

網路安全與危機處理

陳年興

台灣電腦網路危機處理中心主任

中山大學資訊管理學系教授

nschen@cc.nsysu.edu.tw

一. 前言

由於國內外的電視、電影中，對於網路入侵的描述幾乎都是使用密碼猜測(Password guessing)，所以大部分的人對網路系統的入侵行為都會以為是利用破解密碼來達成。事實上，密碼只是系統安全的一部份而已，而入侵的方法與種類，是依不同的系統而有不同的做法。

從 1988 年的 Internet Worm 事件到現在，系統的漏洞不斷被發現，入侵者一直挑戰系統的安全性，即使連美國國防部的電腦亦遭駭客入侵，金融業系統亦遭資料竄改。然而，系統真的是如此脆弱而不堪攻擊的嗎？

從統計資料我們得知，大部分入侵事件的發生，是由於系統管理者與使用者的錯誤設定所造成，亦即主要的問題是由”人”所產生的[1]，因此著重”人”並輔以技術，是維護網路安全十分重要的觀念。

因此，推動”技術人員認證”、”網路安全軟體認證”、”網路保全服務”，便能將技術與管理整合，進而阻止入侵的行為。

然而造成系統面臨危機的原因，並不只有人為的因素而已，尚包括自然災害、機器損壞等等，所以我們並沒辦法保證任何系統是絕對安全的，即使我們可以從技術面防範可能的入侵行為，然而我們無法預測何時系統會遭受到非人為的破壞，例如突如其

來的地震。

既然網路系統的安全問題隨時都有可能發生，那麼，就如同發生意外災害一樣，我們需要緊急的處理程序來將傷害降至最低。

因此，推動”建立國家對外網路連線出口的緊急處理制度”、”建立網路八號分機”、”網路安全相關防衛體系與觀念的建立”，將有助於提升我國對網路危機的處理能力。

整合以上所述，我們認為，如何解決”人”的問題，並訂立正確而有效率的處理程序，是資訊安全中重要的議題。

二．網路安全

底下列出電腦技術發展時，系統安全將面臨的問題：

發展狀況	面臨的問題
電腦更快速、複雜	系統密碼可能在短時間內被”窮舉法”猜出
電腦知識普及、資訊取得容易	未經授權的員工可能取得重要資料
電腦專業人士增加	由程式來破解系統或規避控制
分散式電腦網路系統	產生更多入侵行為及不當存取機會

對於以上問題，我們提出三點建議來減少系統安全上的問題：

(1)技術人員認證

隨著全球網路市場的蓬勃發展，需要大量有關的專業人才來管理網路系統，然而企業面對眾多的應徵者，誰的技術才是值得公司信賴的呢？而系統管理者又該如何評定自我的身價呢？”技

術人員認證”可以提供我們一個評判的標準來解決這些問題。

在國內較為熱門的認證有 Microsoft 的 MCSE(Microsoft Certified Systems Engineer) , NOVELL 的 CNE (Certified NetWare Engineer) 及 Cisco 的 CCIE(Cisco Certified Inter-network Expert)。以 MCSE 而言,它是要表示系統工程師有充分的能力駕馭設置於 Microsoft Windows NT 及其伺服器軟體的資訊系統,可以有效率地進行規劃、建立、維護及支援工作。

另外,國外有一個叫做 CNP (Certified Network Professional)的認證[6],它比較特別的地方,在於你除了必須擁有兩個以上的廠商認證外,還必須擁有兩年以上的相關工作經驗。而目前它所承認的廠商認證包含:

Banyan--CBS CBE,	Cisco-CCIE,
CNX--any version,	Compaq—ASE,
IBM--CLSE PSE CWSE AS/400,	
Lotus-CLP,	Microsoft—MCSE,
Novell--CNE ECNE MCNE,	SCO ACE

總之,對企業來說,取得認證的員工數目越多,代表專業技術能力愈強;對個人來說,取得認證是能力的肯定。當然,一個管理者越了解系統,對系統的安全越有助益。因此,我們應規劃下列系統人員的認證:

<1>網路管理者(Network Master)認證:

包含 TCP/IP、網路實體設施、網路偵錯技術等。

<2>作業系統管理者(Host Master)認證:

包含系統安裝、系統管理等。

<3>伺服器管理者(Server Master)認證:

包含 DNS、WWW、SENDMAIL 等。

(2) 網路安全軟體認證

目前國內似乎並無相關的主管機關或單位，執行網路安全相關產品的認證服務。然而隨著網際網路的迅速發展以及電子商務的推行，我們有必要對於自己的網路安全產品建立認證制度，如此在面對多樣的網路安全相關產品時，消費者在選擇上便可以有所依據。如美國 ICSA 成立的宗旨一樣，網路安全產品的認證制度是希望能提供給消費者採買網路安全相關產品時的參考，減低網路安全上的風險，避免購買到安全沒保障的產品。

