Public Comments on the Review of FIPS PUB 140-1, "Security Requirements for Cryptographic Modules"

(Comments were submitted in response to the Federal Register Notice of October 23, 1998, on Page 56910. The following comments were submitted electronically to 140-1review@nist.gov.)

Sender: eva@email.nist.gov
Date: Wed, 18 Nov 1998 17:14:43 -0500
From: Eva Bozoki <eva@fortresstech.com>
Organization: Fortress Technologies
X-Mailer: Mozilla 3.01Gold (X11; I; Linux 2.0.30 i686)
To: 140-1review@nist.gov
CC: X9F3@X9.ORG
Subject: Comment on FIPS 140-1

To whom it concerns,

I would like to comment on the following FIPS 140-1 requirement: "If a cryptographic module implements a bypass capability, then the current status of the module shall indicate whether or not the bypass capability is activated." (part of AS03.10).

The new generation of VPN devices are PACKET ENCRYPTORs operating at HIGH COMMUNICATION SPEED. For example, the NetFortress VPN-10 and VPN-100 operate above 7 Mbs and above 70 Mbs, respectively (and the even higher ATM speeds are not far ahead). These speeds correspond to an average 7000 and 70000 IP packets/sec. The classification of these packets, as to which one have to be encrypted and which one does not (bypass), are performed automatically by the device. THE DEVICE IS CAPABLE OF HANDLING BOTH TYPES OF PACKETS AT ALL TIMES. The encrypted and unencrypted (bypass) packets are INTERMIXED; a few of one type is followed by a few of the other type.

At these communication rates it is hard to find a packet indicator that operates with appropriate RESOLUTION. For example, a blinking LED would appear to be steady.

Furthermore, at such speeds the indication of an ultra-short "bypass state" essentially loses its SECURITY SIGNIFICANCE. The security-awareness level of an operator (user/crypto-officer) will not increase seeing a steadily blinking LED beyond the level of knowing that he is operating a module that is capable of providing bypass operation (which he knows anyway).

In addition, due to the unlimited (or at least a few thousand) number of simultaneous connections, the RELEVANCE of the bypass state indicator is also questionable. This is because an unencrypted packet leaving the unit cannot instantaneously indicate its destination to the operator (observer).

--
Dr. Eva Bozoki
Chief Scientist/Director of Research
Fortress Technologies
2701 N. Rocky Pt. Rd, Tampa, Fl. 33607

Have you visited our site today?   http://www.fortresstech.com/

From: Ed Scheidt <eds@TECSEC.com>
To: 140-1 Review <140-1review@nist.gov>
Subject: 140-1 Review Comments from TECSEC Incorporated
Date: Tue, 24 Nov 1998 10:21:33 -0500
X-Mailer: Internet Mail Service (5.5.2232.9)

The next version of FIPS 140-1/ANSI X9.66 should incorporate the following comments that have surfaced during my company's development toward an eventual FIPS certification:
>
>1. Eliminate the "overall rating" and let the customer decide, based on
>functional requirements and specific ratings, whether or not the product
>satisfies the need.
>
>2. Need to address the trust model required for an interpretative language
>such as JAVA.
>
>3. Need to change Orange book references to Common Criteria notations.
>
>4. Add a reference to the FIPS for new algorithms that are evolving in
>addition to RSA and Eliptical Curve. The new ANSI standards that will be
>coming on line in 1999 will include expanded roles for asymmetric and
>symmetric algorithm models. As an example, an agreement of symmmetric keys
using the Diffie-Hellman algorithm can be applied to the ANSI model of
Constructive Key Management.

My company would welcome the opportunity to further define the above comments. We look forward to the new FIPS and its associated ANSI documents.

Ed Scheidt
C/Scientist
TECSEC Incorporated
1953 Gallows Road, Suite 220
Vienna, Va. 22182

703-506-9069
703-506-1484 (fax)

Reply-To: "Nicholas Brigman" <nick-brigman@email.msn.com>
From: "Nicholas Brigman" <nick-brigman@email.msn.com>
To: <140-1review@nist.gov>
Date: Sat, 28 Nov 1998 18:25:27 -0500
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 4.72.2110.0
X-MimeOLE: Produced By Microsoft MimeOLE V4.72.2106.4

Committee:

I hope that we can send everybody a singular message by taking components of the FIPS-140-1 process and map them to the common criteria. As a manufacturer, these certification are costly and time consuming. We need a singular message on security products.

In a nutshell that is it.

Nicholas Brigman
RedCreek Communications, Inc.
703-378-3755 V   703-378-3756 Fax

X-Authentication-Warning: wt1.usdoj.gov: x400 set sender to
Richard.W.Bowler@intmail.usdoj.gov using -f
Date: Mon, 14 Dec 1998 8:26:05 -0400
From: Bowler Richard W <Richard.W.Bowler@usdoj.gov>
Subject: 5 year review of FIPS 140-1
To: "'140-1review@nist.gov'" <140-1review@nist.gov> (IPM Return Requested)
Cc: Bell William H <William.H.Bell@intmail.usdoj.gov> (IPM Return Requested),
Ormaner Jerry G <Jerry.G.Ormaner@intmail.usdoj.gov> (IPM Return Requested),
Shiveley Wayne M <Wayne.M.Shiveley@intmail.usdoj.gov> (IPM Return Requested)
X-Mailer: Worldtalk (NetJunction 4.5.1-p4)/STREAM

Mr. Miles Smid:
The Information Security and Records Management Section of the Department of Justice has no objection to the continuation of FIPS PUB 140-1 Security Requirements for Cryptographic Modules. We are interested in reading industry comments on your Web site.
Thanks

R.W.Bowler, Jr.
Richard.W.Bowler@usdoj.gov v&f 202.616.1171 f 202.616.5455
DOJ/IRM/ Infomation Management & Security Staff (IMSS)
1001 G Street NW Suite 850 Washington DC 20530

"Facts are stubborn things and whatever may be our wishes, our inclinations, or the dictates of our passions, they can not alter the state of facts and evidence." John Adams

X-Sender: bobm@cymail.cylink.com
X-Mailer: Windows Eudora Pro Version 3.0 (32)
Date: Fri, 15 Jan 1999 08:48:49 -0800
To: 140-1review@nist.gov
From: bobm@cylink.com (Bob McMillan)
Subject: FIPS 140-1 Comments and Recommendations

January 15, 1999

Information Technology Laboratory
ATTN: Review of FIPS 140-1
Building 820, Room 562
National Institute of Standards and Technology
Gaithersburg, MD 20899

Dear Sir or Madam:
This letter submits comments from Cylink Corporation concerning the NIST review of FIPS 140-1, Security Requirements for Cryptographic Modules. This feedback was requested via a November 1, 1998 letter from Mr. Miles Smid to Mr. Kamy Kavianian of Cylink.

Please see the attachment for our comments and recommendations, and if you wish any further clarification, please contact me at (408)-735-5881 or via email at bobm@cylink.com.

Thank you very much.

Sincerely,

Robert McMillan, Jr.
Manager, Physical Design Engineering
Cylink Corporation

P.S. In parallel, I am also sending a hard copy of these comments to your
address.

[See following page]

RM99007
SUBJECT: FIPS 140-1 Comments and Recommendations
DATE: January 15, 1999
FROM: Robert McMillan, Jr.,
Manager, Physical Design Engineering
Cylink Corporation

The following comments and recommendations regarding FIPS 140-1 are hereby submitted by Cylink Corporation to the Information Technology Laboratory of the National Institute of Standards and Technology.

