

台灣網路安全性之評估

林秉忠*、陳嘉玫*、陳年興*、黃世昆⁺

* 國立中山大學 資訊管理學系

⁺ 中央科學研究院 資訊科學研究所

摘要

電腦網路安全是所有的系統管理者與使用者都很關心的一個課題，但是由於電腦系統的高度複雜，沒有一個管理者可以保證所管理的系統沒有任何的漏洞存在；更由於網際網路的發達，使得系統安全的資訊很容易的在網路上被傳遞。系統管理者如果不能及時取得最新的資訊，就很容易導致系統被駭客侵入。以資訊戰的觀點看來，攻防雙方的關鍵在於新資訊與新技術的產生與取得，能夠掌握新的資訊與技術的一方就擁有主動權。

本研究希望探討網路安全相關技術，收集我國網際網路安全的相關資訊，評估台灣地區網站的安全性，加以分析檢討，並提出改善的建議。本研究調查分為伺服器版本調查以及 CGI 安全檢查兩大階段。由於不同的 Web 伺服器及其各版本有不同的系統安全漏洞，本研究調查除了收集各 Web 版本資訊外，另外針對各版本的 Web 伺服器 具有的系統安全漏洞進行資料收集。

關鍵字：網路安全，網際網路，資訊戰

1. 緒論

近年來由於電腦科技的普及，以及我國大力推動國家資訊基礎建設 (NII)，使得網路普及至各公司行號及家庭中，人們的生活大量倚賴電腦系統的正常運作。在此同時，網路入侵事件也越來越頻繁，根據 CERT/CC 的統計數據，1998 年電腦入侵事件較 1989 年增加了約 30 倍；此外根據美國國防部資訊部門 (DISA) 的統計顯示，透過網路入侵被發現的比例低於百分之四。

根據 FBI 於 1999 年四月提出的一項電腦安全調查報告顯示，有 62% 的單位發現過去一年內有越權的電腦使用；有 57% 的單位指出 Internet 為常見的入侵管道；有 163 個單位在網路入侵事件上遭受損失，損失總額高達一億兩千三百七十萬美元。這些數據顯示了不論個人或企業，皆必須正視網路安全的重要性，以保護重要資料與電腦資產。

隨著網路的日漸普及，透過網路進行入侵行為也越來越普遍，根據 Howard 分析 CERT/CC 自 1989 年至 1995 年的入侵求助事件顯示，透過 Internet 入侵的事件有逐年增加的趨勢[Howard, 1997]。

系統管理者最煩惱也最擔心的問題就是：電腦系統是否有漏洞，因為一旦

系統有未發現的漏洞存在，就隱含了遭受入侵者利用的可能性。系統管理者與入侵者的戰爭中，系統安全漏洞的資訊的獲得是決定性的因素。我們碰到的問題是：這些資訊該如何獲得？有沒有一個好的工具可以協助我們解決系統安全資訊不足的問題？如何有效的評估目前系統的安全狀況？對於目前現有的網路安全問題該如何補強？

國外的研究單位對於網路及作業系統安全檢查工具的研發也相當的熱中，目前已經有相當多的產品出現，例如 COPS (Computerized Oracle and Password System) [Farmer, 1991], Tripwire [Kim, 1994], SATAN (Security Administrator's Tool for Analyzing Network) [Freiss, 1998] 等等。不但有相當多的研究單位對網路安全的議題進行研究，甚至也已經出現許多家生產商業軟體的公司，撰寫安全檢查軟體，提供安全檢查及補強的服務。

本研究將探討網路安全相關技術，這些技術能解決網路安全上面臨的哪些問題，以及這些技術的限制。此外，隨著網路的日漸普及，Web 網站已經成為重要的資訊來源，而 Web 網站內容的竄改更成為最常被發現的駭客攻擊行為之一。因此，本研究希望藉由了解收集並分析 Web 伺服器的安全資訊，評估台灣地區 Web 網站的安全性。

2. 文獻探討

電腦安全涵蓋的範圍大致可以以圖 1 的層級結構來表示：

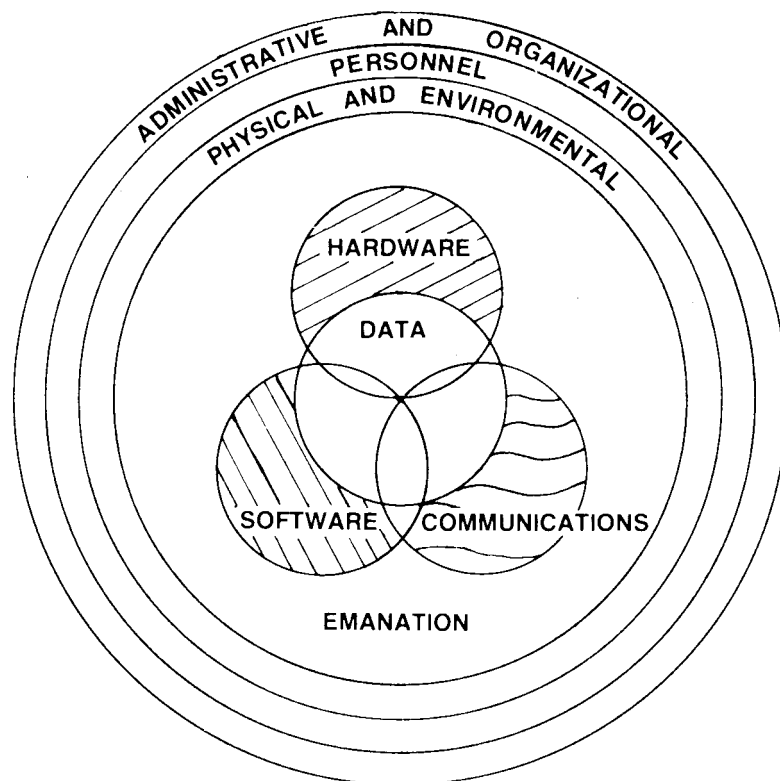


圖 1、電腦安全涵蓋之範圍[Carroll , 1987]