以下條列 ICSA 的做法以供參考[7]：

- <1> ICSA 與擁有測試程式(如 CyberCop Scanner, ISS Scanner) 的廠商或組織簽訂契約，簽約廠商或其它組織必須保證持續開發與維護測試程式。
- <2> ICSA 對於通過認證的產品，每年將有二至四次的不定期測試，若此時產品無法通過測試，將給予廠商二到四周的時間改善，若於期間無法改善，將取消認證資格。
- <3> ICSA 認證將每年更新，以提供使用者最新版本的軟體是否可信賴的參考依據。

我國可以考慮由一公允的技術單位進行網路安全相關軟體的認證，除了可以客觀的分析網路軟體的安全問題外，在對於提升廠商的軟體品質和增加消費者的選購信心上，都有正面的幫助。

(3) 網路保全服務

現今的生活中，假如有歹徒侵入住家，這時若有保全裝置，保全公司將採取迅速的反應，以避免顧客遭受危險或損失。

而網路保全服務的性質，類似於現今的保全公司，亦即在入侵攻擊事件發生時，透過此機制能迅速處理並降低損害。

目前我們可以透過所謂網站快照(snapshot)來建立這樣的機制。意即選定一快照伺服器，對所服務之網站做重點資料的checksum，並按時比對checksum是否正確，若發現錯誤，立即通知快照伺服器管理者與該網站管理者，並透過recovery的機制，先復原舊資料，以增加在該網站管理者登入系統處理前的這段時間裡的”形象存活”機會[4]，而快照伺服器管理者亦於第一時間協助處理，以避免該網站管理者因故無法迅速登入系統，造成系統無人修復的情況。

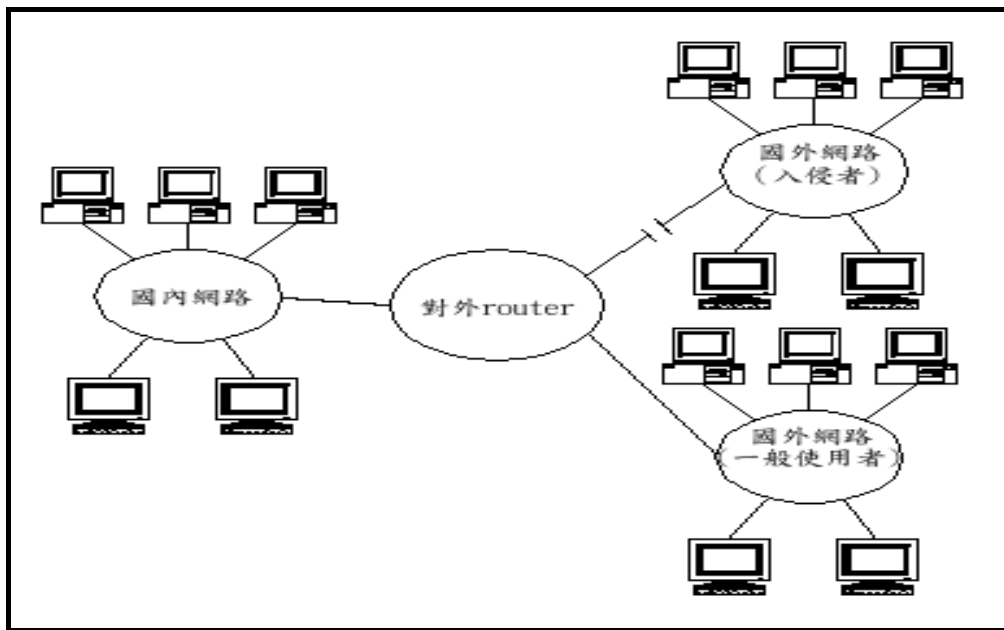
三. 危機處理

網際網路將電腦串連起來成為龐大的系統，因而若有攻擊或入侵的行為產生，這些危害可能迅速就會蔓延開來，所以為了因應遭受網路攻擊可能造成的危害，我們提出以下三點建議：

(1) 建立國家對外網路連線出口的緊急處理制度

當我國遭受到國外資訊戰的攻擊，若能迅速由對外網路連線出口做緊急處理，切斷國外連線，或拒絕國外攻擊位置的連線要求，將可爭取應變時間，減低傷害與損失。

以今年八月初的”政府網站資料篡改事件”為例，此次攻擊者的來源皆為中國大陸的IP位置，故若迅速從管制國外封包進入的Router上阻擋中國大陸部份IP位置，將可防止對方騷擾，如下圖所示。



