多層次網路安全機制探討

作者／李武耀少校

提要

一、孫子兵法虛實篇：「善攻者，敵不知其所守；善守者，敵不知其所攻。」善攻者與善守者皆需掌握敵攻守思維，才能採取獨到攻守策略。在資訊攻防應對中，即是熟知敵資訊戰攻擊戰術，精進我資訊戰防禦能量。

二、多層次網路安全機制乃是針對資訊網路的各種攻擊方式，做全面性的分析與防制，並訂出合適的網路存取機制與監控方法，採取有力的管制保護措施來保護軍事機密與系統安全。

三、攻擊入侵之趨勢有系統漏洞發現快、病毒製程時間短與攻擊手法變化多，國軍資安防護能量的提昇與更新有其必要性。

關鍵詞：網路安全、網路管理、多層次安全架構

壹、前言

孫子兵法虛實篇：「善攻者，敵不知其所守；善守者，敵不知其所攻。」在資訊攻防戰中，即是熟知敵資訊戰攻擊戰術，精進我資訊戰防禦能量，成為資安善守者，使敵攻守無措。

近年來，國軍規劃許多資訊基礎建案，各單位紛紛興建資訊網路平臺，以期能完成C4ISR基礎平台之整合目標。基礎平台可短期建立，資源亦可迅速掛載，然而隨之而來的維護、安全與管理問題卻是需長期經營的。

歸納資安威脅來源，最大的威脅源來自於人[1]，其次才是天然的威脅。目前，國軍資安威脅的假想敵是中共網軍，敵攻我防的情境下，該如何防是本篇論文探討的重點。

貳、本文

隨著網際網路的普及，電腦病毒、蠕蟲、惡意程式散播更加快速。各國政府與民間組織體認到網路攻防是具有國防價值的，因此紛紛投入資訊戰的研究，以期在發生戰事時，能在短時間癱瘓敵方指揮系統，對敵方產生心理的威懾效果，有助於我軍取得最後勝利。

1990 年代中東波灣戰事爆發，各國軍事觀察家皆睜大眼看美國如何打勝這

[1] 呂芳懌，蘇俊維，「網路入侵與防禦策略探討」，第三屆網際網路應用與發展研討會，2002年5月。

場仗。早在 1980 年代美國空軍便開始「資訊戰」戰法研究，成功地應用在波灣戰爭上，各國國防軍事部門自此被大大地啟發與影響，紛紛投入經費研究與研發資訊戰。中共自此更是積極培養「網軍」，即是駭客部隊，攻擊、情搜、破壞敵人指管鏈路，對我國來說是一重大威脅。

談防禦，得先從人員教育開始。入侵攻擊手法不斷翻新且形態繁多[2]，許多安全機制往往祇能從事局部的安全防制，因此，在面對網路各種的安全威脅，必須採取有力的保護措施來保護系統資源的安全。網路要做到比較安全的防禦，必須有全面性的考量，俾阻擋較多的入侵攻擊。目前攻擊入侵有四大趨勢：攻擊過程自動化與攻擊工具的快速更新、攻擊工具的不斷複雜化、漏洞發現快，及防火牆滲透。由於入侵工具不斷的修正與改良，從掃瞄/偵測目標主機的通訊埠、作業系統、應用程式，至漏洞的探勘與攻擊行為的發動，已可以完全自動化一氣呵成，而且可跨作業平台，不但可以隨機地選擇攻擊步驟，或利用事先設計的不同攻擊方法發動攻擊[3]，使得攻擊行為分析與偵測，越來越不容易，使得網路安全管理的挑戰愈來愈嚴苛。

對入侵攻擊的防禦措施，目前的網路系統大部份都是透過防火牆的機制，但是，一般的防火牆對於系統漏洞、缺陷、後門、內部攻擊與病毒等問題，仍無法有效地防制，僅能防範已知的安全威脅，而無法預測新的攻擊方式。

網路防火牆是以防禦外來的威脅為目標，對下述的入侵攻擊項目，卻不易防範[4]：

1.內賊難防

來自內部人員對內部網路的攻擊或竊取機密資料是難以防範的，原因是一般防火牆的存取規則設定是針對網路外部在向內部系統存取的控制，且內部所有系統主機皆暴露於內部網路上，若重要主機沒有另外增加安全機制，則無法防範來自內部的攻擊與竊取行為。