依照一般的分類方式，廣義的電腦安全包含以下幾個構面 [Icove , 1995]：

- 實體安全 (Physical Security)：實體安全保護電腦設施，如實體建築、電腦主機及其周邊、磁碟、報表以及文件等。實體安全避免對這些設施的竊取及破壞。實體安全也確保電腦設施不受天然災害 (如地震、水災、閃電) 以及其他環境因素改變 (如停電、系統過熱) 所造成的傷害。
- 人員安全 (Personnel Security)：人員安全涵蓋的範圍相當廣泛，增進電腦安全僅是加強人員安全的目標之一。人員安全的目的在於阻止來自人員的安全威脅，包括員工、廠商、犯罪者及其他可能的安全威脅來源。針對人員的背景調查以及作業監控是人員安全的重要組成元件。
- 通訊及資料安全 (Communication and Data Security)：通信安全目的在於保障資料傳送的安全，包括了郵件、電訊、傳真以及網際網路通訊的安全。在網際網路日漸風行的今日，網際網路通訊的安全已經成為企業應該特別注重的項目之一。
- 作業安全 (Operations Security)：作業安全的目標在於防止潛在的犯罪者遂行電腦犯罪，並且提高對電腦犯罪的注意。

Carroll [Carrol , 1987]認為在一個共享資源的電腦上，可能發生的攻擊出現在：

1. 中央處理器(Central Processor)
2. 儲存媒介(Storage)
3. 通訊線路(Communication Lines)
4. 遠端之終端機(Remote Terminals)
5. 使用者認證(Users)
6. 系統管理員(Systems Personnel)

可能的攻擊來源及攻擊方式如圖 2 所示。

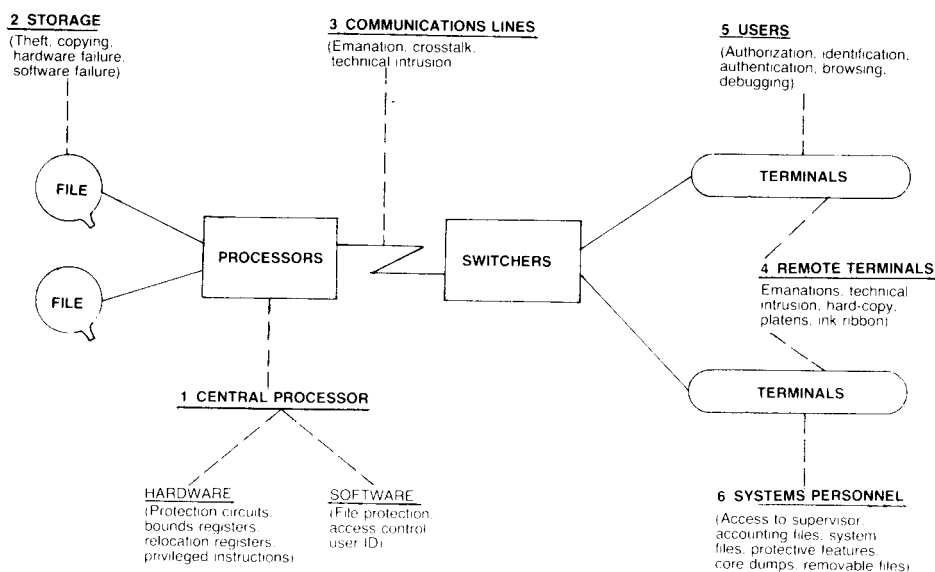


圖 2、資源分享之電腦系統中可能產生的漏洞[Carroll, 1987]

2.1 電腦安全評估

Survivable Network Analysis (SNA) [Ellison, 1999] [Linger, 1998] 是卡內基—美濃大學 (CMU) 軟體工程研究所 (Software Engineering Institute, SEI) 所發展的一套電腦安全評估方法。這套評估方法注重電腦系統的重要服務 (Essential Service) 與重要資產 (Essential Assets) 遭受入侵與攻擊時的存活能力 (Survivability)；存活能力意指在此狀況下電腦系統是否仍能提供正常的服務。而所謂的重要服務與資產指的是電腦系統在提供目標任務時所不可欠缺的功能。

存活能力依循三項重要指標評估，也就是三個 R：Resistance，Recognition，與 Recovery。Resistance 指的是系統抵抗入侵的能力；Recognition 指當系統遭受入侵時，是否能夠發現入侵行為，進而對入侵行為的影響進行評估；而 Recovery 則是整個 SNA 方法的特點，意指在重要服務及資產遭受攻擊時，維持重要服務及資產正常運作，有效的限制傷害的影響，以及在攻擊後完整的回覆服務的能力。

SNA 安全評估方式分為四大步驟：System Definition、Essential Capability Definition、Compromisable Capability Definition 以及 Survivability Analysis。其進行步驟如圖 3 所示。

