Tools and Techniques for SSE-CMM Implementation

Marbin Pazos-Revilla
mpazos@tntech.edu

Ambareen Siraj
asiraj@tntech.edu

Tennessee Technological University, Department of Computer Science

Keywords: SSE-CMM, Model, Security, Tools, Implementation

ABSTRACT:
With the immense popularity of globalization and distributed systems, the need for standardization of organization-wide security practices has become a high priority. Different studies have shown that organization-wide standardization of practices increases productivity, efficiency, and customer satisfaction. The Security System Engineering Capability Maturity Model (SSE-CMM) offers industry practitioners a choice of security engineering standard that can be implemented and integrated at different organizational levels according to assurance needs. Although SSE-CMM provides the necessary roadmap for adopting organization wide quality security engineering practices, it does not specifically point out any tools and techniques that can be used to help reach the goals described in the standard. This paper provides insight into industry practitioners about availability of possible tools and techniques that would aid them in satisfying their assurance needs as per the SSE-CMM model.

1. INTRODUCTION

Globalization of markets, increased use of distributed computing systems and the need for continuity, reusability, efficiency, and assurance, have prompted the adoption of standards in development practices. Different studies have shown that organization-wide standardization of practices increases productivity [7], efficiency, and customer satisfaction. The lack of standardization on the other hand has proven to increase product development costs and decrease customer satisfaction - among other negative factors.

Because of constant emergence of new threats and technology, adopting organization wide standardization of security practices are more critical than in typical software development environment. Industry examples like those of TJ Max, Cisco and Microsoft [11] have shown that the integration of security processes and standards can be of paramount importance if we take into account the massive amount of tangible and intangible damages that result from a single security breach in the system.

Security System Engineering Capability Maturity Model (SSE-CMM) offers industry practitioners a choice of such a standard for security engineering [6]. The SSE-CMM project was initially funded by the National Security Agency (NSA) in 1993 and later emerged to a standard by 1996. Over the years it has transformed to what is known today as ISO/IEC 21827. The SSE-CMM model describes the essential characteristics of an engineering security process that should exist in an organization in order to ensure good security engineering practices. It provides a way to assess and improve capability in the application of security engineering principles, and addresses capability-based assurance [6].

Although SSE-CMM provides the necessary roadmap for adopting organization-wide quality security engineering practices, it does not specifically point out any tools and techniques that can be used to help reach the goals described in the process areas. It does not answer questions such as: how an organization can actually go about implementing security practices? What tools and techniques should an organization use or exercise in order to comply with the SSE-CMM practices? In this paper, we offer security practitioners choices for such tools and techniques that would help them in adopting specific practices in process areas as suggested in SSE-CMM. The purpose of this paper is to assist in selecting appropriate tools and techniques to best satisfy assurance needs as per the SSE-CMM model.

In the rest of the paper, we begin with brief background information on SSE-CMM and then address choices of tools and techniques available for implementing security engineering process areas and lastly conclude.

2. THE SSE-CMM MODEL

SSE-CMM has as an underlying principle that to perform a particular activity periodically and successfully, certain processes need to be present [6]. SSE-CMM highlights the objectives and the activities involved in such processes, what is achieved from performing these activities and the maturity of the processes. As mentioned before, SSE-CMM does not provide a guideline for a specific methodology or process to be used; its usefulness lies in the integration of the existing processes in the organization with those included in the model. In addition, based on each organization’s objectives and goals, some of the processes within SSE-CMM may not be applicable in specific contexts. For this reason, organizations should carefully study the relationships between different practices within the model to determine their applicability as per their need [3].