1. ENGINEERING CHANGE ORDERS (ECOs):

COMMENT:
Once a product has been certified to FIPS 140-1, it is inevitable that the product will undergo subsequent design changes. Many or all of these changes may have nothing to do with the characteristics of the design that are critical to FIPS 140-1 compliance. Although it is vital that a product remain compliant following an ECO, it is highly desirable that the manufacturer's FIPS 140-1-related overhead related to design changes be minimized.
RECOMMENDATION:
NIST should establish a policy regarding post-certification design changes that
a.) Is very clear to manufacturers and laboratories,
b.) eliminates the need to go back to a FIPS 140-1 laboratory in cases where the basic requirements for the cryptographic module are not being affected, and
c.) streamlines the re-evaluation process when FIPS 140-1-related characteristics are affected.

Such a policy might include a self-verification process (similar to the Federal Communications Commission's process regarding electromagnetic interference requirements). For simple changes, the manufacturer would determine on their own if a given design change were relevant to FIPS 140-1, and if compliance were maintained. "Major changes" would still need to be passed through the scrutiny of a FIPS 140-1 laboratory. (The definition of a "Major Change" vs. a "Non-Major Change" would need to be spelled out clearly).

2. PHYSICAL SECURITY REQUIREMENTS:
COMMENT:
A certain FIPS 140-1 Level 2 and Level 3 physical security requirement, as interpreted by NIST, does not adequately reflect a practical assessment of attack threats. It is inappropriate that a laboratory can fail a product by drilling out a self-clinching (press-fit) fastener in situations where the same drill is restricted from putting a hole in the adjacent sheet-metal. For Level 2 and Level 3, the laboratory's drill should be used only to drill-out accessible fasteners that hold on a cover.

RECOMMENDATION:
Re-assess the whole drilling issue and ensure that the resultant interpretation makes sense from a consistency standpoint. If the lab uses a drill to see if a cover can be surreptitiously removed and replaced, that's fine. If the lab is restricted (by FIPS 140-1 requirements for that level) from drilling through other parts of the housing, they should also be restricted from drilling through self-clinching (press-fit) fasteners that cannot be unfastened from the outside.

From: Marc Laroche <marc.laroche@entrust.com>
To: 140-1review@nist.gov
Subject: Proposed Reaffirmation of FIPS 140-1
Date: Wed, 20 Jan 1999 12:17:06 -0500
X-Mailer: Internet Mail Service (5.5.1960.3)

> The purpose of this message is to respond to NIST's request for comments
> in support to five-year review of the FIPS 140-1 standard.
>
> Overall, Entrust Technologies is satisfied with the current FIPS 140-1
> standard and validation program, although we recognize that the standard
> could certainly be improved. We consider that NIST and CSE have been very
> effective in providing timely clarifications and justifications as
> required, which has prevented issues with FIPS 140-1 from becoming
> unresolvable obstacles.
>
> We would like to suggest that these clarifications that NIST and CSE have
> been publishing as "Implementation Guidance for FIPS 140-1 and the
> Cryptographic Module Validation Program" be in fact used to update FIPS
> 140-1. Sections of the standard should be re-written or augmented to
> include the information contained in this document.
>
> We also believe that FIPS 140-2 should describe environmental requirements
> (e.g. Physical Security and Operating System Security) using the CC
> language, i.e. CC Security Functional Requirements (SFRs) and CC Assurance
> components. Each FIPS 140-2 levels would include its own set of
> requirements. In most cases, cryptographic modules are not commercially
> available products per say; they are usually embedded in security products
> or systems which in turn needs to be evaluated to obtain a security
> assurance level. Using CC terminology in FIPS 140-2 would facilitate the
> integration of FIPS 140-2 validated cryptographic modules in CC
> evaluations, thus making it easier for developers, evaluators, certifiers
> and accreditators.
>
> Entrust Technologies is a strong supporter of the FIPS 140-1 program and
> as such, we would like to make ourselves available to participate in any
> FIPS 140-2 discussions or workshops that may come.
>
Regards,

> Marc
> ---
> Marc Laroche
Manager, Product Evaluation
> Entrust Technologies

Tel.: (613) 247-3446 * Fax: (613) 247-3450
> Entrust Validation String

Mark your calendar now for Entrust
June 14-17, Hyatt Grand Cypress Resort, Orlando, FL

From: Burt Kaliski <burt@rsa.com>
To: "'140-1review@nist.gov'" <140-1review@nist.gov>
Subject: RSA Laboratories' comments on FIPS 140-1
Date: Thu, 21 Jan 1999 10:41:57 -0800
X-Mailer: Internet Mail Service (5.5.2232.9)

January 21, 1999

Information Technology Laboratory
ATTN: Review of FIPS 140-1
Bldg. 820, Room 562
National Institute of Standards and Technology
Gaithersburg, MD 20899

Ladies and Gentlemen:

As the division that coordinates standards development activities for both RSA Data Security, Inc. and its parent company Security Dynamics, RSA Laboratories has a strong interest in tracking security technology standards such as FIPS 140-1. RSA Laboratories appreciates NIST's support of this initiative and the opportunity to review and comment on FIPS 140-1.

Secure implementations of cryptography are becoming increasingly important to the computer industry. At the same time, however, many implementations of cryptography are in software only, departing from the traditional view of cryptographic modules as involving dedicated hardware. Though it is expected that smart cards will become a preferred hardware-based cryptographic module, there will continue to be developments that are software only. While FIPS 140-1 goes to some length to cover software-only implementations, some further elaboration would be helpful.

RSA Laboratories therefore recommends that the applicability and/or implementation statements of the standard be revised to reflect emerging issues in the validation of software cryptographic modules. The following questions illustrate some of those issues.

* In some cases, a significant portion of a cryptographic module may be part of the operating system (i.e., outside the control of the vendor who developed the module), for instance as a crypto service provider. In such cases, the source code of significant cryptographic components may not be available for review. If the operating system vendor does not submit the crypto service provider for FIPS 140-1 validation, how would the module vendor proceed in this case?

* What if some components are dynamic, for instance a downloaded browser "plug-in"? This is addressed through module authentication, but more generally, a model should be considered where the entire module, except for some base, can be updated. Indeed, such dynamic updating of crypto components appears to be essential to respond to

vulnerabilities discovered in algorithms and protocols, avoiding for example the difficulty of replacing DES that the industry is currently experiencing.

* What constraints should be imposed on the binding between cryptographic components? For instance, in the example above, how should the module authenticate the integrity of the crypto service provider? Moreover, how should the provider authenticate the authorization of the module or other higher-level applications? FIPS 140-1 addresses these issues peripherally in terms of role-based and identity-based authentication for operators; internal authentication between components needs to be treated as well.

Related to these, we note that Level 2 is allowed for software implementations if and only if their platforms are C2 or better and are multi-user timesharing systems. Recognizing that the time-sharing platforms against which the TCSEC was written have largely been supplanted by single-user desktop workstations, the multi-user timesharing requirement essentially limits mainstream deployments of software implementations to Level 1. The relevance, timeliness, and influence of FIPS 140-1 could be enhanced if all C2 platforms were eligible to support Level 2 products.

Some specific technical comments on the current draft:

* Section 4.7. At Level 1, software modules are limited to access by one user and process at a time. Presumably, this means one "principal" as opposed to one application acting on the principal's behalf. In many cases, the user will authenticate once to the module, which will then provide services to several applications operated by the user, such as a browser and a mail program. The module will thus have more than one application calling it, but only one real user.