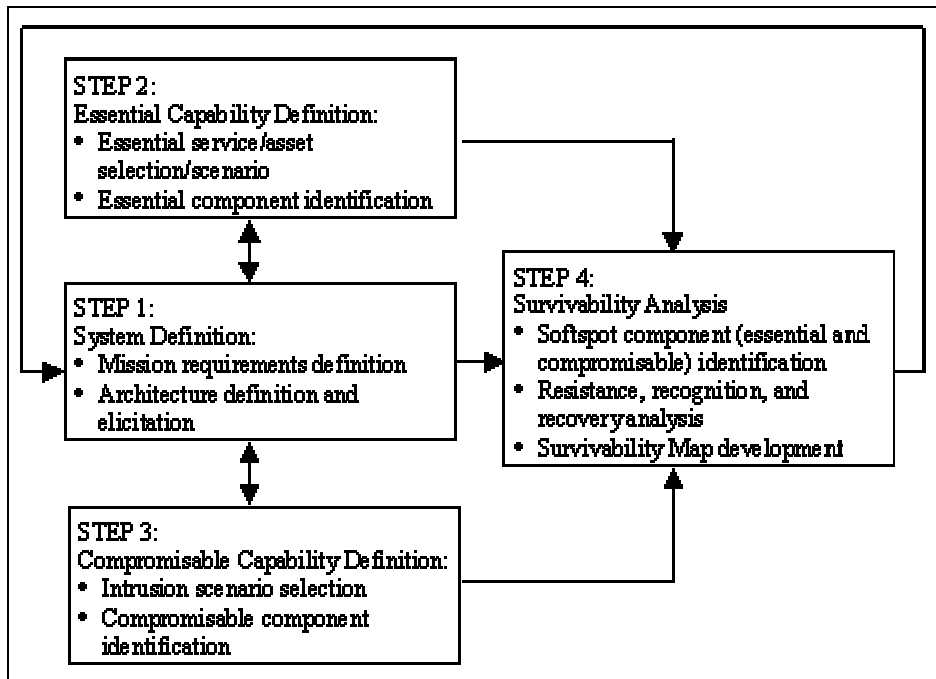
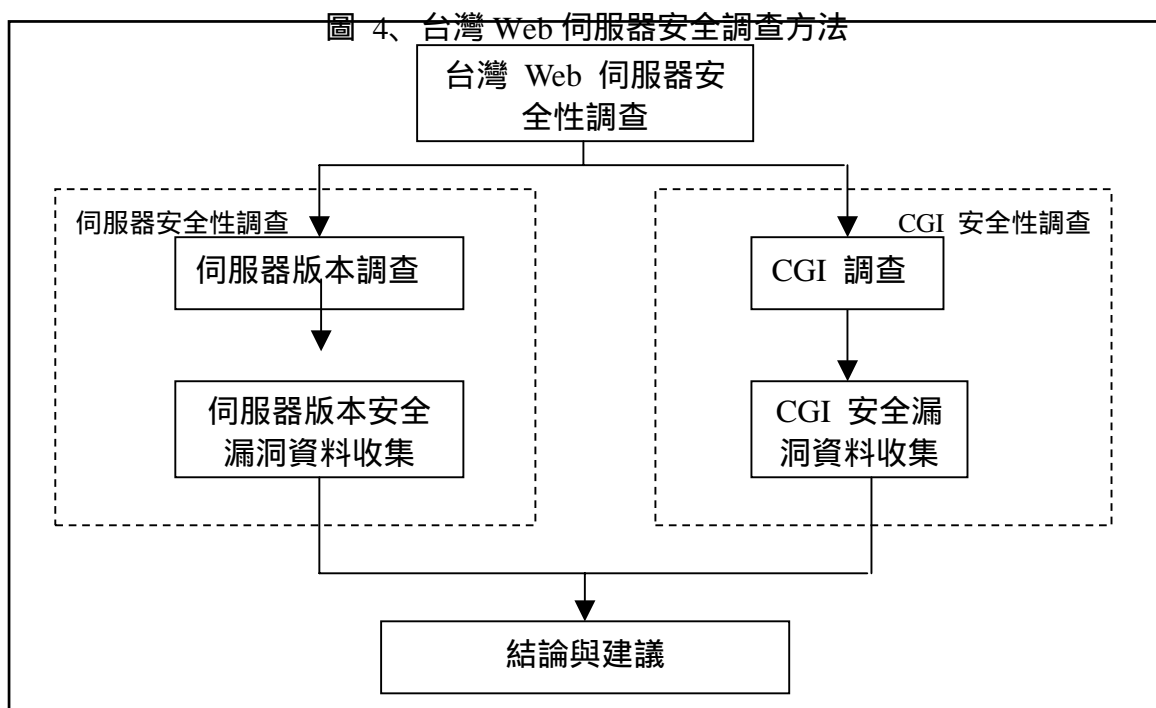


圖 3、Survivable Network Analysis Method [Ellison , 1999]

3. 台灣 Web 伺服器安全性調查

本研究調查分為伺服器版本調查以及 CGI 安全檢查兩大階段，進行的方式如圖 4 所示。Web 伺服器版本調查針對全台灣有登記 Domain Name 的六十萬台主機進行普查，運用程式連接 Port 80 (http)，紀錄各種不同廠牌之 Web 伺服器及其版本分布情形。

此外，由於不同的 Web 伺服器及其各版本有不同的系統安全漏洞，本研究調查除了收集各 Web 版本資訊外，另外針對各版本的 Web 伺服器 具有的系統安全漏洞進行資料收集。



3.1 伺服器版本及安全漏洞資料

對於全球 Web 伺服器的版本調查以及分布, NetCraft 自 1995 年中起進行了持續性的調查, 如圖 5 所示。但是 NetCraft 對於 Web 伺服器的版本統計目的僅在於了解各廠牌伺服器的佔有比例, 並未針對各版本 Web 伺服器的分布比例提出報告, 加上該組織未能有效掌握台灣網路的詳細資料以及網路連線速度不理想, 所提出的報告並不詳細。

根據該組織於 1999 年五月提出之報告, 全台灣約有 13,000 台左右的 Web 伺服器, 然而根據本研究所得之資料, 全台灣 Web 伺服器總數約共有 38,000 台左右。

