SECURITY SYSTEM ENGINEERING CAPABILITY MATURITY MODEL IN THE ICT SECURITY

Petrović R. Slobodan[1], Zoran Čekerevac[2]
Gojko Grubor[3]

ABSTRACT

Security System Engineering Capability Maturity Model (SSE CMM), as a staged model presentation of the process area (PAs), could improve security processes, personal and organizational processes maturity level by prioritizing the next steps for either security, managing or organizational PAs, reflecting reasonable incremental processes improvements. This enables an organization to develop a secure systems or products evolving such a capability in a feasible way over time. The main applications of the model are to (1) guide development of organizations security programs, (2) improve security programs, (3) improve ICT protection profiles and (4) develop security organizations and personal. The assessment methods need to know what maturity actually means for the SSE applications. This paper provides a foundation for defining maturity levels for SSE and insights into the maturity level placement of the PAs reflected to the security program development.

Key words: process, process area (PA), SSE capability maturity model (CMM), capability maturity level

1. INTRODUCTION

Security System Engineering (SSE), based on the Generally Accepted Information Security Principles
and process approach define a balanced set of the security objectives; transform them into security needs through security documents, guidelines and procedures; establish confidence in the security effectiveness; asses acceptance of the residual security risk and integrate all security aspects into a trusted system [4].

[1] Dr Petrović R. Slobodan, Railway College Belgrade, professor
[2] Dr Zoran Čekerevac, Railway College Belgrade, professor and director
[3] Mr. Sci. Gojko Grubor, BEE Republic of Serbia, Information Technology and Internet Agency, security manager

The staged SSE-CMM (*Capability Maturity Model*) [1], determines processes improvement by measuring maturity levels of the key security processes. Security processes maturity levels are determined by: mandatory, repetitive and quantifiable measuring at all levels; method of performance; continuity of control and optimization; progressive improvement; use of standard security processes, policies and procedures; quality of security plan, processes management and institutional support, and performance of the key security process areas (PAs) [6]. The SSE-CMM was developed applying the concepts of statistical process control to the SSE to promote the development of secure systems and trusted products within anticipated limits of cost, schedule and quality, and to improve predictability, control and process effectiveness.

Process is an integrating function for people and technology. It is a set of performed activities to achieve a given purpose and can be defined, managed, measured, controlled and effective. The *defined* process still should be performed and the performed process is actually performed. *The process performance* is a measure of the actual results achieved from following a process (on a particular project). *The process maturity* is an extent to which process is explicitl**y** defined, managed, measured, controlled and effective and implies a potential for growth in capability. *The process capability* is the quantifiable range of expected results, achieved by following a process and a predictor of future project outcomes.
In this paper, applications of the reduced SSE-CMM with focus on security program development and the appraisal method of Certification Authority in the PKI are shown [8].

2. THE SSE CAPABILITY MATURITY MODEL

2.1. THE ARCHITECTURE OF THE STAGED SSE-CMM

The SSE CMM architecture separates basic SE **PAs - domain side** from **capability side** of process management-focused elements. The domain consists of the three **PAs** categories: the **SSE (**engineering, analysis), **management** (project, coordination) and **organization,** (people, process), which include most if not the all of basic practices **(BPs)** in the given category. **A security BP:** applies across the systeme life-cycle; does not overlap with other BPs; represents a “best practice” of the security community; does not simply reflect a state-of -the-art technique; is applicable using multiple methods in multiple business contexts and does not specify a particular method or tool.

The PA is a set of related collectively performed BPs that can achieve a defined security purpose**.** Only performed **BPs** contributes to effectiveness of PAs, but each of PA has not to be performed.

The managing PAs and organizational PAs are essentially similar to the SSE ones (Table T-2.1). Therefore, the PAs and BPs are formally defined by its number, title, goal, and short description in *The Integral catalogue*. Only this approach can provide incremental improvement of the relevant security processes capabilities. The SSE CMM **does not prescribe** specific PAs or BPs; it gives a model to form and categorize the PAs and BPs to cover security product/system life-cycle, meaning the same BPs are applied in the SSE PAs at the all stages of the system life-cycle.

