Mind the Gap: Updating FIPS 140

Steve Weingart
Chief Technology Officer
Futurex
864 Old Boerne Rd.
Bulverde, TX 78163
Weingart@futurex.com

Steve R. White
IBM Thomas J. Watson Research Center
P.O. Box 704
Yorktown Heights, NY 10598
srwhite@watson.ibm.com

Abstract

In order to be secure, modules that provide cryptographic function must do more than simply implement a secure cryptographic algorithm. They must resist system-level attacks, whether by software or hardware, and whether the attack is intended to produce incorrect results or to expose information that should be protected. The details of these requirements change over time. Both attack and defensive technologies improve, turning difficult attacks into easy ones, or expensive defenses into inexpensive ones. The current standard for the security of cryptographic systems is FIPS 140, which lays out four levels of security that have increasingly stringent requirements. This paper argues that changing attack technologies and application requirements have led to a gap in FIPS 140, and that a new level is needed. Such a level is proposed, intermediate between the two highest levels of FIPS 140. The new level allows the validation of commercially feasible products that are more secure than the current Level 3, but that do not carry the difficult burden imposed by the current Level 4 validation requirements.

Introduction

Cryptographic systems must satisfy several requirements in order to be useful. They must function properly, of course, encrypting and decrypting text as their algorithms require. (Though, because these systems are complex, this is not always a given!) They must not be susceptible to software attacks – buffer overflows and the like – that are all too common in software systems. They must not be susceptible to hardware attacks, whether that involves operating the device outside of its specified voltage range, or attempting to probe the system to discover its cryptographic keys or other critical information.

The details of these requirements change over time. Both attack and defense technologies improve, turning difficult attacks into easy ones, or expensive defenses into inexpensive ones. The current standard for the security requirements of cryptographic systems that process sensitive but unclassified data is FIPS 140, which was first adopted by the National Institute of Standards and Technology (NIST) in 1994. It has undergone one revision, from FIPS 140-1 to FIPS 140-2, in 2001. This paper argues that changing attack technologies and application requirements indicate the need for certain changes in the upcoming FIPS 140-3 revision.

The remainder of this paper is organized as follows: First, we discuss the background of FIPS 140; what motivated its creation and the idea behind the level-based system that it uses. Then, we detail some of the important changes in attack technologies, commercial requirements and standards that have occurred since FIPS 140-1 was adopted. Next, we turn to the current status of FIPS 140 and notice that a substantial gap has emerged between the two highest levels of validation in the standard, leaving important applications in the gap. Finally, we propose a modification to FIPS 140 to fill that gap, in the form of a new validation level intermediate between the two current highest ones. This new level is designed to fit the commercial and governmental applications that have evolved in recent years, and to provide a practical way for modules to be validated that provides useful hardware protection without necessarily satisfying the onerous requirements of the highest level of FIPS 140 validation.

Background

In the late 1980's, cryptography was becoming more widely used in the commercial sector and applications such as encrypted radio and software-only cryptography were gaining momentum. So, the U.S. government decided to retire FED-STD-1027, "General Security Requirements for Equipment Using the Data Encryption Standard" [1], replacing it with a new standard for the security of cryptographic devices that were used for protecting sensitive but unclassified data. This new standard was to be called FIPS 140, "Security Requirements for Cryptographic Modules" [2]. Unlike FED-STD-1027, which was specific to the DES algorithm and DES keys, FIPS 140 was to focus on the security of modules that implemented the cryptographic function, independent of the cryptographic algorithm used.

During the development of FIPS 140, a team from IBM developed a classification scheme for the physical security of computing components and systems. This scheme was based on six levels, ranging from systems with virtually no security to systems whose penetration would require the resources and expertise of a national lab [3]. Each level built on the previous level, with additional requirements added as the levels increased. Requirements for the difficulty of mounting a successful attack on the physical security of the system are shown below. There were similar requirements for quality assurance, documentation and functional testing.

