Systems Security Engineering Capability Maturity Model with Support of Simulation and Knowledge Management

Danijela Bambir, Željko Hutinski, Vesna Dušak
Faculty of Organization and Informatics
University of Zagreb
Pavlinska 2, 42000 Varaždin, Croatia
{danijela.bambir, zeljko.hutinski, vesna.dusak}@foi.hr

Abstract. *With the increasing reliance of society on information, the protection of that information and related system is becoming extremely relevant. Because of that, security engineering expanded its domain to many areas like financial transactions, contractual agreements, personal information and the Internet. Therefore, then appeared a need for appropriate methods and practices required by various participants in security engineering process. As a result, SSE-CMM was developed, describing the essential characteristics of an organization's security engineering process. The model consists of five capability levels that address different maturity stages. In this paper it is shown that simulation and knowledge management can be used to support improvement at all five levels of the SSE-CMM. Simulation and KM capabilities at each SSE-CMM level build upon the capabilities of the preceding levels, and match the needs of the security engineering practices at that capability level.*

Keywords. SSE-CMM, simulation, knowledge management

1 Introduction

All participants in information society, like customers and suppliers, are interested in improving the development of security products, systems and services. Improvement can be achieved through successful interconnection of people and technology. To manage cost effectiveness in this interconnection it is relevant to emphasize the quality of the processes being used, and the maturity of the organizational practices present in the processes. These requirements for implementing security in a system or series of related systems are discussed and organized in the SSE-CMM (Systems Security Engineering Capability Maturity Model). The Model is primarily concerned with ITS (Information Technology Security) domain but is also applicable to other security domains. SSE-CMM model is focused on the existing processes in organization so there is no intent to dictate a specific process to be used. Further, the Model is applicable to all types and sizes of security engineering organizations from commercial to government and the academe [13].

2 The SSE-CMM model

There are two important dimensions of the Model, domain and capability. The domain dimension includes all the practices that define security engineering called "base practices". Base practices are organized into 22 bigger groups named "process areas" divided into areas of security engineering and areas that address the project and organization domains.
First eleven process areas in alphabetical order that refer to security engineering:

- PA01 Administer Security Controls
- PA02 Assess Impact
- PA03 Assess Security Risk
- PA04 Assess Threat
- PA05 Assess Vulnerability
- PA06 Build Assurance Argument
- PA07 Coordinate Security
- PA08 Monitor Security Posture
- PA09 Provide Security Input
- PA10 Specify Security Needs
- PA11 Verify and Validate Security

Process areas related to project and organizational practices:

- PA12 – Ensure Quality
- PA13 – Manage Configuration
- PA14 – Manage Project Risk
- PA15 – Monitor and Control Technical Effort
- PA16 – Plan Technical Effort
- PA17 – Define Organization's Systems Engineering Process
- PA18 – Improve Organization's Systems Engineering Process
- PA19 – Manage Product Line Evolution
- PA20 – Manage Systems Engineering Support Environment
- PA21 – Provide Ongoing Skills and Knowledge
- PA22 – Coordinate with Suppliers

The capability dimension consists of "generic practices" grouped in "common practices" that refer to process management and institutionalization. These practices should be performed as a part of doing the base practices. Further, common practices are grouped into five "capability levels" to define major shifts in an organization's manner of performing work processes [13]:

1. "Performed Informally". At this level base practices are generally performed but not adequately planned and tracked. Their performance depends on individuals. Quality of work products is variable due to the lack of control.
2. "Planned and Tracked". Performance of the base practices is planned and managed. Work products satisfy specified requirements. Activities are measured to track actual performance and take corrective actions.
3. "Well Defined". An organization establishes well-defined standard processes. Similar processes used successfully on specific projects are documented. Communication in internal and with external groups is coordinated.
4. "Quantitatively Controlled". Measurement of performed practices is at high level. Measurable quality goals for the work products are clearly stated thus providing prediction of performance.
5. "Continuously Improving". Continuous process improvement is enabled by quantitative indicators from previous level and by implementing new ideas and technologies. Process effectiveness is continuously improving by performing causal analysis of defects and eliminating defect causes.