Also, in some implementations, there may be more than one operating system process accessing the module, for instance if the module is implemented as a shared library rather than a queued service. However, this also would seem to be within the sense of the requirements, provided that the processes are acting on behalf of the same user.

As another example, the user may authenticate as multiple identities at the same time to a given module; perhaps the user has one identity (e.g., distinguished name) for the browser and another for the mail program. While all these variations can be argued to be within the sense of FIPS 140-1 Level 1, it is important to address them specifically, similar to the concerns raised above about other software issues.

* Section 4.8.1. For random or pseudorandom number generation, it is required that all outputs be equally likely (i.e., a uniform distribution). Presumably, this is intended as an approximation, as it is not possible, even for a truly random source, to ensure absolute equality. One way of stating the approximation is in terms of indistinguishability, as is the

standard approach in theoretical cryptography. Either the number of samples required to distinguish the actual source from a uniform source should be impractically large (statistical indistinguishability), or the amount of computation required to distinguish should be impractically large (computational indistinguishability). In either case, the source will be for all practical purposes uniform, since any deviations from uniformity cannot be detected by other components of the system in any reasonable amount of time.

* Section 4.11.2. Is a self-signed certificate an acceptable method for manual-key entry for public keys, where the signature serves as an error-detection code? If so, this should be stated.

RSA Laboratories again wishes to express its appreciation for the opportunity to comment on FIPS 140-1, and looks forward to continuing to work with NIST on the development on standards for security technology.

Sincerely,

Burton S. Kaliski Jr., Ph.D.
Chief Scientist and Director

X-Sender: tygar@ux3.sp.cs.cmu.edu
X-Mailer: QUALCOMM Windows Eudora Pro Version 4.0
Date: Thu, 21 Jan 1999 12:10:20 -0800
To: 140-1review@nist.gov
From: Doug Tygar <tygar@cs.berkeley.edu>
Subject: Comments on FIPS 140-1

Gentlemen:

I am writing this e-mail note in response to your solicitation for comments on the FIPS 140-1 standard (below, I simply refer to this standard as 140.)

I have a number of comments on 140, ranging from minor quibbles to serious concerns. In this note, I am restricting myself to the most serious issues with 140, so that the comments will not get lost in the many responses I expect you to receive.

MY BACKGROUND

My name is Doug Tygar, and I am a (tenured, Full) Professor of Electrical Engineering and Computer Science at the University of California, Berkeley. I also hold an full Professor appointment in UC Berkeley's School of Information Management and Systems. Before I came to UC Berkeley, I was on the faculty of the Computer Science Department at Carnegie Mellon University for 12 years. Although I have accepted a faculty position at UC Berkeley, Carnegie Mellon has take the extraordinary step of retaining my tenured faculty position there as a faculty member on leave, in the hope that I may return. Thus, I also am a tenured Computer Science faculty member at Carnegie Mellon. Prior to my appointment at Carnegie Mellon, I received my PhD from Harvard University, and my AB from UC Berkeley.

My research specializes in innovative applications for tamper-resistant hardware. These applications include such varied activities as electronic commerce, rights management, computer security, key management, access control, file storage, and innovative operating system structures.

I only list a fraction of my honors: I received the National Science Foundation's Presidential Young Investigator Award. I am a member of the National Academy/National Research Council's Committee on Information Trustworthiness (our report "Trust in Cyberspace" was just published as a book by the National Academy Press). I serve on the INFOSEC Research Council's Information Security Science and Technology Study Group. I received research grants and contracts from the Defense Advanced Research Project Agency, from the National Science Foundation, from the National Computer Security Center, from the National Aeronautics and Space Administration, from the US Postal Service, and from numerous private companies. I am also actively working the Federal Reserve Bank System and the Federal Reserve Banks of San Francisco and Cleveland. I have been an invited speaker more than 200 locations including invited lectures at the 100th anniversary of Harvard University's Graduate

School of Arts and Sciences and the 25th Anniversary of Carnegie Mellon University's School of Computer Science, and keynote speeches at major conferences such as Very Large Databases and Principles of Distributed Computing. I have served on program committees or as program committee chair for a number of major conferences in computer security, electronic commerce, and smart cards. I write, teach, and consult actively and widely in tamper resistance, computer security, electronic commerce, and related topics.

Here is some of my research related to tamper-resistant hardware:

With my PhD student Bennet Yee, I designed, implemented, and measured an innovative operating system called Dyad which ran on tamper-resistant hardware provided by IBM. Dr. Bennet Yee is now on the faculty of the University of California, San Diego's Computer Science and Engineering Department.

With my PhD student Sean Smith, I examined the role of secure time keeping on tamper-resistant hardware. After graduating, Dr. Sean Smith first served as a postdoc at Los Alamos National Laboratory, where he was quickly offered a full-time staff position. Dr. Sean Smith is now on the research staff at IBM, where he helped to build and get the first FIPS 140-1 level 4 rating for IBM's 4758 cryptographic coprocessor.

With my PhD student Jean Camp, I investigated the policy role and innovative anonymity structures possible with the use of tamper-resistant hardware. Dr. Jean Camp is now on the faculty at Harvard University's Kennedy School of Government.

With my current PhD student Howard Gobioff and my Carnegie Mellon colleague Prof. Garth Gibson, I am investigating the role the tamper-resistant for standalone (no-server) directly attached "Network Attached Secure Disks".

I have worked with US Postal Service to develop its new "Information Based Indicia Program" standard for secure postage functions that built on 140's standards for tamper resistance (IBIP uses cryptography and a stored value device to support PC-based printing of "postage meter"-style indicia.) I have also participated in directly evaluating purportedly tamper-resistant hardware for the Postal Service. This activity has led to more than a six year long active research relationship with the US Postal Service.

I have taught about tamper-resistance and attacks on hardware at both Carnegie Mellon and UC Berkeley.

140 IS A VITAL STANDARD

Especially as innovative distributed and electronic commerce applications have grown, 140 remains an extremely vital standard. Many organizations and companies have produced what they claim is tamper-resistant hardware, but there is no way for consumers to easily evaluate these claims. I have seen many cases where hardware was produced, along with private laboratory (not NIST approved labs!) studies that claimed that the hardware was secure, but where I and my students could break the hardware in a few minutes.

However, the area of tamper resistance has come under serious attention from a variety of non-governmental sources in the last few years. For example, several university's are actively exploring the area, including my groups at UC Berkeley and Carnegie Mellon, my student's groups at their universities, Ross Anderson's group at the University of Cambridge in the United Kingdom, and Dan Boneh's group at Stanford University. Several private laboratories including Cryptography Research have actively devoted themselves to attacking tamper-resistant hardware. A number of important systems for smart cards (and other token-based devices) for electronic payment, hardware for rights management, set-top boxes, and postal functions are being deployed, and they have come under active attack. In many cases, ordinary consumers bear the loss for these systems in case of failure, so individual consumers need a way

140 is the best and only serious way for most potential system adopters to evaluate hardware security. As such it plays a vital role. Even more important, in many of the systems based on tamper-resistant hardware, ordinary consumers bear the loss in case of system failure (for example, my understanding was that this liability was born in MasterCard's testing of the Mondex system in the United States). Without 140, how could non-technical, ordinary consumers evaluate the security of purportedly secure hardware? While this is a rapidly changing field, and FIPS 140-1 definitely merits revision, it also should continue as a standard.

***Recommendation: NIST should continue to support the FIPS 140 family of standards and related testing activities, although it should continue to actively update those standards.

