Evolving the Evaluation Paradigm

Background

While all intentions are good with respect to evaluating products for their security features and this is recognized as a needed function, it is widely acknowledged that the process for evaluating products and certifying systems is time consuming and very costly. As a result, trusted products and secure systems typically come to market in one of two ways: first, through lengthy and expensive evaluation - resulting in trusted products coming to market long after their features are needed, and systems being deployed that no longer address the current threats; and second, with no evaluation, resulting in buyers relying solely on the claims of the developer.

An important note about trusted product evaluation and secure system certification is that both focus on scrutinizing the end product (that is, the system or product and its documentation) while placing almost no emphasis on the process involved in creating it. The Trusted Computer System Evaluation Criteria (TCSEC) seems to have attempted to define some processes that could allow high assurance to be associated with a system by requiring the use of security testing, formal (mathematical) methods, and configuration management at higher levels. As a result, secure system development efforts have emphasized the use of these specific procedures to reach a high level of assurance in the end product. The benefits of these procedures, however, cannot be realized in an undisciplined environment.

Believing that a new paradigm is needed for providing security and assurance in products and systems, the Systems Security Engineering Capability Maturity Model (SSE-CMM) Project has a goal of providing a mechanism for capability-based assurance, that is, trustworthiness based on confidence in the maturity of an engineering group's security practices and processes.

A recent SSE-CMM pilot had as an objective to investigate the usefulness and contribution of the results of an SSE-CMM appraisal of a product vendor organization to the Trusted Product Evaluation Program (TPEP) process, in particular the Rating Maintenance Phase (RAMP).

This panel will explore some important and controversial issues relating to applying the SSE-CMM model and using appraisal results to help make secure products and systems more readily and promptly available to their end-user. The SSE-CMM Project Sponsor Representative will provide a brief overview of the project and its goals. The TPEP/RAMP Program Representative will discuss the issues regarding use of the SSE-CMM to support product evaluations. The Product Vendor Pilot Organization Representative will discuss whether the SSE-CMM will help their organization through the evaluation process in any way. Finally, the Assurance Approaches Working Group (AAWG) Representative will discuss the group's recent work to analyze candidate alternative assurance approaches/methods, including the SSE-CMM.

Panel Moderator

SSE-CMM Project Sponsor Representative
Mary Schanken, National Security Agency

The United States National Security Agency (NSA), as SSE-CMM Project sponsor, has provided facilitation, technical support, and promotion of the SSE-CMM. The SSE-CMM Sponsor Representative will briefly describe current status of the Project, and the piloting of the model and appraisal method in a number of organizations. The Sponsor Representative will give a high level view of the Project's approach to contributing solutions to this problem.

Assessed Organization Perspective

Product Vendor Pilot Organization Representative
Pat Daggett, Data General

The Product Vendor Pilot Organization Representative will focus on the implications to organizations that would apply the SSE-CMM to their practices. Results of the recent SSE-CMM pilot have given the organization feedback as to its strengths and weaknesses with regard to its practice of security engineering as defined by the SSE-CMM.

The Product Vendor Pilot Organization Representative will present the organizational view of: 1) whether the concepts defined in the model are applicable to the organization; 2) ease of use and applicability of the appraisal method; and 3) the resultant impact/contribution that implementation of SSE-CMM concepts and appraisal results may have on their efforts to meet TPEP/RAMP requirements and to provide assurance to their end-customer.
The Product Evaluator Perspective
TPEP/RAMP Program Representative
K. Kris Britton, Chief TPEP Evaluator, NSA

The Product Evaluator Representative will focus on the evaluation community view of whether the SSE-CMM can contribute to the product evaluation process. A member of the product evaluation community participated on the appraisal team for the most recent SSE-CMM pilot appraisal of a product vendor organization. The Product Evaluator Representative will address the applicability of the SSE-CMM as it relates to the product evaluation process, discussing their view of: 1) whether measurable/predictable processes can help the vendor produce better quality evaluation evidence; 2) whether application of SSE-CMM model and periodic SSE-CMM appraisals could contribute to meeting the RAMP requirements; and 3) the overall usefulness and applicability of the SSE-CMM appraisal results to the evaluation process.

The Assurance Perspective
AAWG Representative
Mary Schanken, NSA

The Assurance Approaches Working Group (AAWG) Representative will provide a discussion on the AAWG’s work to investigate alternative approaches for gaining assurance and to help define alternatives to traditional evaluation by building alternative assurance packages. Among the AAWG’s first tasks was the identification and analysis of candidate alternative assurance approaches/methods, including the SSE-CMM. The AAWG representative will discuss the results of their work, including the AAWG’s view of the contribution that the SSE-CMM can make to the overall satisfaction of assurance requirements/objectives.

Questions and Discussion

Time Remaining