網路安全的理論與實務

楊中皇 著

第八章 密碼模組

http://crypto.nknu.edu.tw/textbook/

第八章 密碼模組

- FIPS 140-2
- 符記保護剖繪 (Token Protection Profile)

密碼學模組標準 FIPS 140-2

- 依據NIST的定義密碼學模組可以是硬體元件或模組、軟體韌體程式或模組、或它們的組合
- 美國於1994年通過FIPS 140-1規範，並於2001年修正為FIPS 140-2。目前FIPS 140-2的規範是國際上業界所公認的密碼學模組標準
- FIPS 140-2標準訂定密碼學模組的四種安全等級，從最低要求的第一級到最高階的第四級，每個安全等級各須滿足11個安全要件。每個安全等級的共同基本需求包括模組輸出入及控制與狀態介面的描述、至少須實現一個核定的密碼學演算法、模組啓動時自我測試密碼學演算法、模組安全政策的定義、授權角色與安全服務的說明、驗證機制的選擇、以及模組須以有限狀態機器描述等。

密碼模組安全等級

- 安全等級一：必須包含至少一種核定的密碼學演算法，且此安全等級允許密碼學模組的軟體或韌體於未被進行資訊安全評估的作業系統上執行。目前通過FIPS 140-2認證的密碼學模組中，約有30%屬於此一等級。例如微軟Windows XP作業系統的核心包含了一個fips.sys檔案，此檔案便是一個通過安全等級一的軟體密碼學模組
- 安全等級二：除了滿足安全等級一的要求外，必須有以角色(role)爲基礎的身分認證來決定模組作業人員是否被授權進行適合該角色的安全服務。密碼學模組軟體與韌體執行用的作業系統也必須通過資訊安全評估一般準則(Common Criteria, CC) EAL2或更高等級的認證。同時也要有可以發現並證明模組是否被更改、入侵的機制，例如封裝、塗層或防撬鎖。目前通過FIPS 140-2認證的密碼學模組中，大約有一半屬於此一等級。符合此安全等級的密碼學模組多爲硬體，但CheckPoint、Sun、Novell等公司也有軟體模組通過此等級的檢驗
- 安全等級三：除了滿足安全等級二的要求外，必須有以身分(identity)爲基礎的認證機制，且作業系統須通過CC EAL3或更高等級的認證。同時要能有效地偵測與回應入侵，包括偵測到入侵時，將模組內部的未加密明文與重要的安全參數予以歸零。目前通過認證的密碼學模組中，大約有21%屬於此一等級。例如GTE公司的SafeKeyper(一個具有金鑰分享功能而用於簽發憑證的硬體設備) 即通過此等級的檢驗
- 安全等級四：此爲密碼學模組截至目前爲止安全等級最高的，除了滿足安全等級三的需要求外，軟體與韌體執行時用的作業系統也必須通過CC EAL4或更高等級的認證。模組也必須要有實體安全機制以提供完整的模組保護外殼，對所有未經授權的使用予以偵測與回應。針對模組外在環境的情況與變動進行監控，如果電壓或溫度不在正常操作範圍時，將密碼安全參數予以歸零。目前通過認證的密碼學模組中僅有不到3%屬於此一等級。例如IBM公司的4758密碼加速卡或S/390密碼加速晶片皆通過此等級的嚴格檢驗

密碼學模組安全要件

十一項安全要件爲密碼學模組在設計與實現階段必須要滿足的需求

1. 密碼學模組定義
2. 密碼學模組埠與介面
3. 角色與服務
4. 有限狀態模型
5. 實體安全
6. 作業環境
7. 密碼金鑰管理
8. 電磁干擾/電磁相容
9. 自我測試
10. 設計保證
11. 避免遭受攻擊

