

序

1991 年，大部分美國人對於 UNIX 與 Internet 的印象還停留在 1988 年曾遭「電腦病毒」肆虐的所在地。而現在，已有超過千萬的美國人把寄送電子郵件、在網路中漫遊或是購物視為日常生活的一部份。在 1991 年當時，我們將 Internet 稱為「地球村」(global village)。時至今日，Internet 則演進成了資訊高速公路，其規模不斷地擴大，也更為擁擠。所有七大洲百餘個國家的使用者們，都會以網路的方式彼此相連。

然而，儘管我們依賴網路服務的程度與日俱增，但是今日的 Internet 並不見得比 1991 年時更安全。打個比方，Internet 已經快速地成為「網際空間」(cyberspace) 的西部蠻荒。雖然學術機構與工業界的領袖長久以來都知道，連在 Internet 上的電腦具有根本上的弱點，但這些瑕疵卻是被通融，而非被改正。因此，我們在過去幾年中，見到許多在網路上違反安全性的事件；其中一個案例是超過 30,000 人的密碼被盜取，帳號被侵入；另外一個案例則是，據傳在一次未經許可的存取中，有超過 20,000 個信用卡號碼被偷取。

電腦犯罪的問題已經日趨嚴重。一個研究分析公司 Yankee Group 最近的調查顯示，因電腦安全問題所造成的生產力、顧客信心與競爭優勢損失，光是在美國企業中，每年就超過 50 億美元。【註 1】其他的研究報告，像是 Computer Security Institute 於 1995 年所發表的 Current and Future Danger【註 2】，其研究指出：

- 光是美國，電腦界與電信界每年遭受的詐騙損失，總和超過百億美元，而且還在增加中。
- 在本次調查的前十二個月內，幾乎有 25% 的機構經歷過可證實的電腦犯罪行為。
- 在 1988 至 1993 的五年期間，商業機密資料的偷竊行為增加了 260%。

另一份 1995 年的研究，Computer Crime in America【註 3】提到：

- 98.5% 的受調查企業，經歷過某種形式的電腦犯罪。
- 43.3% 的企業表示，受害於電腦犯罪的次數超過 25 次。
- 對電腦檔案作未經授權的存取，以供窺探之用（而非完全竊取），在五年之間增加超過 95%。
- 軟體海盜行為——非法複製軟體而侵犯著作權的行為，在過去五年中增加超過 91%。
- 蓄意將病毒引入企業網路的行為，過去五年中增加過 66%。
- 未經授權而存取商業資訊，並偷取機密資訊的行為，過去五年中增加超過 75%。

要記住，大部分的電腦安全事件是不會被發現、或為人所知的。

註 1 《Securing the LAN Environment · The Yankee Group · January 1994 White Paper (+1-617-367-1000)》

註 2 《Current and Future Danger: A CSI Primer on Computer Crime and Information Warfare · Power · Richard · Computer Security Institute · 1995》

註 3 《Computer Crime in America · Carter · David 與 Andra Katz · 密西根州立大學 · 1995》

在 1995 年底，Information Week 雜誌與 Ernst & Young 會計公司針對美國大部分公司做了一份調查，發現在過去兩年中，超過 20 家公司因安全問題而損失超過一百萬美元。這個調查也發現，超過 80% 的公司擁有全職的資訊安全管理人員，而接近 70% 認為電腦安全問題對公司的威脅在最近五年中有所增加。

這些數據對 UNIX 的意義為何？由於 UNIX 被廣泛地應用在 Internet 上，並且在主從式的環境中有其優勢，因此確實有許多 UNIX 機器與這些事件有關。因為 UNIX 在這些環境中會持續地被使用，日後可能涉入更多此類事件——統計數字與趨勢都令人不安。我們希望本書的新版本可以對這些新事件的範圍與數量，作某種程度的限制。

UNIX 的「安全性」？

當本書的第一版在 1991 年發行時，許多人認為「UNIX 的安全性」是很矛盾的說法。這樣的辭彙恰好與「白色的烏鴉」用法相似，互相衝突著。UNIX 高手輕易地侵入系統、奪取控制權、造成極大的混亂，畢竟在電腦社會中可以說是一種傳奇。甚至有些人完全不認為一臺執行 UNIX 的電腦能夠保持安全。