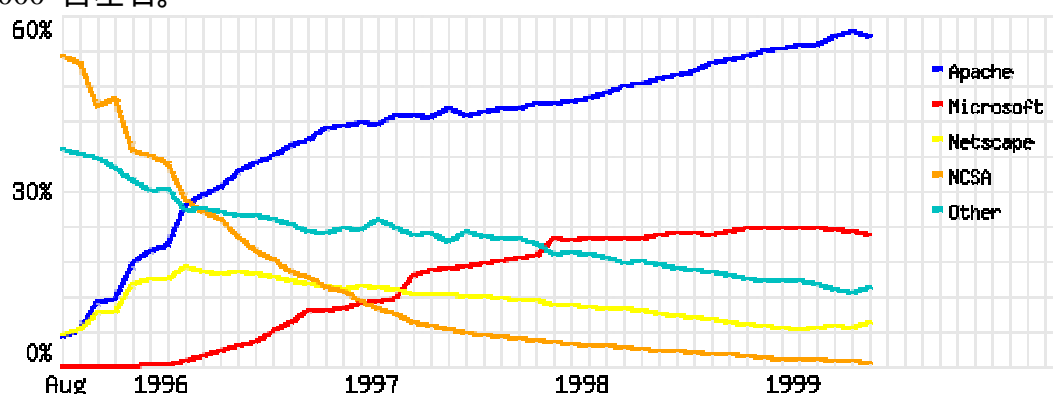


圖 5、Internet Web 伺服器佔有率分布趨勢 (1996-1999)

來源： NetCraft (<http://www.netcraft.com>)

由 NetCraft 的調查報告可以發現, Internet 上的 Web 伺服器以 Apache Web 伺服器佔最大宗, 並且與 Microsoft IIS 伺服器同步成長。由於 Apache Web 伺服器大多以 Unix 平台為基礎, 而 IIS 僅有 Windows NT 的版本, 所以我們可以得知 Internet 上的 Web 伺服器 大多是 Unix-based 的機器。

CERN Web 伺服器由於自 1996 年七月 3.0 版推出後就沒有再更新版本, 由一開始的領導地位已經退出市場。Netscape Web 伺服器也喪失了競爭力, 佔有率不斷下滑。整個 Internet Web 伺服器由 Apache Web 伺服器以及 Microsoft IIS 伺服器兩者相互競爭。

Web 伺服器 名稱	數目	百分比
Microsoft – IIS	16334	42.71 %
Apache	16199	42.52 %
Netscape	2159	5.67 %
Microsoft Personal Web Server	592	1.55 %
Lotus Domino	460	1.21 %
WebSite	424	1.11 %

NCSA	337	0.88 %
CERN	297	0.78 %
Rapid Site	202	0.53 %
其他	1154	3.03 %
總計	38158	100 %

表 1、台灣 Web 伺服器佔有率 (1999/6)

來源：本研究

由本研究調查台灣地區 Web 伺服器的分布與 NetCraft 調查所得的台灣 Web 伺服器版本的分布進行比對，發現兩者的趨勢極為吻合，如表 1 所示。與 NetCraft 調查所得的 Internet Web 伺服器市場佔有率趨勢相比對，台灣地區的 Web 伺服器版本分布與 Internet 環境有相當大的不同。台灣地區的 Apache Web 伺服器與 Microsoft IIS 的比例大約是 1：1，這也顯示了台灣地區的伺服器以 PC 平台為主，執行 Microsoft Windows NT 作業系統。

以下將針對國內兩大佔有率最大的 Microsoft IIS 以及 Apache Web 伺服器，進行探討版本分布與安全性漏洞資料收集與分析。表 2 至 3 為 Microsoft IIS 伺服器之版本分布與安全性漏洞資料；表 4 至 5 為 Apache Web 伺服器之版本分布與安全性漏洞資料。

Web 伺服器 名稱	數目	百分比
IIS – 1.0	62	0.38 %
IIS – 2.0	790	4.84 %
IIS – 3.0	6179	37.83 %
IIS – 4.0	9293	56.89 %
IIS – 5.0	10	0.06 %
總計	16334	100 %

表 2、Microsoft IIS Web 伺服器版本分布 (1999/6)

版本	發表日期	名稱	影響
IIS 3.0/ IIS 4.0	1999/6/23	Double Byte Code Page	若將正在執行 IIS 的機器上，內定語系設定為 Double byte code page(如中文，日文，或是韓文)，而利用特定的 URL 結構來處理分散在虛擬目錄下的檔案需求，這種需求通常可以交由主機端進行處理。由於處理完的結果會以文字模式送回給瀏覽器，因此可能允許程式碼很輕易的被查閱。
IIS 4.0	1999/6/16	IIS Buffer Overflow	Microsoft IIS 4.0 有一個 buffer overflow 的安全性弱點，隱藏在針對 .HTR, .STM, .IDC 等類型檔案做處理的程式庫(library)裡面。

