CERIAS

Metrics Based Security Assessment (MBSA): Combining the ISO 17799 Standard with the Systems Security Engineering Capability Maturity Model (SSE-CMM)

J.E. Goldman, V.R. Christie

[1] Department of Computer Technology, School of Technology, Purdue University, West Lafayette, IN 47907

Abstract

This research introduces the **Metrics Based Security Assessment (MBSA)** as a means of measuring an organization's *information security maturity*. It argues that the historical (i.e., first through third generations) approaches used to assess/ensure system security are not effective and thereby combines the strengths of two industry proven information security models, the *ISO 17799 Standard* and the *Systems Security Engineering Capability Maturity Model (SSE-CMM),* to overcome their inherent weaknesses. Furthermore, the authors trust that the use of information security metrics will enable information security practitioners to measure their information security efforts in a more consistent, reliable, and timely manner. Such a solution will allow a more reliable qualitative measurement of the return achieved through given information security investments. Ultimately, the MBSA will allow professionals an additional, more robust self-assessment tool in answering management questions similar to: "How secure are we?"

Problem

Defining specific, timely metrics in the field of information security is not easy; in fact, such metrics are in their infancy. Though the lack of specific, timely measures with which to measure information security is significant, the overall requirement for information technology security is not questioned by organizations.

However, the need to measure and evaluate the effectiveness of the tools and techniques used to secure today's highly connected, always-on businesses continues to grow. The desire to arrive at a single discrete value by which to buy or rate new technologies and/or to commit organizational resources to information security initiatives has largely been inadequate; in fact, the techniques currently used are neither generally accepted nor reliable measures for rating information technology security or requisite security assurance.

As argued by the National Institute of Standards and Technology (NIST), information security metrics are needed to understand the current state of system security, to improve that state, and to procure/obtain the necessary resources to implement improvements. Effectively, there are no measures, no standard way of scoring security implementations. Unfortunately, the practice of developing information security metrics is an undeveloped science.

Proposed Solution

Using the SSE-CMM as the guiding framework and complementing that with the ISO 17799 Standard, a self-facilitated information security metrics model can be developed that will offer the security community a tool that may be transposed across cultural, organizational and structural jurisdictions. Furthermore, such a model will offer security professionals a flexible tool that can be adapted to their specific needs or easily used as a starting point in designing their own information security metrics. As a final contribution, a model of this nature may be used to better assess the maturity of an organization's information security practices, and provides a clearly defined path toward improvement.

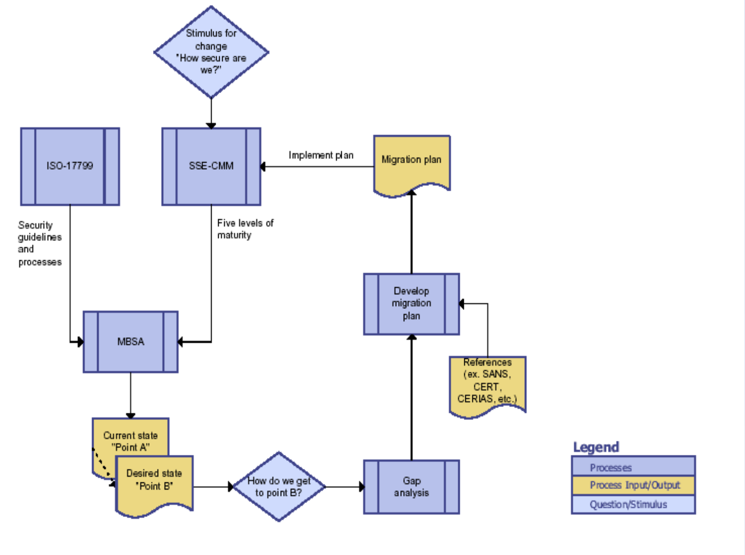

Figure 1 – MBSA Architecture

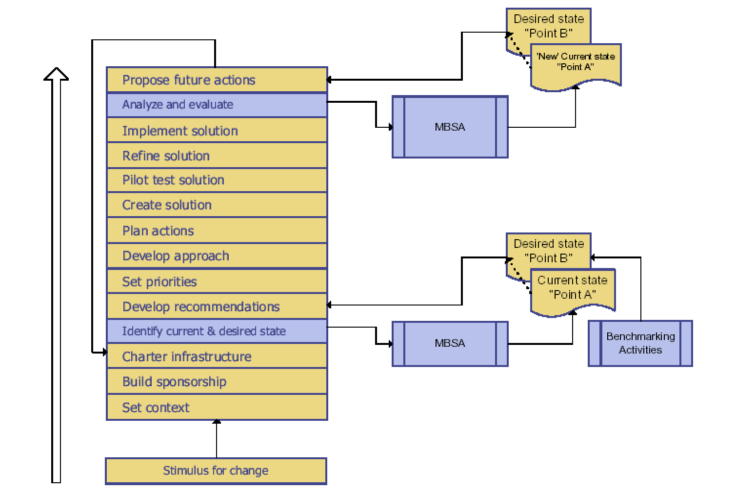

Figure 2 – MBSA to SSE-CMM process model mapping

Legend
2002 – Underlined
2003 – Highlighted
2004 – Box
2005 – **Bold**

Category	Description
Metric	Identify the metric being assessed.
Maturity Level Goal	Identify the SSE-CMM level goal for this control (e.g., Level 2, etc.).
Scale/Rating	Identify the percentage of maturity level goal attainment via the previously documented definitions (see Response Scale, above).
Frequency	Identify: The date of the current assessment An appropriate frequency of assessments (i.e., how often) Proposed date for the next assessment
Implementation Evidence	Justify the assessor's rating of the control.
Data Source	Identify the sources/references/resources used to make the assessment.

Metric	Terms and conditions of employment state employee responsibilities regarding information security and (where appropriate) are continued for a period of time after the employment period.
Maturity Level Goal	Level 3
Scale/Rating	0—1—2—**3**—4—5 N/A Unknown
Frequency	Current Date: Frequency: Next Assessment Date:
Implementation Evidence	Sample only.
Data Source	Sample only.

Figure 3 – Metric templates

PURDUE UNIVERSITY

CERIAS®

Discovery Park
e-Enterprise Center