從那時開始，整個電腦界已經改變了。最近以來，許多人認為 UNIX 是一個較安全的系統...至少，當他們使用 UNIX 是這麼想的。目前，世界上有數百萬人和數千個組織使用 UNIX，而且都沒有發生重大的災難。另外，雖然 UNIX 在設計時，並沒有以軍事等級的安全性做為考量，但它仍能在某種程度上抵抗外界的攻擊，且能保護使用者不會受到系統中其他使用者無心或惡意行為的影響。經過多年來的使用和 research，絕大多數的 UNIX 安全性缺失都已被公開、且加以修正，似乎已經讓這個作業系統變得更加安全。

但事實並非如此。雖然有越來越多人使用 UNIX，但 UNIX 並沒有變得更安全。這是因為作業系統的設計與使用，兩者之間的互動仍存有基本缺陷。UNIX 的超級使用者仍然是被攻擊的焦點：任何可以變成 UNIX 超級使用者的攻擊者或內部人士，可以掌控整個系統、在程式中設置陷阱，並且任意操控電腦中的使用者——有時甚至連使用者自己也不知情。

不過有件事已經在改善了，那就是——我們對於如何保持系統安全性的瞭解程度有所增加。近幾年來，為了幫助系統管理者增進 UNIX 電腦的安全性，已經發展了許多工具程式和技術。另外一個改變就是系統管理者對 UNIX 的瞭解程度：許多公司和組織可以很輕易地聘請到一位專注於系統安全性，且將其視為首要工作的專業系統管理者，進而讓他們的系統變得更加安全。

這本書是

這本書是 UNIX 安全性的實用指南。對使用者而言，我們解釋何謂電腦安全、敘述你可能會遇到的危險、並告訴你如何維持資料的安全性與完整性。對系統管理者而言，我們將詳細解釋 UNIX 系統安全機制的運作方式，以及如何設定與管理你的電腦，以獲得最佳的保護。對所有人而言，我們將試著解釋 UNIX 的本質、其歷史沿革，以及如何順利地使用 UNIX。

這本書適合你嗎？或許吧！如果你正在管理一個 UNIX 系統，你可以從這本書學到許多讓你的電腦更安全的技巧。即使你只是一個普通的 UNIX 使用者，也應該讀讀這本書。如果你對 UNIX 系統完全是新手，閱讀本書將使你獲益良多，因為這本書對 UNIX 作業系統的概要做了完整介紹。你總不會想永遠停留在新手的階段吧！（然而，你可能會想先閱讀 O'Reilly 的其它書籍；在附錄 D 中有一些建議。）

我們在這本書所做的事，主要是蒐集有用的資訊，幫助你考量如何增加 UNIX 系統的安全性，以避免來自內部與外來的威脅。絕大部份的內容都是針對 UNIX 系統管理者所撰寫的。當我們討論資料和命令時，在大多數的例子中都沒有詳細敘述它們的運作方式，而在某些例子中我們也只說明命令的本質以及應該檢查的檔案；因為我們認為一個具有代表性的系統管理者，應該非常熟悉系統中的這些命令和檔案，或者手邊至少擁有可供研讀的技術文件。

本書對某些重點的著墨會比其它部份深，這是考慮到新手的需要。這麼作有兩點理由：確定重要的 UNIX 安全概念能以最完整的方式表達，以及讓讀者可以單獨地閱讀重要的章節（像是檔案權限與密碼）。這麼作，本書就可以標示：「要了解如何設定密碼，請閱讀第三章。」

這本書不是

這本書並不是 UNIX 的使用手冊，也不是系統管理手冊——市面上有其它更適合的書，【註】而且一個好的系統管理者，除了系統的安全性之外，必須了解的東西還很多。本書應該作為使用手冊與系統管理指南的輔助之用。

使用手冊的重要性

有些人可能會認為，一本探討電腦安全的書，卻要求讀者去研究系統的使用手冊，是一種逃避責任的行為。但事實不是如此，而是：電腦廠商更新軟體的速度遠大於（而且很少會預先通知）出版商發行新版書籍的速度。如果你對於如何增進電腦安全性很有興趣，那麼就應該利用額外的時間來閱讀使用手冊，以便驗證我們所說的是否屬實。你也應該在執行中的系統上進行實驗，以確定這些程式的行為正如文件所言。