Level	Name	Description
1	None	The attack can succeed "by accident," without the attacker necessarily being aware that a defense was intended to exist. No tools or skills are needed.
2	Intent	The attacker must have a clear intent in order to succeed. Universally available tools (e.g. screwdriver, nail file) and minimal skills may be used.
3	Common Tools	Commonly-available tools and skills may be used. (e.g. those tools available from retail department or computer stores.)
4	Unusual Tools	Uncommon tools and skills may be used, but they must be available to a substantial population. (e.g. lock pick, logic analyzer; hardware debugging skills, electronic design and construction skills.) Typical engineers will have access to these tools and skills.
5	Special Tools	Highly specialized tools and expertise may be used, as might be found in the laboratories of universities, private companies, or governmental facilities. The attack requires a significant expenditure of time and effort.
6	In Laboratory	A successful attack would require a major expenditure of time and effort on the part of a number of highly qualified experts, and the resources available only in a few facilities in the world.

The scheme dealt primarily with hardware systems and hardware requirements, as did FED-STD-1027. It was designed to give guidance to developers as to the kinds of attacks that should be deterred at each level, and suggested the kinds of technologies that might meet these requirements. It was also intended to be an objective standard for testing and, potentially, validating such systems. The scheme was submitted to the FIPS 140 committee as a suggested starting point for its work.

The FIPS 140 committee adopted a scheme with four levels. (Having six was considered too complex). Like the IBM scheme, each level was built on the lower levels, with requirements added as the level increased. It greatly extended the IBM work to cover all parts of the cryptographic system in detail, expanded its coverage to firmware and software, and added such requirements as formal modeling of the system at the highest level. Below is a summary of two of the eleven sets of requirements in FIPS 140.

Level	Physical Security	Design Assurance
1	Production grade equipment.	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.
2	Locks or tamper evidence.	CM system. Secure distribution. Functional specification.
3	Tamper detection and response for covers and doors.	High-level language implementation.
4	Tamper detection response envelope. EFP or EFT.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.

At Level 1, there are basic security and integrity requirements. However, to a large extent, devices or software packages validated at Level 1 need only show that they have reasonable design assurance, documentation, separation of roles and services, and basic integrity.

At Level 2, simple physical security requirements are added, as well as additional design assurance and a more secure operational environment. The physical security requirements can be satisfied by commonly available technologies such locks or tamper-evident seals on cases.

At level 3, the requirements include: (1) the loading of plaintext security parameters without logical or physical separation of the ports must be prevented, (2) authentication for roles and services must be identity based, and (3) the operational environment must be even more secure. The physical security requirements are increased so that some basic types of entry must be detected and responded to. The design assurance requirements mandate implementation in high level languages to minimize errors, maximize readability and ease evaluation. Level 3 physical security requirements can be satisfied by switches or tripwires on covers and doors, the activation of which causes the device to become unusable or its sensitive information to be erased.

At level 4, the requirements increase dramatically. Tamper/entry detection mechanisms must detect virtually all intrusions. Environmental excursions outside of the operating range must be accounted for by either graceful failure (environmental failure testing), or protection (environmental failure protection). The operating environment requirements also increase. Formal modeling of the software and firmware is probably the most difficult of the Level 4 requirements to meet. Achieving Level 4 physical security requires more sophisticated technology. Single chip modules can be coated with passivation layers that deter probing. Circuitry to be protected can be potted in urethanes or epoxies, making it difficult to get to the circuitry. Conductive meshes that surround the circuitry can detect attempted tampering and cause sensitive information to be erased before tampering can succeed. Other attacks and defenses can be found in *Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses* [4].

Changes since FIPS 140-1 was Adopted

We now turn our attention to the ways in which attack technologies, the standards environment and the business environment have changed since the adoption of FIPS 140-1.

An increasing sophistication in attack techniques was caused by (1) the growing popularity of the Internet and (2) greater proliferation and reduced cost of attack tools and technologies.