SSE PAs (unique**)**	**Management PAs**	**Organizational PAs**
Administer security controls	Ensure quality	Coordinate with suppliers of security systems/products
Assess operational security risk	Manage configurations	Define organization's security engineering process
Build assurance argument	Manage program risk	Improve organization's security engineering process
Coordinate security	Monitor & control technical effort	Manage security engineering support environment
Determine security vulnerabilities	Plan technical effort	Provide ongoing skills and knowledge
Monitor system security posture	*Based on SE-CMM adapted for SSE*	
Provide security input		
Specify security needs		
Verify & validate security		

Table T-2.1. The key PAs in the three categories of the staged SSE CMM, [10]

Generic practices are activities applied to all processes. They address the management, measurement, and institutionalization aspects of a process. Generic practices are grouped into logical areas called "common features" organized into five "capability levels" which represent increasing organizational capability. Each common feature has one or more generic practices. The lowest common feature is *1.1 BPs are Performed.* There is more than one way to group practices into common features and common features into capability levels.

A staged concept of the SSE CMM for security program development (Fig. 2.1) describes the stages through which processes progress as they are defined, implemented, and improved.The model provides a guide for selecting process improvement strategies by determining the current capabilities of specific processes and identifying the issues most critical to quality and process improvement within a particular domain. Process maturity level is achieved by performance of specific PAs at a given stage, enabling an organization to prioritize improvement efforts.

The maturity of the key identified security processes from all of the three categories are measured at the 5 levels (0 level is not performed-missing) by: defining measuring criteria; progressive improvement; prioritising of the BPs performance and maturity improvement; defining security objectives (always tend to the highest 5th level); security

response improvement, and by compliance to security standards and guidelines (ISO/IEC 17799, ISO/IEC 13325, NIST SPs), [9].

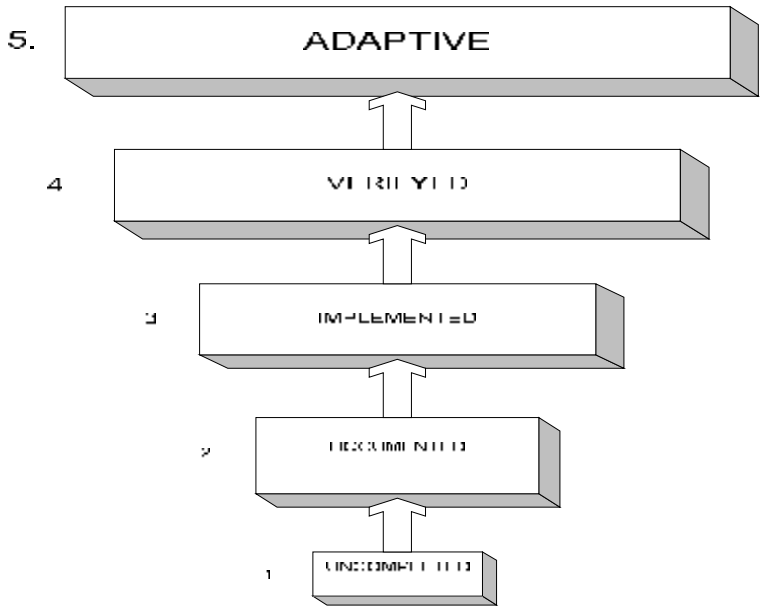

Fig. 2.1. Review of the generic SSE-CMM capability maturity levels [5]

2.2. APPLICATIONS OF THE SSE-CMM IN SECURITY PRACTICE

In the SSE practice the following three most often problems, that the model successfully resolves are noticed: security processes are not well defined and are considered as an separate part of information system development processes; security products/systems suppliers do not use appropriate measures of their SSE capabilities, and the final results of the security products/ systems development are evaluated, instead of processes.

However, an organization does not require the same maturity level of the all security processes what is the main purpose of the SSE-CMM applications. In security practice, the following good results are achieved by use of the SSE-CMM: measurement of security program processes maturity levels, measurement of security products/systems capability levels, measurement of security assurance processes, enhancement of organizations profiles [8], improvement of protection profile processes [12], measurement of security training processes maturity level, improvement of security products/systems accreditation and certification processes, etc.

2.3. THE SSE-CMM OF THE SECURITY PROGRAM DEVELOPMENT

Therefore, a reduced model (SSE-RCMM) is more suitable for security program development, since organizations mainly only tend to achieve the highest capability

level (5), because of financial and other restrictions. In this model security processes maturity levels are measured, too, but organization by itself identifies the key processes and determines: starting level of maturity, dynamics of maturity improvement and acceptable level of capability (e.g. for most government organizations the level 3 is quite sufficient), and the highest capability level (5) for the critical mission security program processes. Identification of the key security process maturity attributes and process capability measurement are two key stages of the model**.**

The SSE-CMM contains 129 BPs, organized into 22 PAs. All major areas of the SSE are organized in 11 PAs with 61 BPs. The remaining 68 BPs, organized in 11 PAs, address the managment and organization domains. The SSE PAs of security program are performed by two key activities: **implementation** (performance of the BAs and PAs) and **institutionalization** (support of organization).