因此，我們建議你每隔幾個月，就回頭重新閱讀使用手冊，以便熟悉你的系統。有時在獲得新的經驗後，重新閱讀使用手冊會帶給你新的體會。另外也可能會提醒你，某些還未用到的新特性。許多成功的系統管理者告訴我們，他們堅持每六到十二個月就將所有的使用手冊重讀一次！

這本書也不是一般的電腦安全書籍——我們已經儘可能將理論性的內容減到最少。因此，這本書並不能幫助你設計新的 UNIX 安全機制，但有一章可以告訴你如何撰寫更安全的程式。

我們也試著減少書中有助於侵入電腦系統的資訊。如果你的目的在此，那麼這本書可能不適合你。

我們也儘量避免提供以下建議：

註 附錄 D 中列出不少這類的書。

- 更換你的標準命令
- 修改系統的核心
- 撰寫大量程式，來保護你的系統

原因在於本書所談的是實際操作。要讓安全機制能夠有效地運作，我們必須採用普遍可行的方法。大部份商業系統的使用者都無法取得原始程式碼，許多人甚至連編譯器都無法取得。雖然可以將某些命令換成 Public Domain（公用領域；共享）的程式，而且這些程式還有原始程式碼，但這些程式不一定能夠支援由各個廠商在系統中所新增的特性。如果我們建議採用這些改變的手法，並不見得適用於所有的作業平台。

管理大幅度的改變，也是一個大問題。這不只是因為進行改變，會使系統變得非常難維護，而且可能會使得許多不同位置的架構和設定，變得無法管理。這也會讓廠商的維護工作變得更加困難——廠商要如何回答不是他們提供的軟體所發生的問題呢？

而且，我們也在網際網路上看到許多程式和建議的修補程式，但這些程式可能無法正確執行，甚至會造成危害。許多商業或教育系統的系統管理者，可能沒有足夠的專業知識來評估系統核心、架構或命令的改變，對整體安全性的衝擊。如果你會定期下載、安裝由他人所發展的修補程式或其他程式，藉以增加系統的安全性，那麼經過一段時間之後，系統的安全性將會變得更糟。

本書所涵蓋的範圍

本書英文版 *Practical UNIX & Internet Security* 共分為六個部份：包含了 27 章與 7 個附錄。本書中文版共分為上下兩冊：上冊書名為《UNIX 與 Internet 安全防護——系統篇》，收錄第 1 到 13 章與相關的附錄。下冊書名為《UNIX 與 Internet 安全防護——網路篇》，收錄第 14 到 27 章與相關的附錄。

上冊，系統篇。

第一部份，電腦安全基礎，提供了安全策略的基本介紹。其中的章節是同時寫給使用者與管理者看的。

第一章，*簡介*，提供 UNIX 作業系統的歷史與 UNIX 安全性的介紹。也會介紹本書所使用的術語。

第二章，*策略與指導方針*，探討「訂定良好策略」在系統防護中所扮演的角色。也會說明，如何在所獲得的效益與需要考慮的成本及風險間取得平衡。

第二部份，使用者的責任，提供 UNIX 主機安全性的基本介紹。其中的章節是同時寫給使用者與管理者看的。

第三章，*使用者與通行密碼*，本章與 UNIX 上的使用者帳號有關，討論的範圍包括：通行密碼的目的，通行密碼的好壞有何區別，並介紹了 crypt() 密碼加密系統的工作原理。