密碼學模組定義

- 必須詳細描述包含密碼學模組所有的硬體、軟體和韌體元件
- 採用的密碼學演算法及操作模式與安全政策等也須述明

密碼學模組埠與介面

- 密碼學模組應透過實體的埠與邏輯的介面定義模組所有進入與離開的點。模組的軟體元件之應用程式介面可以定義爲一個或多個邏輯介面
- 密碼學模組應具備下列四種邏輯介面:
  - 資料輸入介面：除了控制輸入以外的資料，例如明文、密文、金鑰與安全參數等都應該經由此介面進入模組進行處理
  - 資料輸出介面：除了狀態以外的資料皆應由此離開模組。如果模組發生錯誤的狀態則所有的輸出都應被禁止
  - 控制輸入介面：用來控制模組操作的輸入命令、信號、控制資料(包括函式呼叫按鈕、開關、鍵盤等人工控制)等由此進入模組
  - 狀況輸出介面：例如函式呼叫的返回碼、指示燈等用來代表密碼學模組狀況的信號由此介面輸出

角色與服務

- 密碼學模組應該要有下列三種角色：
  - 使用者角色：用來進行一般安全服務的人員
  - 管理員角色：用來設定密碼初始或管理功能(例如金鑰與安全參數的輸出與輸入、稽核功能、或模組的開始設定等)的人員
  - 維護者角色：用來進行實體維護(例如軟硬體診斷)的人員。當進入或離開維護者角色時，所有明文、私密金鑰、即未被保護的安全參數都應該被歸零
- 而對操作人員而言，密碼學模組應該要提供下列三種服務：
  - 狀態顯示：輸出密碼學模組目前的狀態
  - 自我測試：開始與執行模組內部自我測試
  - 允許的安全功能：進行至少一種FIPS 140-2認可的安全功能

有限狀態模型

- 密碼學模組的操作應以有限狀態模型(或等效)來描述，並以有限狀態圖及狀態移轉表來表示
- 模組至少要包含下列的狀態：電源開啓/關閉、密碼管理員服務、金鑰登錄、使用者服務、自我測試、錯誤

實體安全

- 密碼學模組分成下列三種模組實體：
  1. 單晶片密碼學模組：單一積體電路晶片用做獨立裝置，或是晶片嵌入到其他封裝或不能被實體保護的成品中。例如單積體電路晶片的智慧卡
  2. 多晶片嵌入密碼學模組：二或多個相連的積體電路晶片且嵌入到其他封裝或不能被實體保護的成品中。例如轉接器或擴充卡
  3. 多晶片獨立密碼學模組：二或多個相連的積體電路晶片且實體嵌入到被實體保護的封裝中。例如加密路由器或安全無線電

作業環境

- 密碼學模組的作業環境意指模組作用時用到的軟體、韌體與硬體的管理包括作業系統
- 模組用到的所有軟體與韌體的原始碼與執行碼都應該加以保護，避免被未經授權的揭露與修改

密碼金鑰管理

- 密碼學模組金鑰管理的安全要件涵蓋密碼金鑰的整個生命週期、金鑰的元件、與模組用到的密碼安全參數。包括亂數產生(描述使用核可的或未核可的亂數產生器)、金鑰產生(使用核可的或未核可的金鑰產生過程)、金鑰建立(例如使用公開金鑰演算法的自動方式或是人工傳送下載的方式)、金鑰輸入和輸出(描述輸入程序與金鑰輸出程序，使用鍵盤類的人工方式或是利用智慧卡之類的電子方式輸入)、金鑰儲存(金鑰必須以明文或加密的形式儲存，以明文方式儲存的金鑰必須不讓未經授權的操作人員取得)、金鑰歸零(密碼學模組必須提供將未經加密的金鑰與安全參數予以歸零的方式)
- 模組內私密金鑰系統的秘密金鑰與公開金鑰系統的私密金鑰必須加以保護，避免被未經授權地揭露、修改、取代。而模組內公開金鑰系統的公開金鑰亦須加以保護，避免被未經授權地更改或取代

