



From FIPS 140-2 to CC

Yi Mao

PH.D. CISSP, PCI QSA

atsec Information Security Cooperation

www.atsec.com

yi@atsec.com

Agenda



- A secure product from the CC perspective
- A secure product from the FIPS 140-2 perspective
- The common security checkpoints in CC and FIPS 140-2
- Viewing FIPS 140-2 as a pseudo Protection Profile (PP)
- The benefits gained from a FIPS 140-2 certified Cryptographic Module (CM)
- Conclusion



A Secure Product from the CC Perspective

About the **Product**



What is the TOE to be evaluated?

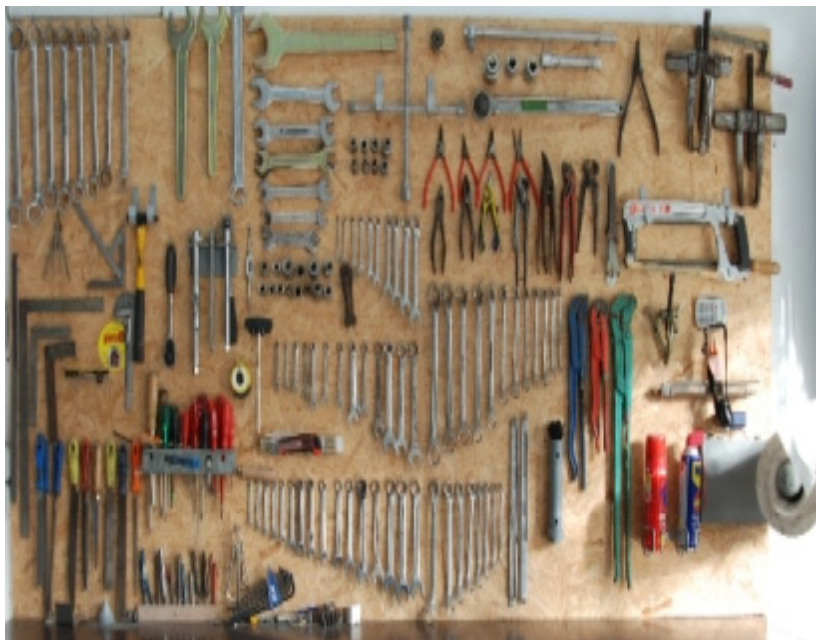
E.g.



About the **Process**



Is the development process well controlled?



VS.



About the Environment



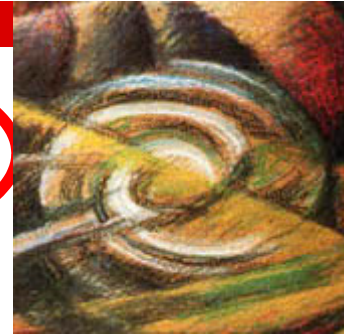
Where and how is the TOE to be used?
Put any restrictions in the ECG.



VS.

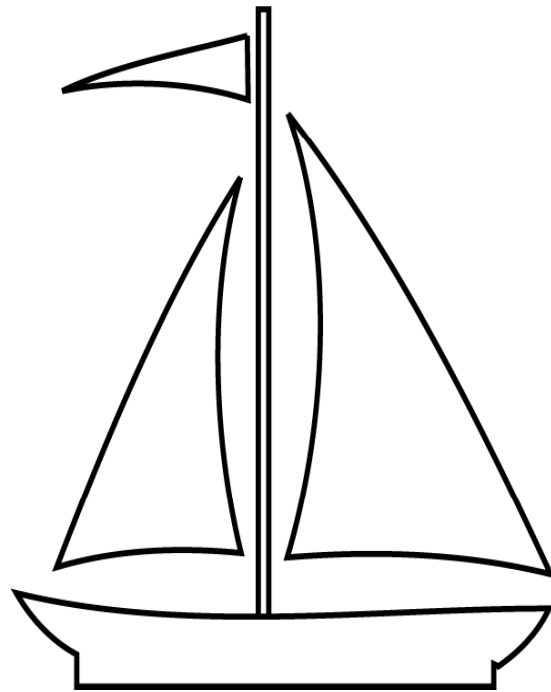


Inspecting the Product **Details**



Is the design secure?

Does the implementation reflect the design?



A Secure Design Means ...



