Proceedings of the 10th WSEAS International Conference on COMMUNICATIONS, Vouliagmeni, Athens, Greece, July 10-12, 2006 (pp355-359)

New Measurement Method For Web Application Security

Suhono H. Supangkat & Hendro Gunawan

Information Technology Research Groups
School of Electrical Engineering and Informatics- Institut Teknologi Bandung Indonesia
Jl Ganessho 10 Bandung Indonesia

suhono@itb.ac.id and hendro1979@yahoo.com

ABSTRACT

This paper propose new measurement method also know as S-vector based on two security standards ISO 17799:2005 and SSE-CMM v3.0, which can be an assessment tool for web application security. S-vector consists of three components, there are procedural, structural and technical aspects. Result suggests that security controls outlined in ISO 17799:2005 can be incorporated into S-vector as procedural and structural components. ISO 17799 controls may be mapped to specific data, specific web applications, or across multiple systems. Eleven of SSE-CMM's security-related process areas can be implemented into an S-vector implementation by providing a framework in which to administer procedural components. The capability levels of SSE-CMM measure a process' maturity and can be integrated into S-vector if scoring objectives are to measure process maturity and not the quality of process output.

Keywords: ISO 17799:2005, SSE-CMM v3.0,S-vector,Measure Process, Web application

1. INTRODUCTION

Security matters have become an integral part of daily life, and organizations need to ensure that they are adequately secured. While legislatures enact corporate governance laws, more and more businesses are seeking assurance that their vendors and partners are properly protecting information assets from security risks and are taking necessary measures to ensure business continuity. Security management certification provides just such a guarantee, thereby increasing client and partner confidence.

A number of best practice frameworks exist to help organizations assess their security risks, implement appropriate security controls, and comply with governance requirements as well as privacy and information security regulations. Of the various best practice frameworks available, the most comprehensive approach is based on the implementation of the international information security management standard, ISO/IEC 17799, and subsequent certification against the British standard for information security, BS 7799.

The SSE-CMM® is a process reference model. It is focused upon the requirements for implementing security in a system or series of related systems that are the Information Technology Security (ITS) domain. However, experience with the Model has demonstrated its utility and applicability to other security domains other than the IT domain. Within the ITS domain the SSE-CMM® Model is focused on the processes used to achieve ITS, most specifically on the maturity of those processes. There is no intent within the SSE-CMM® Model to dictate a specific process to be used by an organization, let alone a specific methodology. Rather the intent is that the organization making use of the SSE-CMM® Model should use its existing processes, be those processes based upon any other ITS guidance document.

The SSE-CMM® has a relationship to ISO/IEC TR 15504, Information technology — Software process assessment, particularly part 2, A reference model for processes and process capability, as both are concerned with process improvement and capability maturity assessment. However, TR 15504 is specifically focused on software processes, whereas the SSE-CMM is focused on security.

The SSE-CMM® has a closer relationship with the new versions of 15504, particularly CD 15504-2, and is compatible with its approaches and requirements.

The purpose of this paper is to analyze ISO 17799 and SSE-CMM to determine if and how each of these two security standards may be integrated into the S-vector methodology. This is a scoring methodology, currently under development, for assessing web

application security. In general, the methodology functions as follows [2]:

- The security requirements for each web application are mapped into a requirements vector that contains a target score.
- A periodic assessment of the web application yields a corresponding application score vector, which can be compared to the application's requirements vector.

The goal of the S-vector methodology is to enable government agencies to prioritize security enhancement projects, evaluate security enhancement strategies, and to measure progress in improving web application security.

Three types of security requirements are mapped into S-vector: technical, structural, and procedural. Technical components include the security services an application provides, such as encryption and authentication [6]. Structural components include the "software structures and designs that help assure the services will be delivered with greater assurance" [6]. Procedural components include the "development, deployment, and management procedures that help assure the services will be delivered with greater assurance"[6]. Technical components, such as encryption and authentication, will largely correspond to the Common Criteria's Protection Profiles [2].

This paper is organized as follows: First, a description of ISO 17799 is provided that contains the standard's history, and applicability to S-vector. Second, a description of SSE-CMM is provided that contains the standard's history, and applicability to S-vector. Third, suggestions on how the two standards may collectively be integrated into the S-vector methodology are discussed.

