資訊安全之認證測試與評比測試

林盈達 林柏青

如果取得認證代表取得入場卷，能在評比中勝出則是市場競爭的一項法寶。隨著各種資訊安全事件層出不窮，安全性的問題日益獲得重視。不管是資訊系統的製造廠商，或是消費者，都會有共通的疑問----到底什麼樣的資訊系統可以稱為一個安全的系統？為了讓系統製造廠商在開發產品時有所依據遵循，以及消費者在採購產品時有個參考，因此需要有安全系統的認證機構來訂定一個安全的系統該具備什麼樣的功能，以及提供市場上產品的安全認證。本篇將介紹兩個主要的安全標準的認證機構：Common Criteria (CC)以及 ICSA Certified Security Associate (ICSA)，以及安全產品測試的準則。但除了安全性和功能性之外，產品本身的效能以及互通性之評比也是個不可忽視的重點。工研院交大網路測試中心將於 2003 年第三季舉辦網路安全產品公開測試，就是針對目前市面上的主要的安全防護產品：(1)多合一防火牆，(2)入侵偵測/預防，(3)防毒系統，(4)內容過濾系統，等四類產品進行安全性、功能性、效能及互通性進行測試，因此本文也將對這項測試的計畫以及希望探討的網路安全產品發展趨勢做個介紹。

一、安全標準與認證

網路安全相關的認證主要可以分為兩大類：一類是對從事網路安全相關工作人員專業技術的認證，另一類則是對網路產品或系統的認證。前者為數頗多，包括 CISSP、SSCP、GIAC、CPP 為主的數十家認證。後者包含本篇介紹的 ICSA 與 CC，相關的認證準則或測試列於表一。

性質	認證名稱	描述	參考網址
一般安全產品	Common Criteria (CC)	提供資訊系統安全程度的評估準則與認證測試	http://www.commoncriteria.org
	General Accepted System Security Principles (GASSP)	提供管理及產品相關的安全性原則	http://web.mit.edu/security/www/GASSP/gassp11.html
特定安全產品	ICSA Certified Security Associate (ICSA)	提供網路安全各項產品個別的評估準則與認證測試	http://www.icsalabs.com
	Open Security Evaluation Criteria (OSEC)	提供網路安全各項產品的個別功能與效能的評估準則，目前以 IDS 產品為主	http://osec.neohapsis.com

	Federal Information Processing Standards (FIPS)	提供加解密功能的驗證	http://csrc.nist.gov/cryptval/

表一、 網路及系統產品認證準則

ICSA 是一家提供網路安全服務的公司 *TruSecure* 下屬的獨立單位，提供了網路安全產品功能性和安全性的認證，以及網路和系統管理人員安全專業技術的能力認證。ICSA 的認證項目以安全性及功能性為主，其認證準則是由諮詢各界的專家、廠商以及使用者的意見制定出來的。由於各項安全技術以及安全威脅不斷的翻新，ICSA 的認證準則每年也會更新，並以更新後的準則來測試產品。另外，因為廠商本身會一直推出新款的產品，如果舊版的產品已經獲得認證，ICSA 也會讓新版的產品自動獲得認證。但是為了確保新款的產品一樣符合原先認證的標準，ICSA 會與廠商簽定條約，要求廠商的產品發展不能違背原先標準。如果 ICSA 抽測發現沒有符合原先認證的內容，廠商會被要求限期改善，否則即吊銷認證。

目前 ICSA 有如下九類的評估準則： (1) antivirus, (2) firewall, (3) Secure Internet filtering, (4) PC firewall, (5) Cryptography, (6) Intrusion detection, (7) IP sec, (8) Web applications, (9) WLAN security。從這些準則項目可以看出 ICSA 認證的對象是以保護內部網路的產品為主。認證的測試是由 ICSA 實驗室或其受過其訓練及授權的實驗室進行。目前獲得認證的各類產品數量請見表二。

產品種類	通過數量
antivirus	65 (scanner detection) 37 (scanner cleaning) 10 (Internet gateway) 6 (for MS exchange server) 6 (for Lotus Notes) 2 (for security service provider) (Note: some products belong to more than one category above)
Firewall	12 (version 4.0 criteria) 27 (version 3.0a criteria)
Internet filtering	N/A
PC firewall	2
Cryptography	28
Intrusion Detection	N/A

IPSec	11 (version 1.1 criteria) 49 (version 1.0b criteria)
Web applications	1
WLAN security	N/A (not start to test yet)

表二、各類通過 ICSA 認證的產品數量

而 CC 則是從幾個主要國家對資訊安全的評估準則所演變出的一個共同認定準則。目前是由美國、英國、德國、法國、加拿大、荷蘭等國家的認證單位共同修訂，目前最新的版本是 2.1 版。CC 涵蓋的範圍很廣，從安全性的政策到產品的功能都有。為了推動對實際的環境及產品安全性的是否符合 CC 的評估，這些官方認證單位共同組成 Common Criteria Recognition Arrangement (CCRA)來協助實際認證工作的進行，資訊產品的廠商可以與 CCRA 認可的測試單位接洽認證事宜。這些測試單位現在分佈在八個國家：澳洲(3)、紐西蘭(1)、加拿大(3)、法國(4)、德國(9)、荷蘭(1)、英國(5)、美國(7)，詳細的測試單位可參考如下網址：http://www.commoncriteria.org/services/LabCountry.htm。目前通過認證的產品種類涵蓋很廣，從資料庫、網路通訊設備、作業系統、智慧卡都有。與 ICSA 的認證較不同的是，CC 較為偏重產品本身的安全性，認證的範圍也較廣，而 ICSA 則較偏重網路安全設備。此外隨著認證的嚴格程度不同，認證的結果也會有等級的區分。目前獲得認證的產品數量也請見表三。