- A well-defined external interface
 - TSFI
- A high-degree of modularity
 - TOE decomposed into components
 - A component decomposed into modules
- Identifiable security components/modules/functions
 - Separation of security enforcing/supporting functions from security non-interfering ones
- Protecting itself against interference, tampering and bypass
 - TOE protection
- Protecting TSF data and user data from unauthorized disclosure and modification
- Vulnerability analysis

Security Functional Requirements

(from the CC V3.1 Part II)



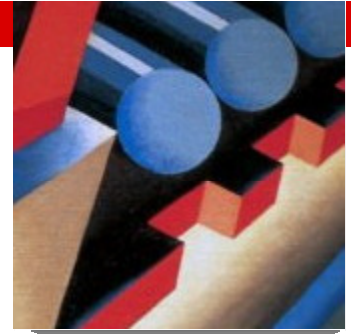
1. FAU (Security Audit)
2. FCO (Communication)
3. FCS (Cryptographic Support)
4. FDP (User Data Protection)
5. FIA (Identification and Authentication)
6. FMT (Security Management)
7. FPR (Privacy)
8. FPT (Protection of the TSF)
9. FRU (Resource Utilisation)
10. FTA (TOE Access)
11. FTP (Trusted Path/Channels)

Mapping to Basic Security Concepts

(from the CBK for CISSP Certification)



- Confidentiality: FCS, FDP, FTP
- Integrity: FCS, FMT, FPT
- Availability: FRU
- Accountability: FAU, FIA
- Privacy: FPR
- Identification: FIA
- Authentication: FIA
- Authorization: FTA
- Auditing: FAU
- Nonrepudiation: FCS, FCO



A Secure Product From the FIPS 140-2 Perspective



FIPS 140-2 and CMVP



- FIPS 140-2 is the current version of the NIST (National Institute of Standards and Technology) and CSEC (Communications Security Establishment Canada) mandatory standard that specifies the security requirements for Cryptographic Modules, and is applicable to all federal agencies in the US and the Government of Canada that use cryptographic-based security system.
- Cryptographic Module Validation Program (CMVP) is a joint effort between NIST and CSEC that oversees the FIPS 140-2 conformance through a module validation process.

A Birds-eye View of FIPS 140-2



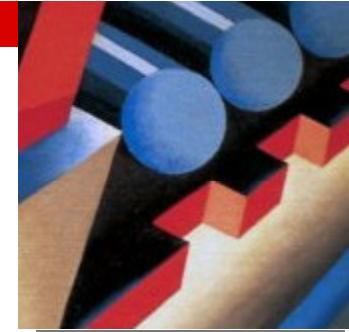
- FIPS 140-2 security requirements cover 11 areas.
- For each area, a CM receives a security level rating (1-4, from lowest to highest) depending on what requirements are met.
- An overall rating is issued for the CM that is the minimum of the independent ratings received in all areas.
- FIPS 140-2 annexes specify approved security functions, protection profiles, random number generators, and key establishment techniques.
- CM validation testing is performed using the Derived Test Requirement (DTR) for FIPS 140-2.
- The CM must implement at least one FIPS-Approved security function. The involved approved cryptographic algorithms are tested under Cryptographic Algorithm Validation Program (CAVP).

Security Areas Covered in FIPS 140-2

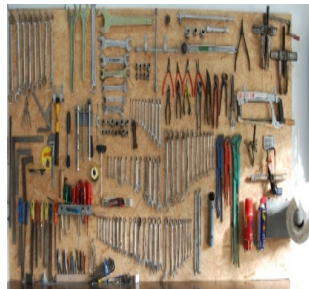


1. Cryptographic Module Specification
2. Cryptographic Module Ports and Interfaces
3. Roles, Services, and Authentication
4. Finite State Model
5. Physical Security
6. Operational Environment
7. Cryptographic Key Management
8. Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)
9. Self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

Mapping to Product/Process/Environment



Module Specification, Port and Interface, Roles/Services and Authentication, FSM, Physical Security, EMI/EMC, Key Management, Self-Tests, Mitigation of Attacks



Design Assurance



Operational Environment

A Secure Design Means ...



- A well-defined external interface
 - Port and Interface
- A high-degree of modularity
 - Module Specification, FSM
- Identifiable security components/modules/functions
 - Separation of cryptographic functions from others
- Protecting itself against interference, tampering and bypass
 - Physical Security, Self-Tests
- Protecting CSPs (Cryptographic Sensitive Parameters) from unauthorized disclosure and modification
 - Roles, Services, and Authentication, Key Management
- Vulnerability analysis
 - Mitigation of other attacks

Requirements for Key Management

(from the FIPS 140-2 DTR Chapter 7)



- General Key Protection Mechanism
- Random Number Generators
- Key Generation
- Key Establishment
- Key Entry and Output
- Key Storage
- Key Zeroization

All of the requirements reflect the well-known CIA security concepts.