2.服務弱點

面對透過系統的漏洞、缺陷或電子郵件的附加檔案所夾帶的後門病毒入侵亦束手無策，例如，透過電子郵件夾帶可對內部發動 DDoS 攻擊的木馬程式時，防火牆是無法阻絕這類對內部的攻擊模式，原因是防火牆僅過濾使用者的合法性，因此，對於防火牆原本系統的漏洞與缺陷，及合法使用者經由電子郵件所夾帶的的檔案，並沒有過濾阻擋，讓病毒入侵。

---

[2] 蘇澈譯，駭客的秘密：網際網路篇，碁峰資訊，1998 年 6 月。

[3] Distributed Denial of Service (DDoS) Attacks/tools, http://staff.washington.edu/dittrich/misc/ddos/, July 2003.

[4] 呂芳懌，蘇俊維，許惟翔，「內部網路安全威脅分析與防制」，2003電子商務與數位生活研討會，2003年4月。

3.大開後門

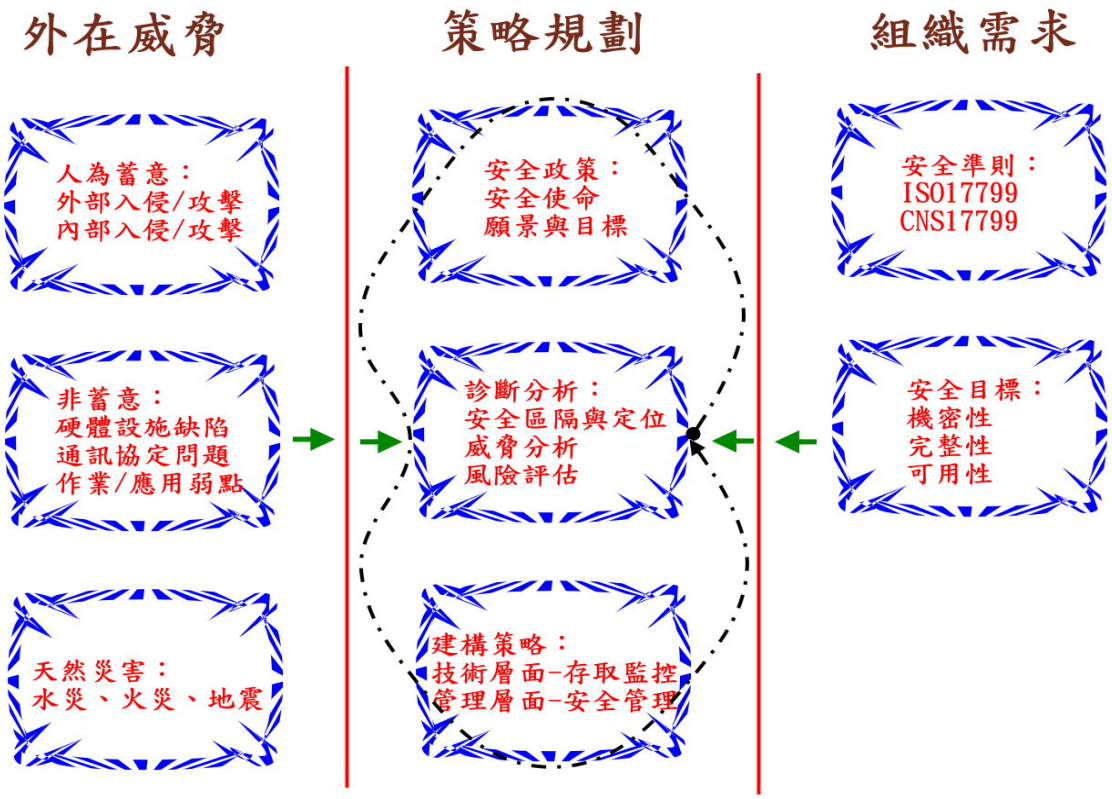
內部人員亦可透過私接數據機撥接連線，這種人為所造成的後門，會吸引有心人士的窺視及竊取撥接連線的資訊（撥接門號、使用者名稱與密碼等），卻無法有效加以防範，原因是這私自架設的撥接連線並沒有經過防火牆安全機制的過濾，使得外部入侵者可以直接入侵攻擊內部網路系統，造成難以估計的損失。