電磁干擾/電磁相容

- 應符合FCC 商業用或家庭用的Class A/B標準，以證明密碼學模組遵循EMI/EMC要件

自我測試

- 密碼學模組在啓動或處於某些情況時，應執行一些特定的自我測試，以確保模組功能正常
- 如果測試失敗時，便應進入錯誤的狀態，並經由狀況輸出介面傳送錯誤指示
- 自我測試又分爲以下兩種：
  1. 啓動測試：在模組啓動時，隨即進行密碼學演算法測試、軟韌體的完整性測試、其他重要功能測試等。測試的結果應經由狀況輸出介面傳送出
  2. 條件測試：在有需要時，可進行金鑰對測試（針對公開密鑰系統）、軟韌體的載入測試(進行核可的軟韌體認證防僞程序)、手動金鑰登錄的測試(金鑰必須附上16位元以上的錯誤偵測碼或輸入兩次以上比較是否相同)、持續亂數產生器的測試(測試會不會重複出現某一固定值)、繞道測試(有些密碼學模組本身允許可選擇性的不執行密碼功能)

設計保證

- 此安全需求是原來FIPS 140-1所沒有而FIPS 140-2新增的安全需求
- 從密碼學模組設計、發展、與作業都能使用最好的方式實施，確保模組能適當地測試、設定、遞送、安裝、開發，同時提供合適的文件說明

避免遭受攻擊

- 此安全需求也是原來FIPS 140-1所沒有的
- 不同密碼學模組型態、實現方式或實現環境可能遭受某些目前仍無法有效測試的攻擊
- 例如電磁洩漏(TEMPEST)、電源分析(power analysis)、時間分析(timing analysis)、錯誤注入(fault induction)等的攻擊，都是分析從模組外面取得的資訊，試圖得到有關模組內部密碼金鑰或安全參數的一些知識

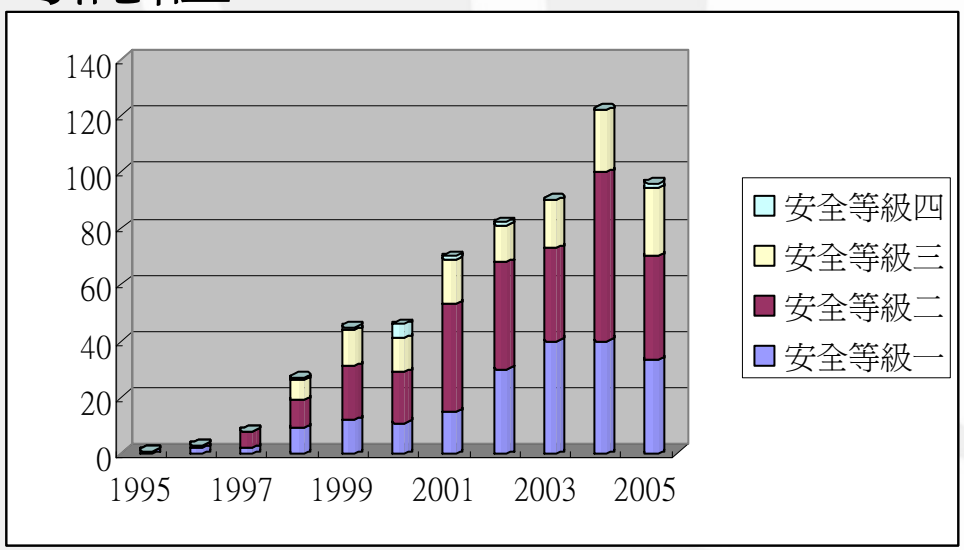
密碼學模組鑑定實驗室

- 目前有十二個NIST授權的FIPS 140-2密碼學模組鑑定實驗室，其中八個位在美國，兩個在加拿大，兩個在歐洲。
- 密碼學模組在申請驗證時，所需準備的文件需求爲下列十二大項(前十一項大致針對上述之安全需求)：