140 NEEDS REVISION

Because of the intense activity on tamper resistant hardware, 140 is being pushed to its limits. Innovative attacks such as those outlined by Ross Anderson and Marcus Kuhn in their "Tamper Resistance: A Cautionary Note" or the power analysis attacks discussed below require active maintenance of the 140 standard. NIST needs to be regularly informed about these advances, and to understand how 140 works in relationship to these standards.

In addition, 140 was originally intended for a fairly narrow domain -- as a security requirement for cryptographic modules. However, as outlined above, people are actively pushing on tamper-resistance for innovative applications such as electronic commerce. For example, I believe that the market and use of stored-value devices for electronic commerce will far exceed the market and use for purely cryptographic functions. It is a testimony to the authors of 140 that it is generally applicable to other domains. However, it is creaking at the edges. In the case of stored-value devices, for example, it is not clear whether the stored-value register should be zeroized if the unit is penetrated. Even worse, even basic functions, such as correctly maintaining the register, are not included in the 140 standard. As I have written about elsewhere (in "Atomicity for Electronic Commerce"), transactional issues are vital for these sorts of systems. To the degree that consumers and system designers depend on the 140 process as a fair referee to evaluate this hardware, 140 needs to be expanded.

***Recommendation: NIST should form a standing advisory board to advise NIST of emerging attacks and applications on tamper-resistant hardware, and should use that information to help guide the development of the 140 standards. In preparing for a 140-2 revision of the standards, NIST should consider new attacks and new applications, to make the standards as useful as possible.

140 NEEDS TO DEAL WITH POWER ANALYSIS

In recent work by Paul Kocher and associates at Cryptography Research, several powerful new attacks were released which measure power consumption by tamper-resistant devices. Using these techniques, Paul Kocher claims to have broken a wide variety of purportedly tamper-resistant hardware. After meeting several times with Paul and seeing demonstrations of the attack, I am convinced this claim is absolutely valid. Moreover, the power analysis attacks are elegantly simple and easy to do. For example, in my security class being taught this semester at UC Berkeley, I am asking students to study power analysis and to exercises related to power analysis attacks on hardware. While I do not think that students can perform the attacks with skill that Paul and his associates have shown, I do think they are clearly capable of doing basic simple and differential power analysis attacks. In other words, this is a real attack, that can be done by ordinary college students and graduate students in electrical engineering and computer science.

If 140 does not deal with this class of attacks, it can not be taken seriously as a standard for tamper-resistant hardware. For this reason, I strongly urge NIST to include power analysis attacks in the standard. While some NIST staff members have expressed to me concern about how this could be integrated in the standard, I do not think that it is any trickier than, for example, the environmental requirements in 140. Here is a brief schema to explain how the requirement could be tested for: manufacturers could be required to submit power traces (with a specified degree of resolution) on a fixed set of encryptions under NIST laboratory supervision. Manufactures would be required to state a minimum number of rounds of encryption to leak a key (or at which a key is not leaked) and this could be used to determine the rate of bit leakage per key. NIST labs could verify this by statistical analysis on the power traces. System support for key replacement after a number of rounds of encryption that was substantially lower than the rate of key leakage would then be required. While this is a sketchy outline, I believe that it is sufficient to illustrate that it is far less daunting to test for vulnerability to power analysis attacks than it is to test, for example, vulnerability to extreme temperature attacks.

In fact, under direction from the US Postal Service, my groups at UC Berkeley and Carnegie Mellon are developing strawman proposals for power analysis tests for USPS's Information Based Indicia Program.

Recommendation: NIST should form a group to recommend improved standards for dealing with power analysis attacks, and should plan on incorporating power analysis in a FIPS 140-2 standard.

140 LAB STRUCTURE NEEDS EXAMINATION

The way in which systems are evaluated against 140 is subject to a variety of pressures. Since labs depend on an inflow of new work for economic survival, there is pressure on the NIST-approved labs to "go easy" on the standards. The central evaluation by NIST of lab results acts a check on this, but there pressure remains nonetheless. Since a considerable portion of 140 testing depends on judgement and subjective evaluation, this is a serious risk.

Similarly, in highly competitive fields (such as postal meter applications under the 140-based IBIP program) large vendors have a strong economic interest in keeping competitors from being approved. It might be possible for a large vendor to try to pressure NIST-approved labs to "go hard" on a smaller competitor. Again, the central evaluation of NIST acts as a check on this (especially if NIST were to expand its oversight role so that it examined the reports for that were rejected as well as well as for products that were accepted), but the pressure remains nonetheless. Since the number of NIST-approved labs is quite small, this is a very real threat.

***Recommendation: NIST should examine and audit all NIST-approved labs on their reports, both positive and negative, to ensure uniform standards. NIST should ask an advisory group to suggest further way to ensure uniform, tough testing by all NIST-approved labs.

I hope that these recommendations are useful to you in your review. I would be happy to provide further information on any of the points discussed, or to help in any other way to make 140 the best possible tamper-resistance standard.

Yours,

Doug Tygar
Professor
Electrical Engineering and Computer Science
Information Management and Systems

University of California, Berkeley
102 South Hall #4600
Berkeley, CA 94720-4600

(510) 643-7855
tygar@cs.berkeley.edu

From: ryanfr@pb.com
X-Lotus-Fromdomain: PBI
To: 140-1review@nist.gov
Date: Thu, 21 Jan 1999 15:46:05 -0500
Subject: Proposed Reaffirmation of FIPS 140-1 Comments

Attached are the Pitney Bowes Inc. comments regarding the Proposed Reaffirmation of Federal Information Processing Standard (FIPS) 140-1.
(See attached file: FIPS 140-1 5 year review comments.doc)

Please feel free t contact me with any questions or comments,

Rick Ryan
Pitney Bowes, Inc.
35 Waterview Drive
Shelton, CT 06484

Phone: (203) 924-3190
Email: ryanri@pb.com

[See the following pages]

Date: January 21, 1999

To: FIPS 140-1 Review Committee

From: Rick Ryan

Subject: FIPS 140-1 Comments

Pitney Bowes has found FIPS 140-1 to be a valuable standard or accessing the security level of a cryptographic module. However, we believe that FIPS 140-1 should include the following revisions to reflect the continually evolving security threats and commercial industry security needs.

Algorithms

Either more algorithms need to be FIPS approved or a better method of dealing with non-approved algorithms needs to be developed. Currently, there are no FIPS approved public key algorithms which can be used to encrypt data. While it is acceptable for a FIPS approved device to implement algorithms which are not FIPS-approved, the cryptographic module must execute these algorithms in a non-FIPS mode. Several devices which have received FIPS certification implement additional algorithms. It is not clear to an end user whether or not these modules properly implement other FIPS security elements when operating in a non-FIPS mode. It would be helpful to have a separate category for non-FIPS approved algorithms allowing the device to still be FIPS approved. Algorithms in this category would still have to comply with other FIPS security requirements (e.g. self-test, continuous RNG test).

Split Ports

The requirement to have physically separate ports for plaintext entry of user authentication data (for FIPS level 3) needs to be modified. The form factor of many devices does not easily accommodate multiple ports (e.g. smart cards, PCMCIA cards). For these devices a logical separation of ports can achieve the desired security goals.
The intended use of the module should be taken into account when determining if separate ports are needed. A cryptographic module which resides on a network should have a separate port for entering plaintext authentication data, due to the threat of interception of that data by a third party (the authentication data could also be encrypted in accordance with FIPS 140-1). However, a smart card which is used for a building access control system has a very low risk of plaintext authentication data being intercepted. In applications such as this only a logical separation of ports should be required. The NVLAP labs should be given discretion to determine whether a separation of ports is warranted.