事實上，為了保障網路上各伺服主機、網路設備與所傳遞訊息的安全，網路安全管理機制與策略，不能不隨著網路結構與應用的改變而調整，如此，方能效防範不當的使用。針對防止網路上的入侵者，可採取許多應對措施：如網路防火牆、電腦防毒軟體、入侵偵測系統、弱點檢查評估與電腦稽核紀錄。除了使用這些資安防護工具以外，「權限管理」也是重要的課題，如何讓合法作業人員取得合理的權限，以及如何防止機密與密碼外洩，都需要不斷地檢討改進，因為最容易發生的危安事件都是出於人員的危機意識不足與危機處理失當。同時，國軍目前實施軍網、民網分離，並要求遵守「國軍個人電腦設備輸出入作業規定」、恪遵實體隔離政策、嚴格資料分級處理、執行安全設定檢查、定期更新病毒訊息、定期檢查「事件檢視」、關閉不必要服務埠與定期備份檔案資料等規定，皆需遵守，以防資安攻擊。

下面將分別在資安防制策略、監控項目與地點、網路防火牆、入侵偵測及存取控制等層面上，一一說明如何適當地利用資訊安全防制、網路封包特徵、身份鑑識技術與行政控管等方式，建構安全的資料存取與傳輸機制，防止未經授權的使用、誤用或濫用等。

參、資安防制策略

網路安全是滴水不露、密不可分、層層防護的系統防護，針對可能的網路安全威脅，須有適當的「網路安全防制策略」（圖一）為組織做最全面的保護，按安全政策的規範與程序推行到整個組織；同時，在技術面有「網路安全防制機制」（表一）將防制策略轉換成安全機制分別實現之。



圖一 防制策略分析之架構[5]

表一 網路安全防制機制(作者整理)

ISO17799 資訊安全標準安全稽核與管理									決策層
技術層面				管理層面					管理層
身份鑑識	多層防禦	傳輸控制	RBAC	風險評估	人員管理	系統維護	實體安全	危機管理	

目錄服務認證、個人防火牆、主機型入侵偵測系統、檔案加解密、SSH、PGP、S/MIME、Kerberos、PKI	7 應用層	技術層
	6 表現層	
	5 會議層	
SSL、SET、防火牆安全防護、網路型入侵偵測系統	4 傳輸層	
防毒系統、防火牆、網路型入侵偵測系統、路由器存取清單、VPN、IPSec	3 網路層	
IP-MAC 網址對應鎖定、交換器存取清單、NAT/NAPT	2 資料鏈結層	
	1 實體層	

[5] 同註 3。

網路安全防制策略定義為：組織為達到網路安全目標，經由威脅分析與風險評估之區隔與定位，訂定之防制策略，包含技術與管理兩層面，如圖一為其示意圖。

一、組織需求

從組織對網路安全的需求思索，包含有：

(一)安全準則

依據ISO 17799/CNS 17799資訊安全管理系統實務準則[6]所提供管理要項、控制目標及方法，建構一套符合組織資訊安全的政策，確保資訊安全，亦可做為IT人員的遵循標準。

(二)安全目標

必須達到組織對資訊安全要求的三大目標，即機密性、完整性、可用性，以確保組織資訊之機密、完整及可用。

二、外在威脅

在面對目前與未來可能的外在安全威脅，應該思考資訊資源遭受入侵破壞的可能性，及發生時會遭受到什麼樣的衝擊，如：

(一)蓄意入侵破壞行為

面對來自網路外部與內部的人為蓄意之入侵攻擊行為，例如，DoS、DDoS攻擊[7]等，必須建立一套資訊安全防範政策落實執行，避免組織資訊資源的損失。

(二)非蓄意破壞行為

面對非蓄意的網路安全問題，例如，硬體設施的缺陷、通訊協定的問題、作業應用系統的缺失等，必須建立系統維護與弱點通報程序，以適時修正，減少系統安全威脅衝擊。

(三)天災所引發的損失

面對不可預測的天災，例如，火災、火災、地震等，我們必須建立一套備份機制與危機處理程序，以降低災害損失。

三、策略規劃[8]

