# *We are Here to Help:*
# *How FIPS 140 Helps (and Hurts) Security*

# *Agenda*

- Who Am I?
- Background
- What is FIPS 140?
- How the validation process works
- Look at the Requirements
- Best/Worst of the Requirements
- What does the future hold?
- Closing/Q&A

# *Who is l0stkn0wledge?*

- Work directly with FIPS 140
  - Over five years experience
  - Seen hundreds of various implementations
- Outside Interests
  - Programmer
  - Lock picker
  - Security Enthusiast

# *Why am I Here?*

- Want to shine a new light on security standards
- Standards often maligned by people as meaningless
  - I suggest they are a good starting point
  - Some guidance better than none at all
- Standards don't protect against everything
  - Standards become dated take long to maintain
  - Enforcement is still on the administrator or end-user
  - Can provide a false sense of security

# *What is FIPS 140?*

- Federal Information Processing Standard 140
  - Defines requirements for cryptographic systems for use in sensitive government systems
- Cryptographic Module Validation Program (CMVP)
  - National Institute of Standards and Technology
  - Communications Security Establishment of Canada
- Has begun seeing acceptance in other non-government arenas

# *Past, Present, and Future of FIPS 140*

- Previous revision was FIPS 140-1
  - Originally published in 1994
  - Items tested under this standard are still valid
- The current standard if FIPS 140-2
  - Originally published in 2001
- The future is with FIPS 140-3
  - Currently in draft form, publishing date unknown
  - Drafting of the standard began in 2005

# *How Does the Process Work?*

- Validations are handled by three parties
  - Product vendors
  - Accredited Labs (Over 15 labs exist)
  - CMVP (both NIST and CSEC)
- Number of labs leads to variance in the testing process
- Government reviews lab reports and issues certificates

# *Diving into the Requirements*

- Three key components to FIPS 140-2
  - FIPS 140-2 Standard
  - FIPS 140-2 Derived Test Requirements (DTR)
  - FIPS 140-2 Implementation Guidance (IG)
- Requirements are divided into eleven sections
- Four increasing levels of security defined
- All documents are available from NIST
  - http://csrc.nist.gov/groups/STM/cmvp/standards.html

# *FIPS 140-2 Standard*

- The core of FIPS 140
    - Original document from which the other two are derived
- Defines the requirements of the standard and the terminology used
- The document can sometimes be vague and open to interpretation

# *Derived Test Requirements*

- Much longer document that details required information
- Organized into Assertions (AS)
    - Direct statements taken from the standard
- Each AS may contain:
    - Vendor Evidence (VEs)
        - Documentation and implementation required from vendors
    - Tester Evidence (TEs)
        - Requirements of documentation review and testing for the labs

# *Implementation Guidance*

- Smallest of the documents
- Intended to provide clarification of other documents
- Supposedly cannot introduce new requirements
    - This doesn't really hold true
- Ties back to both the Standard and the Derived Test Requirements

# *Document Mapping*

generation, and is contained within a defined cryptographic boundary. A cryptographic module shall implement at least one Approved security function used in an Approved mode of operation. Non-Approved security functions may also be included for use in non-Approved modes of operation. The operator shall be able to determine when an Approved mode of operation is selected. For Security Levels 1 and 2, the cryptographic module security policy may specify when a cryptographic module is performing in an

**AS01.03: (Levels 1, 2, 3, and 4) The operator shall be able to determine when an Approved mode of operation is selected.**

**Required Vendor Information**

VE01.03.01: The vendor provided nonproprietary security policy shall provide a description of the Approved mode of operation.

## 1.2 FIPS Approved Mode of Operation

| | |
|---|---|
| Applicable Levels: | *All* |
| Original Publishing Date: | *03/15/2004* |
| Effective Date: | *03/15/2004* |
| Last Modified Date: | *09/12/2005* |
| Relevant Assertions: | *AS01.02, AS01.03 and AS01.04* |
| Relevant Test Requirements: | *TE01.03.01-02 and TE01.04.01-12* |
| Relevant Vendor Requirements: | *VE01.03.01-02 and VE01.04.01-02* |

# *Eleven Sections of Security*

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

# *Take Out Documentation Requirements*

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

# *Cryptographic Module Specification*

- Defines the approved behavior of the validated module
- At Level 1 and 2, the behavior is enforced by user configuration.
    - Potential for errors to be injected in the method
    - Policies can be inconsistent and vague
- At Level 3 and 4, the behavior is enforced through configuration.
    - Stronger restriction but can be limiting to users

# *Cryptographic Module Ports and Interfaces*

- Views the module as a black box
- Defines requirements for types of data flow
- At Level 1 and 2, no physical or logical separation of critical data
- At Level 3 and 4, physical or logical separation of critical data entry/output. Plaintext keys entered via "trusted path" or directly attached cable.