The Internet made the mechanisms for common software attacks widely available. So-called "script kiddies" can download software tools that implement many common attacks and use them effectively without any real knowledge of the underlying mechanism of the attacks. Details of these mechanisms are, however, commonly discussed in public Internet venues, and the level of skill of attackers has increased due to more open discussion and exploration.

Hardware tools became more accessible as well. When FIPS 140-1 was being written in the early 1990's, a good logic analyzer cost over $20,000, was regarded as a specialized tool and was not typically available. They were not yet common in college labs and were just becoming so in typical industrial development labs. Now they are considered basic equipment, just as oscilloscopes were at that time. Today logic analyzers can be purchased for a few hundred dollars over the Internet as a circuit card that plugs into a desktop computer. Likewise scanning electron microscopes, which used to be specialized tools only available to high level research and industrial labs, are now common in most university labs. Laser drilling tools, now fairly common in cellular biology labs, coupled with pico-probes, are much more readily accessible. Using a laser drilling tool, an attacker can cut a hole in the passivation layer of a semiconductor device and use a pico-probe to connect to the circuit beneath. The most powerful new tools in the arsenal are focused ion beam (FIB) tools. FIB tools are still difficult to access, but are available in most university research and industrial labs. FIB performs both microscopic material removal and material deposition and is even more effective at cutting microscopic holes than laser drilling tools. Once the hole is made, it can then be plated with metal to make probing even easier.

The sophistication of industrial machining tools has risen dramatically. Computer numerical controlled machining tools, with control to < 0.001", are now common. They are typically available in high school machine shops and are available for home use. Laser cutting tools are now commonly used for cutting everything from sheet metal, to wood, to textiles. Water machining tools are now in everyday use for cutting brittle materials and plastics.

New attacks have also emerged. Power analysis, where the supply current (I_{cc}) to a module is sampled and analyzed, has proven to be a very effective attack mechanism. Using this method, several teams were successful in extracting secrets from many different modules, especially Smart Cards [5].

Partly in response to the increased availability of attack information and attack technologies, ANSI X9.8, "Banking - Personal Identification Number Management and Security" [6] adopted in 2003, requires active tamper detection and response for banking modules that deal with PINs. This has driven increased interest from the banking and financial communities in secure cryptographic modules. Similarly, the U.S. Postal Service requires substantial security for devices that print postal indicia from postal metering devices at customer locations or via the Internet. In addition to tamper detection and response, the U.S. Postal Service requires either environmental failure testing (EFT) or environmental failure protection (EFP). These new commercial requirements are characteristic of FIPS Level 4 modules, but neither the banking standards nor the Postal Service require that a module meet all of the other FIPS 140 Level 4 requirements.

Current Status of FIPS 140

Since its adoption in 1994, FIPS 140 has been very successful. It is recognized worldwide as the standard for security of cryptographic modules. Hundreds of products have been validated under its provisions and these products are in wide use by corporations and governments

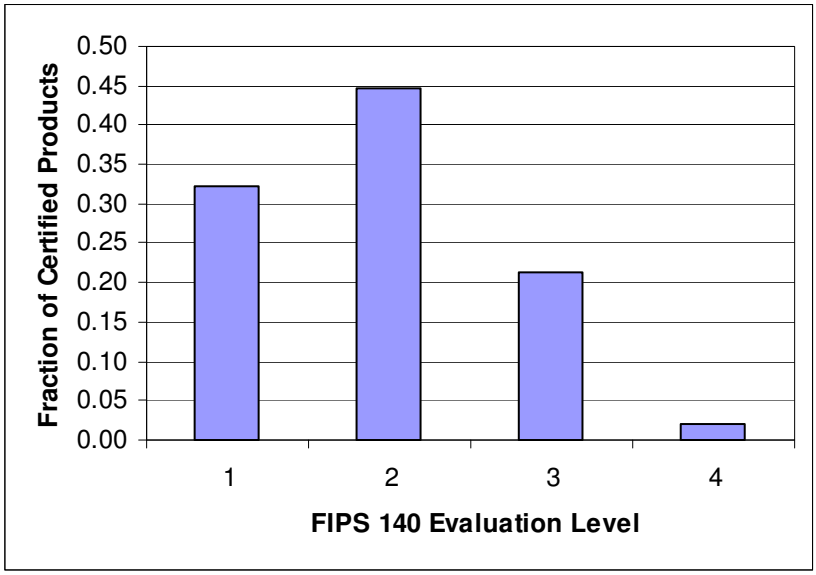
Many of the issues that have arisen since its initial adoption have been addressed in FIPS 140-2, a 2001 revision. Design assurance and key management requirements became more complete. Operational environment requirements were restated in terms of the more current Common Criteria system [7], which replaced the Orange Book standards that were formerly used. A section, "Mitigation of Other Attacks," was added to account for new classes of attacks, such as power analysis, that had not been well-known when the first version of the standard was written.