1. 密碼學模組定義(CRYPTOGRAPHIC MODULE SPECIFICATION) 。
2. 密碼學模組埠與介面(CRYPTOGRAPHIC MODULE PORTS AND INTERFACES) 。
3. 角色、服務與認證(ROLES, SERVICES, AND AUTHENTICATION)：除了需述明密碼學模組之角色與服務外，也要敘述模組所支援的認證機制與用到的資料，以及認證機制的安全性。
4. 有限狀態模型(FINITE STATE MODEL) 。
5. 實體安全(PHYSICAL SECURITY) 。
6. 作業環境(OPERATIONAL ENVIRONMENT) 。
7. 密碼金鑰管理(CRYPTOGRAPHIC KEY MANAGEMENT) 。
8. 電磁干擾/電磁相容(ELECTROMAGNETIC INTERFERENCE/ELECTROMAGNETIC COMPATIBILITY) 。
9. 自我測試(SELF-TESTS) 。
10. 設計保證(DESIGN ASSURANCE) 。
11. 避免遭受攻擊(MITIGATION OF OTHER ATTACKS) 。
12. 安全政策(SECURITY POLICY)：安全政策是密碼學模組操作時所根據的規則，這些規則是以模組操作人員的角色、提供的服務、以及金鑰及安全參數來陳述。

通過FIPS 140-1與FIPS 140-2的密碼學模組數

- 截至2005年11月18日為止，共有157家廠商590種密碼學模組產品通過FIPS 140-2驗證，這些廠商來自美國、加拿大、英國、法國、德國、以色列、澳洲、芬蘭、新加坡等國。我國亦有中華電信公司與網安科技公司的產品取得FIPS 140-2安全等級的認證。



已核定之密碼學演算法

- 根據NIST的統計，申請鑑定的密碼學模組中，大約49%有安全上的缺陷，96%有文件上的錯誤；而密碼學模組內部的密碼學演算法(包含DES、Triple-DES、DSA、SHA-1等)測試則有27%有安全上的缺陷，65%有文件上的錯誤。由於密碼學演算法是密碼學模組的核心，而使用密碼學模組的主要目的即是在應用模組內部的密碼學演算法。密碼學模組內至少須包括一種核定的演算法，若包括數種核定的演算法，那密碼學模組的應用範圍將更為廣大
- 下列演算法為FIPS 140-2已核定的密碼學演算法與操作模式
  - DES (Data Encryption Standard)/Triple-DES
  - AES (Advanced Encryption Standard)
  - DES Modes of Operation
  - Digital Signature Standard (DSS), RSA, ECDSA
  - Secure Hash Algorithm (SHA-1, SHA-2 (SHA-256, SHA-384, SHA-512)
  - HMAC (Keyed-Hash Message Authentication Code)

密碼學模組技術應用趨勢

- 隨著網際網路與全球資訊網的快速成長，網路安全問題也逐漸浮現出來，而使用密碼學模組以保障資訊及網路安全也逐漸形成一種趨勢
- 美國政府自1995年開始，即要求所有公家單位必須採用符合FIPS 140-2規範的密碼學模組
- 合適的密碼學模組可提供多用途的應用，使得密碼學模組能同時提供資料安全、電子商務、電子公文、電子郵件、校園網路安全等多項功能，也可整合到SET、SSL、IPsec、PKI等系統。此外，密碼學模組亦可用於中下游產業，例如網際網路業、電腦週邊業、通訊產品業等

符記保護剖繪 (Token Protection Profile)