依據組織的資訊資源、技術資源、財務資源等能力，建立最佳的安全防制策略。須評估：

(一)安全政策

組織對於網路安全的願景與目標，必須明確訂定規範，包含指導方針、運

[6] ISO/IEC TR 13335，資訊技術－資訊安全管理的指導，經濟部標準檢驗局，2002年。
[7] Distributed Denial of Service (DDoS) Attacks/tools,http://staff.washington.edu/dittrich/misc/ddos/, July 2003.
[8] ISO/IEC 17799：2000（E），資訊技術－資訊安全管理的作業要點，經濟部標準檢驗局，2002年。

作程序、管理規範及人員聘雇合約等，以提供安全管理遵循參考。

(二)診斷分析

對組織資訊資源做一安全威脅分析，評估所面對的資訊安全漏洞、威脅與影響，以做有效監控與防制。並做風險評估與管理，列舉各資產價值、威脅與弱點，以建立監督與控制之機制。

(三)建構策略

在技術層面與管理層面，分別建立存取監控策略與安全管理策略，以防範資訊資源遭受各種安全威脅，確保組織持續運作、減少損失。

四、資安防制機制

瞭解網路所面對安全威脅後，對於這些威脅的可能來源，擬定一套適當的防制機制，如表一所示，做為施行到整個組織的程序與規範，以下分述之。

(一)決策層

資訊安全的管理，是需要組織高階管理階層的支持與認知，經由各層級人員的充份溝通與參與，建立符合組織資訊安全的政策。參照ISO 17799 的資訊安全標準制定符合組織之安全政策與程序，建構資訊安全防護機制，減少組織網路與系統安全的弱點與缺失，並提昇組織的風險控管能力。

因此，透過ISO 17799在幾個資訊安全方面的探討，針對國軍的封閉網路作統一全面的考量。

第一、異常連線檢測：異常連線是指伺服主機、網路線路或網路設備發生TCP 不正常的連線，駭客用以掃瞄網路主機狀態的方式之一，唯此時網路其他部份的運作仍是正常的。導入ISO 17799 9.5.7 與9.5.8 控制方法，監控TCP 的連線狀況，分析兩主機之間連線異常／失敗的原因，可辨識是否有潛在的入侵或非法的網路通訊，方法則是檢查重要主機（例如，檔案伺服器、網頁伺服器）或路由器所發出的ICMP 控制訊息。

第二、軍網防火牆檢測：導入ISO 17799 12.3.1 與12.3.2 控制方法，在軍網與防火牆之間設置N-IDS 與 Honeypot，這種設置方式的目的在保護防火牆本身與分析入侵／攻擊行為，其意義是在防火牆實際遭受攻擊之前預先偵測出來，類似守門員在軍網與內部網路的必經節點上，即時蒐集經過此通道的網路封包，並分析比對Honeypot 所蒐集的偵測、入侵與攻擊的日誌記錄，讓N-IDS 可立即回應TCP RST 封包中斷連線，避免攻擊封包進入內部網路，並即刻通知管理人員做適當處理。

第三、防火牆DMZ區域：導入ISO 17799 9.1.1、9.4.1、9.4.6、10.1.1、10.2.1~4與12.3.1~2 控制方法，在非軍事區內建置N-IDS、H-IDS 與Honeypot，此種混合

建置方式的目的分別是：

1.運用N-IDS 偵測出已穿透（Penetrate）防火牆的攻擊行為，包括：封包及連線，找出防火牆設定與存取規則不足之處，以修正改善之；同時可以監控DMZ內的封包行為，阻止不合法的連線行為與網路封包，一般而言，包括：