Still, advances in attack technologies have significantly changed the landscape. Most Level 4 devices with which the authors are familiar are still very secure despite these advances. Laser drilling is still difficult if the aspect ratio (the ratio of the depth to the diameter) of the hole is very large and multiple materials are used in the potting material. If a large hole is drilled, material heating and cracking would likely cause the package to crack, tripping the required tamper detection circuitry. A smaller hole would likely be so narrow and deep as to be very difficult to use effectively. FIB tools quickly become contaminated if the material being cut has a high organic content, which is typical of the filled epoxies and urethanes used in most designs. Traditional machining tools, even those equipped with numerical control, have not shown to be effective against Level 4 tamper detectors.

The industry now has an increased awareness of software attacks and the ability to respond rapidly with fixes. In addition, software security techniques have improved along with software attack techniques, and sharing of both attack and defense information on the Internet has greatly benefited software security. As a result, most Level 3 devices are fairly secure against software attacks.

On the other hand, Level 3 devices are probably all physically penetrable within a few hours by anyone with reasonable skill and intention. The problem with current Level 3 devices is that their software security is probably adequate but their hardware security is not.

As of August, 2005, 566 products have been validated under the provisions of FIPS 140 [8]. The following graph shows a breakdown by Level of the validated products to date. It is interesting to note that only a few percent of the systems are validated at Level 4. In fact, there are just eleven such systems, and this number includes model revisions. There are only five or six truly distinct devices that have been validated at Level 4.



It could be that the market for Level 4 modules is simply small, perhaps because they are more expensive and often use older technologies because of the expense and time needed to develop the complex systems required by Level 4. Level 4 devices are often limited in function because the formal modeling requirement minimizes the amount of code that a vendor is willing to model formally, and the stringent tamper detection requirements make manufacturing more difficult, and false alarms (both positive and negative) more difficult to avoid.

However, the market for a very secure device may be larger than it first appears. Most banking and financial institutions require Level 3, as do many other commercial customers. If higher security devices with the needed level of function were available, at a reasonable cost, it is likely that they would become required in these environments.

Thus, a gap has appeared between Level 3 and Level 4, and this gap has widened over time. Attack technologies and tools that were rare and expensive when FIPS 140-1 was adopted have become widespread and inexpensive. Commercial requirements, notably from banking, finance and the U.S. Postal Service, demand greater security than is found in Level 3 but do not demand all of the stringent security of Level 4. Finally, Level 4 systems have proven difficult and expensive to create in practice due to those same stringent requirements.

These changes in the environment argue for the introduction of a new level in FIPS 140, intermediate between the current Levels 3 and 4.

A Proposed Update to FIPS 140

The four levels described in FIPS 140-2 roughly correspond to Levels 1, 2, 3 and 6 from the IBM scheme [3]. The proposal suggested in this paper is to add a "Level 3.5", between Levels 3 and 4 of the FIPS 140-2 standard to increase the physical security of the device and make it more appropriately secure for the protection of moderately high value assets. The physical security of this new level would correspond to Level 4 or 5 of the original IBM scheme. The software requirements would also be somewhat more stringent than at Level 3, but would avoid the burden of formal modeling.