Generally, capability involves an organization's potential to perform specific task or whole process expressed as a quantifiable range of expected results. On the other hand, process maturity implies the extent to which a specific process is explicitly defined, managed, measured, controlled and effective. The SSE-CMM model endeavors to measure a potential for growth in capability and indicates both the richness of an organization's process and the consistency with which it is implemented throughout the organization. To check an organization's capability to perform a particular activity it is enough to put the base practice and generic practice together (Fig. 1). As a result of intersection, useful question about organization's capability can be asked. Answering all the questions raised by combining all the base practices with all the generic practices will provide a good picture of the security engineering capability of the organization in question.

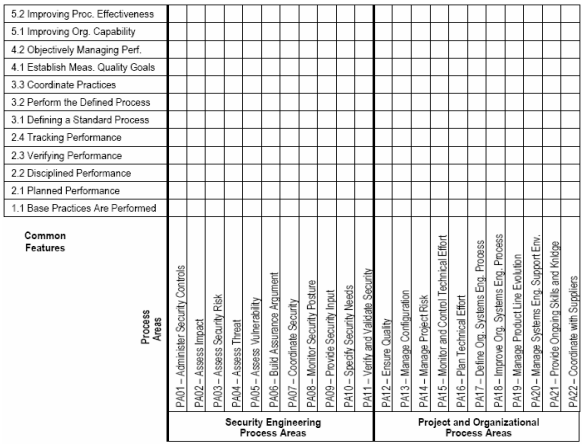

Figure 1. The SSE-CMM model [13]

According to the Model, all requirements for lower capability level have to be fulfilled to make progress from one level to another. In the next section, it will be explained how simulation and knowledge management can help to achieve higher levels of the Model.

3 Simulation in CMM

Various researches have been done on the capability maturity models as a wide accepted framework which shows the evolutionary path from ad-hoc toward mature and capable processes [8]. Furthermore, simulation has also occupied many researchers as a tool for advancing process capabilities and performance. There are many benefits of simulation in process improvements. One important factor is that it provides insights into complex process behavior. Furthermore, it can support project costing, planning, tracking and prediction. To succeed in competitive world, predicting costs is extremely important. In this context, simulation can obtain not only estimates of cost, but estimates of cost uncertainty. It is also valuable in training personnel. At last, simulation can help in decision-making process as a significant influence in communication and consensus building [3].

After all, simulation has already been observed in a way of support of CMM-based process improvement. Results of those researches will be used to think about simulation in the SSE-CMM.

4 Knowledge management in CMM

Knowledge assets involve substantial part of all organizational assets in today's knowledge-based economy. Some authors, like Alan Greenspan, estimate it on 70%. For that reason, it is obvious that great efforts should be made to measure the worth of knowledge assets.

Institutional knowledge assets can be categorized into four areas: expertise, lessons learned, knowledge documents and data. Such categorization follows from three characteristics of knowledge: (a) specific proportion of tacit and explicit content, (b) method of knowledge transfer and contextual value, and (c) life cycle with stress on its shelf time. [7] Although each type of knowledge has its own unique characteristics, a common life-cycle framework can be applied to understand how it can be managed. The four distinct stages of the knowledge life cycle are discovery, capture, sharing and application [2]. In assessing KM capabilities of an organization, identifying how well each stage of the knowledge life cycle is managed becomes relevant. Stages may be assisted by the technology support and the integration of KM-related activities into normal business processes. However, the existence of a positive knowledge-sharing culture is a precondition for an organization to have any capability in KM [1].

To summarize, knowledge needs to be managed in order to maximize its value. According to three previous methods for KM assessment based on CMM [3], next section describes KM in SSE-CMM.

5 Simulation and KM in the SSE-CMM

Up to this point, general concepts of simulation and knowledge management in CMM were discussed to prepare for this step. Taking into account these ideas and embedding them in new environment, the SSE-CMM, has given following results listed in capability levels.

