Innovative Uses of the Common Criteria

Panel Chair: Terry Losonsky, NIAP

Panelists:

Using Common Criteria to Support Certification - Jack Sherwood, SPAWAR USN, John Mildner, SPAWAR USN;

Mapping Product Test Results to Common Criteria - Peter Sargent, COACT Inc.

Session Abstract: The session introduces the audience to innovative ways the Common Criteria is used to solve Information Assurance (IA) challenges.

Using Common Criteria to Support Certification: To date, the Common Criteria has primarily been used for the evaluation of commercial products. The DoD is interested in the certification and accreditation of systems in an operational environment following the US Department of Defense Information Technology Security Certification and Accreditation Process, DODI 5200.40. This briefing addresses the use of the Common Criteria for system-level certification activities, based on the lessons learned associated with an Intrusion Detection System certification demonstration project. First, we discuss some differences between product evaluation and system certification. Then, we describe our methodology of incorporating Common Criteria concepts into the certification security requirements with extensions to address environmental and policy issues. We also show the use of an application matrix that selectively applies individual functional and assurance requirements to one or more subsystems within the larger system. From this example, we observe that use of the Common Criteria aids in the articulation of security requirements and improves the precision of their specification and verifiability over our previous technique.

Mapping Product Test Results to Common Criteria: Vendors can write development test results and map them against a Protection Profile. The results can also be used to develop a Security Target. Beta tests can be mapped as above, which will further enhance both the corporate and market understanding of the product in a common language. This will also make IT information more nationally understood. Interoperability tests mapped to the CC will have a more universal understanding, and be more meaningful to all participants. Proof of Concept test results mapped to the Common Criteria will give all products so tested a meaningful language that will allow readers a common body of knowledge with which to evaluate the results.

Mr. Jack Sherwood is an engineer with the Information Assurance Certification, Evaluation, and Test branch at SPAWAR Systems Center, Charleston. He earned a BS in Physics and an MS in Electrical Engineering from the University of Central Florida. He supports several US Navy certification efforts and has been using Common Criteria requirements as a basis for project security requirements specification. Mr. John Mildner, CISSP, MSEE, is Director of Technical Operations for the Information Assurance Engineering Division at SPAWAR Systems Center, Charleston where he has been employed since 1978. He completed the NSA Outreach program for Service evaluators and participates in US Navy Certification and Accreditation efforts

Peter C. Sargent is the Senior Security Analyst with COACT, Inc., CAFE Lab Manager, and also a certified CC Evaluator and Crypto Module Tester. Mr. Sargent has 21 Years experience in Information Security (INFOSEC), and 18 years of experience using INFOSEC standards to develop, analyze and create solutions for computer and network security deficiencies. While at COACT, he has helped to create the Common Criteria (CC) and CMVP validation programs which COACT Inc. CAFE Labs are using to help security clients test/evaluate their products against CC, FIPS and other International Standards. Mr. Sargent and the CAFE Lab team have created CC Security Targets (ST) to allow clients to be tested under the Common Criteria and the National Information Assurance Partnership (NIAP) methodology.