2.3. THE CAPABILITY MATURITY LEVELS OF THE SECURITY PROCESSES

The SSE-CMM **maturity levels,** defined as an ordinal scale for measuring/evaluating process capability and incremental steps for improving process capability, are achieved by the implementation and institutionalization of specific PAs at a given stage, [12].

The SSE-CMM **capability levels,** based on the SE CMM, are defined as a common set of performed PAs (SSE, managing, organizational) that are providing the main improvement of the security processes performance capability and a logical and structured methodology for improving security processes performances. The staged SSE-RCMM defines five **capability maturity levels** of the security program processes (see Fig.2.1), described as follows, [5]:

Level 1–Uncompleted: the BPs are uncompleted, performed informally butcomplied with the security standards and guidelines (ISO/IEC 17799, ISO/IEC 13335, COBIT...); they may not be strictly planned and tracked; the PAs meets basic security needs.

Level 2– Documented: the BPs are planned, controlled, tracked and documented; management structure is established and roles and responsibilities are assigned; risk management methodology is applied and security plan is approved.

Level 3– Implemented: the BPs and the standard processes are defined, planned, managed and performed; the PAs are complied to the Security Best Practice Standard (ISF V.4, 2003.); awareness, education and training security program is performed; security system audit, management and accreditation/ certification procedures are performed (over system life-cycle).

Level 4 – Verified: the BPs are quantitatively controlled, measured and analyzed; the defined and implemented PAs efficiency and effectiveness are measured**;** information sensitivity are determined and potential threats impact are assessed; program security cost-effectiveness is analyzed; proactive security system is considered to be a part of the organization mission achievement.

Level 5 – Adaptive: the BPs, based on security objectives, are continuously improved and quantitatively measured; continuous processes improvement, enabled by quantitative feedback from the defined processes outputs, are verified; IT security is an integral part of the business activities; system vulnerabilities are managed and continual re-evaluation of combined threats are performed, and an adaptive change management are performed.

3. CERTIFICATION AUTHORITY PROFILE IMPROVEMENT

The SSE-CMM appraisal method, is based upon statistical process control concepts which define the use of process capability. A Certification Authority, as any organization does not require the same level of processes maturity in the PAs. The model measures maturity levels of key CA processes. The profile shown in figure 4.1 is generic and applicable to all types of CA, but the route CA should be at a higher maturity level than subordinate CAs.

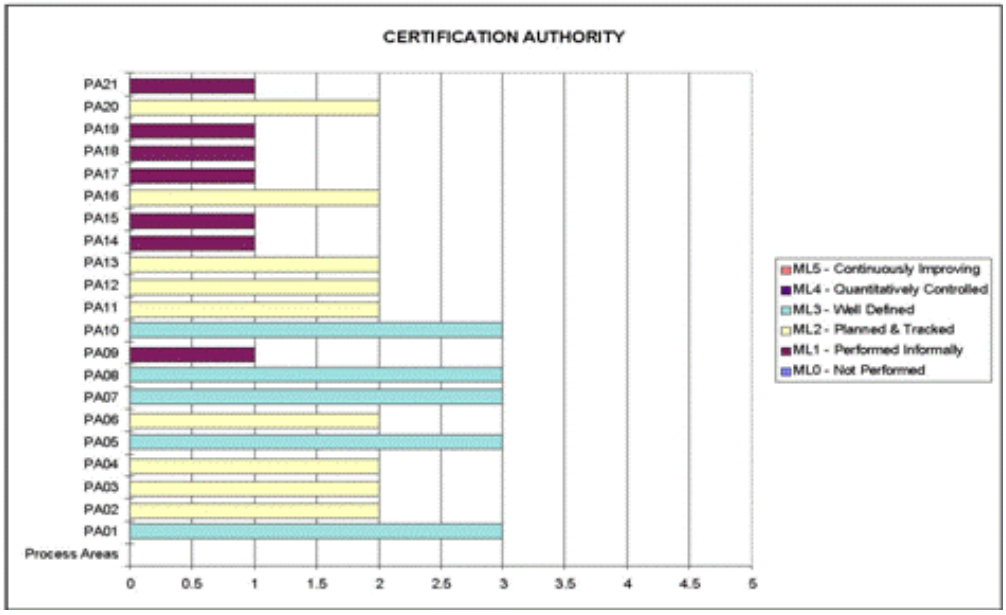

Fig. 4.1. Basic profile of the CAs in the PKI [8]