RNG

Currently only DES or SHA-1 based random number generators are approved. These RNG's must be seeded and, despite the "randomness" test which must be performed, there are no requirements regarding the seeding of these RNG's. When performing the RNG statistical tests there is no requirement that the RNG be "reseeded." In many implementations they are seeded with hardware RNG's already present within the cryptographic module. If the seeding process is weak the RNG will also be weak. The seeding process should be subjected to the same statistical tests as the RNG's. Also, hardware or other RNG's should be allowable provided the statistical tests specified in FIPS 140-1 are passed.

Additional Security Relevant Data Items

Many cryptographic modules protect data other than simply cryptographic keys. While these data are often spelled out in the security policy, there is no FIPS 140-1 requirement that this be the case. There should be FIPS 140-1 requirements that govern how non-cryptographic security relevant data is handled. Many items, such as electronic cash, have security requirements other than secrecy, and may not have secrecy as a requirement. A standard definition of these security requirements would help provide consumers with confidence that the device meets their needs. While this may vary from application to application, a set of guidelines should be established.

TEMPEST

Although FIPS 140-1 was not intended to address TEMPEST, events over the past year (e.g. power analysis attacks) have highlighted the need to address such issues. Since TEMPEST type attacks are no longer theoretical and do not require vast resources to perform, these issues must be addressed by a revision of the FIPS 140-1 standard.
Regards,

Rick Ryan
Pitney Bowes, Inc.
35 Waterview Drive
Shelton, CT 06484

Phone: (203) 924-3190
Fax: (203) 924-3385
Email: ryanri@pb.com

From: "Nate Jensen" <njensen@datanomix.com>
To: <140-1review@nist.gov>
Subject: Comments regarding FIPS 140-1 review
Date: Thu, 21 Jan 1999 14:44:02 -0700
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 4.72.3110.5
X-MimeOLE: Produced By Microsoft MimeOLE V4.72.3110.3
X-Info: Datanomix, Inc.

Attached is a Word document entitled "Recommendations for FIPS 140-1 Evaluation." This document is written with comments in particular respect to implications the FIPS 140-1 standard has on non-Federal Internet users. Thank you for your consideration.

Sincerely,
Nate Jensen

[See the following pages]

Recommendations for FIPS 140-1 Evaluation:

Implications of FIPS 140-1 for Public Internet Users

Nate Jensen

First Data Corporation/Datanomix

Englewood, Colorado

January 21, 1999

Implications of FIPS 140-1 for Public Internet Users

The FIPS 140-1 standard has been developed with the scope of Federal computer systems and the cryptographic modules they use. FIPS 140-1 is also used within private sector computer systems as a standard to protect sensitive business data. However, the cryptographic requirements set forth in FIPS 140-1 do not address application of its standards to public, non-Federal users. If the FIPS 140-1 requirements were to be extended to the public users of Federal Internet systems, it would be difficult if not impossible to enforce the 140-1 standard.

Implications for Internet Clients

One problem is that some of the popular Web browsers are not capable of being configured to use cipher suites that contain only FIPS certified algorithms. If all Internet clients were capable of utilizing cipher suites with only FIPS approved algorithms, it would not be reasonable to expect all users in the general public to be technically capable of configuring their browsers to utilize only FIPS compliant cipher suites.

Using Only FIPS Approved Algorithms

Enforcing the FIPS standard on public Internet users today would severely limit the number of secured/encrypted connections that occur over the Internet because not all Internet clients would be capable of using only FIPS approved algorithms.

Levels of FIPS 140-1

The FIPS 140-1 standard does not define whether a public (non-Federal) computer user accessing a Federal (Internet) site should adhere to the same level of FIPS 140-1. FIPS 140-1 evaluation should address whether the same level of FIPS 140-1 be expected of public (non-Federal) computer users accessing a Federal system.

Certain implementations of FIPS 140-1 levels 3 and 4 could involve or require the use of hardware-based cryptographic modules. Such an expectation of all Internet users accessing the given Federal Internet site would not be practical. To expect public computer users to adhere to the same level of security would severely limit the possibility of allowing the public computer user to access Federal Internet sites.

Conclusion

The reevaluation of the FIPS 140-1 standard should address the implications of expanding access of Federal Internet systems to non-Federal entities. Whether the reevaluated version of the FIPS 140 standard include such specifications is the decision of the NIST committees involved. Consideration of the FIPS 140-1 requirements and public Internet use has long-term implications and if the FIPS 140 standard cannot address these aspects, it may be beneficial to consider a newer FIPS standard that will govern the cryptographic modules of non-Federal clients accessing Federal (Internet) systems.

Original-Encoded-Information-Types: IA5-Text
UA-Content-Id: FIPS 140-1
Autoforwarded: FALSE
Priority: Normal
Importance: Normal
Sensitivity: Personal
Date: Thu, 21 Jan 1999 18:10:00 -0500
From: Wynelle Prangley <Wynelle.Prangley@usda.gov>
Subject: FIPS 140-1
To: 140-1review@nist.gov (Receipt Notification Requested)
Cc: Arnold.Bresnick@usda.gov (Receipt Notification Requested),
BARRY.WASSER@usda.gov (Receipt Notification Requested)
X-Mailer: Worldtalk (NetJunction 4.5.1-p4)/MIME

USDA has no comments and recommends reaffirming the standard.

Patrick Cain
GTE
Internetworking
10 Fawcett St, MS
12/2A
Cambridge, MA
02138

January 21, 1999

Information Technology Laboratory
ATTN: Review of FIPS 140-1
Bldg. 820, Room 562
National Institute of Standards and Technology
Gaithersburg, MD 20899

Sir/Madame:

This message is in response to your request for comments on the usefulness and/or suggested revisions to FIPS 140-1. GTE Internetworking continues to deliver products certified to FIPS 140-1 and believes that the current standard adequately addresses security issues defined when the standard was approved. However, five years after its approval, the increase in computing power and experiences with the certification process has shown that some gentle tweaking of the standard would be beneficial to users of the FIPS 140-1 certified devices. I do not believe that the theory behind building secure systems has changed enough in the past five years, or will in the pending five years, to necessitate a complete overhaul of this standard.

Although not formally speaking for GTE Internetworking, my suggested areas for improvement in FIPS 140-1 are explained below.

1. Section 4.7, Operating System Security.
The current standard requires the use of an NCSC Orange Book certified operating system when an operating system is required. As the science of operating system trustability has evolved, the U.S. Orange Book is being superceded by international efforts as in the ITSEC and Common Criteria. We feel that when rating levels are discussed within this section, equivalent ITSEC/Common Criteria based levels should also be identified. This modification would allow a vendor to develop products for the international market and still meet the stringent FIPS requirements after the completion of one, not two, costly operating system evaluations.

2. Section 4.3.3, Operator Authentication and 4.8.3 Key Entry and Output.
One of the most common techniques to satisfy the level three and four requirements for key entry is using split key technology. The current standard levies no requirements on the trustable audit requirements in the lifecycle of a key. It is our feeling that better tracking of critical keys is necessary (e.g., which key splits were used to recombine a critical private key or the fact that a key was resplit, destroyed, etc) to apportion liability amongst the different key split holders. Although this may sound like an enormous burden on a cryptographic module, a small number of very short audit messages

retained within the module boundary would allow for more accurate control and identification of rogue key operations. Although not replacing the system audit function, a module audit function could allow for more specific traceability to critical module operations.

