Title of Panel: Testing of Cryptographic Modules Against FIPS 140-2

Panel Chair: Nelson Hastings, National Institute of Standards and Technology (NIST)

Panel Members: Annabelle Lee, NIST
Ray Snouffer, NIST

Session Abstract:

Federal agencies, industry, and the public now rely on cryptography to protect information and communications used in critical infrastructures, electronic commerce, and other application areas. Cryptographic modules are implemented in these products and systems to provide cryptographic services such as confidentiality, integrity, non-repudiation and identification & authentication. Adequate testing and validation of the cryptographic module against established standards is essential for security assurance. Both Federal agencies and the public benefit from the use of tested and validated products. Without adequate testing, weaknesses such as poor design, weak algorithms, or incorrect implementation of the cryptographic module, can result in insecure products.

On July 17, 1995, NIST established the Cryptographic Module Validation Program (CMVP) that validates cryptographic modules to Federal Information Processing Standard FIPS 140-1 (Security Requirements for Cryptographic Modules), and other FIPS cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment (CSE) of the Government of Canada. Products validated as conforming to FIPS 140-1 are accepted by the Federal agencies of both countries for the protection of sensitive information. Vendors of cryptographic modules use independent, accredited testing laboratories to test their modules. NIST's Computer Security Division and CSE jointly serve as the validation authorities for the program, validating the test results. Currently, there are four National Voluntary Laboratory Accreditation Program (NVLAP) accredited laboratories that perform FIPS 140-1 compliance testing, three in the U.S. and one in Canada. As of August 2000 over 100 cryptographic modules from more than forty separate vendors have been validated through the program. The number of validated modules has nearly doubled each year of the program's existence.

The underlying philosophy of the CMVP is that the user community needs strong independently tested and commercially available cryptographic products. The CMVP must also work with the commercial sector and the cryptographic community to achieve security, interoperability and assurance. Directly associated with this philosophy is the goal of the CMVP to promote the use of validated products and provide Federal agencies with a security metric to use in procuring cryptographic modules. The testing performed by accredited laboratories provides this metric. Federal agencies, industry, and the public can choose products from the CMVP Validated Modules List and have confidence that the products meet the claimed level of security. The program validates a wide variety of modules including general encryption products, secure radios, Virtual Private Network (VPN) devices, Internet browsers, cryptographic tokens and modules that support Public Key Infrastructure (PKI). Currently, validation services are provided for FIPS 140-1 & 2, the Data Encryption Standard (DES and Triple DES), the Digital Signature Standard, the Secure Hash Standard, and the Skipjack Algorithm.

The CMVP offers a documented methodology for conformance testing through a defined set of security requirements in FIPS 140-1 & 2 and other cryptographic standards. NIST developed the standard and an associated metric (the Derived Test Requirements for FIPS 140-1) to ensure repeatability of tests and equivalency in results across the testing laboratories. The four commercial laboratories provide vendors of cryptographic modules a choice of testing facilities and promote healthy competition.

The panelists will provide detailed information on the philosophy and goals of cryptographic module testing, the DTR, conformance/compliance testing, and cryptographic module laboratory accreditation.

Ray Snouffer, NIST, will provide an overview and discuss laboratory accreditation, including the determination of laboratory proficiency.

Nelson Hastings, NIST, will discuss conformance/compliance to the DTR including specific examples from areas of the standard.

Annabelle Lee, NIST, will discuss the philosophy, structure, and development of the DTR.

Points of Contact Information and Biographies:

Annabelle Lee, NIST
301.975.2941 (phone)
301.948.1233 (fax)
annabelle.lee@nist.gov

Ms. Lee has over 25 years experience in Information Systems. Prior to working at NIST, Ms. Lee worked for the Mitre Corporation as a Lead Engineer in the Criminal Justice and Public Safety Division. She provided support to the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division and the El Paso Intelligence Center (EPIC) Information System (EIS) for the Drug Enforcement Administration. She was also author and co-author of documents in the “rainbow” series, the security standard for the federal Government. Currently, Ms. Lee is a Computer Specialist in the Information Technology Laboratory, Computer Security Division. Ms. Lee supports the Cryptographic Module Validation Program (CMVP) serving as the primary point of contact for three of the four testing laboratories. She also is the technical lead for the update of FIPS 140-1, *Security Requirements for Cryptographic Modules*. In addition, Ms. Lee recently authored the *Guideline for Implementing Cryptography in the Federal Government*.

Ray Snouffer, NIST (primary point of contact)
301.975.4436 (phone)
301.948.1233 (fax)
ray.snouffer@nist.gov

Mr. Snouffer has worked as a mathematician for the U.S. Federal Government since October of 1987. He began his career with the Defense Information Systems Agency (DISA) serving in a variety of roles including senior mathematician, lead software developer, and Project Officer for the Strategic Defense Analysis Project. In June of 1994, Mr. Snouffer accepted the position of Deputy National Program Manager for the U.S. Government’s Key Escrow program at the National Institute of Standards and Technology (NIST); taking over the position of National Program Manager in November of 1995. Since January 1997, Mr. Snouffer has served as the Program Manager for the Cryptographic Module Validation Program and now also serves as the supervisor of the Cryptographic Security Testing Program Area of NIST’s Computer Security Division.

Nelson Hastings, NIST
301.975.4634 (phone)
301.948.1233 (fax)
nelson.hastings@nist.gov

Dr. Hastings joined the Computer Security Division of National Institute of Standards and Technology in 1997. He currently supports projects in public key infrastructure interoperability and the Cryptographic Module Validation Program (CMVP). He received a Bachelor of Science degree in Electrical and Computer Engineering from the University of Missouri-Columbia and a Master of Science degree in Electrical Engineering from Western Michigan University. In 1999, he received a Doctor of Philosophy degree from the Iowa State University where his dissertation topic was a structured testing framework for PKI.