(1)不允許由DMZ 內的主機，向Intranet 內部伺服主機要求連線。

(2)亦不允許DMZ 主機上種植木馬。

(3)向Intranet 內部伺服主機發動DDoS 攻擊。

(4)有異常或變形的ICMP 封包進出。

2.在DMZ中的各重要主機上，例如，對外服務的DNS、Mail、FTP 等伺服主機架設H-IDS，目的是彌補N-IDS的不足，方法則是蒐集主機的系統記錄，以比對N-IDS 未偵測出來的可疑的攻擊模式或特徵。

3.在DMZ 設置Honeypot 模擬一重要主機，蒐集並分析穿透防火牆入侵／攻擊的資訊與行為，瞭解系統的漏洞或缺失，以修正系統安全措施。

第四、網路骨幹：導入ISO 17799 9.4.7 與9.4.8 控制方法，在網路骨幹（Backbone）與重要子網路上建置N-IDS，並隱形於網路上以偵測所有主機，並可同時監測網路流量與重要的網路資源，增加偵測機率。

第五、重要主機：導入ISO 17799 10.2.1 控制方法，在重要主機上設置H-IDS，目的是偵測特定主機的入侵與攻擊，將所蒐集到的系統記錄與H-IDS 的攻擊特徵分析模組相比對，例如，特殊字串比對或封包特徵是否遵循RFC 標準等，若發現有符合攻擊特徵者，立即中斷此連線，並通知管理人員做適當的處理及反制。H-IDS能偵測個別使用者的上線使用記錄，例如，使用者的連線、對重要檔案修改或刪除、用哪些程式開啟哪些檔案、系統對外開啟 連接埠的記錄等，及監測兩主機之間點對點的加密連線，提供管理者詳盡的記錄與點對 點連線的防護。

第六、使用者身份驗證密碼：防止未經授權的使用者擷取系統資訊，也可防止合法使用者存取授權以外的資訊。

1.導入ISO 17799 9.4.6 控制方法，在必要時利用網址轉換（NAT）機制轉換內部網址，不讓外部使用者知道內部的IP 位址，因而，亦無從直接加以攻擊。

2.導入ISO 17799 9.5.1~4 控制方法，在使用者帳號與密碼控管存取權限外，可以訂定較為嚴謹的鑑識存取機制，例如，指紋、聲紋比對、智慧卡等，增加破解的困難度。

3.導入ISO 17799 9.4.4 控制方法，建議利用MAC 的唯一識別特性，因為在網際網路上的每個網路介面，都有一個特定的網際網路位址（Internet Address,

即IP Address），這些位址是由32位元的數字所組成，當兩部主機欲在網際網路上溝通 時，會藉由網域名稱系統（Domain Name System,DNS）所提供IP 位址與主機名稱（Host Name）的動態對映，辨識出該主機所在網域，再將此封包訊息傳送至該網域。而在區域網路（LAN）中，當一個乙太（Ethernet）網路封包由一部主機傳送至另一部主機時，是由一組48 位元的乙太網路位址（MAC）決定此封包傳送到那個介面。利用合法的IP 與該主機唯一的MAC（IP_MAC）配對使用，正面表列合法的IP_MAC，訂定對伺服主機安全存取的過濾機制，例如，僅允許特定且合法 的IP_MAC 存取／維護檔案伺服器，以過濾不合法的封包，多一層身份存取鑑識。

第七、網路傳輸控制

1.導入ISO 17799 9.4.7、9.8.1 與9.8.2 控制方法，在網路連線後，對資訊流向應做適當的監控管理，而僅允許合法的帳號及網路位址對特定資料的存取。例如，從外部網路傳送進來的封包來源IP 卻是屬於本內部網路的位址；相對的從內部網路傳送出去的封包來源IP 卻不屬於本內部網路的位址，前者表示有人冒用本內部主機之IP 傳送封包，後者則表示有某一網路主機T已遭到入侵，而入侵者以T為跳板且以假IP去攻擊其他主機。這類不合法的封包傳輸，必須予以阻斷及禁止存取。

2.導入ISO 17799 9.4.8 控制方法，建議設定內部重要主機S傳送資料的路由繞送規則R，讓合法使用者向S 要求資料時，S 會依循我們所設定的路由路徑R傳送給使用者；對於不合法的使用者，則不提供路由服務，使之無法向S 提出服務要求，防止不合法的存取服務。