產品種類	通過數量
Database	8
Communications	3
Networking	30
Operating systems	10
Smart Cards	8
Access controls	13
Miscellaneous	14

表二、各類通過 CC 認證的產品數量

二、測試規範及標準

ICSA 的認證項目是以功能性的驗證為主，每樣受測產品各類認證的準則逐一測試。以防火牆類為例，每樣防火牆產品都必須經過這幾大項的測試：(1)事件登錄，(2)管理的功能，(3)在系統斷電後設定的持續性，(4)功能性，(5)產品本身的安全性，(6)文件等。每大項都有詳細的規範產品該具備什麼樣的能力。以斷電後的持續性為例，就規範了防火牆規則的設定在電源恢復後必須與原來的

設定相同，或是應該擋掉所有的封包，以免讓入侵者在還沒重新設定前有機可乘；所有登錄的資料不能因為斷電遺失；管理防火牆的認證設定不能遺失等準則。除了這些基本的測試外，每樣防火牆產品也必須在住戶端、中小企業、大型公司行號等使用的定位之間選擇一項進階的驗證大項，例如在哪個定位應該要能處理哪些應用層協定的流量等等。測試報告中會詳實的列載受測產品的軟硬體及文件規格、設定方式，以及每項準則驗證的結果。

與 ICSA 準則不同的是，CC 並沒有針對各項產品類別提出個別的評估準則。而是以比較一般性的角度來看一個安全的系統該具備哪些功能，以及該如何達到安全性。CC 的認證準則分為三個部分，第一個部分為介紹及針對系統的安全性及評估方式提出一般性架構；第二部分則定義了功能性類別，規範了 11 項安全性功能的類別：(1)稽核(audit)，(2)加密支援，(3)不可否認(non-repudiation)的通訊，(4)使用者資料保護，(5)識別與認證，(6)安全管理，(7)隱私，(8)安全功能的防護，(9)資源使用，(10)系統存取，(11)受信賴的傳輸通道(trusted channel)等項目。以稽核為例，規範了該記錄的內容(日期、時間、事件型態等)、記錄的時機(開啟及關閉記錄功能、事件發生等)等項目。第三部分包括產品從開發、運送、操作等整個產品生命週期要提供安全擔保(assurance)所需遵循的準則、安全的評估要項(要達到安全的目標、產品描述、安全性環境、功能、安全擔保)等，最後並提供評估之後的安全性等級劃分(Evaluation Assurance Level, EAL)，相當一般人熟知的 A1/B3/B2/B1/C2/C1/D 的等級。一樣是分成七個等級，從最底層的 EAL1 到最高的 EAL7。只是後者為美國標準，而這裡是各國公認的國際標準。

三、安全性網路產品的公開評比

綜觀整個網路產品的發展，早期的發展主要在解決的就是連結性(connectivity)的問題。當有線的連結逐漸普及之際，安全性(security)、服務品質保證(QoS)、行動性(mobility)等議題就漸獲重視。特別是安全性產品，對企業或各機關學校而言，已經從一個選擇性的項目，逐漸變成不可或缺的必備產品。就安全性網路產品而言，能夠賣得好的不一定要有得到認證，但卻可以增加用戶的信心，提高購買意願。相反的，得到認證的產品不見得就會得到市場的認同，用戶還會在意功能與效能。因此，就一個設備廠商而言，取得認證有時是入場卷，能夠在評比中勝出更是行銷的法寶。

工研院交通大學網路測試中心，早在成立之前就於 2001 年及 2002 年辦理兩次網路安全產品的公開測試評比，並分別先後發表於 2001 年 2 月以及 2002 年 5 月的網路通訊雜誌。由於網路產品的重要性，測試中心亦將於今年第三季第三度舉辦網路安全產品的公開測試評比。評分指標包含產品的功能、互通性、安全性、

效能等四大項。這一次的測試範圍較前兩次更為擴大。一方面，我們發現目前的網路安全產品有多樣化的趨勢，單一的防火牆及 VPN 不再能完全滿足客戶的需要，入侵的偵測，甚至防護，網路防毒的問題，不當內容的過濾已經不容再忽視。我們也看到許多產品，提供了多合一的解決方案，也就是把前述的功能整合在一個 box 上，以 " 俗擱大碗 " 的態勢吸引客戶。然而，多合一的解決方案同時也引起一些問題，在多項功能同時打開之後，對效能的衝擊會有多大？由於上述問題都同時面臨封包內容的處理，而不再是只有處理第三、四層的標頭就已足夠。部分產品甚至有封包內容處理的 ASIC 解決方案，硬體的加速對效能的提升有多大的幫助，會是一個有趣的議題。另外，市面上也有不少專屬的入侵偵測/防護，網路掃毒、內容過濾的專屬軟硬體，這些產品在面對多合一的方案時，在功能及效能上是否能具有競爭優勢？還是會逐漸被多合一方案取代？另一個有趣的議題是 open source 的軟體也可以做到前述的功能，我們也希望了解目前這些軟體相較於市場上的產品，它究竟在功能和效能上能達到什麼樣的地步？是否每位使用者都必需購買廠商的安全性產品，還是某些需求用 open source 就已足夠？除了過去各家產品的比較外，這些是我們希望在這次公開測試中所討論的新議題。

這次測試將受測產品分成四大類：(1)多合一防火牆，(2)入侵偵測/防護，(3)網路防毒，(4)內容過濾。各邀請了約 7 到 11 家廠商來參與這次測試。目前已經開始邀請各家廠商，預計在六月中收齊產品開始測試，九月初發布測試結果，並舉辦研討會討論相關技術及趨勢，敬請各界拭目以待!