			這個漏洞可能引發 DoS 攻擊,並可能造成任意程式碼得以在 伺服器 上被執行。
IIS 4.0	1999/6/15	Malformed HTR Request	這個漏洞可以導致對 伺服器 的 DoS 攻擊,或在特定情況下,允許任意的程式碼在 伺服器 上執行。
IIS 4.0	1999/5/7	IIS File Viewers	IIS 跟 Site Server 上有一些檔案瀏覽的安全性弱點,使遠端使用者得以瀏覽任意檔案。
IIS 4.0	1999/5/7	IIS Showcode ASP	IIS 4.0 在安裝時放置了一些內定的 ASP 檔案,其中之一就是 showcode.asp,由於這個 ASP 並未檢查對方的身分,遠端使用者可以透過此 ASP 檔,以 WWW 的權限瀏覽同一個 volume 中的任意檔案。
IIS 3.0 / IIS 4.0	1999/4/11	Using FSO and ASP to Read Server Files	遠端使用者可以透過 ASP,利用 ‘../’ 的方式瀏覽檔案。可以讀取系統任意檔案。例如： http://www.server.foo/showfile.asp?file=../global.asa
IIS 1.0 / IIS 2.0 / IIS 3.0 / IIS 4.0	1998/7/8	IIS Multiple Data Streams	Microsoft NT 支援 Multiple data stream 功能,導致遠端使用者可以瀏覽在 NTFS 上的任何檔案
IIS 3.0/ IIS 4.0	1998/7/1	IIS \$DATA Error	遠端使用者可以藉由以下的方式 http://xyz/myasp.asp::\$DATA 瀏覽伺服器端的 ASP 檔原始碼。
IIS 4.0	1998/1/8	Back Door Access to Protected Files	由於系統設計時忽略了 Windows 相容 DOS 8+3 檔名的設計,遠端使用者可將長檔名轉換為 DOS 8+3 格式的檔名瀏覽,忽略原本的存取限制。
IIS 3.0	1997/6/25	Denial of Service Attack	遠端使用者可以送出超過規定長度的 URL request,導致 IIS 伺服器當機。
IIS 3.0 及之前的版本	1996/3/5	.BAT CGI Script Hole	遠端使用者可以下載任何 CGI 檔案,並且可以透過 IIS Web Server 執行 NT 主機中 DOS 指令。

表 3、Microsoft IIS 伺服器安全漏洞

Web 伺服器 名稱	數目	百分比
Apache 0.6.5	2	0.01 %
Apache 0.8.14	2	0.01 %

Apache 0.9 alpha	5	0.03 %
Apache 1.0.0	266	1.64 %
Apache 1.0.1	1	0.00 %
Apache 1.0.2	13	0.08 %
Apache 1.0.3	46	0.28 %
Apache 1.0.5	10	0.06 %
Apache 1.1 beta	12	0.07 %
Apache 1.1.0	18	0.11 %
Apache 1.1.1	378	2.33 %
Apache 1.1.3	458	2.83 %
Apache 1.2 beta	687	4.24 %
Apache 1.2.0	453	2.80 %
Apache 1.2.1	264	1.63 %
Apache 1.2.3	13	0.08 %
Apache 1.2.4	1556	9.61 %
Apache 1.2.5	1280	7.90 %
Apache 1.2.6	1705	10.53 %
Apache 1.2.7	2	0.01 %
Apache 1.3 alpha	24	0.15 %
Apache 1.3 beta	305	1.88 %
Apache 1.3.0	672	4.15 %
Apache 1.3.1	1165	7.19 %
Apache 1.3.2	856	5.28 %
Apache 1.3.3	3680	22.72 %
Apache 1.3.4	1351	8.34 %
Apache 1.3.6	999	6.17 %
總計	16199	100 %

表 4、Apache Web 伺服器版本分布 (1999/6)

版本	發表日期	名稱	影響
Apache 1.2.4	1999/4/26	NTX Enhanced Server	遠端使用者可以藉由 NTX extension 的漏洞取得 root 權限。
Apache 1.2.5 之前的版本	1998/1/6	cfg_getline()	使用者可以造成 cfg_getline() 函式 buffer overflow，獲得遠端以 apache 身分讀取檔案的權限。
Apache 1.2.5 之前的版本	1998/1/6	mod_include()	使用者可以透過 mod_include() 的函式造成 apache 的 child process

			進入無窮迴圈。
Apache 1.2.x/ Apache 1.3	1997/12/30	Apache DoS	遠端使用者可以在 URL request 中加入大量的 '/'，造成系統判斷路徑的錯誤，使得 CPU 負荷大量增加，造成 DoS 狀態。
Apache 1.1.3	1997/1/13	mod_cookie	遠端使用者可以造成 buffer overflow 的狀態，進而執行任何程式。
Apache 1.1.3	1997/1/11	Directory Index	遠端使用者可以利用假造的 URL 請求，獲得根目錄下所有的檔案清單。
Apache 1.0.3 之前的版本	1996/4/16	Escape Shell Command	遠端使用者可以利用此一漏洞執行任何程式，並且可以讀取所有擁有者為 WWW 的檔案；甚至可以利用 xterm 獲得完整的使用權限。

表 5、Apache 伺服器安全漏洞

根據版本收集的結果以及各伺服器漏洞的資料，我們可以得出台灣地區 Web 伺服器若遭遇惡意攻擊時的存活率。由於 Web 伺服器本身並不需要管理者(Unix 下為 root，NT 下為 Administrator)權限來執行，因此我們假設所有的伺服器都以正確的權限安裝，攻擊 Web 伺服器只能獲得 WWW 使用者的權限。

由於所有的伺服器都回傳了版本的訊息，所以版本訊息不列入 Information Leakage 的考慮之中，由於 CGI 程式碼內含有資料庫設定以及檔案位置等重要安全訊息，因此 Information Leakage 考慮否能瀏覽 CGI 原始碼以及獲得目錄下檔案列表之情形。至於 Relay of Internet Attack 的攻擊方式與伺服器設定有關，無法由伺服器版本資訊獲得，在此不列入調查之內。

綜合之前收集到針對 Web 伺服器安全漏洞的資訊，我們可以歸納出四種不同的攻擊方式：伺服器設定資料洩漏(Information Leakage)、服務阻絕(Denial of Service)、遠端越權讀取(Remote File Read)、以及獲得管理者權限(Web Administrator's Shell)；我們可以依照不同的攻擊強度的進行評估。表 6 為各攻擊強度下台灣 Web 伺服器的存活率。存活率的定義為： $(Total\ Hosts - Not\ Vulnerable\ Hosts) / Total\ Hosts$ 。

攻擊方式	Information Leakage	Denial of Service	Remote File READ	Web admin shell
存活率	20878/38158 (54.71 %)	14514/38158 (38.04 %)	15853/38158 (41.55 %)	20710/38158 (54.27 %)

