Encryption Testing and Certification

Introduction

With the introduction of encryption technology on transport products, service providers and customers often ask how they can test the encryption solution to ensure it meets its stated capabilities and provides the desired level of encryption. This document describes the concerns surrounding encryption solution testing, and the external certification processes available to address those concerns.

New Technology Paradigm

The introduction of integrated encryption technology in optical transport platforms offers tremendous opportunities to service providers and end-users alike. As an integrated solution eliminates separate and dedicated encryption appliances—and thus simplifies the network topology and the deployment of encryption services—it introduces new entrants in this market segment.

Whether it is service providers offering a new value-added managed service, or enterprises considering a simplification of the encryption service architecture, the introduction of a new technology typically generates the need to test or type approve the new solution. In the case of encryption technology, a frequent question is "How can one test the encryption?" The following sections discuss the processes related to encryption solution validation.

The Encryption Process

From a Wikipedia entry, "In cryptography, encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (in cryptography, referred to as ciphertext)."

There are numerous ways to obfuscate transmitted information so intermediaries cannot access the plaintext without knowledge of the key. These methods can range from simple to complex scrambling techniques that render data more difficult to decipher, to a vast array of true encryption algorithms. The encryption algorithms also range from simple to elaborate, and can be proprietary or standards-based. Whereas proprietary encryption algorithms are used for specific applications, standards-based algorithms are primarily used for most applications, from enterprises in the financial or healthcare verticals to many government agencies. This document focuses on standards-based encryption ciphers, although the concepts can be extended to other algorithms.

Encryption Standards

There are many standards-based encryption algorithms, ranging from the original Data Encryption Standard (DES) to its successor, Advanced Encryption Standard (AES), which has various key sizes (56-, 128-, 256-bits). These standards are published by the National Institute of Standards and Technology (NIST), a non-regulatory agency of the U.S. Department of Commerce. These standards are published as U.S. Federal Information Processing Standard (FIPS) publications. As an example, the AES-256 encryption algorithm was published as FIPS PUB 197 (FIPS 197)[1].

In addition to algorithm-specific standards such as FIPS 197, NIST also publishes standards coordinating the requirements and standards for cryptographic modules that include both hardware and software components in FIPS 140-2[2]. There are also similar frameworks defined for computer systems implementations such as Common Criteria for Information Technology Security Evaluation (CC).

Encryption Algorithm Testing

Since AES-256 is a standard, there must be a defined methodology to ensure an implementation meets the published standard. In other words, one should be able to validate that given a plaintext string and a specific key, the output of the encryption algorithm is the correct one. Such a methodology does exist with the use of Known Answer Test (KAT) vectors. Before exploring this more, it is important to understand that the cryptographic algorithm is only one part of a complete integrated encryption solution.

In its most simple form, an encryption system could be the cipher alone. However, a complete encryption solution encompasses not only the algorithm, but also other cryptographic elements, to ensure the overall solution is secure. These other elements can include key management, monitoring functions, traffic adaptation functions, and various physical and mechanical considerations.

As such, testing the encryption algorithm alone provides some reassurances regarding the overall solution's performance, but is not complete itself. In addition, since the encryption algorithm is part of a more complex system, the ability to test it independently with KAT vectors is virtually impossible without intimate knowledge of the complete solution's architecture. This is where independent certification of encryption solutions becomes important.

CAVP and CMVP

NIST and the Communication Security Establishment of Canada (CSEC) have jointly established, and are operating, both the Cryptographic Algorithm Validation Program (CAVP)[3] and Cryptographic Module Validation Program (CMVP)[4]. The CAVP encompasses validation testing for FIPS-approved and NIST-recommended cryptographic algorithms. Cryptographic algorithm validation is a prerequisite to the CMVP. The CMVP validates cryptographic modules compliance to FIPS 140-2 and other FIPS cryptography-based standards.