2. S-vector

The focus of the S-vector methodology is on the security of web applications. However, it is understood that a supporting security infrastructure is needed in order to develop an asset inventory, a risk assessment, and security policies that result in the requirements to be mapped into S-vector. SSE-CMM process areas are geared toward policies at the project or organizational level. Many of ISO 17799 controls are also geared across a project (e.g., operating system, networks, servers) or organization (e.g., security policy). S-vector is geared toward assessing the security of individual web applications and their data. This section first provides a recommendation for applying ISO 17799 to S-vector, along with an example of a potential implementation. Next, recommendations for applying SSE-CMM to S-vector are provided.

2.1. How ISO 17799:2005 concepts can be applied to the S-vector methodology

This section provides a list of recommended ISO 17799 areas to be incorporated into an S-vector implementation. ISO 17799 does not contain a scoring metric for evaluating implemented ISO 17799 controls. The second part of this section describes a potential scoring metric that could be applied to an S-vector implementation containing ISO 17799 controls.

Applicable ISO 17799:2005 Areas

Table 1 below indicates which of the eleven ISO 17799:2005 areas are recommended for S-vector. Recommended ISO 17799 controls include both application-level and organization-level controls that impact web application security. Recommended ISO 17799 controls that do not map to S-vector components generally relate to organization-level controls that apply across applications.

Table 1. ISO 17799:2005 areas related to S-vector

		Maps to S-vector Components		
ISO 17799 areas	Recommended for S-vector	Procedural	Structural	Technical
Security policy	X	X		
Organizing information security	X			
Asset management	X			
Human resources security	X			
Physical and environmental security				
Communications and operations management				
Access control	X		X	
Information systems acquisition, development and maintenance	X	X	X	
Information security incident management	X	X	X	
Business continuity management				
Compliance				

S-vector will not be used to define suggested policies and controls from ISO 17799. Instead, S-vector can be used to evaluate the existence, quality, or maturity of relevant security policies and controls.

Potential Scoring Metric for Incorporated ISO 17799:2005 Controls

A 5-level (1-5) scale can be used for scoring the quality of each control. For the requirements vector, each checked control receives a target score of 1-5, indicating the desired quality of the control. Desired quality level is commensurate with the priority level attributed to the control. Unchecked controls receive

a value of "0". This control could be grouped in the following hierarchy by scope and topic: Procedural components→ Organization-level controls→ Operating System controls→ Separate system utilities from application software. Scores may be sub-totaled for each of these groupings.

2.2. How SSE-CMM concepts can be applied to the S-vector methodology

As explained in the previous section, SSE-CMM is comprised of process areas and capability levels – either or both of which can be applied to S-vector. In other words, it is possible to incorporate the eleven security-related process areas as procedural components within S-vector while using a metric scheme different from SSE-CMM's capability levels. Likewise, it is possible to apply SSE-CMM's capability levels as a metric scheme for assessing the maturity of all S-vector procedural components regardless if components originate from SSE-CMM's process areas or not.

Applicable Process Areas

Each of the eleven security-related process areas (PA01-PA11) is geared toward building a management framework in which to administer security controls across a project or organization. The remaining eleven process areas (PA12-PA22) are general practices that apply to systems engineering in general, and are believed to be outside the scope of S-vector, so therefore are not recommended for an S-vector implementation. Table 2 shows SSE-CMM process areas that are related to S-vector.

Table 2. SSE-CMM process areas related to S-vector

		Maps to S-vector Components		
SSE-CMM Security-Related Process Areas	Recommended for S-vector	Procedural	Structural	Technical
PA01 Administer Security Controls	X	X		
PA02 Assess Impact	X			
PA03 Assess Security Risk	X			
PA04 Assess Threat	X			
PA05 Assess Vulnerability	X			
PA06 Build Assurance Argument	X			
PA07 Coordinate Security	X			
PA08 Monitor Security Posture	X	X		
PA09 Provide Security Input	X			
PA10 Specify Security Needs	X			
PA11 Verify and Validate Security	X	X		

SSE-CMM lists the eleven security-related process areas in alphabetical order and does not provide, nor recommend, a sequential order of execution. Figure 1 is provided in an effort to visualize how the various process areas are believed to inter-relate.

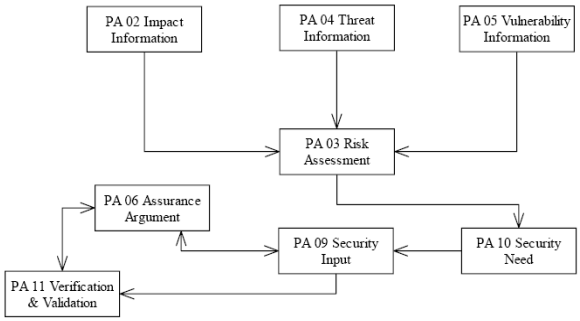

Figure 1. Relationships between SSE-CMM Security-related Process Areas

SSE-CMM process areas provide a management framework because they are at a high level of abstraction. Specific methodologies are neither recommended nor provided. The process areas aid in building a framework by outlining the need to identify, define, prioritize, and monitor security-related practices across a project or organization. The specific details on how to accomplish these practices are not provided. Once the base practices of a process area have been implemented, the maturity of those processes is assessed via the generic practices associated with capability levels.