The common checkpoints in CC and FIPS 140-2

Counterparts between CC and FIPS 140-2

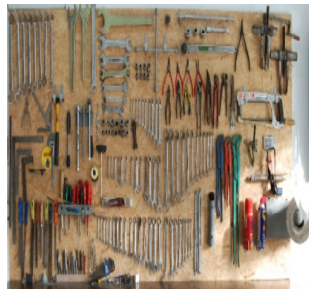


CC	FIPS 140-2
Target of Evaluation (TOE)	Implementation under Test (IUT) Cryptographic Module (CM)
Security Target (ST)	Security Policy (SP)
Security Functions	Cryptographic security functions
TOE Security Function (TSF) data and user data	Keys and Cryptographic Sensitive Parameters (CSPs)

A Common Tripod Strategy of Product-Process-Environment



Evaluate the design and implementation of a CM/TOE: what is it and how does it work?



Check its development process: how is it made?



Inspect its operational environment: how is it to be used?

Same Set of Questions Addressed



- What is the scope and boundary of CM or TOE?
- Does it have a well-defined external interface?
- Does it have a high-degree of modularity?
- Does it have identifiable security functions?
 - (e.g. authentication, authorization, access control, data encryption)
- How does it protect itself against interference, tampering and bypass?
- Does it meet the data (TOE assets vs. FIPS CSP) protection requirements?
 - protection against unauthorized disclosure/modification/ unauthorized substitution of data
- Are there any vulnerabilities? What are the countermeasures?
 - Vulnerability analysis in CC vs. Mitigation of other attacks in FIPS

Assuring the Data Protection



Requirements in FIPS 140-2	SFRs in CC
Roles, Services, and Authentication Key Storage	Access control policy and functions (FDP_ACC and FDP_ACF)
Key Entry Key Exit	Import from outside of the TOE (FDP_ITC) Export from the TOE (FDP_ETC)
Key Generation Key Establishment Cryptographic functions	Inter-TSF user data confidentiality transfer protection (FDP_UCT) Inter-TSF user data integrity transfer protection (FDP_UIT)
Key Zeroization	Residual information protection (FDP_RIP)



Viewing FIPS 140-2 as a Pseudo Protection Profile

Relating FIPS 140-2 to CC



In reality:

- FIPS 140-2 is a standalone standard distinct to CC family standards.
- When the operational environment of a CM is modifiable, the operating system requirements of the CC are applicable at FIPS Security Levels 2 and above.

The analysis shows:

- Although FIPS 140-2 is specialized to address the security requirements for the cryptographic modules, it has much in common with CC.

Possible comparisons:

- FIPS 140-2 requirements could be interpreted as a prescribed “protection profile” (in essence, rather than in format) for cryptographic modules.
- The definition of a PP turns the CC evaluation of products from the same product category into a de-facto conformance testing and FIPS 140-2 by definition is just that -- a conformance test.

BSI PPs for Cryptographic Modules

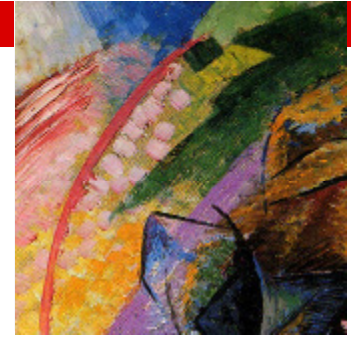


- BSI-CC-PP-0044 (dated on 28th October 2008)
Common Criteria Protection Profile
Cryptographic Modules, Security Level “Low”
- BSI-CC-PP-0042 (dated on 7th March 2008)
Common Criteria Protection Profile
Cryptographic Modules, Security Level “Moderate”
- BSI-CC-PP-0045 (dated on 24th July 2008)
Common Criteria Protection Profile
Cryptographic Modules, Security Level “Enhanced”