- 美國國防部於2002年三月公佈第三版的公開金鑰基礎建設(Public Key Infrastructure，以下簡稱PKI)與金鑰管理基礎建設(Key Management Infrastructure，KMI)符記(Token)保護剖繪(Protection Profile)
- 此保護剖繪是以ISO 15408標準之資訊技術安全評估共通準則(Common Criteria for Information Technology Security Evaluation，簡稱CC)爲基礎，提出一套詳盡的規範，用來確認美國國防部推動公開金鑰基礎建設與金鑰管理基礎建設兩者所使用的符記硬體裝置的安全需求
- PKI/KMI符記是一個用來儲存密碼學金鑰與公開金鑰憑證的硬體裝置，且具備提供使用者身份認證(user identity authentication)的功能。依據美國國防部對該保護剖繪的定義，此符記可達到CC安全等級的EAL第四級要求，而且此符記的安全功能可涵蓋美國國防部所有人員與供應商的金融(電子商務及付款)、安全電子訊息、身分識別、安全資訊儲存、存取控制等多種應用
- 使用者身份認證是資訊或網路應用最基本的安全需求。近年來國內屢次發生的信用卡或銀行提款卡被盜用案件，明顯暴露出磁條卡儲存的資料無法被有效地保護，而磁條卡與個人識別碼(PIN)的結合僅能提供薄弱的單向使用者身份認證功能。PKI/KMI符記內建數位簽章、對稱式與非對稱式加解密等多種安全機制，不僅可直接用來支援高安全性的互動式使用者身份認證，且可用於電子公文、電子商務等應用

美國國防部PKI/KMI符記的硬體裝置種類

符記外觀	說明
IC卡	大小如信用卡的接觸式或非接觸式智慧卡
USB碟	外觀如USB隨身碟，但內含智慧卡晶片
PCMCIA卡	大小如筆記型電腦PCMCIA介面卡，但內含安全晶片，資料傳輸速度高
iButton鈕扣	達拉斯半導體公司的非接觸式硬體裝置，通常外觀如同鈕扣或戒指

PKI/KMI符記內部必須具有的密碼學演算法

演算法種類	說明
數位簽章演算法	包括1024/2048位元RSA、 1024位元DSA、384位元ECDSA
金鑰交換演算法	包括1024/2048位元RSA、1024位元 Diffie - Hellman、1024位元KEA、以及384位元ECKEA橢圓曲線金鑰交換演算法
對稱式演算法	包括128/192/256位元AES、DES、Triple DES、Skipjack
雜湊演算法	包括SHA-1、MD-5、SHA 256、SHA 384、SHA 512

PKI/KMI符記安全管理

步驟	說明
符記描述	● 微處理器硬體規格 ● 記憶體種類(ROM、EEPROM、RAM等)、大小與位址配置 ● 實體IC積體電路佈局圖 ● 所有啓動與未啓動的硬體安全功能 ● 所有啓動的硬體安全功能 ● 軟體規格 ● 所有啓動與未啓動的軟體安全功能 ● 所有啓動的軟體安全功能 ● 狀態圖
安全環境	● 操作時的環境假設 ● 可能受到的威脅 ● 安全政策
安全目的	● 保護資料避免被揭露或竄改 ● 使用者與系統管理者身分認證 ● 應用程式的控制管理 ● … …
安全需求	● 功能需求 ● 安全確保需求

PKI/KMI符記的安全目的

1. Protection of Authentication Data
2. Authentication of Users and SSOs
3. Control of Applications
4. Cryptography
5. Data Access Control
6. Data Read Format
7. Enforce data exchange confidentiality
8. Environmental Stress
9. Preservation of secure state for failures in critical components
10. Information Leak
11. Initialization
12. Probing by Selected Inputs
13. Encryption of Stored Keys
14. Life-Cycle Functions
15. Logical Protection
16. Multiple Applications
17. Physical Protection
18. Resource Access
19. Role Management
20. User Data Control
21. Secure Host Communications
22. Self-Test
23. Set up Sequence
24. Respond to Tamper
25. Trial-and-Error Resistance
26. Linkage
27. Destruction of Volatile Memory

PKI/KMI符記的安全功能需求

安全功能需求分爲七類：密碼學支援(Cryptographic support，FCS)、使用者資料保護(User data protection，FDP) 、身分證明與確認(Identification and authentication ，FIA)、安全管理(Security management，FMT)、安全功能的保護(Protection of the security functions，FPT)、資源利用(Resource utilization ，FRU)、可信賴的通道(Trusted path/channels ，FTP)

