They agreed that the findings represented weaknesses in their security engineering practices that should be addressed.

On of the biggest concern is the amount of time required to do an accurate appraisal. During the pilots, the focus was on learning about the model and method. Because of that, some activities took longer than anticipated or longer than would be practical in a non-pilot application. Teamwork is a key factor, and the level of experience on the team may strongly influence the efficiency of the appraisal. Increasing the team's efficiency will be addressed in future project work and upcoming pilots.

Developmental Assurance

Developmental assurance is a hotly debated topic in recent security conferences and literature. The current approach to assurance relies on a series of criteria that are evaluated for each intended product or system, based on its intended operating environment and the perceived threats in that environment. As the number and variety of secure systems and products increases, and operating environments and security threats become increasing diverse, this approach is becoming increasingly expensive to apply. Customers are looking to

developmental assurance methods, such as the SSE-CMM, to be used to reduce the extent to which product-based criteria are used, and to reduce the evaluation and accreditation time.

Conclusions

While the results of the early pilots are encouraging, additional pilots are needed to examine other aspects of the model and method. Upcoming pilots will include various types of organizations and use of the full model. The SSE-CMM model and assessment methodology will be refined based on feedback from the pilot program.

The SSE-CMM project must further explore the relationship among current approaches to assurance. Based on the results to date, it is expected that the use of the SSE-CMM will increase dramatically in the next few years, and that the model will become a de facto industry standard. Project efforts for 1997 will include drafting language for the SSE-CMM's use in government procurements, both directly and indirectly, as a measure of organizational systems security engineering capability.

Acknowledgments

The terms Capability Maturity Model and CMM are registered service marks of Carnegie Mellon University.

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, February 1993.

[2] Bates, Roger, et al, "A Systems Engineering Capability Maturity Model, Version 1.1." CMU/SEI-95-MM-003, November 1995.

[3] Canadian Security Establishment (CSE), "The Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)", Version 3.0, January 1993.

[4] Common Criteria Editorial Board, "Common Criteria for Information Technology Security Evaluation, CCEB-96/011, Version 1.0," 31 January 1996.

[5] Department of Defense, "Department of Defense Trusted Computer System Evaluation Criteria (TCSEC, Orange Book)", WD 5200.28-STD, December 1985.

[6] International Standards Organization (ISO), "Baseline Practices Guide," January 1995.

[7] ITSEC Editorial Board, "Information Technology Security Evaluation Criteria, Harmonized Criteria of France, Germany, Netherlands, and UK," Herausgeber: Der Bundesminister des Innern, Bonn, May 1990

[8] National Institute of Standards and Technology (NIST) and National Security Agency (NSA), "Federal Criteria for Information Technology Security," December 1992.

[9] SSE-CMM Project, "Systems Security Engineering Capability Maturity Model, Version 1.0," 21 October 1996.

[10] Project web site: http://aslan.ncsa.uiuc.edu/html

Author Biography

Dr. Rick Hefner has over 20 years of experience in system and software development, research, and management. He is a frequent lecturer at national conferences, and instructor at USC, UCLA, and Cal State Long Beach. Dr. Hefner is currently the Manager of Process Technology for TRW's Software Process Engineering Group. His interests include process improvement, system engineering, software management, training, and technology transfer.