Alternative Assurances Panel

This panel will present related applications of the Systems Security Engineering Capability Maturity Model (SSE CMM), an update and strategic plan for the Trusted Capability Maturity Model (TCMM) and the Network Rating Methodology (NRM). These initiatives address alternate assurance through the use of process related vice traditional accreditation or evaluation approaches. They are an important collection of metrics that can be used to insure security compliance from developer, service providers, and operational sites. These initiatives can help us to address some of the concerns mentioned 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.

Panelist: Christina R. Cheetham ccheetha@radium.ncsc.mil

Chris Cheetham is with the National Security Agency and specializes in information security and developmental assurance. She has eleven years in all phases of the system life cycle process, both in Industry and Government. She has held positions as a software developer, manager, and researcher on a variety of government programs. Currently she provides technical oversight to the Systems Security Engineering Capability Maturity Model Project being developed jointly with Government and Industry. She also participates in the National Information Assurance Partnership (NIAP) Common Criteria Testing Program (CCTP) development activity; the Office of Secretary of Defense and Software Engineering Institute's joint Industry government Integrated Capability Maturity Model (CMMI) development effort; and the Critical Infrastructure Protection directive (Presidential Decision Directive 63) . She has a B.S. in Computer Science from The George Washington University, and a M.S. degree in the Management of Information Systems from Strayer College.

Panelist: LT Renell D. Edwards redwards@radium.ncsc.mil

A commissioned officer from the Naval Reserve Officer Training Corp (NROTC) Unit, Florida A & M University where she received her Bachelor of Science degree in Mathematics. She has nine years of active duty with a military career as follows: Information Analyst, Chief of Naval Operations World Wide Military Command and Control System (WWMCCS) Operational Support Detachment: DEC88-SEP91; ADP Liaison Officer to National Military Command Center, Defense Information Systems Agency: OCT91- AUG94;

Student, Naval Postgraduate School (NPS): SEP94-SEP96; and Project Manager

(PM), National Security Agency (NSA): OCT96-Present. Unique in that her tour history at Navy, Joint and DoD commands, combined with computer science Masters degree work at NPS, affords her the ability to provide technical insight as she currently manages the Trusted Capability Maturity Model (TCMM) project and previously co-managed the Network Rating Methodology project while assigned to NSA. In addition, she's had experience with the Navy's Status of Resources and Training System (SORTS), Casualty Reports (CASREP), Movement Reports (MOVREP), and Employment Schedule (EMPSKD) reporting systems; Joint Visual Integrated Display System (JVIDS); the Crisis Management ADP System (CMAS); and the Joint Global Command Control System (GCCS).

Panelist: Charles G. Menk, III cmenk@radium.ncsc.mil

Charles Menk graduated from Marquette University with a BS in Computer Science in 1987. He served as an Officer in the USN from 1987-1995, and as a Trusted Product Evaluations Program evaluator from 1990-1993. Mr. Menk received his Masters of Engineering Science in Computer Science from Loyola College of MD in 1995. He is a Certified Information Security Analyst and is currently serving as a Lead System Security Engineer in the Developmental Assurances Branch.

Panelist: Todd D. Schucker tschucke@radium.ncsc.mil

Mr. Todd D. Schucker is a 1982 graduate of the Pennsylvania State University, he holds a Bachelor of Science Degree in Computer Science. Mr. Schucker has worked at the National Security Agency since 1980 as a Computer Science Student Assistant, Programmer, Systems Analyst, Systems Administrator, Adjunct Faculty member, Team Leader, Project Manager, and as a Branch Chief. His contributions to the Information Systems Security Organization include teaching introductory classes to Information Systems Security; initiating a National Systems Certification and Accreditation Program; and promoting the development and use of security process management efforts including the Network Rating Methodology, the Trusted Capability Maturity Model, and the Systems Security Engineering Capability Maturity Model.

Panel Chair: Mary D. Schanken schanken@romulus.ncsc.mil

Ms. Mary Schanken is Chief, Developmental Assurances for the National Security Agency (NSA). As an Information Systems Security expert, her specialty is developing alternative methods of assurance for producing products, systems, and services that maintain and protect information. Most recently, she has been assigned to assist in 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 Organization Service Center. She completed her Computer Science degree from the University of Maryland Baltimore County, and graduate work in Computer Systems Management from the University of Maryland University College.