3.導入ISO 17799 9.4.8 控制方法，在封包的流向與流量控管上，可以對TCP/IP 協定的TCP、UDP 及ICMP 封包，在不同的環境上，做不同層次的控管，例如，一般傳統的DoS攻擊或掃瞄偵測，都是送出大量OSI 第三層封包進行攻擊，或利用 TCP／UDP 封包探測目標系統，甚至運用很少被監控或過濾的ICMP封包（例如，ICMP Echo、ICMP Echo Reply等建立後門），以竊取資訊，或將攻擊指令封裝於封包內進行系統攻擊等。因此，必須有效控管封包的流向與流量，才可以有效地發覺 可能的入侵管道。

4.導入ISO 17799 9.7.1 與9.7.2 控制方法，在重要節點上，例如，路由器、防火牆、伺服主機，記錄網路使用狀況、日誌記錄（Audit log）及建立系統存取稽核機制，以便後續之追蹤或監控，以提供路由／存取控制的修正資訊。

5.導入ISO 17799 9.4.1、9.4.5、9.4.9與10.3.1控制方法，對於以明文方式傳送的網路服務，例如，FTP、Telnet，易被駭客擷取／竊聽，必須做網路連線的控

管，並關閉不必要的通訊埠，避免駭客／入侵者直接對系統在該種服務上之弱點進行入侵及建立後門。

(二)管理層

資訊安全的管理，可分別從技術與管理兩方面著手，以達成組織資訊安全目標與政策，分述如下：

1.技術角度

資訊安全在技術層面，為確保網路存取的安全性，可以經由網路的安全威脅分析，瞭解資訊系統與網路所存在的弱點及潛在威脅，對系統與網路施以技術層面的存取監控[9]，例如，嚴謹的身份鑑識、採用 RBAC 的存取控制機制、網路傳輸的控制[10]、多層防火牆的防禦、非軍事區系統的設置等，以阻絕不合法的網路傳輸與存取，避免機密資料的竊取與破壞，保障組織資訊資源的安全。

2.管理角度[11]

資訊安全在管理層面，要適當的保護組織資訊資產的安全，可以經由風險評估及管理，瞭解資訊資產的類型及其個別價值，評估資訊安全漏洞對資訊設備的威脅與影響，以可接受的成本，實施保護與控制措施，例如，人員安全管理控制、系統維護控制、建立實體環境的安全防護、資料輸出與輸入控制、應變及緊急處理計畫之規劃等，防制可能影響資訊安全的風險，將危害減至最小。

(三)技術層

在網路的存取控制上，我們可以利用網路協定中各階層封包的特性，設定網路存取規則，有效監控網路封包傳輸行為，分述如下：

1.OSI應用層

可利用應用層防火牆與主機型入侵偵測系統，在應用層透過應用代理程式處理客戶端的連線要求，與檢查對主機作業系統或應用程式的攻擊行為，例如，FTP 服務程式，有自己對應的 FTP Proxy 代理程式處理連線要求，與執行檔的稽核值試算等，避免入侵者的直接連線攻擊，與應用程式的緩衝區溢位攻擊等。

利用 RBAC 的存取控制機制，管理每位使用者對組織資源的使用權限，例如，對於不同職責的使用者給予不同的存取權限，讓每位合法的使用者，僅

[9] D. Ferraiolo and R. Kuhn, "Role-Based Access Control," Proceedings of 15th NIST-NCSC National Computer Security Conference, October 1992.

[10] Z. Tari and Shun-Wu Chan, "A Role-Based Access Control for Intranet Security," Internet Computing, IEEE, Vol. 1, Issue: 5, pp. 24-34, September 1997.