第四章，*使用者、群組與超級使用者*，描述如何利用 UNIX 的群組控制檔案與設備的存取，也會討論 UNIX 的超級使用者與其所扮演的角色。

第五章，*UNIX 檔案系統*，討論了 UNIX 檔案系統所提供的安全措施，以及如何以檔案擁有者對檔案與目錄的存取權，對一群使用者或電腦系統中所有的人作限制。

第六章，*密碼學*，討論編碼與訊息摘要在安全性中所扮演的角色，包含：PGP 郵件套件與數種常見編碼方式的討論。

第三部份，系統安全，主要是針對 UNIX 系統管理者。敘述如何設定 UNIX 將侵入的機率減到最低，以及限制一般使用者取得超級使用者權限的機會。

第七章，*備份*，討論如何與為何要對你所儲存的資料，作「檔案式」(archival) 備份。包含了各類機構所適用的不同備份策略。

第八章，*保衛你的帳號*，描述某些電腦「怪客」(cracker) 一開始用來侵入電腦系統的手法。了解這些「門路」並將其關閉，你就可以增進電腦的安全性。

第九章，*完整性的管理*，討論如何監督檔案系統中未經授權的更動。這包括：使用訊息摘要與唯讀磁碟，以及 Tripwire 工具程式的設定與使用。

第十章，*稽核與登錄*，討論 UNIX 所提供的「登錄」(logging) 機制，用來幫助稽核系統的使用與行為。

第十一章，*防禦程式化的威脅*，這與電腦病毒、電腦蟲，以及特洛伊木馬有關。本章包含：詳盡的小技巧，可用來抵禦這些電子害蟲。

第十二章，*實體的安全性*。如果有人因無法侵入你超級安全的系統，惱羞成怒地以大錘頭砸爛你的電腦，又該如何處理呢？本章描述了你的電腦與其中的資料所面臨的實體危險，並討論防範之道。

第十三章，*人員的安全性*，主要是考量你所雇用的人，以及他們是否適合你的整體安全措施。

下冊，網路篇。

第四部份，*網路與 Internet 的安全性*，這是關於個別的 UNIX 電腦之間，以及與外界的連線方法，並介紹這些系統被攻擊者破壞後，可能接著侵入你電腦系統的方法。由於許多的攻擊事件都來自於外界，因此對任何擁有對外連線之電腦系統的人來說，不能不讀這一部份。

第十四章，*電話的安全性*，描述數據機的工作原理，並提供逐步指令，用以測試連接在電腦上之數據機，是否隱藏了潛在的安全問題。

第十五章，*UUCP*，這是 UNIX 到 UNIX 的複製系統，可以使用標準的電話線來複製檔案、傳送電子郵件，以及交換新聞。本章會解釋 UUCP 的工作原理，以及如何確保不會損害你的系統。

第十六章，*TCP/IP 網路*，提供 TCP/IP 網路程式工作所需的背景知識，並描述可能產生的安全問題。

第十七章，*TCP/IP 服務*，討論了 UNIX 系統中常見的 IP 網路服務，並附上常見的問題與陷阱。

第十八章，*WWW 的安全性*，描述執行 WWW 伺服器時，一些能避免產生安全問題的論點。這裡所探討的論點，同樣可以應用在其它以網路為基礎的資訊伺服器上。

第十九章，*RPC、NIS、NIS+ 與 Kerberos*，討論了多種網路資訊服務。其中涵蓋了一些工作的原理，以及常見的陷阱。

第二十章，*NFS*，描述了 Sun Microsystems 之網路檔案系統的工作原理，以及潛在的安全問題。

第五部份，*進階主題*，討論各機構的網路與 Internet 互連所產生的問題。其中也涵蓋了一些經由較佳的程式技巧來增進安全性的方法。

第二十一章，*防火牆*，描述如何設置各種類型的防火牆，來保護內部網路免於受到外界攻擊者的攻擊。

第二十二章，*包裹程式與代理程式*，描述了一些常見的「包裹程式」(wrapper) 與「代理程式」(proxy)；它們可以保護你的機器與其中的程式，而不必用到原始程式碼。

第二十三章，*撰寫安全的 SUID 程式與網路程式*，描述自行撰寫軟體時常見的陷阱。並且對如何撰寫強固的軟體抵抗不懷好意的使用者這方面，提供了一些小技巧。

第六部份，*處理安全事件*，其中包含了一些在系統安全遭到損害時，應該執行的動作。這一部份也會幫助系統管理者保護系統，以免遭到誤用權限之被授權使用者的損害。

第二十四章，*找出侵入動作*，包含逐步的指示，以供你在發現未經授權人員正在使用你的電腦時，來執行。

第二十五章，*阻斷服務、攻擊與解決方法*，描述了合法的授權使用者能夠搞亂系統的方法，以及如何發現誰在做什麼事，並採取行動的方法。

第二十六章，*電腦的安全性與美國的法律*。有時，你唯一可以做的事，就是提出告訴，或是嘗試將入侵者送入監獄。本章說明了發生安全問題之後，在法律問題上可以求助的對象，並討論為何法律手段常常無法奏效。其中也涵蓋了一些：當執行伺服器的站台連線到廣域網路（譬如 Internet）時，逐漸浮現出令人憂慮的問題。

