National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

FIPS 140-2
Cryptographic Modules

Ken Lu

Communications Security Establishment

CMVP Symposium 2004

14 September 2004

$E = MC^2$

E – Energy

M – Motivation

C – Capability

C – Cash

Presentation Outline

- FIPS PUB 140-2 Security Requirements for Cryptographic Modules
- Derived Test Requirements
- Implementation Guidance

FIPS 140-2
4 Security Levels

- Level 1 – The lowest level of security
- Level 2 – Adding more security to Level 1
- Level 3 – Adding more security to level 2
- Level 4 – The highest level of security

FIPS 140-2
11 Requirement Areas

1. Cryptographic Module Specification
2. Cryptographic Module Ports and Interfaces
3. Roles Services and Authentication
4. Finite State 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 Boundary

Section 4.1

A Cryptographic boundary shall consist of an explicitly define perimeter that establishes the physical bounds of a cryptographic module.

Physical Security

Section 4.5

A cryptographic module shall employ physical security mechanisms in order to restrict unauthorized physical access to the contents of the module and to deter unauthorized use or modification of the module when installed.

Physical Security (Cont.)

Section 4.5

3 Physical embodiments:

- Single-chip cryptographic modules
- Multiple-chip embedded cryptographic modules
- Multiple-chip standalone cryptographic modules

- Software module is not subject to physical security requirements when it is solely protected by the host platform.
- Firmware modules, IG 1.3

Physical Security (Cont.)

Section 4.5 Table 2

- Level 1 – Production-grade components
- Level 2 – Evidence of tampering
- Level 3 – Tamper response and zeroization circuitry
- Level 4 – EFP or EFT for temperature and voltage

FIPS Cryptographic Module

Section 4.1

A (FIPS) cryptographic module shall implement at least one (FIPS) Approved security function and used in an (FIPS) Approved mode.

FIPS Approved Security Functions

Annex A

4 FIPS-approved symmetric key algorithms

- Advanced Encryption Standard (AES), FIPS 197
- Skipjack Algorithm, FIPS 185 (EES)
- Data Encryption Standard (DES), FIPS 46-3
- Triple-DES, FIPS 46-3

FIPS Approved Security Functions (Cont.)

3 FIPS-approved algorithms for digital signatures

- Digital Signature Algorithm (DSA), FIPS 186-2
- RSA (as specified in ANSI X9.31)
- Elliptic Curve DSA (ECDSA; ANSI X9.62)

FIPS Approved Security Functions (Cont.)

Secure Hash Algorithms (SHA), FIPS 180-2

- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

FIPS Approved Security Functions (Cont.)

Message Authentication Code (MAC)

- DES MAC and Triple-DES MAC
- Enhanced Security DES MAC
- Keyed-Hash (HMAC), FIPS 198
- FIPS 113

FIPS Approved Security Functions (Cont.)

- Random Number Generation
  - FIPS 186-2 appendix 3.1 and 3.2
  - ANSI X9.31
  - ANSI X9.62
- Symmetric Key Establishment
  - AES Key Wrap Specification (Draft)
  - Key Management using ANSI X9.17, FIPS 171

FIPS Mode of Operation

Non-Approved security functions may also be included for use in Non-Approved modes of operation

Level 1 and 2

Security Policy may specify when a (FIPS) cryptographic module is performing in an (FIPS) Approved mode of operation

Level 3 and 4

A (FIPS) cryptographic module shall indicate when an (FIPS) Approved mode of operation is selected

FIPS Mode of Operation (Cont.)

Non-Approved security functions may be used in Approved modes of operation

Asymmetric Key Establishment Techniques

- Diffie-Hellman
- EC Diffie-Hellman
- Key Wrapping using asymmetric keys
- MQV
- EC MQV

Key Establishment Protocols

- TLS
- IPSEC

Cryptographic Key Management

Section 4.7

Secret keys, private keys, and Critical Security Parameters (CSP) shall be protected within the cryptographic module from unauthorized disclosure, modification, and substitution

Public keys shall be protected within the cryptographic module against unauthorized modification and substitution

Cryptographic Key Management (Cont.)

Lifecycle

- Key generation
- Key establishment
- Key distribution
- Key entry/output
- Key storage
- Key zeroization

Cryptographic Key Management (Cont.)

Secret and private keys may be manually entered or outputted

Level 1 & 2

in plaintext form

Level 3 & 4

- in encrypted form
- using split knowledge procedure

Ports and Interfaces

Section 4.2

4 Logical Interfaces

- Data input interface
- Data output interface
- Control input interface
- Status output interface

Ports and Interfaces (Cont.)

Plaintext cryptographic keys, CSPs

Level 1 and 2

may be input / output via shared physical or logical ports and interfaces

Level 3 and 4

– Shall be directly entered separate physical or logical interface using trusted path

Roles, Services and Authentication

Section 4.3

Roles

- User Role
- Crypto Officer Role
- Maintenance Role
- Other Roles

Roles, Services and Authentication (Cont.)

Services

- Show Status
- Perform Self-Tests
- Perform Approved Security Function
- Bypass
- Other Services

Roles, Services and Authentication (Cont.)

Operator Authentication

Level 1

- Not required authentication mechanisms

Level 2

- Role-based authentication

Level 3 & 4

- Identity-based authentication

Operational Environment

Section 4.6.1

Operating System

- Level 1 – Single operator mode of operation
- Level 2 – Protection Profile in Annex B evaluated CC EAL2
- Level 3 – Protection Profile in Annex B evaluated CC EAL3
- Level 4 – Protection Profile in Annex B evaluated CC EAL4

Self Test

Section 4.9

Power-Up Tests

- Cryptographic algorithm test
- Software/Firmware integrity test
- Critical function test

Self Test (Cont.)

Conditional Tests

- Pair-wise consistency test
- Software/Firmware load test
- Continuous RNG test
- Bypass test

Finite State Model

Section 4.4

State transition diagram/table

- Power on/off states
- Crypto officer states
- Key/CSP entry states
- User states
- Self-test states
- Error states
- Bypass states
- Maintenance states

Mitigation of Other Attack

Section 4.11

The attacks outside of the scope of the standard

- Power analysis
- Timing analysis
- TEMPEST

Electromagnetic Interference/ Electromagnetic Compatibility EMI/EMC

Section 4.8

Level 1 & 2

Conform to 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e. for business use)

Level 3 & 4

Class B (i.e. for home use)

Design Assurance

Section 4.10

- Configuration Management
- Delivery and Operation
- Development
- Guidance Documents

Security Policy

Appendix C

Specification of the cryptographic security

- Security rules derived from FIPS 140-2
- Security rules imposed by the vendor

$E = MC^2$

E – Energy

M – Motivation

C – Capability

C – Cash

Easy Questions?