This section is organized in the form of questionnaire so as to ensure clarity and uniformity of all security base practices. Project and organizational base practices are not included in this activity because they are not directly connected with security engineering.

5.1 PA01 – Administer Security Controls

1: Simulation is used for raising security awareness.
2: Simulation is used for establishing responsibilities for security controls (role play) and managing the configuration of system security controls.
3: Simulation is used for security training and education of all users and administrators.
4: Simulation is used for determining quantitative performance limits of the system security control configuration.
5: Simulation is used for maintaining and improving control mechanisms.

1: Documents on security controls can be found.
2: Documents describing security roles and responsibilities are made and distributed. Database describing the current state and changes of the system security configuration is maintained.
3: Security engineering working group which is responsible for resolving security related issues is established. Lessons learned and other training materials are captured.

4: Database is expanded by numerical values for tracks and changes of the system security control configuration.
5: Experts improve control mechanisms regarding to the impact of lessons learned and collected data.

5.2 PA02 – Assess Impact

1: Simulation is used for raising impact awareness.
2: Simulation is used for identifying impacts and selecting impact metrics.
3: Simulation is used for managing the relationships between different metrics.
4: Simulation is used for monitoring and measuring ongoing changes in the impacts.
5: Simulation is used for analyzing impact changes and predicting new ones.

1: The list of general impacts can be found and distributed.
2: Documents including lists of impacts, impact metrics are created and shared in the organization.
3: Impact metric relationships and combination rules are stored in documents and distributed through the organization. Data stored in databases are available for decision making.
4: Database is expanded by numerical values for tracks and changes in impacts and easy to access and manipulate.
5: Impact monitoring reports and impact change reports are communicated.

5.3 PA03 – Assess Security Risk

1: Simulation is used for raising risk awareness.
2: Simulation is used for identifying exposures (threat/vulnerability/impact triples) and assessing their risk.
3: Simulation is used for assessing the total uncertainty associated with the risk for the exposure.
4: Simulation is used for monitoring and measuring ongoing changes in the risk spectrum and changes to their characteristics.
5: Simulation is used for selecting new risk analysis method.

1: The list of general risks can be found and distributed.
2: Documents concerning system exposure lists, exposure risk list and exposure priority table are created and shared in the organization.
3: Exposure risk with associated uncertainty and risk priority lists are stored in documents and distributed through the organization. Data stored in databases are available for decision making.
4: Database is expanded by numerical values describing changes in risks and easy to access and manipulate.
5: Risk monitoring reports and risk change reports are communicated.

5.4 PA04 – Assess Threat

1: Simulation is used for raising threat awareness.
2: Simulation is used for identifying applicable threats arising from natural or man-made sources.
3: Simulation is used for assessing the likelihood of an occurrence of a threat event.
4: Simulation is used for monitoring and measuring ongoing changes in the threat spectrum and changes to their characteristics.
5: Simulation is used for analyzing threat changes and predicting new ones.

1: The list of general threats can be found and distributed.
2: Documents describing natural and man-made threats and their scenario descriptions are created and shared in the organization.
3: Threat table with associated units of measure and location ranges, threat agent descriptions and threat event likelihood assessment are documented and distributed through the organization. Data stored in databases are available for decision making.
4: Database is expanded by numerical values describing changes in threats and easy to access and manipulate.
5: Threat monitoring reports and threat change reports are communicated.

5.5 PA05 – Assess Vulnerability

1: Simulation is used for raising vulnerability awareness.
2: Simulation is used for identifying system security vulnerabilities.
3: Simulation is used for assessing the system vulnerability and aggregate vulnerabilities that result from specific vulnerabilities and combinations of specific vulnerabilities.

4: Simulation is used for monitoring and measuring ongoing changes in the applicable vulnerabilities and changes to their characteristics.
5: Simulation is used for selecting new vulnerability analysis method.