[11] 行政院及所屬各機關資訊安全管理要點，http://www.dgbas.gov.tw/eyimc/switch6/law/af08.htm，2003年7月。

能存取所賦予的資訊資源，避免逾越權限的存取[12]。

2.OSI 網路層與傳輸層

可利用封包過濾式防火牆與網路型入侵偵測系統，在網路層監控 IP 標頭內容，例如，來源與目的 IP 位址、TCP/UDP 來源埠與目的埠等，阻止不符合網路存取規則的網路封包；在傳輸層監控 TCP 連線狀態，例如，失敗連線與阻斷連線，避免非法的入侵掃瞄探測行為。

3.OSI 資料鏈結層

在乙太網路環境下，可利用網路介面卡的乙太網路位址（MAC）唯一識別的特性，在資料鏈結層監控封包所傳送 MAC 內容，再與該主機所對應之合法 IP 位址做為網路存取控制之識別，此 IP_MAC 可以加強網路身份的鑑識，並可以防止不合法位址的存取。

肆、資安防護作為

一、在個人電腦安全設定方面

1.持續更新作業系統[13]

作業系統要是有出現 Bug 就會給有心人可趁之機，而防範的方法就是持續的更新作業系統來修補 Bug，不過這不能抵擋未知的病毒或是隱藏的 Bug。Unix Like 的作業系統的安全性相較於 Windows 來說安全性較高，而且能夠容忍的負載也比較大，就算遇到了阻斷服務攻擊也可以支撐一段時間，可以給網管人員暫時的時間處理問題。除了作業系統之外，應用軟體也會有 Bug 產生，盡量使用穩定且安全的版本不讓駭客有可趁之機。

2.關閉Broadcast功能

Broadcast 會造成不必要的網路流量，一般的 Router 可以阻擋全域廣播來區隔廣播領域，但是並沒有禁止指定網域的廣播，也就造成了可趁之機。一般的情況下，外部的機器並不會需要對內要求廣播，所以這項功能是可以關閉的。如此也可以減少部分的流量和 Router 的負擔。不過網管人員和 WinNT 有時候會需要用到 Broadcast 的功能，如果關掉了會造成使用上的不便，所以需要搭配存取控制來使用。

3.封包過濾

限制封包的來源和目的，甚至可以限制封包的目的 Port。建立存取列表，

[12] 東海大學網路安全白皮書，http://dado.thu.edu.tw/research/p2/2/whitepaper.htm，2003年7月。

[13] R. Power, "2002 CSI/FBI Computer Crime and Security Survey," Computer Security Institute, 2002. (Available: http://www.gocsi.com/, July 2003.)

把不符合條件的封包全部過濾，可以減少網路的流量也增加了網路安全性。但是封包過濾會降低封包通過路由器的時間，同時也增加了路由器的負擔，如果封包過濾的條件式太過複雜，會導致網路變慢的反效果。

關閉 ICMP 的 Echo Reply 功能：不過有可能會導致 Ping 的指令無法使用，造成使用上的不便。如同前面所說，網管人員也會需要用到 ICMP 的指令來檢測網路流通，如果關閉了此功能會增加網管人員的負擔。

4.安裝防火牆

防火牆可以過濾封包，阻擋掉駭客蓄意製造的封包，也可以限制網路存取的權限。如果搭配防毒軟體，可以防止惡意病毒的入侵也可以避免網路從內部被破壞。不過防毒軟體的病毒碼必須要常常更新，不然裝了也是白裝。硬體的防火牆效能比較好，而且比較好管理和維護。

5.人為因素

離開主機一定要登出。使用有編碼過的網路連線，像是無線網路的 WEP，不使用 Telnet 改用 SSH （secure shell），以免被封包竊取。使用像是 ICQ 等直接連線軟體要小心，ICQ 的漏洞不少，很容易可以查到對方的 IP 也可以查到開啟的 Port，進而可以進行破壞。網路上陌生人給的軟體，圖片，影片都有可能是病毒隱藏的所在，一執行就會被植入了木馬程式。