第二十七章，*你可以相信誰？*這一章是總結，重點在於：有時在線路的另一邊，你必須相信一些事情及一些人。然而，你所相信的是正確的嗎？

附錄

第七部份，附錄，包含了許多有用的列表與參考資料。

附錄 A，*UNIX 安全性的核對清單*，其中包含一份本書所建議之核對清單。

附錄 B，*重要的檔案*，是一份 UNIX 檔案系統中重要檔案的列表，以及它們所隱含之安全意義的簡要討論。

附錄 C，*UNIX 行程*，是一份 UNIX 系統管理行程的技術性討論。它也描述了一些行程的特別屬性，包括 UID、GID 與 SUID。

附錄 D，*書面的資料來源*，包含與電腦安全相關的書籍列表、文章與雜誌。

附錄 E，*電子化的資訊來源*，這是一份在 UNIX 中能夠使用的重要安全工具列表，其中也包括如何在 Internet 中尋找的指引。

附錄 F，*各類組織*，包含一些希望見到電腦世界變得更安全的組織，其名稱、電話號碼與地址。

附錄 G，*IP 服務一覽表*，列出了所有常見的 TCP/IP 協定，加上它們的埠編號，以及在防火牆中建議的處理方式。

哪一種 UNIX 系統？

UNIX 如此風行，所產生的副作用就是：世界上有許多不同版本的 UNIX；今天，幾乎每個電腦製造商都有自己的一套。直至目前為止，只有 AT&T 所賣出的 UNIX 作業系統可以稱為「UNIX」——這是由於許可證的限制。其他廠商採用的名稱包括 SunOS (Sun Microsystems)、Solaris (Sun Microsystems)、XENIX (Microsoft)、HP-UX (Hewlett-Packard)、A/UX (Apple)、DYNIX (Sequent)、OSF/1 (Open Software foundation)、Linux (Linus Torvalds)、Ultrix (Digital Equipment Corporation) 與 AIX (IBM) ——以上只是略舉一隅。實際上每一個提

供 UNIX 或類似 UNIX 作業系統的供應商，都做了一些改變。有些改變是小幅度的，但有些則非常顯著。有些改變產生了巨大的安全問題，而通常又有許多並不明顯。不是每一家廠商在進行改變之前，都會考慮到所產生的安全問題。

當我們撰寫本書第一版時，UNIX 有兩大主要族系：AT&T System V 與 Berkeley 的 BSD。也有其它較小的變形，如 AT&T System III、Xenix、System 8 等等。多年來，System V 與 BSD 系統間都有嚴重的分歧。工業界與政府大部份都是採用 System V，因為它是受支援的「官方」版本的 UNIX。而 BSD 則較受學術單位與研究者歡迎，因為它較具彈性、延展性與額外的功能。

我們在第一章曾提到，UNIX 的兩大族系在幾年前以 System V Release 4（通常稱為 V.4，或是 SVR4）的型態結合在一起。許多在 BSD 4.3 UNIX 中的優點被加入 SVR4，這造就了一個集此兩者之長的系統（遺憾的是也有所短）。這代表了目前現代化之 UNIX 版本中最具影響力的部份，當然有些值得注意的例外，就是「自由」（free）的 UNIX 版本：BSD 4.4、FreeBSD 與 Linux。

本書涵蓋了各種常見之 UNIX 版本的安全問題。特別是，我們在此處所嘗試呈現的是關於 SVR4 的題材；另外再標註与其它版本不同之處。因為我們對 BSD 系列之 UNIX 版本有長時間的經驗（與喜好），我們常會使用「衍生自 BSD 的特色」（BSD-derived features）與「衍生自 AT&T 的特色」（AT&T-derived features）兩項術語，來表示不同的特色。雖然 SVR4 兼容這兩種特色，但是你可以把「衍生自 BSD」一詞當作 BSD 系統、Ultrix、SunOS 3.x 與 4.x、Solaris 2.x，以及 SVR4；而把「衍生自 AT&T」一詞則當作 System V Release 3、Solaris 2.x，以及某個版本的 AIX 與 HP-UX。

在本書中，關於特定 UNIX 命令、選項與副作用的特定細節，是奠基於作者本身在 AT&T System V Release 3.2 與 4.0、Berkeley UNIX Release 4.3 與 4.4、NEXTSTEP、Digital UNIX（OSF/1 的新名稱）、SunOS 4.0 與 4.1、Solaris 2.3 與 2.4，以及 Ultrix 4.0 上的經驗。同時，我們也獲益於技術審閱者在 AIX、HP-UX 與 Linux 上的長期經驗。由於這些系統足以代表目前使用中的大部分 UNIX 機器，這些敘述對於大部分讀者會接觸到的機器來說，應該是足夠了。