1: The list of general vulnerabilities can be found and distributed.
2: Documents describing vulnerability lists and attack plans are created and shared in the organization.
3: Penetration profile including results of the attack testing and vulnerability property tables are documented and distributed through the organization. Data stored in databases are available for decision making.
4: Database is expanded by numerical values describing changes in vulnerabilities and easy to access and manipulate.
5: Vulnerabilities monitoring reports and vulnerabilities change reports are communicated.

5.6 PA06 – Build Assurance Argument

1: Simulation is used for raising awareness of customer's security needs.
2: Simulation is used for identifying the security assurance objectives.
3: Simulation is used for defining a security assurance strategy to address all assurance objectives and evidences.
4: Simulation is used for performing quantitative analysis of achieved assurance objectives.
5: Simulation is used for maintaining and improving security assurance strategy.

1: The list of general customer's security needs can be found and distributed.
2: Statement of security assurance objectives is created and shared in the organization.
3: Security assurance strategy is defined and distributed. Evidences stored in repository (database) are available for decision making.
4: Assurance evidence analysis results are obtained and stored in database.
5: Assurance argument with supporting evidence is communicated and periodically reviewed.

5.7 PA07 – Coordinate Security

1: Simulation is used for raising awareness of security engineering activities between all the involved parties.
2: Simulation is used for identifying coordination objectives and coordination mechanisms.
3: Simulation is used for coordinating security decisions and recommendations.
4: Simulation is used for performing quantitative analysis of achieved coordination objectives.
5: Simulation is used for maintaining and improving coordination objectives and mechanisms.

1: There is a general willingness to participate in security engineering activities.
2: Working group memberships and schedules, organizational standards, communication plans and communication infrastructure requirements are identified.
3: Coordination is facilitated by procedures for conflict resolution, meeting agendas, goals, action items and action item tracking.
4: Achievement of coordinated activities is tracked in database.
5: Recent improvements in coordination objectives and mechanisms are implemented.

5.8 PA08 – Monitor Security Posture

1: Simulation is used for raising awareness of all breaches of security.
2: Simulation is used for analyzing event records and identifying security incidents.
3: Simulation is used for monitoring changes in threats, vulnerabilities, impacts, risks, the environment and security safeguards.
4: Simulation is used for measuring all the changes.
5: Simulation is used for reviewing the security posture of the system to identify necessary changes and managing the response to security relevant incidents.

1: List of potential breaches can be found and distributed.
2: Documents and data describing events, log records and sources, incidents are identified and distributed.
3: Any external or internal changes that may affect the security posture of the system are

documented and tracked. Data stored in databases are available for decision making.
4: Database is expanded by numerical values describing external or internal changes and easy to access and manipulate.
5: Regarding to assessment of significance of changes, new security incidents responses are implemented.

5.9 PA09 – Provide Security Input

1: Simulation is used for understanding of security input needs.
2: Simulation is used for determining security constraints and considerations.
3: Simulation is used for identifying solutions (alternatives) to security related engineering problems.
4: Simulation is used for measuring engineering alternatives using security constraints and considerations.
5: Simulation is used for providing security related guidance to engineering groups.

1: There is an existence of a list of common security input needs.
2: Agreements between security engineering and other disciplines are identified. Security constraints and considerations are determined.
3: Solutions to security related engineering problems are identified and documented.
4: Engineering alternatives are measured and compared in quantitative terms.
5: Security related guidance to engineering groups (system architects, designers, implementers, users) is provided.

5.10 PA10 – Specify Security Needs

1: Simulation is used for understanding of the customer's security needs.
2: Simulation is used for identifying the laws, policies, standards, external influences and constraints that govern the system in order to identify system security context.
3: Simulation is used for capturing high-level goals that define the security of the system.
4: Simulation is used for defining and measuring a consistent set of requirements which define the protection to be implemented in the system.
5: Simulation is used for obtaining and improving agreement that the specified security requirements match the customer's needs.