(2) 建立網路八號分機

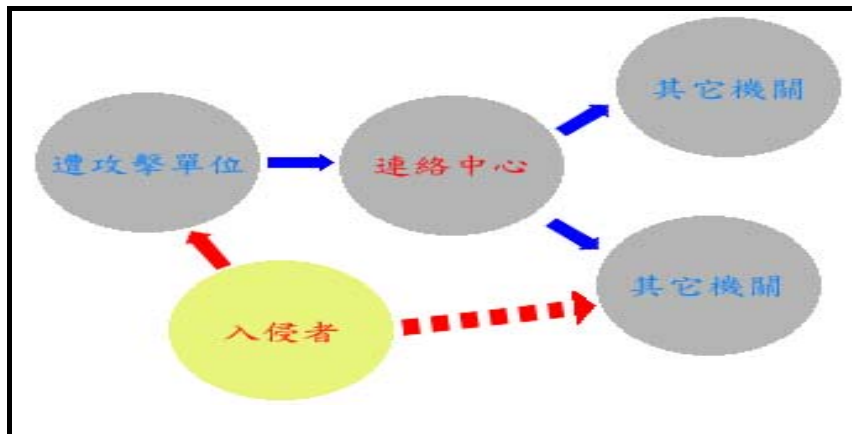
當網路系統遭到入侵，系統管理者可能不知道入侵者來自何方，亦沒有人知道入侵者的下一個目標會是哪裡，然而一旦攻擊行動蔓延開來，可能造成驚人的損失。

我們提出“網路八號分機”，目的便是在於成立一個緊急連絡網，以便迅速對入侵事件做出因應行動，其主要的功能分為以下三點：

<1> 入侵通報

一個入侵者是無法同時攻擊所有的主機，所以當某一網站發現攻擊動作或是已被入侵，若能透過連絡網，告知其他管理者相關的訊息以做為防備，將有助於防止災害的擴大。

基本的架構，應有一連絡中心以負責接受回報與執行並分派連絡工作，底下為示意圖：



<2>追蹤入侵者

當發現入侵者源位置來自國內，可透過“網路八號分機”，請該來源位置的管理者協助追蹤入侵者身份，以防制電腦犯罪事件。

<3>入侵記錄與分析

透過“網路八號分機”的機制，我們可以將每一個入侵事件的資料記錄起來，這將有助於了解入侵者的手法，並提供電腦犯罪的分析，以協助電腦犯罪案件的偵查。

(3) 網路安全相關防衛體系與觀念的建立

台灣電腦網路危機處理中心(TWCERT)於本次“政府網站資料篡改事件”中，迅速蒐集資料，並提出緊急處置方案與協助處理系統安全問題，於平時亦提供技術諮詢與入侵事件求助和系統安全資料的發送。但是由於一般機關遭攻擊時，可能覺得礙於聲譽，故不願做入侵事件求助，不過從“台灣 Web 伺服器安全性調查”[5]，我們可以知道，事實上有許多的問題存在於大部分的系統中。

政府應從政策面、市場面以及教育訓練上著手，除了宣導網路安全的重要性、訓練相關人員的技能之外，也要強化網路安全相關體系的建立、加強網路安全服務組織(例如 TWCERT)的功能與運作、宣導正確面對入侵事件的態度，如此才能落實

資訊安全的危機處理。

四. 討論內容

1. 網路安全

- (1) 網路安全軟體認證制度的建立
- (2) 技術人員認證制度的建立
- (3) 網路保全機制的建立

2. 危機處理

- (1) 國家對外網路連線出口的緊急處理制度的建立
- (2) 網路八號分機制度的建立

五. 參考資料

[1] [沈碧容, 1996]沈碧容譯, Richard H. Baker, “Network Security – How to Plan for it and Achieve for it.” (中譯:網路安全手冊-個人應用篇), 1996

[2] [沈碧容, 1996]沈碧容譯, Richard H. Baker, “Network Security – How to Plan for it and Achieve for it.” (中譯:網路安全手冊-企業應用篇), 1996

[3] [白方平, 1998]白方平譯, Clifford Stoll, “The Cuckoo’s Egg – Tracking a Spy Through the Maze of Computer Espionage” (中譯:捍衛網路), 1996

[4] [黃世昆, 1999], “網路系統存活管理”, 1999

[5] [陳年興 林秉忠, 1999], “網路環境下之系統安全評估”, 1999

[6] [Certified Network Professional Program , 1998],“What is the CNP Program?”, 1998

[7] [Peter Tippett , 1998],“ICSA Product Certification: Goals and Generic Criteria”, 1998