注意 在整本書中，我們一般會將 System V Release 4 稱為 SVR4。當我們使用 SunOS 而不加版本號碼時，你可以假設我們指的是 SunOS 4.1.x。當我們使用 Solaris 而不加版本號碼時，你可以假設是 Solaris 2.x。

許多 UNIX 廠商會修改他們所提供之部份系統命令的基本行為，而 UNIX 廠商又是多如牛毛。因此，我們不會嘗試敘述每個廠商、每種版本的每項特別功能——這只會讓本書變得更厚、更難閱讀罷了。同時也會讓本書變得不準確，因為有些廠商會常常更動系統。而且，我們很不願意敘述那些未經我們詳細測試之平台上的特別功能。不論你是系統管理者或是普通使用者，有一點很重要：你應該針對所使用的特定 UNIX 系統閱讀其參考文件，以便了解本書內文與實際命令語法間的差異。這在需要依靠程式的輸出或行為來確認或增進系統的安全性時，尤其重要。

注意 在撰寫本書時，我們希望能對使用者與系統管理者，提供增進系統安全性的資訊。我們儘可能試著保證本書提供之一切資訊的正確性與完整性。然而，如前面所提，我們無法確定能夠涵蓋一切，也無法完全知道每個版本所包含的怪行及其所做的修改，再加上每種 UNIX 衍生系統的安裝方式。由於有這麼多的版本，要將相似、但不同的版本搞混，是很容易的事。因此，我們無法承諾，在遵照我們所有的建議之後，你的系統就不會被侵入；但是我們可以承諾，被攻擊的成功率會降低。我們鼓勵使用者告訴我們，他們的經驗與書中範例間的顯著差異；這些差異可能會在未來的版本中提出。

「安全」的 UNIX 版本

隨著時間的演進，許多廠商都發展出「安全」的 UNIX 版本，通常稱作「受信賴的 UNIX」(trusted UNIX)。這些系統會將各種政府標準文件中所敘述的機制、性能提昇與控制手法，加以具體化。這些加強安全性的 UNIX 版本，將會運作在「多層級安全性」(Multi-Level Security, MLS) 以及「區隔模式工作站」(Compartmented-Mode Workstation, CMW) 的環境中——它們在設計上有嚴格的限制，以防止不同安全類別(如機密與極機密)中的資料與程式碼產生混雜。Trusted Xenix 與 System V/MLS 便是兩種較為人知、可信賴的 UNIX。

「自由 UNIX 版本」面面觀

撰寫一本像這樣的書，其中的困難在於 UNIX 的版本實在太多了。而它們又各有差異：有些還不算多，有些則大不相同。正如你所見到，我們的問題是，在兩個作業系統間，即使是很小的差異，都可能造成整體安全性的巨大改變。只要更改一個檔案的保護設定，就可以將一個安全的作業系統變成不安全。

Linux 作業系統將事情變得更為複雜。這是因為 Linux 是一個不受制約、變動極大的系統。Linux 的版本極多。其中有些差異較小，像是一兩個修補程式；而有些則有極大的不同，像是不同的核心程式、驅動程式，或根本在安全型態上是不同的。

Linux 並非自由 UNIX 版本的唯一形式。在 Berkeley 4.3 釋出之後，Berkeley Computer System Research Group (CSRG)(以及一群在 Internet 上的志願團隊)正在發展一個最終的版本 BSD 4.4，以擺脫所有 AT&T 的程式碼。在某個階段，這個計畫分成了幾派，最後產生三個作業系統：BSD 4.4、NetBSD 與 FreeBSD。目前，它們各自又有好幾個版本。還有以 Mach 為基礎，再由許多來源處取得類似 UNIX 的工具程式，所集成的系統。

今日，自由 UNIX 版本的世界已是一片混亂。就像商業 UNIX 版本一樣，有幾千個版本在改進與發展。因此，如果你想安全地執行 Linux、NetBSD、FreeBSD，或是任何其它的類似系統，極為重要的一點是：你必須確切了解在電腦上執行的是什麼軟體。光是閱讀手冊可能還不夠！你可能必須閱讀程式碼，可能必須確認你所閱讀的程式碼在經過編譯之後，的確會產生你所執行的二進位碼！

