

初探美國電腦安全資源中心之公開資訊安全資源

國家資通安全會報 技術服務中心

游啟勝 (csyu@icst.org.tw)

摘要

電腦安全資源中心是最知名的資訊安全標準文件及指引文件網站，提供了相當豐富的電腦安全技術文件資源，著名的有美國聯邦政府使用的密碼演算法標準、相關的聯邦政府資訊處理標準系列文件及各式各樣的安全指引手冊，供外界學習及研究各種安全議題。另外，還有完全公開的 ICAT 漏洞資料庫可供有興趣的資訊安全產品及服務開發者使用。對於資安從業人員來說，這是一個不可不知的網站。

一、簡介

電腦安全資源中心（CSRC，Computer Security Resource Center）是美國國家標準與技術局（NIST，National Institute of Standard and Technology）所屬電腦安全部門（CSD，Computer Security Division）下的一個網站，其中蒐集了許多資訊安全的相關文件，著名的美國聯邦政府密碼演算法標準、相關的聯邦政府資訊處理標準系列文件及各式各樣的安全指引手冊都可以在網站中找到。本文首先簡介電腦安全部門的各研究領域，接下來整理此網站所公開的一些重量級與實用的技術文件及指引文件，供想要瞭解資訊安全技術或導入資訊安全管理制度的讀者參考。

二、電腦安全資源中心文件分類

電腦安全資源中心的文件資源可分為以下數類：

I 密碼標準與應用（Cryptographic

Standards and Application）

專注於發展密碼方法來確保資訊資源的完整性、機密性及可信賴性。研究領域包含：公開金鑰加密技術、先進認證系統、密碼協定及介面、公開金鑰認證管理、智慧標記（smart tokens）、密碼金鑰信託（key escrowing），及安全架構。並協助密碼學應用與國家基礎建設密碼學部份的相關實作。

此分類主要的研究成果包含了：

- U AES 加密標準
- U 密碼標準工具庫
- U 金鑰復原及 S/MIME
- U 公開金鑰基礎建設（PKI）

I 安全性測試（Security Testing）

專注於與政府及產業界合作，藉由發展及應用各式測試、衡量、驗證相關的安全稽核工具、技術、服務及支援程序來建立更安全的資訊系統與網路。研究領域包含發展及維護安全

指標、安全評量方法及測試方法。

此分類主要的研究成果包含了：

- U 自動化安全功能測試
- U 共通規格
- U 密碼模組驗證
- U IPsec

I 安全研究與新興科技 (Security Research/Emerging Technologies)

專注於研究必須加以了解或可以用於加強安全的新興科技，並找出及減少其可能具有的弱點。研究領域包含：入侵偵測、防火牆、掃描工具、安全測試平台 (Test bed)、弱點分析及解決、存取控制、事件應變、主動式程式碼及網際網路安全。

此分類主要的研究成果包含了：

- U 自動化安全功能測試
- U 角色式存取控制
- U IPsec
- U 行動安全
- U 智慧卡安全與研究
- U 垃圾郵件科技研討會
- U 無線安全

I 安全管理與指引文件 (Security Management and Guidance)

專注在發展安全管理指引文件。研究領域包含：風險管理、安全程序管理、安全訓練及認知、永續營運計畫、人員安全等。

此分類主要的研究成果包含了：

- U 自動化安全自我檢查工具
- U 電腦安全指引文件 (特別出版品、FIPS 出版品、跨部門安全報告、安全通訊)
- U 聯邦部門安全實例
- U 系統發展資訊安全議題

I 推廣認知及教育 (Outreach Awareness and Education)

專注於宣導認知資訊安全的需求與重要性，並推廣了解資訊弱點與矯正方法。

此分類主要的研究成果包含了：

- U 資訊安全認知、訓練及教育
- U 電腦安全資源中心網站
- U 聯邦電腦安全程序管理者論壇

I 聯邦資訊安全管理法案實施計劃 (Federal Information Security Management Act Implementation Project)

主要是支援實行 2002 年 12 月所通過的電子化政府法案下的聯邦資訊安全管理法案 (FISMA)。

三、著名技術文件及指引文件

電腦安全資源中心網站公開了許多有參考價值的技術文件及指引文件。這些文件主要可以分為三類，文件編號 SP 開頭的為特殊出版品，而 SP-800 系列為各種資訊安全指引文件，文件編號以 FIPS 開頭代表為聯邦標準文件。以 DRAFT 開頭的則為初稿文件，內容可能是指引文件或標準文件，後文所介紹的文件，讀者可以根據文件編號在網站的對應區域中找到。

以下整理了一些比較實用的文件：

I 作業系統加強安全指引文件

作業系統安全是做好個人電腦資訊安全的第一步驟，若能教育使用者事先對作業系統進行安全加強，不但

能減少安全事件發生的機率，所需要耗費的成本也較事後的事件應變及處理來得低的多。電腦安全資源中心有提出幾個電腦作業系統安全加強相關的指引文件，包含了：

- Ø SP 800-68：微軟 Windows XP Professional 作業系統安全加強：安全設定清單：<http://csrc.nist.gov/itsec/guidance/WinXP.html>，包含了 Windows XP Professional 的安全加強文件與適用於數種應用環境的設定範本。
- Ø SP 800-43：Windows 2000 Professional 系統管理指引：<http://csrc.nist.gov/itsec/guidance/W2Kpro.html>，包含了 Windows 2000 Professional 的安全加強文件與二種設定範本。
- Ø SP 800-70：資訊科技產品安全組態檢查清單程序：<http://csrc.nist.gov/checklists/index.html>。