The SSE-CMM model is divided in two different but inter-related sections or dimensions: domain and capability. Different process areas and activities are described for both sections. The domain related practices are geared towards security domain while the capability practices are more general and apply to a wide range of domains. The capability dimension represents practices that indicate process management and institutionalization of capability [10]. Process areas covering security engineering in the domain dimension are enumerated as follows and could be further divided in three categories: security engineering, project, and organizational PAs, which are listed below including their associated process areas.
Security Engineering

1. Administer Security Controls (PA01)
2. Assess Impact (PA02)
3. Assess Security Risk (PA03)
4. Assess Threat (PA04)
5. Assess Vulnerability (PA05)
6. Build Assurance Argument (PA06)
7. Coordinate Security (PA07)
8. Monitor Security Posture (PA08)
9. Provide Security Input (PA09)
10. Specify Security Needs (PA10)
11. Verify and Validate Security (PA11)

Project

12. Ensure Quality (PA12)
13. Manage Configuration (PA13)
14. Manage Project Risk (PA14)
15. Monitor and Control Technical Effort (PA15)
16. Plan Technical Effort (PA16)

Organizational

17. Define Organization’s Systems Engineering Process (PA17)
18. Improve Organization’s Systems Engineering Process (PA18)
19. Manage Product Line Evolution (PA19)
20. Manage Systems Engineering Support Environment (PA20)
21. Provide Ongoing Skills and Knowledge (PA21)
22. Coordinate with Suppliers (PA22)

The capability dimension is composed of six maturity levels, which go from 0 to 5 depending on the support for their respective practices as shown in figure 1. For details on what each of these level entail, readers are encouraged to find additional information in [6].

![Maturity Level Pyramid](image)

In this paper, we focus our discussion on the domain dimension of SSE-CMM, especially on process areas in Security Engineering category, as these are geared towards development of security processes. Moreover, since Security Engineering is considered to be divided in three basic groups, Risks, Engineering and Assurance; an organization could have the flexibility to excel or concentrate in selected specific areas following the example of CMMI [2].

Capability Maturity Model Integration or CMMI allows companies to integrate effective process improvement practices across different levels of organizations and can be implemented applying the continuous or staged model. The continuous model of CMMI, where organizations can choose their own process areas to excel upon, offers a more flexible roadmap to adopt organization-wide engineering practices than the stringent staged model. As in the staged model of CMMI, in order to achieve a specific maturity level not only each of the activities listed under this level must be performed, but also those listed under any level below it. The staged model may seem inflexible in some situations but it clearly allows a comparison and differentiation among companies in the same industry. The continuous model on the other hand, allows more flexibility by permitting organizations to focus on the process areas that best satisfies their objectives. With such thought, in this paper we address the process areas under engineering division of security engineering in SSE-CMM.

3. SECURITY PRACTICES AND PROCESSES UNDER SSE-CMM AND CONSIDERATIONS FOR IMPLEMENTATION

In this section, we briefly introduce each process areas (PAs) as published in version 3.0 of SSE-CMM and highlight some available tools and practical approaches to implement the practices described in the process areas.

**PA01 – Administer Security Control**

The goal of Administer Security Control is to ensure that the intended security for the system conceived at design time, is in fact achieved by the system in its operational state [2]. Among the best practices under this PA, are the management of security awareness, training, and education programs for all users and administrators; establishment of responsibilities, accountability for security controls, their effective communication, and management of periodic maintenance of security services.

These best practices are very much self-explanatory when it comes to their implementation. When implementing security practices within an organization, regardless of how big or small they are, communication and training are both very important. Every user or employee should be aware of the policies and procedures and how to follow them and know who to contact in case of any incident. One inadequately informed employee can easily be that one weakest link that threats can potentially exploit. A common example is the use of default passwords.

The management and maintenance of security services guarantees that security implementations are not outdated and can keep up with changing technologies and the surrounding environment. It is important to integrate security without compromising it, in a manner that facilitates maintenance and adaptability.

Communications practices could be implemented in various forms depending on the operating system platforms used in the organizations. A local network web server, wiki site, web forum, or Microsoft SharePoint [12] hosted on a server, could serve as centralized resources for employees to refer for updated information regarding the security policies, procedures and services within the organization. A secure web server hosting the documentation on policies, security structure, roles
and responsibilities should be made available to users/employees.