Applicability of the Capability Levels

The capability levels are used to assess the maturity of a given process. Their applicability depends on an S-vector component's scoring objective. If the objective is to assess the quality of a process' output, the capability levels may not be appropriate because they are not designed for this purpose. However, the capability levels are applicable to S-vector if a component's scoring objective is to determine that the component has been well defined and is being tracked and monitored. A requirement S-vector can be populated with a target capability level. An assessment is then performed to determine the actual capability level. Capability levels can be assessed in strict conformance to SSE-CMM guidelines via the generic practices for each capability level. On the other hand, the assessment of the capability levels can be personalized to accommodate S-vector or OA/OIT scoring objectives. If the capability levels were applied to S-vector, it would be helpful to use the SSAM for conducting appraisals because the appraisal methodology is provided in detail. It is, however, important to understand how SSAM assesses capability levels per process area. In general,

SSAM assesses each base practice (BP) individually for capability level 1 to determine if each BP is performed – at least informally. For the remaining capability levels 2 – 5, the process area as a whole is assessed to determine the maturity of the entire process area. This means that SSAM does not assess the maturity level of individual BPs within a PA. As a result, it is possible for a PA to be awarded a high capability level, while there is BPs within that PA that is insufficiently implemented. Secondly, the SSAM assumes that either an SSE-CMM appraisal is performed in conjunction with an SE-CMM appraisal, or processes similar to those outlined in SE-CMM (or SSE-CMM PA12 – PA22) are in place prior to the appraisal.

3. SIMULATION

This section provides a simulation of S-vector. Based on table 1, ISO 17799 areas that related to S-vector components, so table 3 shows example of ISO 17799 areas rating. Based on table 2, SSE-CMM areas that related to S-vector components, so table 4 shows example of SSE-CMM process areas rating. Figure 2 shows parameter from ISO 17799 (table 3) and SSE-CMM (table 4) in one axis. Finally, figure 3 shows simulation rating of S-curve.

Table 3. Example ISO 17799 areas rating

ISO 17799 areas	Rating
Security policy	3
Organizing information security	3
Asset management	2
Human resources security	2
Access control	2
Information systems acquisition, development and maintenance	1
Information security incident management	2

Table 4. Example SSE-CMM process areas rating

PA Title	Rating
Administer Security Controls	1
Assess Impact	3
Assess Security Risk	3
Assess Threat	3
Assess Vulnerability	3
Build Assurance Argument	1
Coordinate Security	3
Monitor System Security Posture	2
Provide Security Input	1
Specify Security Needs	3
Verify and Validate Security	2