I 新興科技安全

前文提及在電腦安全部門中，會針對各種有機會普及的新興科技加以研究其安全性，並提出建議，以下是一些整理：

- Ø SP 800-72：PDA 鑑識指引文件：<http://csrc.nist.gov/publications/nistpubs/800-72/sp800-72.pdf>。
- Ø DRAFT SP 800-58：VoIP 系統的安全考量：http://csrc.nist.gov/publications/drafts/NIST_SP800-58-040502.pdf。
- Ø SP 800-48：無線網路安全：802.11、藍芽及手持裝置：

http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf。

I 安全防護與事件處理

- Ø SP 800-61：電腦安全事件處理指引：<http://csrc.nist.gov/publications/nistpub/800-61/sp800-61.pdf>。
- Ø SP 800-51：使用 CVE（Common Vulnerabilities and Exposures）弱點命名規則：<http://csrc.nist.gov/publications/nistpub/800-51/sp800-51.pdf>。
- Ø SP 800-50：建立資訊科技安全認知與訓練程序：<http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf>。
- Ø SP 800-42：網路安全測試指引：<http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf>。
- Ø SP 800-41：防火牆與防火牆規則設定指引：<http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf>。
- Ø SP 800-40：安全修補程式管理程序：<http://csrc.nist.gov/publications/nistpubs/800-40/sp800-40.pdf>。
- Ø SP 800-45：電子郵件安全指引：<http://csrc.nist.gov/publications/nistpubs/800-45/sp800-45.pdf>。
- Ø SP 800-44：公開網頁伺服器安全加強指引：<http://csrc.nist.gov/publications/nistpubs/800-44/sp800-44.pdf>。
- I SP 800-64：在資訊系統發展週期的安全考量：

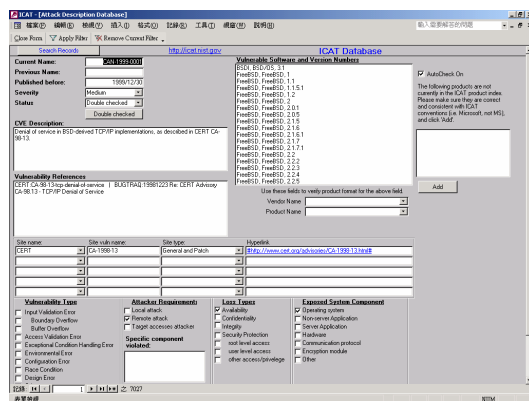
- <http://csrc.nist.gov/publications/nistpub/800-64/NIST-SP800-64.pdf>。
- Ø SP 800-31：入侵偵測系統：
<http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf>。
- I 資訊安全產品選擇
- Ø SP 800-52：TLS 選擇與使用指引文件：
<http://csrc.nist.gov/publications/drafts/draft-SP800-52.pdf>。
- Ø SP 800-36：資訊安全產品選擇指引：
<http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf>。
- I 著名的聯邦標準：
- Ø FIPS 46-3：資料加密標準 (DES)，包含了 Triple DES：
<http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>。
- Ø FIPS 180-2：安全雜湊函式標準：
<http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchange notice.pdf>，包含了 SHA-128、SHA-256、SHA-512 系列雜湊演算法。
- Ø FIPS 186-2：電子簽章標準 (DSS)
<http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf>。
- Ø FIPS 197：Advanced Encryption Standard (AES)：
<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>，AES 加密標準，是美國繼 DES 之後，為因應電腦運算能力突飛猛進所推出的第二代加密標準。
- Ø FIPS 198：The Keyed-Hash

Message Authentication Code (HMAC)：

<http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf>。

四、ICAT 漏洞資料庫

電腦安全資源中心另外有一個比較少人知道的資源是 ICAT 漏洞資料庫 (<http://icat.nist.gov/>)，ICAT 是與 OSVDB (<http://www.osvdb.org>) 相似的開放式漏洞資料庫，資料庫完全與 CVE 漏洞編號相容，並提供純文字及 Microsoft Access 資料庫二種格式下載整個資料庫，另外不論是商業廠商或是自由軟體創作者都可以依照 ICAT 的使用條款將自身的產品與服務與 ICAT 漏洞資料庫進行整合。ICAT 中也內建了一個圖形的漏洞搜尋介面 (如圖一)，供使用者以各式條件查詢整個資料庫，選擇整合開放式漏洞資料庫可免去自行蒐集漏洞資料的煩惱。



圖一：ICAT 漏洞搜尋介面

五、結論

電腦安全資源中心中公開了許多內容豐富的資訊安全技術文件，其中不乏有重量級的密碼演算法標準文件與實用的資訊安全指引手冊，文件的

品質也相當高，常常是鉅細靡遺地對某個資訊安全議題進行描述，因此對有需要對這些議題進行研究的人來說是非常好的參考文件。

最後，因為網站上的文件數目眾多，若是使用者想在有新的文件或是現有文件有更新時收到通知，可以在 <http://csrc.nist.gov/compubs-mail.html> 訂閱電腦安全資源中心的 Maillist，可免去自行瀏覽網站的困擾。