3. Section 4.9, Cryptographic Algorithms
The standard currently states "Cryptographic modules shall employ FIPS approved cryptographic algorithms." The implication is that an approved device would ONLY use FIPS approved algorithms anywhere in its device -- irrespective of the security impact. Unfortunately, there are a number of vendor proprietary or internationally standardized algorithms that are very useful in devices. In most cases, these algorithms have no bearing on the security functions applicable to the user, but may be very beneficial to the manufacturer or system administrator. We have seen a number of products in the past that had to reduce the security of their systems because they were required (by one of the NVLAP labs but not another) to delete all but ONLY FIPS approved algorithms. We suggest a clarification to the wording in this section to allow consistency amongst the NVLAP certification labs.

Sincerely,

Patrick Cain

Date: Thu, 21 Jan 1999 16:29:38 -0800 (PST)
From: Monique Morin <morin@cory.EECS.Berkeley.EDU>
To: 140-1review@nist.gov
Subject: FIPS 140-1 comments

TO: Information Technology Laboratory / NIST
FROM: M. M. Morin (morin@cory.eecs.berkeley.edu)
DATE: January 21, 1999
RE: FIPS 140-1

My name is Monique Morin and I am currently taking computer science classes at University of California at Berkeley. I have a strong interest in computer security and have recently become aware of proposed power analysis attacks.

Power analysis attacks are based upon the fluctuations in power consumption exhibited by the hardware of a cryptographic module. The hardware behaves differently based upon the mathematical functions required by the cryptographic protocol being used. A more detailed explanation is located at the website of the company "Cryptography Research" (http://www.cryptography.com).

In reviewing FIPS 140-1, I understand that TEMPEST related attacks were considered out of scope in 1994; however, I believe power analysis attacks and related requirements should be incorporated into a revised 140-1 and the validation program.

FIPS 140-1 in its qualifications section states "The requirements are designed to protect adversaries mounting cost-effective attacks on unclassified government or commercial data (e.g. hackers, organized crime, economic competitors). The primary goal in designing an effective security system is to make the cost of any attack greater than the possible payoff." My cursory review of power analysis attacks leads me to believe that such attacks are within the purview of the standard.

As a student, I plan to explore this subject further over the next few months. Thank you for your consideration in this matter.

CEAL Comments

January 25, 1999

Cryptographic Equipment Assessment Laboratory (CEAL)

A CygnaCom Solutions Laboratory

Cryptographic Equipment Assessment Laboratory
A CygnaCom Solutions Laboratory

CYGNACOM SOLUTIONS

Introduction

The FIPS 140-1 comments that CygnaCom's Cryptographic Equipment Assessment Laboratory have made are broken down into the eleven different sections of the standard. A Miscellaneous section has also been added to discuss requirements and suggestions that may not fit into a specific section of the requirements.

Cryptographic Module Design and Documentation

Suggestion/Comment	**Requirements Affected**
• A specific format for security policies should be followed by vendors. Specifically, this will ensure that agencies interested in purchasing these devices know the exact configuration of the "FIPS mode," as well as the services available for each role in "FIPS mode." Some government agencies are not well versed in what the certification means.	AS01.07
• Operating system configuration should also be included in the security policy for a software device.	AS01.07
• Explicit Assertion, VEs, and TEs should be written to define a "FIPS mode" in the security policy.	Add New Assertions
• If a system/supports a function/service whose use would take the module out of FIPS mode, can this simply be enforced by the security policy?	General

Module Interfaces

Suggestion/Comment	**Requirements Affected**
• Whole section needs to be rewritten for software cryptographic modules.	Entire Section
• Maintenance Access Interface needs clear and explicit guidance. Some vendors currently call it to be a factory service or process. In addition, some of the responsibilities are given to the Crypto-officer role (i.e., initialization).	AS02.03 - AS02.08
• Interleaving messages are possible for some modules. The individual messages are defined as users. As these interleaved messages move through the module, there are process separation requirements. However, the Standard does not seem to address these data partition requirements.	

Roles and Services

Suggestion/Comment	**Requirements Affected**
• The show status should be made more liberal for the following two reasons: – In the packet, connectionless, and virtual connection environments, it is more important, useful and meaningful to be able to obtain the configuration information on the module as opposed to specific status at a specific or even each instance. – In today's environment, a physical display and human feedback is not meaningful for every module. It is sufficient in certain environments that the status is made available by the module to a computing element upon query posted to the module.	AS03.08
• Is remote authentication (login) acceptable? At what level and under what conditions. Perhaps is may be necessary to define manual and electronic entry of authentication information, similar to key distribution requirements or define a set of authentication requirements.	General
• Clarification needs to made between role-based authentication and identity-based authentication. There is a loophole in the Role-based/Identity-based requirement. A vendor can logically say that the identity-based requirement is met for a submitted module that has a single user and the service performed by the user specifies the role the user is in. The vendor claims to meet identity-based authentication and in fact it does not meet even for role-based. But there is nothing in the DTR to contradict the vendor's argument.	AS03.14 - AS03.17
• Must there always be two roles defined? For some devices (i.e, link encryptors, modems, and other VPN type devices), there may not be a practical need to have two roles. Initialization is done at the factory and then the only practical role is the User role. A Crypto-officer role seems to only be significant when there is a configuration element to the device. If configuration is not possible for a module, then the Crypto-officer role should not be required.	AS03.02

Finite State Machine Model

Suggestion/Comment	**Requirements Affected**
• Have other formal methods been considered?	Entire Section

Physical Security

Suggestion/Comment	**Requirements Affected**
• There is no description on how big the ventilation holes should be for a level 2 device. There is a limit on level 3 device, but not on a level 2 device. It seems that any Module can have 5" area ventilation hole and pass FIPS. There should be a limitation on specifying the size of ventilation opening at a level 2 also.	AS05.11 or AS05.21
• EFT/EFP testing procedures should be clarified. Especially voltage. The DTRs specifies large positive and negative voltage, what about amperage?	AS05.06
• How can we ensure consistency between labs for physical testing? Please consider adding this to the agenda for lab meetings.	General
• It appears that physical requirement for level 3 and level 4 are almost unachievable for a software cryptographic module. Is this intentional? Could a case be made for satisfying all level 3 requirements except for physical?	General
• Adding to the previous comment, is it reasonable to consider adding another embodiment for a module to be software?	General
• There is no specific requirement or directions for vibration testing. I.e., TE05.02.01 states that "The tester shall verify from vendor documentation that the module is at least typical commercial grade in regard to reliability and shock and vibration." Perhaps more guidance should be added for the testers.	AS05.02

Software Security

Suggestion/Comment	**Requirements Affected**
• Valid reasons (or examples of valid reasons) for using low-level languages at Level 3 should be listed.	AS06.06

Operating System Security

Suggestion/Comment	**Requirements Affected**
- We may want to relax in terms of C2 and B1 in terms of formal evaluation. For example, the things of interest to us in C2 are: TCB self-protection, process isolation, DAC, I&A, and object reuse (to zeroize keys when deleted). We could make these the requirements. Similar list could be developed for B1	AS07.05
- We should require auditing at level 2 since OS brings their own set of problems.	General - Level 2
- There should be some kind of mapping from Common Criteria certification to meet the operating system requirements.	General
- It seems odd that modules that use general-purpose operating systems have a great deal of requirements and that sophisticated module have limited authentication and audit, etc. requirements. Shouldn't the mechanisms that drove the need for "C2" for general-purpose operating systems also be applicable for complex modules that do interleaved processing (i.e., routers) have the same requirement for mechanisms?	General - Level 2
- C2 systems support DAC and when properly configured prevents Trojan Horses and acan provide identity-based authentication. It is not clear how the addition of B1 (data labeling MAC) add to a level 3's security. Trusted Path requests at a level 3 are optional.	General - Level 2