PA02 / PA03 / PA04 / PA05 – Assess Impact/ Assess Security Risk/ Assess Threat/ Assess Vulnerability

Impact assessment is a very important aspect when engineering security, most importantly when applied to areas such as risk, threat and vulnerability. It allows a balance between the tangible and intangible consequences of an unwanted incident, its frequency of occurrence, and the cost of preventing it.

Security risk assessment is very closely linked with impact assessment but it focuses on the study of the probability of occurrence of a certain unwanted event that could threaten the capabilities or assets of the system. Due to their close relationship \( (\text{risk} = \text{asset value} \times \text{threat rating} \times \text{vulnerability rating}) \) [13], impact assessment, security risk assessment, threat assessment and vulnerability assessment process areas are analyzed in the following section.

Among the best practices listed under SSE-CMM supporting assessment, are the identification of assets that support key operations of the system in focus, the selection of appropriate metrics for assessment in the different areas, the characterization and identification of impacts, risks, threats and vulnerabilities, and the monitoring of ongoing changes to ensure that the understanding of processes is preserved.

Several tools are available to help in this type of discovery process. However prior to their usage, careful study should highlight the crucial points where these tools would serve their purpose. It could possibly be where users have a window of interaction with the outside world with potential to external threats; however, potential threats could also be internal; requiring more cautious examination. With the help of risk and impact assessment practices, it is possible to gather enough information about possible threats, vulnerabilities and their impact on the system as to justify the action for their prevention and protection against them.

In this regard, a possible choice in vulnerability assessment software is eEye Retina Network Security Scanner [4]. It provides a centralized comprehensive view of system vulnerability, with multiplatform support of security risk assessment, security best practices, policy enforcement and regulatory audits [4]. Retina is an all-in-one tool for security assessment across the organization, capable not only of providing useful information in forms of reports, but also providing the possibility of acting on them by patching vulnerabilities and other means.

Nessus Security Scanner is another tool choice in this respect. It is free of charge, supported and maintained by the software community and backed up by thousands of users worldwide. It provides high speed discovery, configuration auditing, asset profiling, sensitive data discovery and vulnerability analysis [18]. Tenable Network Security Inc. [18], the sole sponsor of Nessus, also provides among its weaponry of tools, 1) Security Center a centralized security management and assessment tool, 2) Passive Vulnerability Scanner, and 3) Log Correlation Engine - among other tools to analyze and help correlating events under a wide range of operating systems.

The figure below shows a sample section of a comprehensive report generated by Nessus when used on a network of over 15 hosts. This report shows a suggestion about how to mitigate the security vulnerability along the problem description (“NetBIOS name exposed”). A more comprehensive report can be found in [18].

Figure 2 – Sample Nessus Report (Tenable)

PA06 – Build Assurance Argument

This process area addresses assessment of security needs with supporting evidence or proof (e.g., reports, graphs, logs, etc.). Among the practices in this process area are the identification of security objectives, identification and gathering of evidence supporting these objectives, defining a strategy to address the security objectives, and providing assurance argument that clearly demonstrates that the security needs of the customers are met [3].

The increased usage of wide and distributed varieties of information technology resources in organizations has made the usage of effective, efficient and concise methods of assurance argument more critical. At The Center for High Assurance Computer Systems, Naval Research Laboratory, tools have been studied to address these needs among them the VNRM (Visual Networking Rating Methodology) and its successor named SANE (Security Assurance and Navigation Environment) [14]. Both of these tools provide an easy to use visual environment which allows composing evidence from four different sources such as Physical, Technical, Operational and Personnel, and specifying how each of this evidence contributes to the overall argument of systems in their operational environment [14]. These tools are not publicly available but a VNRM demonstration video and further information can be found in references listed in [14] and [19].

Available network and vulnerabilities scanners provide the benefit of comprehensive reports, and can be used to support assurance arguments. Running the reports before and after applying required security measures such as installation of patches to operating systems, closing unnecessary ports/services, implementing firewalls and others, can serve as evidence that the security requirements are met.

PA07 – Coordinate Security

Communication is always critical in a group environment. Security engineering is not an exception. This particular practice is concerned about security coordination and open communication among all project personnel and external groups.