表 6、各種不同攻擊強度下台灣 Web 伺服器存活率

3.2 CGI 安全調查

根據上節所得之 Web 伺服器版本調查報告，針對架設有 Web 伺服器的主機進行抽測，檢查 Web 伺服器上是否有危險的 CGI 存在。一共抽測了全台灣 1190 台的 Web 伺服器，約佔全台灣 Web 伺服器比例的 1/30。表 7 顯示抽樣調查樣本分布；表 8 為本研究抽樣調查之調查結果。

總數	COM	EDU	NET	ORG	GOV
1190	898 (75.46 %)	118 (9.92 %)	30 (2.52 %)	75 (6.30 %)	69 (5.80 %)

表 7、CGI 安全檢查抽樣調查樣本分布

名稱	總數	COM (COM%)	EDU (EDU%)	NET (NET%)	ORG (ORG%)	GOV (GOV%)
AT-admin.cgi	8	3(0.33%)	2(1.69%)	2(6.67%)	1(1.33%)	0(0.00%)
AnyForm2	7	2(0.22%)	2(1.69%)	2(6.67%)	1(1.33%)	0(0.00%)
CGImail.exe	6	2(0.22%)	1(0.85%)	2(6.67%)	1(1.33%)	0(0.00%)
Count.cgi	358	285(31.74%)	22(18.64%)	12(40.00%)	14(18.67%)	23(33.33%)
THC-backd00r	24	13(1.45%)	5(4.24)	5(16.67%)	1(1.33%)	0(0.00%)
UnlG-backd00r	7	2(0.22%)	2(1.69%)	2(6.67%)	1(1.33%)	0(0.00%)
_vti_inf.html	278	184(20.49%)	37(31.36%)	7(23.33%)	29(38.67%)	21(30.43%)
administrators	9	3(0.33%)	1(0.85%)	3(10.00%)	2(2.67%)	0(0.00%)
aglimpse	7	2(0.22%)	2(1.69%)	2(6.67%)	1(1.33%)	0(0.00%)
anyboard.cgi	8	3(0.33%)	2(1.69%)	2(6.67%)	1(1.33%)	0(0.00%)
args.bat	8	2(0.22%)	3(2.54%)	2(6.67%)	1(1.33%)	0(0.00%)
authors.pwd	9	3(0.33%)	1(0.85%)	3(10.00%)	2(2.67%)	0(0.00%)
bdir.samples	4	2(0.22%)	1(0.85%)	0(0.00%)	1(1.33%)	0(0.00%)
bnbform.cgi	11	6(0.67%)	2(1.69%)	2(6.67%)	1(1.33%)	0(0.00%)
campas	6	2(0.22%)	1(0.85%)	2(6.67%)	1(1.33%)	0(0.00%)
carbo.dll	4	2(0.22%)	1(0.85%)	0(0.00%)	1(1.33%)	0(0.00%)
cgiwrap	16	4(0.45%)	8(6.78)	3(10.00%)	1(1.33%)	0(0.00%)
classifields.cgi	8	3(0.33%)	2(1.69%)	2(6.67%)	1(1.33%)	0(0.00%)
codebrws.asp	94	59(6.57%)	18(15.25%)	2(6.67%)	5(6.67%)	10(14.49%)
codebrws.asp 2	33	22(2.45%)	6(5.08%)	1(3.33%)	1(1.33%)	3(4.35%)
counter.exe	20	15(1.67%)	2(1.69%)	2(6.67%)	1(1.33%)	0(0.00%)
dispopenedfile	26	18(2.00%)	4(3.39%)	2(6.67%)	1(1.33%)	1(1.45%)

