

FIPS Overview

Chong Chee Wah
MD & Founder
Clearbridge InfoSec



Agenda

- FIPS Overview
- FIPS Security Levels
- FIPS Documentations
- FIPS & CC

FIPS Overview

Federal Information Processing Standards
Publication 140-2 (FIPS PUB 140-2)

**Security Requirements for Cryptographic
Modules**

FIPS Overview

Applicable:

- Federal Agencies (US and Canada)
- Use cryptographic-based security system
- To protect sensitive information
 - Sensitive but unclassified information
- In computers and telecommunication systems

FIPS Overview

CMVP:

- Cryptographic Module Validation Programme
- Validates the crypto module to FIPS 140-2
- Established by US (NIST) and Canadian Govt (CSE)
- Under CMVP:
 - Vendors use independent accredited labs
 - Labs are accredited by National Volunteer Laboratory Accreditation Programme (NVLAP)

FIPS Overview

Areas covered:

- Secure Design & Implementation of Crypto Module
 - CM specifications, ports & interfaces
 - Roles, services and authentication
 - Finite state model
 - Physical protection
 - Operational environment
 - Key management
 - EMI/EMC
 - Design Assurance & Mitigation against other attacks

FIPS Security Levels

Security Levels:

- 4 Security Levels:
 - Increasing and quantifiable:
 - Level 1 (lowest) to Level 4 (highest)
- In Future 140-3:
 - 5 levels

FIPS Security Levels

FIPS 140-2 Level 1:

- Basic level:
 - No physical protection mechanism
 - Production grade components
 - Software & Firmware of CM could run on general purpose computing platform with unevaluated OS
 - Suited for low level security applications where there are other security controls in place

FIPS Security Levels

FIPS 140-2 Level 2:

- Enhances physical protection:
 - Tamper evidence – seals or pick-resistant locks
- Min – role-based authentication
- Software & Firmware of CM could run on general purpose computing platform with OS:
 - Evaluated to CC EAL 2
- Highest level for Software-based products

FIPS Security Levels

FIPS 140-2 Level 3:

- Enhances physical protection:
 - Tamper resistance – detect and respond to tampering
 - Strong enclosures or anti-tampering circuitry
- Min – identity-based authentication
- Software & Firmware of CM could run on general purpose computing platform with OS:
 - Evaluated to CC EAL 3
 - Meets PP with added trusted path requirements
- Physically separated ports : CSP

FIPS Security Levels

FIPS 140-2 Level 4:

- Enhances physical protection:
 - Complete envelope around CM – anti-tampering
 - Detect against Voltage / Temp fluctuations - zeroise
- Min – identity-based authentication
- Software & Firmware of CM could run on general purpose computing platform with OS:
 - Evaluated to CC EAL 4
- Physically separated ports : CSP

FIPS Documentation

- Appendix A:
 - Summary of Documentations required
 - Checklist
- Covers all 10 areas under the security requirements

FIPS Documentation

- Crypto Module Specifications:
 - Specs for all software, hardware, firmware of components in crypto module
 - Specs for crypto boundary around these components
 - Description of physical config of CM
 - Specs for all physical ports & logical interfaces
 - Specs for all manual or logical controls of CM
 - Lists all approved and non-approved security mechanisms and their modes of operations
 - Specs for design of all software, hardware and firmware components

FIPS Documentation

- Crypto Module Specifications:
 - Block diagrams of all components, interconnects:
 - Include microprocessors, i/p & o/p buffers
 - control buffers, working memory, program memory
 - Key storage, PT/CT buffers
 - Specs for all security related information:
 - Secret & private crypto keys
 - Authentication data
 - CSPs
 - Specs for CM security policies

FIPS Documentation

- Self Tests:
 - Specs for self tests:
 - Power-up self tests
 - Conditional self tests
 - Specs for error states when self-tests fail:
 - Necessary actions to exit error state and resume opn
 - Specs for all security functions critical to conduct of power up and conditional tests
 - Specs for bypass mechanisms (if implemented), logic and switching procedures

FIPS & CC

- FIPS 140-2:
 - Test Crypto Module against a defined set of security requirements:
 - Covers a wide range – sec functions, crypto algo etc
 - Very specific concern on crypto implementations
- CC:
 - More generic security evaluation of IT Systems
 - Which may include crypto modules
 - But not as detail as FIPS for crypto:
 - Checking for performance as claimed

FIPS & CC

- Trend:
 - Achieve CC certification for the IT products
 - For specific crypto module:
 - Achieve FIPS certification
- NVLAP:
 - Most testing labs perform both CC and FIPS testing
 - Requirements on personnel is similar:
 - Technical professionals – competent, experience
 - Highly skilled

Clearbridge InfoSec

- Clearbridge InfoSec:
 - Independent Information Security Consultancy Firm
 - Offers high value-add & niche consultancy services
- Our Strengths:
 - Technical Expertise
 - Independent
 - Experience
 - Trusted
 - Well-plugged in – Local Govt Requirements

Clearbridge InfoSec

- Consultancy Services
 - Sec Strategic Planning
 - Sec Arch & Design
 - Sec Risk Assessment
 - Sec Framework Dev
 - Sec Policy Dev
 - Sec Standard Dev
- Training Services

- Assurance & Assessment Services
 - Security Testing
 - Vulnerability Assessment
 - Product Evaluation
 - Sec Std-based testing

The End



Contact Information:
cheewah@clearbridge-infosec.com