Several tools can be used for communication and coordination purposes. However, it is always important to establish policies, procedures and agreements on the format of information exchange (e.g., text files, mp3 videos, etc.), media
to be used (e.g., tapes, DVDs, etc), expectations and frequency of information sharing events.

Email has wide impact in daily communication and can be utilized as a very important tool to consider in this process of coordination. However, email is not well fitted to discussion environments where large groups are involved. For these cases, electronic discussion forums, formal scheduled meetings, online live discussion meetings tools such as those offered by WebEx [20], and FutureU Illuminate Live (FutureU) could be utilized. Also instant messaging tools such as Ipswitch IM [9] could serve the purpose more efficiently, since they allow secure instant messaging infrastructure with little network overhead.

**PA08 – Monitor Security Posture**

Security Posture serves as a follow up of every external or internal security related event and ensures that all breaches and potential events that could lead to a breach are reported and addressed properly. Hence this practice is also very closely related to the vulnerability and security assessment practices previously discussed.

This practice is highly significant as it relies on the most important factor of the entire security process - the human factor. The human factor is one of the major reasons why information system attacks can become successful [15]. Regardless of what tools we use to support the security engineering process, the human factor is always crucial to the success or failure of the overall security engineering process. The security posture rests to a great extent in properly following the policies and procedures established. It is human nature sometimes to find shortcuts, alternative easier solutions and personalize a certain procedure without formally informing higher authority in the process - not realizing that by doing so; we potentially jeopardize the entire system.

Due to today’s complex information technology environment it has been a difficult task to find tools specifically developed to track or enforce this particular practice effectively. Same is true for the assurance argument process area. Due to the complexity involved, choices are limited in this regard. IBM offers the Tivoli Security Operations Manager (TSOM) and its family of products at a premium [8]. TSOM centralizes and collects security data from disparate security solution throughout the technology infrastructure of an organization, in order to improve its security operations and information risk management, allowing IT staff to perform more pertinent and productive tasks [8].

Tools available at no charge such as those mentioned previously in PA07, could help in monitoring the security posture. Still it is up to the management and other personnel involved in the project to make sure that the policies and procedures are followed. This involves reporting, identification of potential breaches, and monitoring the changes in impact, risks and environment.

**PA09/PA10 - Provide Security Input/ Specify security Needs**

The specification of security needs involves defining the security requirements of the system in order to meet the legal, functional, and organizational objectives taking into account the current environment of the system [3]. This process should identify the purpose of the system and provide high level views of system operations, as well as the goals of the system under a security context.

For the purpose of representing security needs and the related documentation, Use Cases [1] and Misuse Cases [16] approaches could provide a clear view of needs, actors, activities involved and their interrelationship and dependencies from a desired and hostile point of view. Use cases describe the functionality of a system from the external users’ perspective in a way that they can be easily understood [21]. On the other hand, a Misuse Case is a use case from the point of view of an actor hostile to the system or a threat [17] - representing scenarios of how the system could be compromised. An Automated Teller Machine (ATM) example of both representations is included in figure 3. In the figure, it is fairly simple to note and distinguish the different interactions between the customer, the ATM machine, and the bank. This interaction within the ATM machine is represented by the Use Case which represents the expected functional requirements of the system (normal arrows). The interactions from the attacker’s point of view are added to form the Misuse Case. Arrows with rectangle show hostile actions against the system, while arrows with circles show actions necessary to mitigate the hostile actions.

**Figure 3. - Example of Use/Misuse Cases (ATM System)**

The information provided in the security needs specification should be used, updated and further refined as needed. The information should be properly disseminated to designers, developers, and users, ensuring that everyone has a clear and common understanding of security needs facilitating their implementation and operation. In this regard, besides formal meetings, MS SharePoint portal could be used to inform the entire engineering organization of the results of the security input process and also additional tools such as email would be helpful.