Cryptographic Key Management

Suggestion/Comment	**Requirements Affected**
- Key generation requirement (AS08.04 and IG 8.1) should probably be relaxed to include ANY random number generator's and/or pseudo-random number generators that provides equivalent randomness as the three approved methods (NIST should specify criteria for checking randomness).	AS08.04
- Requirements should be added for what we call "Key Derivation." For example, a device that uses a password that is turned into a symmetric key used to decrypt information within the device.	General

• IV generation is discussed in the Implementation Guidance. However, no requirements are stated for IV distribution. I.e., should they be encrypted when distributed electronically?	General
• Can the key archiving requirement be considered as part of the key output requirements?	AS08.20
• Manual key distribution (manual key entry/electronic key entry) and Electronic key distribution needs to be clarified.	AS08.09 - AS08.16
• Assertion 08.13 and Assertion 08.18 should be combined.	AS08.13 & AS08.18
• Does the Key destruction requirement apply to a level 4 device that zeroizes upon tamper detection? Is it required to have a key destruction service or capability?	AS08.19
• RSA keys have some generation requirements, as will future algorithms that are added. Should we expect specific key generation parameters to be included as part of FIPS 140-2?	AS08.04

Cryptographic Algorithms

Suggestion/Comment	**Requirements Affected**
• ECDSA?	AS09.01
• Explicitly state non-approved algorithms	AS09.01
• A requirement should be stated that non-FIPS approved algorithms should not be used in FIPS-mode.	General
• Should RSA be allowed for encryption/decryption for data?	General

EMI/EMC

Suggestion/Comment	**Requirements Affected**
• None, unless TEMPEST and other side channel attacks will be tested under FIPS 140-2.	General

Self-Tests

Suggestion/Comment	**Requirements Affected**
• We should strengthen the software firmware test by requiring a FIPS approved authentication technique. Assertion 07.02 states that a FIPS approved authentication technique (FIPS PUB 113 or digital signature) shall be applied to the cryptographic software within the cryptographic module. Also, in the self-tests section Assertion 11.14 states that an EDC or FIPS approved authentication technique shall be calculated on and stored with all software and firmware residing in the module. We suggest that AS11.14 be changed to match that of AS07.02 and remove AS07.02 all together (or DES MAC/digital signatures for Level 3/4 requirements).	AS11.14 & AS07.02
• Bypass self-test does not have sufficient detail as compared to the other self-test descriptions. Perhaps a separate assertion should be developed for the bypass requirement (to make it more clear for vendors). Also, we suggest making the bypass self test a conditional or power-up self-test (option to vendor).	AS11.15

• What factors or criteria does a lab use to determine a statistical random number generator test that is, "equivalent or superior randomness checking?" Does this require that labs review proofs and perform statistical analysis?	AS11.16

Miscellaneous

Suggestion/Comment	**Requirements Affected**
• We are assuming that all implementation guidance will somehow be incorporated into the Standard (via Notes or direct rewording of the requirements).	Implementation Guidance - General
• With reference to Implementation Guidance 9.2, it seems a bit silly to have a FIPS approved device that only performs SHA-1 hashing. Perhaps require that a device support at least one FIPS approved encryption or digital signature algorithm?	General
• Software devices need to be better addressed in standard and DTR.	Software General
• This is just the CEAL dreaming but require that vendor's provide information for all VEs contained in a single document.	Vendor Documentation
• In the FIPS 140-1 Standard itself, definitions for the following terms should be added in the definitions section: – Electronic key distribution – FIPS mode – Tamper detection – Tamper response – Tamper evidence – "or equivalent"	Standard
• Perhaps consider changing the review cycle from a five year period to a three year period. Technology is moving so fast, as witnessed by the number of Implementation Guidance issued, it might warrant a shorter review cycle.	General

Excerpts from *Validating a High-Performance, Programmable Secure Coprocessor*.
IBM Research Report RC21416, IBM T.J. Watson Research Center.

....

Our Experiences

....

Finite State Machine Additional confusion arose from the terminology used in software FSMs. In many parts of the academic software verification community, "state" is the configuration of the system, which is transformed by execution of code. However, the 140-1 validation process as practiced inverts these terms: "state" corresponds to execution of a portion of software, and another term must be invented for the configuration of the system that is transformed during these "states."

Even in describing the requirements, we stumble over the above-noted problem with the FIPS FSM use of the term "state." Many software verification colleagues measure verification complexity in terms of the number of system configurations, which they term "states." But the number of possible system configurations is not a function of the number of FSM-states; a system with 100 FSM-states may only have 100 possible configurations, or 2^{100}, or more. (It all depends on the size of the system state and how the FSM transitions change it). Consequently, effectively communicating the complexity of verifying software modeled with an FSM was a continual problem.

....

Experience with Algorithm Tests Overall, we lost about a month of calendar time due to unnecessary iterations between us and our evaluation laboratory trying to debug—via long distance—our code, the testing tools, and the test data. We failed at least one iteration of DSS testing because of typographic errors in the data formatting. The inexpressiveness of the DSS validation tool also proved frustrating—we also failed one iteration because, where the standard was ambiguous on some minor implementation point that was irrelevant from security and usage perspectives, we chose an option different from the option the test tool chose. (However, this latter data—the *reason* the test failed—was unavailable.)

....

Beyond FIPS 140-1

This development and validation work gave us a unique exposure to the FIPS 140-1 standard and process. One cannot go through such a process without analyzing the process itself. In this section, we quickly present some suggestions for possibly improving the standard and the validation process in its next revision, FIPS 140-2.

Not Just Crypto Boxes As we have noted, secure coprocessors are finally migrating from research prototypes to commercial products. Recent examples include the new generation of postal meters, our device, and various proposed rights-management tokens. We suspect many more will emerge.

Work in this area has long cited the FIPS 140 standard as a specification of tamper resistance—since nothing else exists. However, FIPS 140-1 was clearly aimed at only those tamper-resistant modules whose purpose was to perform some suite of cryptographic services. But in order to apply to these new generations of devices, FIPS 140 needs to be broadened to tamper-resistant modules whose purpose is something else, such as "securely load and execute various programs" or "maintain a monetary balance and modify it only under appropriate conditions."

This aim, coupled with the direction of technology, leads to a mismatch that may only grow worse. A revised standard might avoid this mismatch by generalizing the notion of what a secure module might do. For example, the standard could generalize SRDI to be not just cryptographic keys, but any data item critical to secure and correct operation of the module, and generalize the security properties that a module enforces for its SRDI beyond "keep it secret." (Natural examples already exist for integrity-only SRDIs—and requirements for currently unforeseen SRDI properties will undoubtedly emerge with new modules.) The revised standard might also generalize the notion of "users" and "officers" beyond "someone in the same room as the module." For example, it is very natural to authenticate a module service request using a public-key signature—but the signer could very well be an *organization* (e.g., PKI certificate authorities are usually not *people*) at some distant point in space and time.

Context of Module FIPS 140 intends to specify module security assurance levels. But in many cases, the security of a module depends on the broader context of its use—not just on the module itself.