另外，請注意我們不可能敘述（甚至知道）所有可能的變形與隱含意義，因此不該假定本書能夠涵蓋你系統中所有的枝微末節，如果懷疑，動手檢查就是了。

安全的 UNIX 系統，一般會加上額外的功能，包括：存取控制清單、資料標記，與加強的稽核功能。它們也會移除一些 UNIX 的傳統功能，譬如：超級使用者的特殊存取權限，以及某些設備檔案的存取權。除了這些改變之外，與標準的 UNIX 並沒有什麼兩樣。

這些系統在某些特定的政府部門之外，並不常見到。對我們來說，這些系統是否能夠受大多數人的歡迎，是很有疑問的，因為許多功能只有在考量軍事安全的情況下才較合理。而另一方面，也有一些改進能夠用在商業環境上，像是 C2 安全等級已經可以在許多 UNIX 版本上見到了。

今日，受信賴的 UNIX 系統，在許多的環境中都較難使用，也較難移植程式，而在取得與維護上更是昂貴。因此，我們在本書並不會自找麻煩地多占篇幅。如果你擁有這樣的系統，我們建議你仔細地再三閱讀廠商所提供的文件。如果這些系統能夠被多一點人接受，我們會在新版中加以說明。

本書的慣例

以下是本書所使用的慣例：

- 斜體字用來表示 UNIX 檔案、目錄、使用者、命令與群組名稱，以及系統呼叫、密碼與 URL。在新的術語與概念出現時，也作為強調之用。
- 定寬字 (courier) 用來表示範例程式碼，以及系統的任何輸出。
- 定寬斜體字 (courier) 用在範例程式碼中，表示變數的輸入與輸出（例如，檔案名稱）。
- 定寬度粗體字 (courier) 用在使用者的輸入上。

- **刪除字**用來表示不會在電腦螢幕上顯現、而由使用者輸入的字，這主要用在「通行密碼」(password)與「通行密語」(passphrase)上。

請注意，call() 用來表示系統呼叫，是為了和命令的表示法有所區別。在本書的第一版中，我們將命令表示成 command(1)，而將呼叫表示成 call(2) 或 call(3)，其中的數字表示該命令或呼叫所屬之 UNIX 程式設計手冊的段落編號。由於不同廠商在文件的段落編號上日漸分歧，我們在這一版中不再使用這種作法。（要知道位於哪個段落，請參閱你的手冊索引。）這種 call() 的習慣用法，在分辨像是 crypt 命令與 crypt() 函式庫常式時很有用。

% 是 UNIX 之 C shell 的提示符號。

\$ 是 UNIX 之 Bourne shell 或 Korn shell 的提示符號。

是 UNIX 之超級使用者的提示符號 (Korn、Bourne 或 C shell)。這通常會用在應該由 root 執行的範例中。

正常來說，我們會在範例中使用 Bourne 或 Korn shell，除非要特別標示不同之處，才會用 C shell。

[] 會在程式語法的說明中，用以括住選項值。（決不應該輸入括號本身。）

CTRL-X 或 ^X 代表使用控制字符。用法是先按著 **CONTROL** 鍵，再輸入 X 字符。

除非特別聲明，否則所有的命令之後都需要加上 **RETURN** 鍵。

感謝

我們要感謝許多人，有了他們的幫助，才使本書的第一版與更新的第二版得以順利推出。

第一版

本書的第一版最初是經由 Victor Oppenheimer、Deborah Russell 以及 O'Reilly & Associates 的 Tim O'Reilly 等人建議才產生的。

我們由衷感謝那些仔細審閱第一版手稿的人士：Matt Bishop (UC Davis)、Bill Cheswick、Andrew Odlyzko 與 Jim Reeds (AT&T Bell Labs)(也要感謝 Andrew 與 Brian LaMacchia 針對早期草稿中與網路安全有關的部份所做的批評)、Paul Clark (Trusted Information Systems)、Tom Christiansen (Convex Computer Corporation)、Brian Kantor (UC San Diego)、Laurie Sefton (Apple)、Daniel Trinkle (Purdue's Department of Computer Sciences)、Beverly Ulbrich (Sun Microsystems) 以及 Tim O'Reilly 與 Jerry Peek (O'Reilly & Associates)。也要感謝 Chuck McManis 與 Hal Stern (Sun Microsystems)，他們審閱了 NFS 與 NIS 的部份。我們感激 Willian Cook (Assistant U.S. Attorney) 與 Mike Godwin (Electronic Frontier Foundation) 審閱了有關法律的章節。Fuz Jntfgnss (Purdue) 提供了與編碼章節有關的回饋——感謝！Steve Bellovin (AT&T)、Cliff Stoll (Smithsonian)、Bill Cook 與 Dan Farmer (CERT) 都提供了精神上的支持與有用的評論。感謝 Jan Wortelboer、Mike Sullivan、John Kinyon、Nelson Fernandez、Mark Eichin、Belden Menkus 與 Mark Hanson 挑出的打字錯誤！也要感謝 Barry Z. Shein (Software Tool and Die)，他是圖像與 UNIX 歷史學家，Steven Wadlow 提供點子給 Lazlo Hollyfeld。Dennis Ritchie 的引句是取自於 Simson Garfinkel 在 1990 年夏天與他進行的一次會面。