The main new requirements are: (1) a full coverage tamper detection and response system, but with a lower overall sensitivity requirement than Level 4, (2) design assurance requirements that seek somewhat more verification than Level 3, but not the formal modeling of Level 4 and (3) EFT/EFP requirements that ensure that the device will only operate while the voltage and temperature are within the manufacturer's specified operating range.

This is the proposed new Level 3.5 in terms of the eleven criteria in FIPS 140-2.

For a multi-chip embedded or stand-alone module:

> Cryptographic Module Specification: Unchanged, same for all levels
>
> Cryptographic Module Ports and Interfaces: Unchanged, same for all levels
>
> Roles, Services and Authentication: Unchanged, same as for current Levels 3 & 4
>
> Finite State Model: Unchanged, same for all levels
>
> Physical Security: Tamper detection and response envelope, maximum undetected hole size 1- 1.25 mm (0.040" – 0.050"), EFT/EFP

Operational Environment: Same as current Level 3

Cryptographic Key Management Unchanged, same as for current Levels 3 & 4

EMI/EMC: Unchanged, same as for Levels 3 & 4

Self Tests: Unchanged, same for all levels

Design Assurance: Same as for Level 3 + informal model/code walkthrough/demonstration of protection from well known threats such as buffer overflow

Mitigation of Other Attacks: Unchanged, same for all levels

Physical Security for Single Chip Module: Strong removal resistant and penetration resistant passivation/potting

All other requirements the same

Below are the changed requirements stated as the requirements sections from FIPS 140-2.

Multiple-Chip Embedded and Standalone Cryptographic Modules

SECURITY LEVEL 3.5

In addition to the requirements for Security Levels 1, 2, and 3, the following requirements shall apply to multiple-chip embedded cryptographic modules for Security Level 3.5.

- The cryptographic module components shall be covered by potting material or contained within an enclosure encapsulated by a tamper detection envelope (e.g., a flexible Mylar printed circuit with a serpentine geometric pattern of conductors or a wire-wound package or a non-flexible, brittle circuit or a strong enclosure) that shall detect tampering by means such as cutting, drilling, milling, grinding, or dissolving of the potting material or such that any entrance larger than 1 - 1.25 mm (0.040" – 0.050"), will be detected.
- The cryptographic module shall contain tamper response and zeroization circuitry that shall continuously monitor the tamper detection envelope and, upon the detection of tampering, shall immediately zeroize all plaintext secret and private cryptographic keys and CSPs. The tamper response and zeroization circuitry shall remain operational when plaintext secret and private cryptographic keys or CSPs are contained within the cryptographic module.

Single-Chip Cryptographic Modules

SECURITY LEVEL 3.5

In addition to the requirements for Security Levels 1, 2, and 3, the following requirements shall apply to single-chip cryptographic modules for Security Level 3.5.

- The cryptographic module shall be covered with a hard, opaque removal-resistant coating with hardness and adhesion characteristics such that attempting to peel or pry the coating from the module will have a high probability of resulting in serious damage to the module (i.e., the module will not function).
- The removal-resistant coating shall have solvency characteristics such that dissolving the coating will have a high probability of dissolving or seriously damaging the module (i.e., the module will not function).

Design Assurance

SECURITY LEVEL 3.5

In addition to the requirements for Security Levels 1, 2, and 3, the following requirements shall apply to cryptographic modules for Security Level 3.5.

- Documentation shall specify an informal model that describes the rules and characteristics of the cryptographic module security policy. The model shall be specified using a written language and clearly show how the code implements the security policy.
- Documentation shall specify a rationale that demonstrates the consistency and completeness of the model with respect to the cryptographic module security policy.
- Documentation shall specify an informal proof of the correspondence between the model and the functional specification.
- For each cryptographic module hardware, software, and firmware component, the source code shall be annotated with comments that specify (1) the preconditions required upon entry into the module component, function, or procedure in order to execute correctly and (2) the postconditions expected to be true when execution of the module component, function, or procedure is complete. The preconditions and postconditions may be specified using any notation that is sufficiently detailed to completely and unambiguously explain the behavior of the cryptographic module component, function, or procedure.
- Documentation shall specify an informal proof of the correspondence between the design of the cryptographic module (as reflected by the precondition and postcondition annotations) and the functional specification.

