The National Security Agency's Use of the Systems Security Engineering Capability Maturity Model (SSE-CMM)

Panel Chair:

Ms. Mary D. Schanken
National Security Agency
9800 Savage Road
Ft. Meade, MD 20755-6740
(410) 854-4458
schanken@nsa.gov

Panelists:

Mr. Paul W. Boudra
National Security Agency
9800 Savage Road
Ft. Meade, MD 20755-6730
(410) 854-7262
PWBoudr@missi.ncsc.mil

Mr. Charles G. Menk III
National Security Agency
9800 Savage Road
Ft. Meade, MD 20755-6752
(410) 854-6041
cmenk@radium.ncsc.mil

Session abstract

The current ways that commercial security products and services come to market are inadequate. Products and systems either go through a lengthy and expensive evaluation process, which result in a product or a system that no longer meets current needs, or they go through little or no external evaluation, leaving the buyer to trust the providers' claims. Further, services are all marketed on this caveat emptor basis (buyer beware.)

The National Security Agency (NSA) has been involved in efforts to help customers judge the full spectrum of Information Systems Security (INFOSEC) products, systems, and services while possibly minimizing the expense and time involved in the current evaluation/certification processes. An effort that NSA sponsored was the development of a Capability Maturity Model (CMM) for security engineering.

NSA began the effort to develop a CMM for security engineering in 1993, with the hopes that the security engineering community would become involved to help define the criteria against which they might be assessed in the future. Learning from the past, NSA believed this approach would be more successful and accepted than if NSA were to issue it as a requirement. Over 50 government, industry, and academic organizations developed the Systems Security Engineering Capability Maturity Model (SSE-CMM) and its appraisal methodology. This panel will address a few of the ways that the National Security Agency is using the SSE-CMM.

Brief summary of panelist's topics

Presentation:

The NSA is developing an Industrial ISSE Certification Program to help customers of ISSE services identify qualified ISSE Service Providers and to raise the quality of the service provided throughout the community. Mr. Boudra will discuss the process being used to develop the criteria for the Certification Program and the relationship of the System Security Engineering – Capability Maturity Model to that criteria.

Presentation:
Mr. Menk will address the IACMM, NVLAP SSE Criteria, and the BCMM

The INFOSEC Assessment CMM (IACMM) is designed to measure the capability of an INFOSEC assessment organization. The purpose is to help build a cadre of INFOSEC assessor organizations that are well equipped to provide valid site assessments to their customer base. The goal is to help alleviate the huge demand for NSA resources to conduct all such assessments by providing a standardized metric that customers could use to delineate supplier capability to address the specific customer INFOSEC assessment needs. This program is currently supported via the NSA INFOSEC Assessment organization but is targeted as a potential National Information Assurance Partnership (NIAP) program.

As part of the NIAP, the SSE-CMM was used to capture process-related security awareness activities that are included in the NIST National Voluntary Laboratory Accreditation Process (NVLAP) Handbook 150-20: "Information Technology Security Testing - Common Criteria". The inclusion of this set of queries closes the gap between product and process assurance issues in the Common Criteria lab accreditation program.

The Business Capability Maturity Model (BCMM) was developed in order to measure the Information Systems Security Organization's Business Health. The focus is on the supporting business processes that any organization relies upon to ensure appropriate and timely execution of its mission objectives (i.e. Product and/or Service-based). At this time, three pilot appraisals and eight BETA appraisals have been conducted.

Background of audience
This panel will be of interest to those who realize the importance of having processes in place in order to gain security assurance. The best technical solutions are useless if the correct security processes are not in place to insure that they are implemented correctly.

Short bio of panel chair and speakers

Ms. Mary Schanken is a Senior Computer Scientist and has been employed with the National Security Agency (NSA) since 1977. Her area of expertise is in developing and implementing alternative methods of assurance (other than those provided by traditional evaluation) for producing products, systems, and services that maintain and protect information. She is a member of the Chief Information Officers Council Federal Best Security Practices subcommittee and is addressing the concerns outlined in Presidential Decision Directive 63, which calls for a national effort to assure the security of the increasingly vulnerable and interconnected infrastructures of the United States. She was a key contributor in the development of the Trusted Computer System Evaluation Criteria Rainbow Series, the Federal Criteria and the international Common Criteria. Ms. Schanken began her Information System Security career as a Trusted product Evaluator. She previously held the position as the first Chief of the NSA Information Systems Security Service Center (NISSC.) She was a member of the International Common Criteria Assurance Approaches Working Group. She served as government lead for the development of the Systems Security Engineering Capability Maturity Model (SSE-CMM) which is the product of a voluntary collaboration of 50 government and industry organizations to meet the needs of the security engineering community. She participated in appraisals to validate the model and its appraisal methodology. She is currently focusing her efforts on implementing the SSE-CMM within the Department of Defense. She is also a Lead Assessor and a Proficiency Test Grader for the National Voluntary Laboratory Assessment Program (NVLAP) under the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS.) She completed her Computer Science degree from the University of Maryland Baltimore County, and graduate studies in Computer Systems Management from the University of Maryland University College. She has completed both the Strategy and Policy and the National Security Decision Making curricula and is currently enrolled in the Joint Maritime Operations curriculum at the Naval War College.

Mr. Paul Boudra has been working at the National Security Agency since 1973. He has a BS and MS in Electrical Engineering from Louisiana State University. In his early years at NSA he conducted speech compression research. He contributed to the speech algorithms in several generations of Secure Telephone Units. He was a systems engineer for several key distribution systems including the KDC-II that supported the STU-II telephones and the Electronic Key Management System. He is currently Technical Director of a division that does Information System Security Engineering (ISSE) for a variety of customers. He is responsible for developing an ISSE training program for NSA and for developing an Industrial ISSE Certification Program.

Mr. Charles G. Menk III, is employed with the National Security Agency. He is a 1987 graduate from Marquette University with a BS in Computer Science, and a graduate from Loyola College of MD with a Masters of Engineering Science (CS) in 1995. He served as US Naval Officer from 1987 to 1993, as Computer Systems Evaluator from 1990 to 1996, and as Lead System Security Engineer on the SSE-CMM development effort from 1996 to 1999 as a member of the SSE-CMM Author Group, and Appraisal Methodology Working Group. He is a co-author of the INFOSEC Assessment CMM, developer and co-author of SSE Business CMM, co-author of the NVLAP process improvement criteria and has participated in 19 CMM appraisals, 17 of which he facilitated. He is a trained ISSO 9000 Lead Auditor.