二、在個人網路使用安全設定方面

1.個人電腦及伺服器應安裝防毒軟體，定期或不定期進行偵測、掃毒，並隨時更新病毒碼及掃描引擎，以防止病毒入侵。

2.謹慎使用可掃除電腦病毒及系統回復軟體;使用前應充分了解電腦病毒特性，以及確定解毒軟體的功效。

3.若遭病毒感染後，應立即追蹤病源並掌握擴散狀況，且徹底進行消毒。

4.不任意進入主題或意圖不明的電腦網站。

5.傳送電子郵件前應先檢查本身是否含有病毒，收件後亦應先檢查確定後再開啟。

6.安裝網路防毒系統，以攔截、防制病毒進入區域網路，使電腦病毒無法侵入單位內部。

7.檔案伺服器（FTP）上傳及下載之檔案應先進行掃毒。

8.做好系統備援環境並定期備份資料，以防系統遭破壞時能配合災變應變程序即時恢復運作，例如資料碟備份或Ghost。

9.不開啟來路不明的電子郵件，不安裝、不執行來路不明的軟體。

10.關閉不必要的網路服務。

11.隨時注意電腦網路安全相關議題，定期檢視系統記錄檔、安裝最新修補程式，並建立網路保全重大事件聯絡之管道。

三、在資料封包安全管制方面

要檢查這些封包內容，必須建置入侵偵測系統（Intrusion Detection System,IDS）[14]，而在不影響網路效能的情況下，於網路系統重要節點蒐集各種封包，並分析之，做法則是透過封包的監視、安全審計與攻擊辨識等，判斷是否有違反安全策略或攻擊行為，即時地向管理人員反應與警示，以提昇系統安全[15]。

在充分瞭解網路面臨的入侵攻擊及威脅後，我們將提出利用網路封包的特徵、身份鑑識與多層防禦等機制，來建構一個比較安全的防護系統，以有效保護內部重要主機及其中的資料。在技術層面之控制，置重點於電腦系統在技術層面執行安全控制，因此，而對系統的弱點、缺失、不完善及漏洞，必須適當地利用身份鑑識、存取控制[16]、傳輸控制等不同安全等級的工具或技術彌補之，以建構安全偵測防護體系。另外，在技術層面上應有嚴謹的身份鑑識，內部設立強韌的使用者身份驗證機制可採用晶片卡配合密碼，使其不易遭破解，可以防止未經授權的使用者擷取系統資訊，也可以防止合法使用者存取授權以外的資訊。

伍、結論

現今之戰爭型態，勝負成敗之決勝點，首在於資訊與情報的掌握；敵我雙方，孰可竊取得知對方的機密資料，即可率先知悉對方之一舉一動，而洞察機先，搶佔優勢位置。因此，網路防禦之首要任務，在於確保我方之通訊與資訊安全。

許多單位在網路工程初期建設時，工程主要由單位資訊官負責建置，而網路真正的維護管理人員隨著人員調動及交接時，新進人員由於缺乏對系統的瞭解，造成維護管理工作只是浮於表面。常常由於網路管理人員在平時的維護過程中，忽視了對網路安全管理的重視，加上內部人員未確實遵守軍網與民網實體分離的規定，使得系統很脆弱，從而給不法入侵者以可乘之機。

---

[14] B. Mukherjee, L. T. Hoberlein and K. N. Levitt, "Network Intrusion Detection," IEEE Network, Volume: 8, Issue: 3, May 1994, pp. 26-41.

[15] 賽門鐵克公司，入侵偵測系統－降低網路安全風險，http://www.symantec.com/region/tw/enterprise/article/intrusion_detection.html，2003年7 月。

[16] 強化企業資安利器：入侵偵測，http://taiwan.cnet.com/enterprise/people/story/0,2000040558,20063241-2,00.htm，2003 年7 月。

資訊安全的確保首先是人員的心態，不可馬虎，或因循苟且。一切必須依照規定，比照標準作業程序，依序確認經理手續，並確實填寫與紀錄表簿冊。並且，將一切通資處理設備，例如電腦，儲存設備，傳輸設備...等，皆必須依照該設施所處理執行的資料機密等級，予以分類與標籤，確實控管所有硬體設施的現有狀況。最後也是最重要的，是軍民網分離，以及公務不家辦。存放重要資料之設備，切忌不可與民用網路連上，不可公務家辦，連過民網的電腦不可以再連軍網，目的就是要防止與外界的直接或間接接觸，以 OSI 七層的觀念來解釋，越下層的過濾機制是越穩定、越沒有漏洞的，而想阻擋資料外洩的最佳手段就是直接從實體層下手，也就是網路線不要往外接，才能有效防止駭客跟木馬。