This new level is in line with the ANSI X9.8 banking and financial industry requirements in that it requires active tamper detection and response. It is in line with the U.S. Postal Service requirements in that it also requires EFT/EFP. It allows devices to satisfy these important commercial needs without burdening them with the more onerous requirements of Level 4, and it allows FIPS 140 validation to attest that these requirements are met.

Devices built to this new level should be reasonably easy to design and manufacture. The IBM 4755 cryptographic coprocessor [9] was designed to approximately this level. (Since the card predated FIPS 140 and was never validated, it is difficult to make an exact comparison.) The card used a full coverage tamper membrane with 0.01" silver/carbon ink silk screened lines on 0.02" centers. The device was easy to manufacture, had high yield and reliability and was produced for about six years with thousands of units delivered to the field.

Conclusion

FIPS 140 has been very successful in standardizing the security performances of cryptographic devices for the non-classified community. However, several important changes have occurred since its adoption, and these indicate the need to update the standard. The first is that the evolution of technology has caused physical attacks that were once difficult and expensive to mount to now be relative easy and inexpensive to carry out. The second is that important application requirements from the banking and financial communities, and the U.S. Postal Service, specify greater security than current FIPS 140 Level 3 modules provide, while not needing the substantially greater security of Level 4.

This paper proposes a new level, intermediate between the current Levels 3 and 4, intended to meet these important commercial and governmental requirements, and to make it easier for such modules to achieve FIPS validation without having to satisfy the more demanding requirements of Level 4. The proposed new level requires a hardware tamper response system, more stringent design assurance than Level 3 without requiring the formal modeling of Level 4, and EFT/EFP requirements that ensure that the device will only operate while in its specified operating envelope.

No doubt the standards for security of cryptographic devices will continue to evolve. The intent of this paper is to suggest an update to FIPS 140 that satisfies the requirements of current and emerging users, and to put it on a strong foundation for further evolution.

References

[1] U.S. General Services Administration, "FED-STD-1027**,** General Security Requirements for Equipment Using the Data Encryption Standard" (April 14, 1982) http://www.faa.gov/and/and300/and360/govdocs/Fed-Std-1027.pdf

[2] U.S. National Institute of Standards and Technology, "FIPS PUB 140-2, Security Requirements for Cryptographic Modules" (May 25, 2001) http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[3] Weingart, S., White, S., Arnold, W. and Double, G., "An Evaluation System for the Physical Security of Computing Systems," in Proceedings of the 6th Computer Security Applications Conference (1990), pp. 232-243.

[4] Weingart, S., **"**Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses," in Proceedings of Cryptographic Hardware and Embedded Systems - CHES 2000: Second International Workshop, Worcester, MA, USA (2000), pp. 302–317.

[5] Chari, S., Jutla, C., Rao, J. and Rohatgi, P., Power Analysis: Attacks and Countermeasures, Programming Methodology, Springer-Verlag New York, Inc., New York, NY (2003), pp. 415-439

[6] American National Standards Institute, "ANSI X9.8, Banking - Personal Identification Number Management and Security" http://webstore.ansi.org/ansidocstore/dept.asp?dept_id=80

[7] International Standards Organization, "Common Criteria for Information Technology Security Evaluation" http://niap.nist.gov/cc-scheme/index.html

[8] National Institute of Standards and Technology, Cryptographic Module Verification Program web site http://csrc.nist.gov/cryptval/

[9] Double, G.P. and Weingart, S.H., "Data Protection by Detection of Intrusion into Electronic Assemblies," U.S. Patent 5159629 (Oct. 27, 1992)