Satisfying CC Cryptography Requirements through CAVP/CMVP Certifications

International Crypto Module Conference
May 19, 2017

leidos

Synopsis

- Background
- NIAP policy relating to cryptographic requirements
- NIAP’s CAVP Mapping guideline
- Specific requirements and how they are satisfied
- Considerations for vendors
- Conclusions

Background

- Common Criteria evaluations in the US are conducted against NIAP-approved Protection Profiles
- NIAP-approved Protection Profiles specify assurance activities to be performed by the evaluation team
- Assurance activities are defined for each functional and assurance requirement specified in the Protection Profile
- Assurance activities define required content for Security Targets (STs) and guidance documents, and required testing
- Successful completion of assurance activities establishes adequate evidence the product satisfies the requirements specified in the Protection Profile

Background

- Many NIAP-approved Protection Profiles include requirements for cryptographic functionality:
  - Basic functions, such as symmetric and asymmetric encryption and decryption, and hashing
  - Key management capabilities, such as key generation, key destruction, and key establishment
  - Secure protocols, such as IPsec, TLS and SSH
- As with non-cryptographic functional requirements, these have associated assurance activities, including testing
- Test activities may comprise detailed tests drawn from NIST validation testing specifications, or explicit reference to those testing specifications

NIAP Policy

- Promulgated in Scheme Policy Letter #5
- Regardless of how test activities for cryptographic requirements are specified, all cryptography in the Target of Evaluation (TOE) for which NIST provides validation testing must be NIST validated
- This can be demonstrated through identification in the ST of CAVP certification for the claimed cryptographic functions, or identification of CMVP certification of the cryptomodule included in the TOE
- The ST must indicate all requirements for which a CAVP certificate is claimed and include: the cryptographic operation; the NIST standard; and the CAVP Certificate number

NIAP CAVP Mapping Guide

- Published as Addendum to Scheme Policy Letter #5
- Lists applicable CAVP validation list with modes, states, key sizes, etc. required to meet specific cryptographic requirements
- For example:

  FCS_COP.1(1) [from Network Device collaborative PP]

  The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in [CBC] mode and cryptographic key sizes [128 bits, 256 bits] that meet the following: AES as specified in ISO 18033-3, [CBC as specified in ISO 10116].
- Required CAVP certification:

  AES Validation List

  CBC (e/d; 128, 256)

Satisfaction of Specific Requirements

- Symmetric encryption/decryption – AES validation with appropriate modes and key sizes
- Digital signature services (generation/verification) – RSA, DSA, ECDSA validation lists with appropriate key/modulus sizes or curves
- Cryptographic hashing – SHS validation list with appropriate SHA algorithm (SHA-1, SHA-256, SHA-384, SHA-512)
- Keyed-hash message authentication – HMAC validation list with appropriate hash algorithms (HMAC-SHA-1, etc.)
- Deterministic Random Bit Generation – DRBG validation list with appropriate algorithm and supporting validations (e.g., CTR_DRBG with AES-128, AES-256, AES CAVP cert)

Satisfaction of Specific Requirements

- Asymmetric key generation – RSA, DSA, ECDSA validation with FIPS 186-4 key generation and appropriate key/modulus sizes or NIST curves
- Key establishment – depends on scheme and base specification (SP 800-56A or SP 800-56B), but may require KAS or CVL validation

Considerations for Vendors

- Operational Environment
  - CAVP certifications identify the specific Operational Environment (processor, operating system) on which algorithm testing occurred
- NIAP requirements:
  - for firmware and hardware cryptographic implementations, the OE must correspond exactly to the hardware platforms specified in the ST
  - for software cryptographic implementations, minor OE software version variations that do not affect interfaces used by the TOE are considered equivalent (e.g., Linux 3.13, Linux 3.16), and processors in the OE that are implemented by the same manufacturer in the same family as hardware listed in the ST are also considered equivalent (e.g., Intel i3, i5, i7)

Considerations for Vendors

- Third-party cryptographic modules
  - OpenSSL does not (yet) support FIPS 186-4 key generation for RSA
  - Vendors incorporating OpenSSL in their products likely will need to patch the OpenSSL module (e.g., RedHat has issued such a patch) or develop their own implementation – in either case, the vendor will need to obtain their own CAVP validation for RSA key generation
  - OpenSSL is not validated on every conceivable OE – vendors incorporating an unsupported OE in their product will need to obtain their own CAVP validations for all claimed algorithms

Conclusions

- Understand the cryptographic requirements of the target PP
- Determine if your intended cryptographic module has all the appropriate CAVP certifications and your product matches the Operational Environments for those certifications
- Plan for circumstances in which you will need to obtain your own CAVP certifications
- Do all this before you start your CC evaluation

Questions?

Author Contact Information

- Tony Apted, Leidos CCTL Technical Director
  - anthony.j.apted@leidos.com

leidos