SFRs in BSI CM PPs



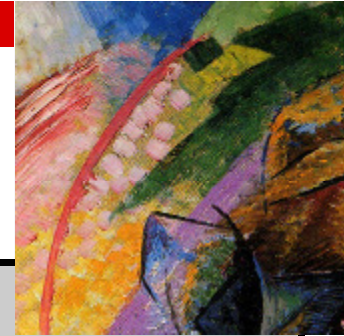
SFRs in PP 0044 SL “Low”	FCS_CKM FCS_COP FCS_RNG FTP_ITC	FIA_ATD FIA_UID FIA_UAU FIA_USB FIA_AFL	FDP_ACC FDP_ACF FDP_ITC FDP_ETC FDP_UCT FDP_UIT FDP_RIP	FMT_SMF FMT_SMR FMT_MOF FMT_MTD FMT_MSA	FPT_STM FPT_TDC FPT_FLS FPT_EMSEC FPT_PHP FPT_RVM FPT_SEP FPT_TST	
Additional SFRs in PP 0042 SL “Moderate”				FMT_MOF for Adm FMT_MTD for Audit		FAU_GEN FAU_SAR FAU_STG
Stronger SFRs in PP 0045 SL “Enhanced”				FMT_MSA		FAU_STG.4



Gained Benefits of a FIPS 140-2 Certified CM Applied to a CC evaluation

Crypto Requirements in US NDPP

(10 December 2010, Version 1.0)



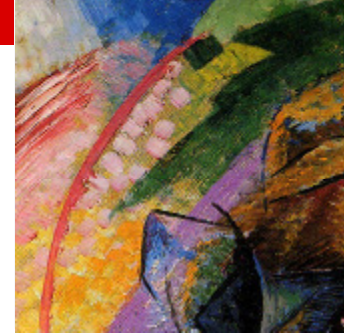
SFRs of FCS in NDPP	Referenced Crypto standards
FCS_CKM	FIPS 140-2 (Security Requirements for CM)
FCS_COP	ANSI X9.80 (Prime Number Generation and Testing)
FCS_RBG_EXT	ANIS X9.31 Appendix 2.4 using AES
FCS_COMM_PROT_EXT	NIST SP 800-57 (Recommendation for Key Management)
	NIST SP 800-56A (Recommendation for RSA-based Key Establishment Schemes)
	NIST SP 800-56B (Recommendation for elliptic curve-based Key Establishment Schemes)
	FIPS PUB 186-3 (Digital Signature Standard)
	FIPS PUB 197 (Advanced Encryption Standard)
	NIST SP 800-38A/B/C/D/E
	NIST SP 800-90 (Deterministic Random Bit Generator)
	CAVP Validation System (AESVS, RSAVS, DSAVS, ECDSAVS, HMACVS, RNGVS, etc.)

Crypto Requirements in US NDPP (Continued)



- **FMT_MTD**, TSF data including crypto information
- **FMT_SMF**, managing the TOE updates by verifying the digital signature of the updates
- **FPT_ITT**, using FCS-specified service to protect TSF data from disclosure and to detect modification of TSF data
- **FPT_TUD_(EXT)**, using FCS-specified digital signature or hash function to verify the TOE updates
- **FTP_ITC**, using FCS-specified service to provide a trusted communication channel between itself and authorized IT entities to protect from data disclosure and to detect data modification
- **FTP_TRP**, using FCS-specified service to provide a trusted communication path between itself and remote administrators to protect from data disclosure and to detect data modification

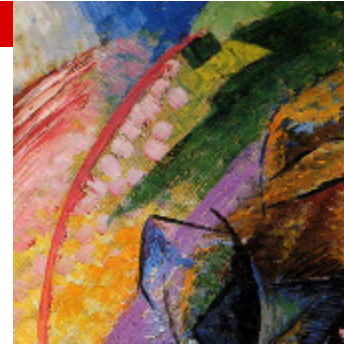
A Working Example



Suppose an OpenSSL-like Crypto library version “a.b.c” was:

- Implemented the following cryptographic algorithms and protocol
 - Triple-DES
 - AES
 - HMAC
 - SHA
 - RSA KeyGen, SignGen and SignVer
 - DRBG
 - DH key establishment protocol
- Certified under FIPS 140-2 for a software module at SL 1
- Embedded in a type of network device products, say routers, to primarily provide IPsec functionality.

A Working Example (Continued)



Suppose that kind of routers version “x.y.z” was:

- to be US NDPP compliant
- to be certified under CC

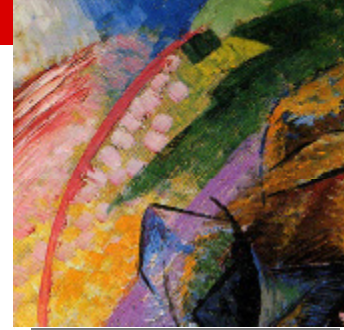
Question:

How much can having a FIPS 140-2 certified crypto component contribute toward its containing TOE becoming CC-certified?