The following PAs that are used regularly in the CAs and gives at highest benefits are the most important: administer security controls (PA01), assess vulnerability (PA05), coordinate security (PA07), monitor security (PA08) and specify security needs (PA10), and require being

at the highest capability level. Implemented and well defined capability level 3 is considered appropriate. The PAs used on a periodic bases and also important are placed at lower level 2: the **SSE PAs -** to assess impact (PA02), security risk (PA03) and threat (PA04) and to build security assurance argument (PA06) and to evaluate security products/systems (PA11); then the **management PAs -** to assure quality (PA12), configuration management (PA13) and to plan technical efforts (PA16), and the **organizational PAs-** to manage support environment (PA20). Performance of the other infrequent **SSE PAs-** to provide security input (PA09); the **management PAs –** to asses risk (PA14), to control of security development (PA15), and **organizational** PA - to define the SSE processes (PA17), enhance the SSE processes (PA18), mange security products evaluation (PA19) and to provide current security knowledge and skill (OP21), are assigned to the lowest level of maturity for this profile.

General metric system procedure for the SSE CMM consists of the following activities [9]:
- Give score (1 – 5) to all the PAs, showing maturity levels, and displace them.
- Summarize all the PAs scores, showing PAs capability at each capability level.
- Difference between the PAs capability levels at measured and basic profile, represents measure of PAs progressive and incremental capability maturity level improvements.

6. CONCLUSIONS

1. The SSE CMM measures maturity levels of the relevant security processes that an organization implements to achieve tended capability maturity levels of the security PAs.
2. Improvement of the system life-cycle security program, security assurance, security software products/systems and training processes capability maturity levels, enhancement of organizations profiles and seciriity profile are the main areas of the SSE CMM application.
3. The SSE RCMM for security program development provides trustfulness that an organization implements specified security program with available budget and adequate security components in timely manner, by measurement of specified processes maturity levels.
4. The SEE CMM PAs are complemented to the security standards and guidelines (ISO/IEC 17799, ISO/IEC 13325, and NIST Special Publications).
5. The SEE CMM measures capability maturity level of an organization to perform the SSE processes, identify strength and weaknesses and focus to the most beneficial processes.

REFERENCES:

1. Bate Roger and all, *A Systems Engineering Capability Maturity Model V.1.1*, Software Engineering Institute, US DoD, 1995
2. Ferraiolo Karen & Sachs Joel E., *Distinguishing Security Engineering Process Areas by Maturity Levels*, USA Columbia, 1996 ferraiolo@md.arca.com, sachs@interramp.com
3. Ferraiolo Karen M.**,** *Considerations for Re-architecting the SEI CMM and Building Engineering CMMs*, Arca Systems, Inc. 1995, ferraiolo@arca.va.com

4. Ferraiolo Karen M., *The Systems Security Engineering Capability Maturity Model,* Arca Systems, Inc., October 24, 1996 ferraiolo@arca.va.com
5. Grubor Gojko, Mr Sci, BEE, *Model of security program development in Public Administration information system Republic of Serbia*, Local Government Conference, Serbian Chamber of Commerce and Industry, December 2004.
6. Hefner Dr. Rick and Warren Monroe, *System Security Engineering Capability Maturity Model*, TRW, CA, 1997 rick.hefner@trw.com
7. Hefner Rick, Ph.D, *Lessons Learned with the Systems Security Engineering Capability Maturity Model*, rick.hefner@trw.com
8. Hopkinson John P., *System security engineering capability maturity model - Organization profiles*, EWA-Canada, John.Hopkinson@sympatico.ca
9. Hopkinson John P., *The Relationship Between The SSE CMM and IT Security Guidance,* EWA-Canada, 1999, John.Hopkinson@sympatico.ca
10. http://www.csz.com/secat, *Overview of the Systems Security Engineering Capability Maturity Mode l(SSE-CMM),* SECAT LLCSystems Engineering Capability Assessment & Training,, 1996.
11. Martin James, *Systems Engineering Guidebook,* AT&T Bell Labs, USA, 1999.
12. The SSE-CMM Project Team, SSE-CMM®Model Description Document Version 3.0, June 15, 2003., *www.sei.cmu.edu/ideal/ideal.html*
13. Williams Jeffrey R., Ferraiolo Karen M., *P^3I – Protection Profile Process Improvement,* Arca Systems, Inc., william@arca.com, ferraiolo@arca.com