**PA 11 - Verify and Validate Security**

Verification and Validation are very often associated with correctness and effectiveness and span across the entire information system of organizations including architectures, policies and operational concepts. The product(s) associated with this process area may be fed back as an important source of information to engineering teams at any time during the lifecycle of the security engineering process [3].

Similar to PA06, assessment tools such as network vulnerability scanners/auditing, enterprise product solutions like TSOM [8], or in-house software validation tools can be used. This would help to verify the applied solutions against the security requirements and architectures using testing, demonstration, analysis and other methods - while still providing traceability between solutions and requirements. In this process area, the applied solutions would also need to be verified against specific operational security needs of the customer.
4. UTILITY GRID

In this paper we have highlighted several utilities that could facilitate the implementation of several process areas as outlined in SSE-CMM - specifically those under risks and security process engineering. These utilities are just a small fraction of products in the software market and do not include hardware appliances. There are a wide variety of software/hardware tools that could complement the tools mentioned in this paper, however, the tools and techniques covered, provide a good starting point for implementing SSE-CMM practices, even at the enterprise level. For easier reference, we include a tabulated list below (Table 1) with the URLs of the resources and their opportunity of usage in the SSE-CMM process areas discussed.

<table>
<thead>
<tr>
<th>Utility</th>
<th>URL / Usage</th>
<th>PA</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS SharePoint</td>
<td><a href="http://www.microsoft.com/sharepoint/default.msp">http://www.microsoft.com/sharepoint/default.msp</a></td>
<td>PA01</td>
</tr>
<tr>
<td></td>
<td>Group Collaboration and Centralized Information Sharing</td>
<td>PA09</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PA10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PA03</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PA04</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PA05</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PA06</td>
</tr>
<tr>
<td></td>
<td>VULNERABILITY SCANNER</td>
<td>PA11</td>
</tr>
<tr>
<td>Nessus</td>
<td><a href="http://www.nessus.org/nessus/Vulnerability">http://www.nessus.org/nessus/Vulnerability</a> Scanner</td>
<td>PA02</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PA03</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PA04</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PA05</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PA06</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PA11</td>
</tr>
<tr>
<td>WebEx</td>
<td><a href="http://www.webex.com/Online">http://www.webex.com/Online</a> Meeting and Collaboration</td>
<td>PA07</td>
</tr>
<tr>
<td>Elluminate Live</td>
<td><a href="http://www.elluminate.com/Online">http://www.elluminate.com/Online</a> Meeting and Collaboration</td>
<td>PA07</td>
</tr>
<tr>
<td>Ipswitch IM</td>
<td><a href="http://www.ipswitch.com/Secure">http://www.ipswitch.com/Secure</a> Instant Messaging</td>
<td>PA07</td>
</tr>
<tr>
<td>Use Cases</td>
<td><a href="http://en.wikipedia.org/wiki/Use_cases%20diagram">http://en.wikipedia.org/wiki/Use_cases%20diagram</a></td>
<td>PA09</td>
</tr>
<tr>
<td></td>
<td>Capture systems’ functional requirements</td>
<td>PA10</td>
</tr>
<tr>
<td>Misuse Cases</td>
<td><a href="http://ezyweb.easyjet.co.uk/~iany/consultancy/misuse_cases.ppt">http://ezyweb.easyjet.co.uk/~iany/consultancy/misuse_cases.ppt</a></td>
<td>PA09</td>
</tr>
<tr>
<td></td>
<td>Use Cases with hostile intent</td>
<td>PA10</td>
</tr>
</tbody>
</table>

| 5. CONCLUSIONS |

There is no silver bullet in the application of security engineering standards. Although the majority of related publications do provide abundance information on the SEE-CMM model, they do not address how an organization can actually implement the recommended practices and what tools are available to serve their purpose. In this paper, we have provided readers with a list of some common and readily available tools to address the process areas in SEE-CMM. The tools are not necessarily appropriate in all environments. Careful planning and study of individual organization’s context is necessary before applying them to actual security engineering environment. However, most of these tools are based on standards and have proven to be very useful in addressing security and communicational needs of organizations worldwide.

6. REFERENCES