Note:

- The working example has the CM as its core component of the TOE and their boundary could be more or less the same.
- The larger the crypto portion of the TOE the more benefit you will have from the FIPS certification of the CM. The flip side of this is also true.

Gained Benefits



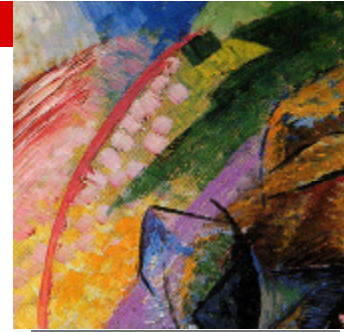
The following required crypto-related SFRs in the US NDPP are satisfied:

- **FCS_CKM** (Crypto Key Management including generation and zeroization)
- **FCS_COP** (Cryptographic Operation)
- **FCS_RBG_EXT** (Random Bit Generation)
- **FCS_COMM_PROT_EXT** (Communications Protection)
- **FMT_MTD** (Management of TSF Data)
- **FMT_SMF** (Specification of Management Functions)
- **FPT_ITT** (Internal TSF Data Transfer Protection)
- **FPT_TUD_(EXT)** (Trusted Update)
- **FTP_ITC** (Inter-TSF Trusted Channel)
- **FTP_TRP** (Trusted Path)

The required self test SFR in the US NDPP is also satisfied:

- **FPT_TST.(EXT)** (TSF Testing during initial start-up)

Gained Benefits (Continued)



The required SARs in the US NDPP are met by the crypto library component and hence, are partially satisfied:

- **ADV_FSP.1** (Basic Functional Specification)
The Security Policy of the CM can serve as the FSP during CC evaluation.
- **AGD_OPE.1** and **AGD_PRE.1** (Operational and Preparative user guidance)
Crypto officer and user guidance documentation for the Operational Environment requirements in FIPS 140-2 can be re-used for the AGD class during CC evaluation.
- **ATE_IND.1** (Independent testing - conformance)
Covered by the functional test done for the FIPS 140-2 conformance test.
- **AVA_VAN.1** (Vulnerability analysis)
The thorough review on design documentation and source code, the functional and penetration test conducted contributes to the vulnerability analysis.
- **ALC_CMC.1** and **ALC_CMS.1** (Labeling of the TOE and its CM coverage)
The section of Design Assurance in FIPS 140-2 checks the healthy of the develop process including unique labeling of the component and the usage of configuration management system.

Conclusion



- A FIPS 140-2 conformance test and a CC evaluation can go hand in hand.
- While achieving FIPS 140-2 certification has its own merits, in the meantime, it can also serve as a stepping stone to reach a CC certification, especially for organizations new to compliance with security standards.
- Those who desire to archive CC certification for products containing a crypto module should consider to get the CM FIPS 140-2 validated.
- Those who have got a FIPS 140-2 certificate for their crypto module could consider to advance to CC certification for products containing the certified CM.

References



1. Erin Connor, FIPS 140 & CC – How do they get along, the 11th ICCC
2. Eugene Polulyakh, FIPS and the Common Criteria finding the least common denominator, the 11th ICCC
3. Security Requirements for Network Devices (pp_nd_v1.0.pdf), 10 December 2010, Version 1.0, IAD
4. Common Criteria Protection Profile Cryptographic Modules, Security Level “Low”, BSI-CC-PP-0044, V1.0, 28 October 2008
5. Common Criteria Protection Profile Cryptographic Modules, Security Level “Moderate”, BSI-CC-PP-0042, V1.01, 7 March 2008
6. Common Criteria Protection Profile Cryptographic Modules, Security Level “Enhanced”, BSI-CC-PP-0045, V1.01, 24 July 2008
7. FIPS PUB 140-2 Security Requirements for Cryptographic Modules, Issued May 25, 2001
8. Derived Test Requirements for FIPS PUB 140-2, 4 January 2011, Draft

Acknowledgements



A special thanks goes to:

- Ingo Hahlen for pointing me to the set of BSI cryptographic Module protection profiles
- Apostol Vassilev for reviewing the slides and for helpful comments
- Courtney Cavness for the language editing



Thank you for
your attention!