# *Roles, Services and Authentication*

- The name says it all
- At Level 1, no authentication
- At Level 2, role-based authentication
  - No accountability
  - Password lengths can be enforced through policy
- At Level 3 and 4, identity-based authentication
  - Users are uniquely identified and credentialed
  - Password requirements are system enforced

# *Password Requirements*

- Fall well short of required security
  - 1 in 1,000,000 chance of success
    - Met by a simple 4-character alphanumeric password
    - No restriction on types of passwords
  - 1 in 100,000 chance of multiple successes
    - Typically enforced via lockout
    - Ignores long-term attacks, requirement based on one minute
- The future might be brighter (more to come)

# *Physical Security*

- Not applicable to software modules
- Requirements divided by module embodiment
    - Single chip, multi-chip standalone, multi-chip embedded
- No physical security at Level 1
- At Level 2, opacity and tamper evidence
- At Level 3, tamper response
- At Level 4, tamper detection

# *What is Opacity?*

- Subjective requirement on visibility of system internals
- Ventilation can be tricky for many networking modules
- The interpretation has changed over time
    - Previously seeing make/manufacture of components was required
    - Now it seems even profile and outline of components is sufficient visibility

# *Opacity Examples*

# *Tamper Evidence and Response*

- At Level 2, it must be apparent an attacker compromised the module
  - Limited testing makes this a weak requirement
  - Labs cannot “add new materials”
- At  Level 3, the module must respond to tamper if doors/covers removed
  - Stronger requirement for modules with doors/covers
  - Requires keys to be zeroized and includes requirements for powerless zeroization

# *Operational Environment*

- At Level 1, “single-user mode”
  - Definition has changed over time
  - Original definition is unrealistic
- At Level 2+, the requirement for CC validated operating systems
  - Greatly limits the platforms that can be supported
  - Questionable improvement of security over Level 1

# *Cryptographic Key Management*

- Random Number Generation
- Key Generation
- Key Establishment
- Key Entry/Output
    - Only requirements that varies across levels
- Key Storage
    - Requirements are mostly meaningless
- Key Zeroization

# *Random Number and Key Generation*

- Requirements for approved RNGs
  - Only deterministic RNGs are listed as approved
- Symmetric key generation just makes use of approved RNGs
- Asymmetric key generation must follow approved methods
  - Methods are described in FIPS 140-2 Annex A
  - Currently includes FIPS 186-2/3 and ANSI X9.31

# *Key Establishment and Entry/Output*

- Requirements vary by distribution method
- Manual Distribution
    - Largely impractical but relatively secure methods
        - Secure Carrier, Key loader, tokens, etc.
- Electronic Distribution
    - Keys over unsecured media (LAN, WAN, etc.)
        - TLS, SSH, Diffie-Hellman
- Manual distribution can be plaintext at low levels
- Electronic distribution is always encrypted

# *Key Storage and Zeroization*

- No requirement for the form of stored keys
- Other requirements for storage are vague at best
  - “Association” of key and “entity”
- Key zeroization is simply overwriting of keys
  - Using 0's, 1's or random data
  - This service needs to exist for all plaintext keys
  - Can be performed procedurally, doesn't need to be automatic (except for tamper at Level 3/4)

# *Self-Tests*

- Power-up Self-Tests
  - Health checks of the approved algorithms
  - Integrity tests for firmware/software
- Conditional self-tests
  - Performed on certain operations
  - Continuous RNG Test
  - Pairwise consistency test
  - Firmware load test
  - Bypass Test
  - Manual Key Entry Test

# *Best and Worst of the Requirements*

**Best**

1. Enforcing stronger algorithms
2. Physical security at higher levels
3. Bypass tests

**Worst**

1. Limitations on physical security testing
2. Limited zeroization requirement
3. Hardware centric
4. No key storage protection required.
5. Ignorant of side-channel attacks

# *The Future is Yet to Come*

- New revision of the standard is being drafted
  - FIPS 140-3, over 7 years in development
- New requirements when (if) available:
  - Authentication enforced by module, no more end-user control over password length, format, etc.
  - Side-channel testing requirements at higher levels, at a minimum for single-chip modules
  - Improved zeroization requirements, limitations of procedural zeroization

# *The Future is ???*

- Unclear, the timeline has been changed before
- Best guesses are 2012/2013
- New requirements analysis is purely speculative
    - Current public draft is dated
    - Newer NIST internal drafts likely have some changes
- Improvement over FIPS 140-2, still not perfect

# *Summary*

- FIPS 140-2 provides some good requirements that can improved upon baseline security
- While it is a good first step, it doesn't guarantee you are any safer
- Recommend incorporating some of the good into projects

# *Important Links*

- http://csrc.nist.gov/groups/STM/cmvp/
- http://csrc.nist.gov/groups/STM/cavp/
- http://csrc.nist.gov/groups/STM/cmvp/standards.h
-

# *Q&A*