For example, if a module M authenticates its officers using public-key or symmetric-key cryptography, then these officers have private keys somewhere other than module M. The revised standard might address how officers control and store these private keys—since the security of M depends on these issues.

For another example, assuring that the design of some module is tamper-resistant is meaningful only if means exist to assure some relevant set of users/officers that a particular instance of this module is genuine (meets this design) and non-tampered. How does an officer know it's really an untampered module when he first opens up the box from the factory? If a module is permitted to suspend certain protections when it is returned to a secure factory vault, how does the module itself determine when it is back in the factory? (How does the factory authenticate that this is a real, untampered module?) A revised standard could address these issues by considering broader issues of the *lifecycle* of the device, and its tamper-assurance goal. For example, it could require partitioning physical locations into "trusted" and "untrusted" sets, and then require documentation that: tamper protections are enabled before a module transitions from a trusted to an untrusted place, and remain enabled throughout the module's stay in the untrusted place; methods exist to authenticate that a genuine module is untampered whenever it transitions from an untrusted place to a trusted place; and methods exist for a "relevant party" to authenticate an untampered module as such, even in an untrusted place.

(Although not required by the standard, our architecture and our validation documentation explicitly addressed these lifecycle issues.)

Tamper Resistance for Software FIPS 140 provides various levels of assurance that a module can resist tamper. Consequently, the FIPS 140-1 process specifies various tests and rules regarding how the module *hardware* resists penetration attempts.

However, FIPS 140-1 does not specify a similar set of rules for resisting *software* penetration. Admittedly, software penetration (offense and defense) is an ever-evolving field. But (in addition to preserving the software design and verification requirements of FIPS 140-1), perhaps FIPS 140-2 might explicitly address some basic principles. For example, validation might require that the vendor demonstrate how maliciously malformed or out-of-spec input cannot compromise module security; how interruptions (such as maliciously timed power failures) cannot compromise module security; and what precautions exist to prevent compromise due to the unforeseen bugs (such as wild pointers) that almost always exist in complex software.

Since this level of implementation detail is largely orthogonal to the security architecture, it would make more sense to require this level of analysis in *addition* to the formal verification. Perhaps the highest level of FIPS 140-2 could also require resisting some degree of free-form software tiger-team attack, as FIPS 140-1 Level 4 does for hardware.

(Our FIPS 140-1 Level 4 module was developed in continual consultation with our own software penetration team; although not required, we included in our validation submission an explicit analysis documenting our module's resistance to this family of attacks.)

Software Engineering Practices History shows that security vulnerabilities in software often result from bugs, and that good software engineering practices can reduce the chance for such bugs. Consequently, we recommend that FIPS 140-2 be broadened to include more explicit assurance about software development and testing practices not explicitly related to security.

For example, FIPS 140-2 might require the vendor to use some subset of standard software engineering practices, such as documented unit testing, along with a good test harness and regression testing; code reviews; structure charts and data flow diagrams; function-point analysis; defect and resolution tracking; and source code configuration management. (We used many of these practices in the development of our module anyway.)

Low-Level Languages FIPS 140-1 requires that software be written in a high-level language, with rare exceptions. However, these exceptions did not explicitly include several areas where engineering dictates that using assembly language is the best approach.

In particular, consider module software that executes on an internal embedded processor. For initial power-on self tests, for transitions between software components before an operating system has been established, and for many components of standard operating systems, code needs to work in CPU modes that high-level languages have difficulty accommodating.

A revised standard might broaden the areas where low-level language is permitted (e.g., to explicitly include the above), but require that such portions of code be adequately pseudo-coded in the accompanying documentation (to reconcile this broadening with the need to make the code easy for the evaluation laboratory to analyze)

Random Number Generation We strongly recommend that FIPS 140-2 reflect the fact that high-quality hardware RNGs exist. If the output of a hardware RNG is still to be filtered first through a PRNG, we recommend that FIPS 140-2 at least encourage the PRNG to be reseeded as often as possible from the hardware RNG (in order to maximize the entropy). (We do this anyway.)

A “cryptographically secure RNG/PRNG” is the building block for many protocols, and users will assume that a RNG/PRNG that meets the FIPS standard is indeed cryptographically secure. A revised standard might take more steps to ensure that this is true. For example, if FIPS 140-2 broadens to include hardware RNGs and/or additional (unspecified) PRNGs, we recommend the addition of a test or requirement that provides assurance regarding the *unpredictability* of these bits. If FIPS 140-2 preserves the current 140-1 interpretation that “the only RNG is one of these three PRNGs,” we recommend dispensing with the statistical tests. (In this context, the statistical tests only measure the quality of the PRNG algorithm, which makes no sense if one is constrained to a set of approved algorithms.) Finally, a truly random source of bits will fail some of the FIPS 140-1 tests occasionally. We recommend broadening FIPS 140-2 to explicitly address this fact.

Algorithm Validation We recommend that FIPS 140-2 revisit the test tools to eliminate the unnecessary iterations that we and others have faced. Specifically, we recommend that the test tools (with source code) be available to the vendors themselves, so that they can check their own work before submitting to the validation lab. (If that is not possible, then perhaps a FIPS 140-2 authority can publish sufficient examples of *all the tests* in algorithm validation.)

Level 4 Penetration As we noted, the FIPS 140-1 Level 4, specification that “any physical penetration must be detected” has proven to be impractical to assure and test. We recommend that the FIPS 140-2 process establish a fixed printed specification for the maximum undetected penetration that is allowed, and any special conditions relevant to that penetration (i.e. conductive/non-conductive drill or probe, etc).

Level 3$\frac{1}{2}$ A vast difference exists between the physical security necessary for a multi-chip module to pass FIPS 140-1 Level 3, and the physical security necessary for FIPS 140-1 Level 4. We are concerned that Level 3 is currently too soft, but Level 4 may be to difficult/costly for applications of low to moderate value.

We recommend that FIPS 140-2 fill the gap between Level 3, where simply potting the unit may fully suffice as physical security, and Level 4, where the module must detect and respond to virtually any penetration. To this end, we propose a “Level $3\frac{1}{2}$” tamper detection envelope as in FIPS 140-1 Level 4, but with less stringent requirements. For example, if Level 4 ends up with a maximum sized penetration detection requirement of X, then Level $3\frac{1}{2}$ should have a maximum sized penetration detection requirement of approximately $10X$ to $100X$, and a significant reduction of the stringency of testing. This will permit designers to produce a good, full-featured, design without the extreme manufacturing requirements that FIPS 140-1 Level 4 now entails. (Rather than adding a new level, another alternative might be to increase the physical security requirements of FIPS 140-2 Level 3 to those described here for Level $3\frac{1}{2}$.)

Power Analysis One often encounters reluctance in discussing *power analysis* due its rumored part of classified TEMPEST. However, since power analysis has become a well-known public topic, a revised standard should have a clear specification about EM leakage and how testing will be performed (as with the current EMI requirements), or a statement that this is beyond the scope of FIPS 140. (However, given the success of power attacks, it seems that it should be included somewhere in the rubric.)

Terminology We also recommend that a revised standard clarify two areas of potentially confusing terminology.

- As noted above, the use of “state” in FIPS FSMs needs to be distinguished the use of “state” by the software verification community.
- FIPS 140-1 requires *role-based authentication* at the lower levels and *identity-based authentication* at the upper levels. The relatvely recent security research area of *role-based access control (RBAC)* is similar to the former in name. However, in content, RBAC is sufficiently similar to the latter (basing access control on both the identity and the role of the subject) that colleagues familiar with RBAC would sometimes transpose the FIPS 140-1 terms.