edit.pl	25	13(1.45%)	6(5.08%)	5(16.67%)	1(1.33%)	0(0.00%)
environ.cgi	16	6(0.67%)	4(3.39%)	4(13.33%)	2(2.67%)	0(0.00%)
exprcalc.cfm	26	18(2.00%)	4(3.39%)	2(6.67%)	1(1.33%)	1(1.45%)
faxsurvey	93	88(9.80%)	1(0.85%)	3(10.00%)	1(1.33%)	0(0.00%)
filemail.pl	24	13(1.45%)	5(4.24%)	5(16.67%)	1(1.33%)	0(0.00%)
files.pl	25	13(1.45%)	6(5.08%)	5(16.67%)	1(1.33%)	0(0.00%)
finger	54	31(3.45%)	13(11.02%)	3(10.00%)	3(4.00%)	4(5.80%)
fpcount.exe	6	2(0.22%)	1(0.85%)	2(6.67%)	1(1.33%)	0(0.00%)
glimpse	7	2(0.22%)	2(1.69%)	2(6.67%)	1(1.33%)	0(0.00%)
guestbook.cgi	18	10(1.11%)	3(2.54%)	2(6.67%)	3(4.00%)	0(0.00%)
handler	11	5(0.56%)	3(2.54%)	2(6.67%)	1(1.33%)	0(0.00%)
htmlscript	6	2(0.22%)	1(0.85%)	2(6.67%)	1(1.33%)	0(0.00%)
info2www	8	3(0.33%)	2(1.69%)	2(6.67%)	1(1.33%)	0(0.00%)
jj	30	14(1.56%)	10(8.47%)	3(10.00%)	2(2.67%)	1(1.45%)
maillist.pl	24	13(1.45%)	5(4.24%)	5(16.67%)	1(1.33%)	0(0.00%)
man.sh	8	3(0.33%)	1(0.85%)	3(10.00%)	1(1.33%)	0(0.00%)
newdsn.exe	234	158(17.59%)	36(30.51%)	4(13.33%)	17(22.67%)	19(27.54%)
nph-publish	6	2(0.22%)	1(0.85%)	2(6.67%)	1(1.33%)	0(0.00%)
nph-test.cgi	39	23(2.56%)	9(7.63%)	2(6.67%)	3(4.00%)	2(2.90%)
openfile.cfm	26	18(2.00%)	4(3.39%)	2(6.67%)	1(1.33%)	1(1.45%)
perl.exe	8	3(0.33%)	2(1.69%)	2(6.67%)	1(1.33%)	0(0.00%)
perlshop.cgi	8	3(0.33%)	2(1.69%)	2(6.67%)	1(1.33%)	0(0.00%)
pfdisplay	8	3(0.33%)	2(1.69%)	2(6.67%)	1(1.33%)	0(0.00%)
phf..classic	22	10	6(5.08%)	3(10.00%)	1(1.33%)	2(2.90%)
php.cgi	9	3(0.33%)	3(2.54%)	2(6.67%)	1(1.33%)	0(0.00%)
rguest.exe	6	2(0.22%)	1(0.85%)	2(6.67%)	1(1.33%)	0(0.00%)
search97.vts	6	2(0.22%)	1(0.85%)	2(6.67%)	1(1.33%)	0(0.00%)
sendmail.cfm	26	18(2.00%)	4(3.39%)	2(6.67%)	1(1.33%)	1(1.45%)
service.pwd	18	12(1.34%)	2(1.69%)	2(6.67%)	1(1.33%)	1(1.45%)
showcode.asp	4	2(0.22%)	1(0.85%)	0(0.00%)	1(1.33%)	0(0.00%)
shtml.dll	257	166(18.49%)	39(33.05%)	5(16.67%)	31(41.33%)	16(23.19%)
shtml.exe	305	198(22.05)	37(31.36%)	6(20.00%)	35(46.67%)	29(42.03%)
survey.cgi	8	3(0.33%)	2(1.69%)	2(6.67%)	1(1.33%)	0(0.00%)
test.cgi	69	38(4.23%)	19(16.10%)	4(13.33%)	2(2.67%)	6(0.00%)
textcounter.pl	24	13(1.45%)	5(4.24%)	5(16.67%)	1(1.33%)	0(0.00%)
uploader.exe	18	5(0.56%)	8(6.78)	3(10.00%)	2(2.67%)	0(0.00%)
users.pwd	9	3(0.33%)	1(0.85%)	3(10.00%)	2(2.67%)	0(0.00%)

view-source	7	2(0.22%)	2(1.69%)	2(6.67%)	1(1.33%)	0(0.00%)
visadmin.exe	6	2(0.22%)	1(0.85%)	2(6.67%)	1(1.33%)	0(0.00%)
webbbs.cgi	8	3(0.33%)	2(1.69%)	2(6.67%)	1(1.33%)	0(0.00%)
webdist.cgi	10	4(0.45%)	3(2.54%)	2(6.67%)	1(1.33%)	0(0.00%)
webgais	10	4(0.45%)	2(1.69%)	2(6.67%)	2(2.67%)	0(0.00%)
websendmail	8	4(0.45%)	1(0.85%)	2(6.67%)	1(1.33%)	0(0.00%)
wguest.exe	6	2(0.22%)	1(0.85%)	2(6.67%)	1(1.33%)	0(0.00%)
whois_raw.cgi	8	3(0.33%)	2(1.69%)	2(6.67%)	1(1.33%)	0(0.00%)
wrap	10	5(0.56%)	2(1.69%)	2(6.67%)	1(1.33%)	0(0.00%)
www-sql	8	3(0.33%)	2(1.69%)	2(6.67%)	1(1.33%)	0(0.00%)
wwwboard.pl	173	135(15.03%)	21(17.80%)	10(33.33%)	3(4.00%)	4(5.80%)

表 8、CGI 安全檢查調查結果

由 CGI 的漏洞分布看來，可以很明顯看出不論在任何網域下，漏洞皆集中在數個 CGI 上。這些 CGI 包括了 counter (Count.cgi , counter.exe)，留言版 (wwwboard.pl)。另外，一些 IIS 內定的 CGI (_vti_inf.html , codebrws.asp , newdsn.exe , shtml.dll , shtml.exe)也常常沒有被管理者注意而遺留在系統 CGI 目錄內。

從這些分布趨勢看來，可以看出政府的網站大部分採用 IIS 的伺服器，因此對於一般 Unix 上的 CGI 幾乎完全免疫，但是對於 IIS 內定的幾個 CGI 漏洞並有加以注意，與其他的網域安全性相比，並沒有比較安全。

4. 結論與建議

對於改進各國的網路安全現況，Howard 的研究指出，政府應該採取以下措施：

1. 增加對於網路危機處理的預算，尤其是對網路危機處理中心 (CERT) 等單位。
2. 鼓勵使用者採取簡單的安全預防措施。
3. 鼓勵 ISP 業者加強網路安全。
4. 要求政府各單位採取適當的措施，保護機密性之資料。

由表 6 看來，台灣的 Web 伺服器單就 Web 程式而言，受攻擊的存活比例均不到五成五 (最高 54.71 %) 令人相當憂心。另外如果獲得管理者的使用權 (Web Administrator Shell) 便可任意修改網頁，因此有高達 45.73% 的 Web 網站直接攻擊 Web 伺服器便可更改網頁，使得網頁的內容非常可能遭受竄改。如果我們要將 Web 當作一個資訊的來源，或是在網站上推動電子商務，如此的安全性是令人無法接受的。

令人意外的是，這些有問題的主機大部分是使用 Microsoft IIS 伺服器，與一般系統管理者的印象不同。我們建議使用 Microsoft IIS 的企業應該注重 IIS 程式的更新與漏洞的補漏發布。這些資訊可以在微軟所提供的 Microsoft Security Bulletin (<http://www.microsoft.com/security/>) 中找到，或是由台灣電腦危機處理中心(<http://www.cert.org.tw>)的電子郵件群組中獲得。