Vendors of cryptographic modules use independent, accredited Cryptographic and Security Testing (CST) laboratories to test their modules. The CST laboratories use the Derived Test Requirements (DTR), Implementation Guidance (IG), and applicable CMVP programmatic guidance to test cryptographic modules against the applicable standards. NIST's
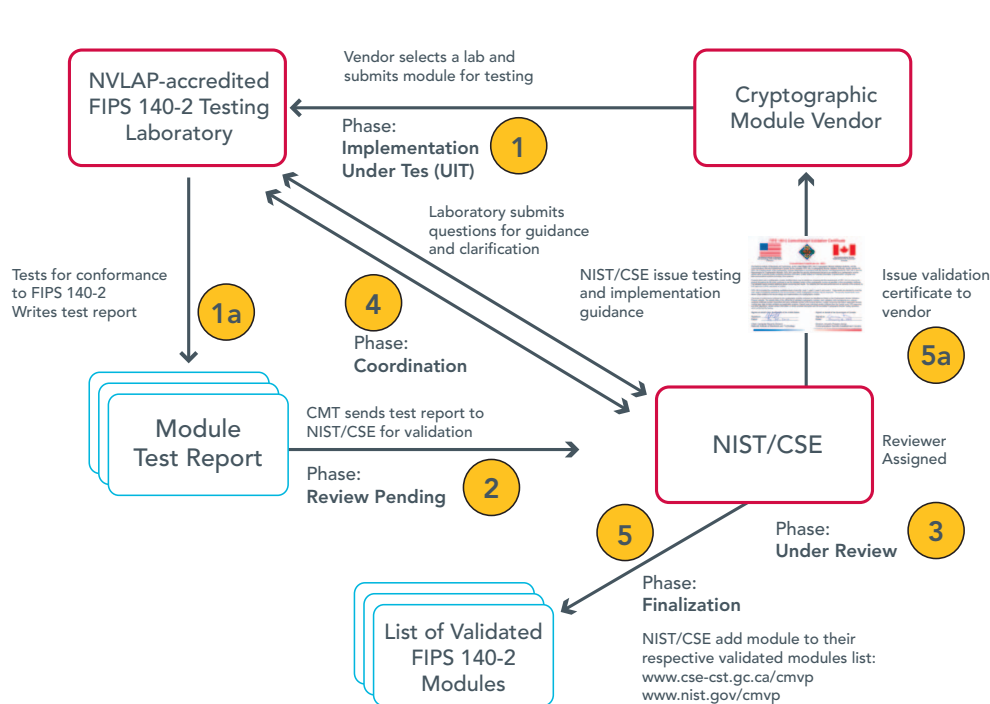
Figure 1. General flow of FIPS 140-2 testing and validation

Computer Security Division (CSD) and CSEC jointly serve as the Validation Authorities for the program, validating the test results and issuing certificates.

For AES-256 validation through the CAVP process, the independent accredited CST laboratories use the Advanced Encryption Standard Algorithm Validation Suite (AESAVS)[5], which describes the AES Know Answer Test (KAT).

The CMVP, as indicated above, is an encompassing certification process that assesses a cryptographic module for compliance against FIPS 140-2. The CMVP process is divided in five stages, as illustrated in Figure 1.

FIPS 140-2

The FIPS 140-2 publication coordinates the requirements and standards for cryptographic modules that include both hardware and software components. There are four different levels of security defined by FIPS 140-2: Levels 1 to 4, each imposing different levels of requirements in each of the eleven areas covered by FIPS 140. The eleven areas are:

1. Cryptographic Module Specification
2. Module Ports and Interfaces
3. Roles, Services, and Authentication
4. Finite State Model
5. Physical Security
6. Operational Environment
7. Cryptographic Key Management
8. Electromagnetic Interference/ Electromagnetic Compatibility Testing (EMI/EMC)
9. Self-Tests
10. Design Assurance
11. Mitigation of Other Attacks

As part of the CMVP process, each of the above areas is assessed against the requirements defined for the four different levels. A module must meet all requirements defined for a specific level to be granted a certificate at that level, although it may meet requirments for a higher level in some areas.

Independent Certification

The CAVP and CMVP processes offer an independent assessment and certification of an encryption solution using well established and standards-based methodology, thereby providing service providers and end-users assurances that the encryption solution has demonstrated compliance to the defined standards having successfully completed the rigorous laboratory testing and reviews mandated by the standards. The certification status of an encryption solution undergoing such a certification is a public record published by NIST[6], which also maintains a repository to verify the validity of a FIPS certificate.

References

[1] FIPS 197, Advanced Encryption Standard (AES), http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[2] FIPS 140-2, Security Requirements for Cryptographic Modules, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[3] Cryptographic Algorithm Validation Program (CAVP), http://csrc.nist.gov/groups/STM/cavp/index.html

[4] Cryptographic Module Validation Program (CMVP), http://www.nist.gov/itl/csd/sma/cmvp.cfm

[5] Advanced Encryption Standard Algorithm Validation Suite (AESAVS), http://csrc.nist.gov/groups/STM/cavp/documents/aes/AESAVS.pdf

[6] Modules in process, http://csrc.nist.gov/groups/STM/cmvp/inprocess.html

Specialists in unlocking network potential to help you change the way you complete.