1: The list of general customer's security needs can be found and distributed.
2: Customer security needs statement, security constraints, security profile and expected threat environment are identified and listed.
3: Operational/environmental security policy and system security policy are established and shared.
4: Security related requirements are defined and measured. Traceability matrix is determined to map security needs to requirements to solutions to tests and test results.
5: Approved security objectives and security related requirements baseline are stated and implemented.

5.11 PA11 – Verify and Validate Security

1: Simulation is used for raising awareness of verification and validation of security.
2: Simulation is used for identifying verification and validation targets.
3: Simulation is used for defining verification and validation approach.
4: Simulation is used for providing verification and validation results.
5: Simulation is used for improving verification and validation approaches.

1: There is a general willingness to verify and validate security.
2: Verification and validation plans are identified.
3: Test procedures, analysis, demonstration, observation plans and traceability approach are defined and documented.
4: Raw data from test, analysis, demonstration, observation, problem reports, inconsistencies and ineffective solutions are stored and measured.
5: Experts improve verification and validation approaches regarding to the lessons learned and collected data.

6 Conclusion

A CMM is a framework for evolving an engineering organization from an ad hoc, less organized, less effective state to a highly structured and highly effective state. Use of such a model is a means for organizations to bring

their practices under statistical process control in order to increase their process capability.

In this article, general concepts of simulation and knowledge management in CMM were discussed to present the idea of their usability in security engineering. The SSE-CMM model was described and interpreted through capability levels. Every security base practice was looked from simulation and knowledge management perspective. Obtained descriptions of base practices in the form of questionnaire present the elements of further research in this area.

References

[1] Adams G L, Lamont B T: **Knowledge management systems and developing sustainable competitive** advantage, Journal of Knowledge Management, 7(2), 2003, pp. 142-154

[2] Berztiss A T: **Capability Maturity,** Encyclopedia of Knowledge Management (Schwartz D G), Idea Group Reference, 2006, pp. 24-29

[3] Berztiss A T: **Capability maturity for knowledge Management**, Proceedings of the 13th International Workshop on Database and Expert Systems Applications, 2002, pp. 162-166

[4] Christie A M: **Simulation in Support of CMM-based Process Improvement**, The journal of Systems and Software 46, Elsevier Science Inc., 1999, pp. 107-112

[5] Ferraiolo K, Sachs J E: **Distinguishing Security Engineering Process Areas by Maturity Levels**, available at http://www.google.hr/search?q=Distinguishing+Security+Engineering+Process+Areas+by+Maturity+Levels&btnG=Tra%C5%BEi&hl=hr&sa=2, Accessed: 10th June 2008

[6] David M, Idelmerfaa Z, Richard J: **Managing and organizing concurrent processes according to the CMM levels**, Concurrent Engineering-Research & Applications 13(3), 2005, pp. 241-251

[7] Kulkarni U, Freeze R: **Measuring Knowledge Management Capabilities**, Encyclopedia of Knowledge Management (Schwartz D G), Idea Group Reference, 2006, pp. 605-613

[8] Miller M J, Pulgar-Vidal F, Ferrin D M: **Achieving Higher Levels of CMMI Maturity using Simulation**, Proceedings of the 2002 Winter Simulation Conference, USA, 2002, pp. 1473-1478

[9] Murray E J: **Knowledge Management System Success Factors**, Encyclopedia of Knowledge Management (Schwartz D G), Idea Group Reference, 2006, pp. 436-441

[10] Payne S C: **A Guide to Security Metrics**, available at http://www.sans.org/reading_room/whitepapers/auditing/55.php, Accessed: 11th June 2008

[11] Raffo D M, Vandeville J V, Martin R H: **Software Process Simulation to Achieve Higher CMM Levels**, The journal of Systems and Software 46, Elsevier Science Inc., 1999, pp. 163-172

[12] Systems Security Engineering Capability Maturity Model (SSE-CMM) Project, Model Description Document, Version 3.0, Carnegie Mellon University, Pittsburgh, Pennsylvania, 2003, available at http://www.sse-cmm.org/docs/ssecmmv3final.pdf, Accessed: 30th May 2008