National Information Systems Security Conference

October 16-19, 2000

Title of Panel: A Protection Profile for FIPS 140-2, Lessons Learned

Panel Chair: Miles Smid, CygnaCom Solutions

Panelists:

Miles Smid
Cygnacom Solutions
Suite 100W
7927 Jones Branch Dr.
McLean, VA 22102
703-848-0883 x203, miles.smid@entrust.com

Jean Petty
CygnaCom Solutions
Suite 100 W
7927 Jones Branch Dr.
McLean, VA 22102
703-848-0883, jean.petty@entrust.com

Shari Galitzer
CygnaCom Solutions
Suite 100 W
7927 Jones Branch Dr.
McLean, VA 22102
608-663-6332 x209, sgalitzer@tds.net

Ray Snouffer
NIST
MS 8930
100 Bureau Drive
Gaithersburg, MD 20899
301-975-4436, rsnouffer@nist.gov

Abstract:

The National Institute of Standards and Technology's (NIST's) Cryptographic Module Validation program has been highly successful validating over 95 cryptographic modules as being compliant with the U.S. Government's "Requirements for Cryptographic Modules" (FIPS 140-1). Recently, NIST has drafted a revision of the standard (Draft FIPS 140-2). This revision offers several improvements over the original standard but the testing process remains basically intact. However, NIST and the National Security Agency have formed the

National Information Assurance Program (NIAP) whereby security products may be validated against Protection Profiles based on the Common Criteria. Validations performed under the Common Criteria program have the advantage that they are mutually recognized by each of the countries participating in the Common Criteria Mutual Recognition Program. Thus, the potential for one-stop-testing is increased.

This presentation will explore the technical feasibility of developing a Common Criteria based Protection Profile for Draft FIPS 140-2. It will present the work of CygnaCom Solutions to map the Device Test Requirements of the draft standard into Common Criteria components and to develop the profile itself. The presentation will cover the lessons learned when trying to map a previously existing standard into the Common Criteria and in developing the corresponding protection profile. Conclusions as to the technical difficulty of such an effort will be given.

Brief summary of panelist's topics:

An Introduction to FIPS 140-1/2, Security Requirements for Cryptographic Modules; Miles Smid

The essential features of FIPS 140-1 and the Common Criteria will be presented along with the new features of FIPS 140-2. Mr. Smid will offer opinions as to why the NIST/CSE Cryptographic Module Validation Program has been successful.

Mapping FIPS 140-2 into the Common Criteria, Lessons Learned; Shari Galitzer

When mapping the standard into the common criteria one has to be creative in dealing with certain issues. This presentation describes the issues and how they were addressed.

A Protection Profile for FIPS 140-2, Lessons Learned; Jean Petty

Developing a FIPS 140-2 PP requires selecting the proper EAL level(s) and specifying the appropriate CC components in order to cover every FIPS 140-1 requirement. This talk will summarize the Protection Profile that was actually developed.

Where Do we Go from Here? Ray Snouffer

Now that the profile is complete what will be done with it? What other security Standards and Protection Profiles will likely have product testing programs in the future?

Background of Audience

This session would be of interest to those who are familiar with the Common Criteria and who are interested in the issues that may arise when one tries to develop a protection profile for an existing standard.

Biographies:

Miles Smid chaired the government/industry group that developed FIPS 140-1 and managed the NIST Cryptographic Module Validation Program before his retirement from government 1999. He now servers as director of the CygnaCom Cryptographic Equipment Assessment Laboratory (CEAL) Laboratory.

Shari Galitzer served as a TCSEC evaluator at Mitre. At CygnaCom Shari develop the Security Targets for cryptographic products. She has also developed the draft Protection Profile for the DOD Class 4 PKI.

In 1995, **Jean Petty** joined the CygnaCom Cryptographic Equipment Assessment Laboratory as Quality Control Manager. Over the next three years she performed several FIPS 140-1 validations. In 1999 she transferred to the Security Evaluation Laboratory and developed a Protection Profile for key recovery products. Jean is currently a security consultant.

Ray Snouffer served on the Cryptographic Services Working Group that developed the Common Criteria components for cryptographic functions. Ray is currently manager of the NIST Cryptographic Module Validation Program and is the Contracting Officer's Technical Representative for the project under which the FIPS 140-2 protection profile was developed.