All panelists, as well as the chair may be reached on
(410)859-6094 voice or (410)859-4661 fax or by mail
National Security Agency
9800 Savage Road Ste 6740
Attn: V243
Ft. Meade, MD 20755-6740

Ms. Cheetham will address the following:

The Systems Security Engineering Capability Maturity Model (SSE-CMM) describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering. The Profiles, Assessments, and Metrics (PAM) Committee of the SSE-CMM Project has established two subcommittees for establishing metrics for use with the SSE-CMM. The Process Metrics Action Committee (PMAC) is establishing metrics to measure the way in which an SSE CMM process is performed. The Security Metrics Action Committee (SMAC) is establishing what elements of security are addressed by the SSE-CMM and identifying metrics for measuring those elements of security. It is expected that organizations will select security goals based, for example, on their missions, customers, and work products. The SSE-CMM Project has begun by identifying overall security goals in relation to the SSE-CMM process areas that relate to product development, system operations, and security services. The activities tied to the goal's applicable objectives become the basis for identifying metrics. Acceptable security metrics are based upon threat, impact, and/or vulnerabilities to an organization, project, or system. Process metrics support project management, product quality management, organizational performance, and process improvement.

Mr. Menk will address the following:

Since it's inception in 1993, the SSE-CMM has under gone many refinements. Today it has become a welcome name in the security industry where metrics have been lacking and assurance waning. Specifically, the Common Criteria Testing Program and the INFOSEC assessment communities are working on interpretations of the SSE-CMM to address developmental assurance needs within their areas of expertise.

A major milestone in the use of the SSE-CMM is its acceptance in the international realm as well. The Canadians are actively implementing programs that require the SSE-CMM in certain acquisition arenas. The French, German, US and British members of the Alternate Assurance Working Group for the Common Criteria have embraced the SSE-CMM as a method for providing assurances in support of the requirements called out at the EAL3 level of the Common Criteria.

Although the SSE-CMM was conceived and born from government funding, the project has grown and is currently maintained by over 60 government, and commercial entities. For further information, please review the SSE-CMM website at www.sse-cmm.org or call V243 at (410) 859-6094.

LT Renell D. Edwards will address the following:

The Trusted Capability Maturity Model (TCMM) project is an integrated reference model derived from the software assurance principles contained in the Trusted Software Methodologies (TSM) and software process improvements described in the Software Engineering Institute's (SEI) Capability Maturity Model (CMM). TCMM exist to tailor the software CMM for the purpose of transferring software assurances to the developmental process and thereby significantly reduce the expensive lengthy post development testing and evaluation cycle. The TCMM simultaneously targets providing a more reliable, quality software process managed product. Its purpose is consequently significant to life critical applications such as warfare and financial systems.

History:

- Motivation
  - Decrease Reliance on Traditional Evaluations
  - Reduce Developmental Time & Cost
  - Use Proven Process Improvement Techniques Combined With Software Security Attributes
  - Assess Ability of Companies to Build Quality Software
- SEI CMM for Software
  - Sponsored by DoD through Advance Research Projects Agency (ARPA)
  - Measure Maturity of Development Process
  - Establish Goals for Process Improvement
  - Compelling Returns of Investment Evidence
- Trusted Software Methodology
  - Developed for the Strategic Initiative Organization System
  - Reduce Potential for Software Defects
  - 25 Principles Derived from Software Threats and Corresponding Process Vulnerabilities

Value:

The TCMM helps support the Information System Security Organization's goals of developing innovative high assurances ideas and solutions that will ultimately affect the war fighter (our primary customer) and the security of our nation. The two innovative ideas (software process improvement and software assurances) combined provide safeguards and countermeasures against software threats and corresponding vulnerabilities. The TCMM thus places mechanisms within critical software lifecycle that will counter insider threat WRT error introduction whether malicious or inadvertent. This threat could exist and manifest as vulnerabilities in Administrative procedure, Software development procedure, Control Policies, or Requirements.

Mr. Schucker will address the following:

The purpose of developing a Network Rating Methodology (NRM) is to provide a framework and common terminology for assessing the security protection provided by a network within the context of its mission and operational environment to determine its strengths and vulnerabilities. Obtaining knowledge of the security posture of ones system is a high priority for any system manager. For business and mission reasons, we often connect our networks to other networks. It is no longer prudent to be content with simply understanding the risks involved in running our data on our own networks. We must be able to view, analyze, and understand the network assurance not only for our own networks, but also for those other networks to which we may entrust our data resources. There is a strong need for a methodology which will allow network managers to compare security needs, practices, and protective provisions using a common terminology and common means of assessment. Implementation of the NRM will produce a matrix comprised of security services and system attributes affected by the services. Such claims are supported by another level of evidence and reasoning. These elements can be organized into a simple hierarchy to form a convincing case providing statements of confidence in parts of the network and provide a universally acceptable assessment report.