FIPS 140

From Wikipedia, the free encyclopedia

The 140 series of **Federal Information Processing Standards** (FIPS) are U.S. government computer security standards that specify requirements for cryptography modules. As of December 2016, the current version of the standard is FIPS 140-2, issued on 25 May 2001.[1]

Contents

Purpose of FIPS 140

The National Institute of Standards and Technology (NIST) issues the 140 Publication Series to coordinate the requirements and standards for cryptographic modules which include both hardware and software components for use by departments and agencies of the United States federal government. FIPS 140 does not purport to provide *sufficient* conditions to guarantee that a module conforming to its requirements is secure, still less that a system built using such modules is secure. The requirements cover not only the cryptographic modules themselves but also their documentation and (at the highest security level) some aspects of the comments contained in the source code.

User agencies desiring to implement cryptographic modules should confirm that the module they are using is covered by an existing validation certificate. FIPS 140-1 and FIPS 140-2 validation certificates specify the exact module name, hardware, software, firmware, and/or applet version numbers. For Levels 2 and higher, the operating platform upon which the validation is applicable is also listed. Vendors do not always maintain their baseline validations.

The Cryptographic Module Validation Program (CMVP) is operated jointly by the United States Government's National Institute of Standards and Technology (NIST) Computer Security Division and the Communications Security Establishment (CSE) of the Government of Canada. The use of validated cryptographic modules is required by the United States Government for all unclassified uses of cryptography. The Government of Canada also recommends the use of FIPS 140 validated cryptographic modules in unclassified applications of its departments.

Security levels

FIPS 140-2 defines four levels of security, simply named "Level 1" to "Level 4". It does not specify in detail what level of security is required by any particular application.

- FIPS 140-2 Level 1 the lowest, imposes very limited requirements; loosely, all components must be "production-grade" and various egregious kinds of insecurity must be absent.
- FIPS 140-2 Level 2 adds requirements for physical tamper-evidence and role-based authentication.
- FIPS 140-2 Level 3 adds requirements for physical tamper-resistance (making it difficult for attackers to gain access to sensitive information contained in the module) and identity-based authentication, and for a physical or logical separation between the interfaces by which "critical security parameters" enter and leave the module, and its other interfaces.
- FIPS 140-2 Level 4 makes the physical security requirements more stringent, and requires robustness against environmental attacks.

In addition to the specified levels, Section 4.1.1 of the specification describes additional attacks that may require mitigation, such as differential power analysis. If a product contains countermeasures against these attacks, they must be documented and tested, but protections are not required to achieve a given level. Thus, a criticism of FIPS 140-2 is that the standard gives a false sense of security at Levels 2 and above because the standard implies that modules will be tamper-evident and/or tamper-resistant, yet modules are permitted to have side channel vulnerabilities that allow simple extraction of keys.

Scope of requirements

FIPS 140 imposes requirements in eleven different areas:

- *Cryptographic module specification* (what must be documented)
- *Cryptographic module ports and interfaces* (what information flows in and out, and how it must be segregated)
- *Roles, services and authentication* (who can do what with the module, and how this is checked)
- *Finite state model* (documentation of the high-level states the module can be in, and how transitions occur)
- *Physical security* (tamper evidence and resistance, and robustness against extreme environmental conditions)
- *Operational environment* (what sort of operating system the module uses and is used by)
- *Cryptographic key management* (generation, entry, output, storage and destruction of keys)
- *EMI/EMC*
- *Self-tests* (what must be tested and when, and what must be done if a test fails)
- *Design assurance* (what documentation must be provided to demonstrate that the module has been well designed and implemented)
- *Mitigation of other attacks* (if a module is designed to mitigate against, say, TEMPEST attacks then its documentation must say how)

Brief history

FIPS 140-1, issued on 11 January 1994, was developed by a government and industry working group, composed of vendors and users of cryptographic equipment. The group identified the four "security levels" and eleven "requirement areas" listed above, and specified requirements for each area at each level.

FIPS 140-2, issued on 25 May 2001, takes account of changes in available technology and official standards since 1994, and of comments received from the vendor, tester, and user communities. It was the main input document to the international standard ISO/IEC 19790:2006 *Security requirements for cryptographic modules* issued on 1 March 2006.

FIPS 140-3 is a new version of the standard which is currently under development. In the first draft version[2] of the FIPS 140-3 standard, NIST introduced a new software security section, one additional level of assurance (Level 5) and new Simple Power Analysis (SPA) and Differential Power Analysis (DPA) requirements. The draft issued on 11 Sep 2009, however, reverted to four security levels and limits the security levels of software to levels 1 and 2.

Criticism

Due to the way in which the validation process is set up, a software vendor is required to re-validate their FIPS-140-validated module for every change, no matter how small, to the software; this re-validation is required even for obvious bug or security fixes. Since validation is an expensive process, this gives software vendors an incentive to postpone changes to their software and can result in software that does not receive security updates until the next validation. The result may be that validated software is less safe than a non-validated equivalent.[3]

See also

- Common Criteria

References

1. "FIPS General Information" (https://www.nist.gov/itl/fipsinfo.cfm). NIST. 2010-10-05. Retrieved 2013-05-18.
2. "FIPS-140 -3: DRAFT Security Requirements for Cryptographic Modules (Revised Draft)" (http://csrc.nist.gov/publications/PubsDrafts.html#FIPS-140--3). NIST. 2013-03-07. Retrieved 2013-05-18.
3. "Is FIPS 140-2 Actively harmful to software?" (https://blogs.oracle.com/darren/entry/fips_140_2_actively_harmful). Darren Moffat, Oracle Solaris. 2014-04-16. Retrieved 2017-03-18.

External links

- "Federal Information Processing Standards (FIPS) Publications" (http://csrc.nist.gov/publications/PubsFIPS.html). NIST. 2013-02-05. Retrieved 2013-05-18.
- "Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules" (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm). NIST. 2013-05-17. Retrieved 2013-05-18.

Retrieved from "https://en.wikipedia.org/w/index.php?title=FIPS_140&oldid=808400623"

This page was last edited on 2 November 2017, at 17:06.
Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

- Contact Wikipedia
- Developers
- Cookie statement