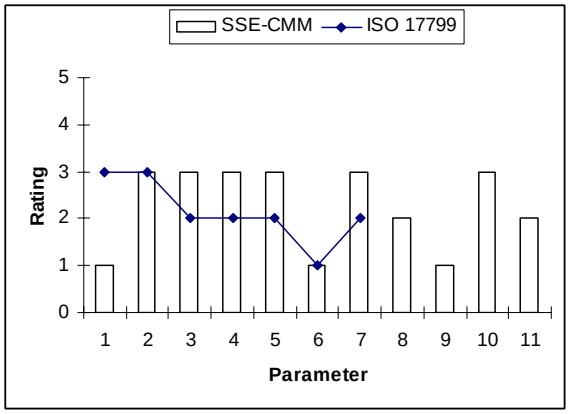

Figure 2. Rating of SSE-CMM and ISO 17799

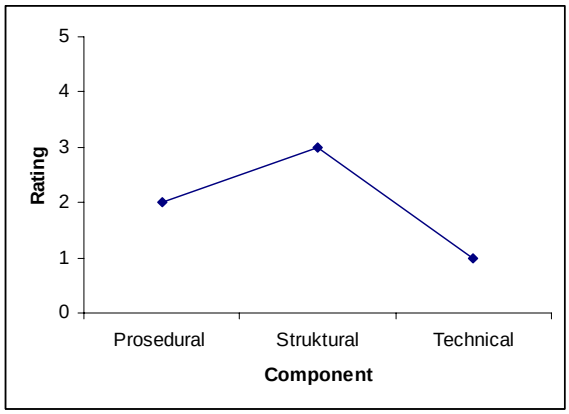

Figure 3. Rating of S-curve

4. ANALYSIS

The eleven security-related process areas in SSE-CMM can be used to develop and administer a security framework. ISO 17799:2005 can be used as a guideline for specific security controls (procedural and structural, not technical) that can in turn fit into the security framework established by SSE-CMM. SSE-CMM provides a higher level of management abstraction than does ISO 17799, which makes possible the use of both standards in support of an S-vector implementation. ISO 17799 provides specific controls that can populate security vectors for application security, while SSE-CMM establishes a mature, institutionalized framework for security administration. Both elements are critical success factors for an S-vector implementation. Specific controls are needed to populate security vectors (ISO 17799). However, a security infrastructure must be in place in order for these controls to be developed, monitored, measured, and controlled (SSE-CMM). No overlap or redundancy is found between ISO 17799 and SSE-CMM. In fact, the two standards complement each other. Finally, it is possible to apply SSE-CMM capability levels to ISO 17799

controls – provided the scoring objective is to assess the maturity of the control and not the quality of the output from the control. The benefit of using SSE-CMM to develop and maintain a security framework is that by following the model, there is a higher assurance that the processes put in place will reach a desired level of maturity and will be maintained on a continuous basis. Otherwise, an asset inventory, a risk assessment, or a security policy document could be developed and not maintained. This would result in an outdated security framework and outdated policies, which would lead to ineffective system security. The benefit of integrating ISO 17799 controls into S-vector procedural components is that ISO is an internationally recognized standard. ISO 17799 offers a comprehensive set of procedural controls that can be used to support web application security.

5. CONCLUSION

S-vector provides a mechanism for assessing a web application and comparing the actual score against a target score. While ISO 17799 provides a list of security controls as guidelines, it does not provide a method for evaluating the implementation of those controls. SSE-CMM provides a framework for administering security processes. However it does not provide the level of detail required of S-vector to assess web application security. The S-vector methodology contains technical, procedural, and structural components, and therefore provides a more comprehensive assessment of web application security than ISO 17799 and SSE-CMM. Neither of these two standards contains all three types of components. However, ISO 17799 and SSE-CMM provide elements that may be used to populate procedural components of an S-vector. They also provide guidelines for a security infrastructure that operates across applications.

6. REFERENCES

[1]. _____," Systems Security Engineering Capability Maturity Model (SSE-CMM)", Mode description version 3.0, 2003.

[2]. Barton, R., Hery, W., Liu, P. et al, A Scoring Vector for Managing Web Application Security, NSF Full Proposal, Mar 2004.

[3]. Bisson, J., Saint-Germain, R., The BS 7799 / ISO 17799 Standard, White Paper, Callio Technologies, https://www.callio.com/files/wp_iso_en.pdf

[4]. Cheetham, C., Ferraiolo, K., The Systems Security Engineering Capability Maturity Model, 3rd Combat Symposium, 1998, 1998The_SSE-CMM.ppt, http://www.sse-cmm.org/lib/lib.asp

[5]. Ferraiolo, Karen, "The Systems Security Engineering Capability Maturity Model (SSE-CMM)", ISSEA, 2002

[6]. Hery, W., Liu, P., Strawman S-vector Structure, 2003, eBusiness Research Center, Penn State University

[7]. ISO/IEC 2005, ISO/IEC 17799 Information technology – Code of practice for information security management, Reference number ISO/IEC 17799:2005(E)

[8]. Lucent Technologies, Information Security Management: Understanding ISO 17799, White Paper, http://www.lucent.com/knowledge/archives/0,1981,inDocTypeId+115-inPageNumber+1-inByLocation+0-SORT+D,00.html

[9]. M, Karen, "Combining a CMMI SCAMPI with an ISO/IEC 21827 (SSE-CMM) Appraisal "Seattle, 2004

[10]. Myagmar, Suvda, "Threat Modeling Networked and data-centric systems" Urbana-Champaign, 2001

[11]. Pattinson, F., Comparing ISO 17799:2000 with SSE CMM V2, Phi Solutions, Sep 19, 2002, http://www.phi-solutions.com/documents/ISO17799_SSE_CMM_comparison.pdf

[12]. SECAT LLC, Overview of the Systems Security Engineering Capability Maturity Model (SSE-CMM), http://www.secat.com, 1996

[13]. "Systems Security Engineering Capability Maturity Model (SSE-CMM) Appraisal Method (SSAM)", Version 2.0, 1999.