由表 8 中我們可以發現，大部分的漏洞都是由幾個 IIS 預設的 ASP 程式造成的，因此我們建議使用 Microsoft IIS 伺服器作為 Web 伺服器的組織必須詳細檢查 IIS 伺服器的設定值及 ASP 程式的安全。

在 CGI 安全檢查的執行上，我們並沒有特意分散這些有問題 CGI 的偵測動作，因此在系統的紀錄上會留下某一特定 IP 連續對系統內部 CGI 進行偵測之紀錄，在某種程度上，這種行為可以被解釋為攻擊之前的準備，或是解讀為攻擊行為。然而，在本研究掃描之 1190 台主機中，僅有一台主機發現並詢問此一行為，顯示管理者並不常翻閱系統紀錄檔。假設真正對 CGI 漏洞進行攻擊，管理者也無法發現。因此我們建議系統管理者裝設系統紀錄檔分析程式，幫助系統管理者分析並檢視系統紀錄檔，以即時發現並處理入侵行為。

綜合以上結果，整理出以下之建議：

系統管理者：

1. 採用各種系統安全稽核工具，例如 Tripwire、COPS、TIGER 等。
2. 參考系統安全設定相關文獻，並關閉不必要之網路服務。
3. 定期檢視系統紀錄檔，並且利用系統紀錄之分析工具輔助紀錄之整理及分析。
4. 定期進行系統備份。
5. 建立網路安全重大事件聯絡之管道。
6. 注意各網路系統安全研究相關機構發表之訊息。

政府機關及企業：

1. 加強系統稽核及員工安全控管。
2. 採用網路安全加強機制，如防火牆、入侵偵測系統、網路安全掃描程式等。
3. 機密資料離線儲存，或運用加密技術進行加密。
4. 進行網路安全之風險分析，並採取適當之因應措施。

ISP 業者：

1. 提供網路使用者加密通訊之機制。
2. 加強對網路基礎建設相關設施之保護。
3. 促成保護消費者隱私及個人相關資料相關機制之建立。
4. 建立網路危機及入侵事件因應機制。

政府政策：

1. 加速網路犯罪相關法律之審查與推行。

2. 加強執法機關對網路犯罪偵查之能力。
3. 增加對網路安全相關處理單位之經費，如台灣電腦危機處理中心。
4. 鼓勵企業及 ISP 採取增進網路安全之措施。

參考文獻

- [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), 天下文化, 1996.
- [陳年興, 1998] 陳年興, 林秉忠, “TW-CERT 現況介紹”, *TWNIC Newsletter 98-1*, 1998.
- [陳嘉玫, 1998] 陳嘉玫, 張景翔, “企業使用 Internet 對內部控制之影響 – 一個風險分析方法”, Jan, 1988.
- [沈碧容, 1996] 沈碧容譯, Richard H. Baker, “Network Security – How to Plan for it and Achive for it.” (中譯:網路安全手冊-個人進修篇), 和碩文化, 1996.
- [沈碧容, 1996] 沈碧容譯, Richard H. Baker, “Network Security – How to Plan for it and Achive for it.” (中譯:網路安全手冊-企業應用篇), 和碩文化, 1996.
- [尚青松, 1994] 尚青松譯, Katie Hafner, John Markoff, “Cyberpunk – Outlaws and Hackers on the Computer Frontier” (中譯:電腦叛客), 天下文化, 1994.
- [Anonymous, 1997] Anonymous, “Maximum Security – A Hacker’s Guide to Protecting Your Internet Site and Network,” *Sams.net Publishing*, 1997
- [CSI, 1997] Computer Security Institute, “Computer Crime Costs \$100 Million,” *Internal Auditor*, June 1997, pp9.
- [Bishop, 1995] Bishop, “A Taxonomy of Unix System and Network Vulnerabilities”, Technical Report CSE-95-10, *Department of Computer Sciences, University of California at Davis*, May 1995.
- [Bynes, 1999] Bynes, “Information Risk Management: Why Now?,” <http://www.icsa.net/library/research/irm.shtml>, Mar. 1999.
- [Carroll, 1987] Carroll, “Computer Security 2nd Edition”, *Butterworth-Heinemann*, 1987.
- [Ellison, 1999] Ellison, Linger, Longstaff, and Mead, “A Case Study in Survivable Network System Analysis,” <http://www.sei.cmu.edu/publications/documents/98.reports/98tr014/98tr014abstract.html>, Mar. 1999.
- [Farmer, 1991] Farmer, and Spafford, “The COPS Security Checker System”, *Purdue University Report*, 1991.
- [Freiss, 1998] Freiss, “Protecting Networks with SATAN,” *O’Reilly & Associates, Inc.* 1998.
- [Howard, 1997] Howard, “An Analysis of Security Incidents on the Internet

- 1989-1995,” <http://www.cert.org/research/JHThesis/Start.html> . April 7, 1997.
- [Icove , 1995] Icove, Seger, and VonStorch, “Computer Crime – A Crimefighter’s Handbook,” *O’Reilly & Associates, Inc.* 1995.
- [Kim , 1994] Kim and Spafford, “The Design and Implementation of Tripwire: A File System Integrity Checker”, *ACM Conference on Computer and Communication Security* , 1994.
- [Linger , 1998] Linger, Mead, and Lipson, “Requirements Definition for Survivable Network Systems,” *IEEE Proceedings of the International Conference On Requirements Engineering*, Apr. 1998.
- [Rainer , 1991] Rainer, Snyder, and Carr, “Risk Analysis for Information Technology,” *Journal of Management Information Systems*, Vol 8, No. 1. Summer 1991, pp129-147.