1.	Cryptographic key generation	FCS
2.	Cryptographic key distribution	
3.	Cryptographic key access	
4.	Cryptographic key destruction	
5.	Cryptographic operation	
6.	Subset access control	FDP
7.	Security attribute based access control	
8.	Basic data authentication	
9.	Export of user data without security attributes	
10.	Subset information flow control	
11.	Simple security attributes	
12.	Limited illicit information flows	
13.	Import of user data without security attributes	
14.	Basic internal transfer protection	
15.	Subset residual information protection	
16.	Authentication failure handling	FIA
17.	User attribute definition	
18.	Verification of secrets	
19.	Timing of authentication	
20.	Re-authenticating	
21.	Protected authentication feedback	
22.	User identification before any action	
23.	Management of security functions behavior	FMT
24.	Management of security attributes	
25.	Secure security attributes	
26.	Static attribute initialization	
27.	Management of TSF data	
28.	Management of limits of TSF data	
29.	Secure TSF data	
30.	Revocation	
31.	Security roles	
32.	Assuming roles	
33.	Abstract machine testing	FPT
34.	Failure with preservation of secure state	
35.	Inter-TSF detection of modification	
36.	Basic internal TSF data transfer protection	
37.	Passive detection of physical attack	
38.	Resistance to physical attack	
39.	Function recovery	
40.	Non-bypassability of the TSP	
41.	TSF domain separation	
42.	TSF testing	
43.	Maximum quotas	FRU
44.	Inter-TSF trusted channel	FTP

PKI/KMI符記的安全確保需求

安全確保等級	確保元件
ACM (Configuration Management)	ACM_AUT.1, ACM_CAP.4, ACM_SCP.2
ADO (Delivery and operation)	ADO_DEL.2, ADO_IGS.1
ADV (development)	ADV_FSP.2, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, ADV_RCR.1, ADV_SPM.1
AGD (Guidance documents)	AGD_ADM.1, AGD_USR.1
ALC (life cycle support)	ALC_DVS.1, ALC_LCD.1, ALC_TAT.3
ATE (test)	ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2
AVA (vulnerability assessment)	AVA_MSU.2, AVA_SOF.1, AVA_VLA.3

PKI/KMI符記內金鑰與憑證佔用空間估計表

假設使用2048位元RSA

金鑰或憑證資料	**EEPROM** 佔用空間(位元組)
目前的根憑證中心（root CA）憑證	1,500
下次的根憑證中心憑證	1,500
簽章用金鑰對	768
建立共通金鑰用金鑰對	768
對稱式金鑰	32
符記儲存用金鑰	32
一般身分用金鑰與憑證	2,000
電子郵件加密用金鑰與憑證	2,000
網路登錄（log-on）用金鑰與憑證	2,000
KMI管理員用金鑰與憑證	2,000
群體或組織用金鑰與憑證	2,000

參考資料

- Department of Defense, *Public Key Infrastructure and Key Management Infrastructure Token Protection Profile V3.0*, http://www.niap.nist.gov/ cc-scheme/PP_PKIKMITKNPP-MR_V3.0.pdf, March 2002.
- ISO/IEC 15408 — *Information technology — Security techniques — Evaluation criteria for IT security (Common Criteria, CC, Version 2.1)* — Part 1: Introduction and general model, Part 2: Security functional requirements, Part 3: Security assurance requirements, 1999.
- Dallas Semiconductor Corp., *iButton*, http://www.ibutton.com/
- W. Rankl and W. Effing, *Smart Card Handbook*, 3rd edition, John Wiley & Sons,2004.
- Smart Card Security User Group, *Smart Card Protection Profile* V3.0, http://niap.nist.gov/cc-scheme/PP_SCSUGSMPP_V3.0.pdf, September 2001.
- NIST, *SKIPJACK and KEA Algorithm Specifications*, May 1998, http://csrc.nist.gov/CryptoToolkit/skipjack/skipjack.pdf
- NIST, FIPS 140-2, *Security Requirements for Cryptographic Modules*, June 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
- NIST, Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules, http://csrc.nist.gov/cryptval/140-1/140val-all.htm