在 O'Reilly & Associates 有許多人協助本書第一版的出版工作。Debby Russell 編輯此書。Rosanne Wagger 與 Kismet McDonough 進行改寫與製作。Chris Reilley 繪製圖樣。Edie Freedman 進行封面與內部設計。Ellie Cutler 編製索引。

特別要感謝 Kathy Heaphy，也是 Gene Spafford 堅忍支持的妻子，以及 Georgia Conarroe，是他在 Purdue University 的 Department of Computer Science 的秘書。他們在我們撰寫本書第一版時，給予莫大的支持。

第二版

我們感謝所有幫助我們改進本書第二版的人士。這本書以及完成它所需要的工作量，遠遠超過我們的想像。我們在 1995 年一月開始改寫本書，而在 1996 年三月完成，比我們預期的時間延後了好幾個月。

我們感謝 Purdue University 的 Computer Sciences Department，以及 COAST Laboratory 的朋友，他們審閱了本書早期的草稿：包括 Mark Crosbie、Bryn Dole、Adam Hammer、Ivan Krsul、Steve Lodin、Dan Trinkle 與 Keith A. Watson；Sam Wagstaff 也評論了個別的章節。

感謝我們的技術審閱者：Fred Blonder (NASA)、Brent Chapman (Great Circle Associates)、Michele Crabb (NASA)、James Ellis (CERT/CC)、Dan Farmer (Sun)、Eric Halil (AUSCERT)、Doug Hosking (Systems Solutions Group)、Tom Longstaff (CERT/CC)、Danny Smith (AUSCERT)、Jan Wortelboer (University of Amsterdam)、David Waitzman (BBN)，以及 Kevin Ziese (USAF)。也要感謝我們的特定產品審閱者，他們仔細地閱讀文字，辨認問題，並加上針對特別 UNIX 版本或產品的有用內容。包括 C.S. Lin (HP)、Carolyn Godfrey (HP)、Casper Dik (Sun)、Andreas Siegert (IBM/AIX)，以及 Grant Taylor (Linux)。

有許多人審閱了特定的章節。Peter Salus 審閱了簡介那章；Ed Ravin (NASA Goddard Institute for Space Studies) 審閱了 UUCP 那章；Adam Stein 與 Matthew Howard (Cisco) 審閱了網路的章節；Lincoln Stein (MIT Whitehead Institute) 審閱了全球資訊網那章。Wietse Venema 審閱了包裹程式那章。

《Essential System Administration. O'Reilly & Associates, 1995》一書的作者 Aeen Frisch，很大方地允許我們摘錄該書關於存取控制列表的部份。

感謝許多在 O'Reilly & Associates 的人士，他們將我們的手稿轉換成最後的成品。Debby Russell 再度執行編輯工作，並協調審閱的流程。Mike Sierra 與 Norman Walsh 提供了難以計量的幫助，將 Practical UNIX Security 的原始 troff 檔轉成 FrameMaker 的格式，並管理越來越大、且複雜的 Frame 與 SGML 工具。Nicole Gipson Arigo 是非常好的產品經理，Clairemarie Fisher O'Leary 協助生產流程，並管理承攬人的工作。Kismet McDonough Chan 進行了品質保證的審閱，而 Cory Willing 則校對手稿。Nancy Priest 建立了我們的內部設計。Chris Reilley 繪製圖樣。Edit Freedman 重新設計封面，而 Seth Maislin 提供我們完整可用的索引。

感謝 Gene 的妻子 Kathy 與女兒 Elizabeth 長期忍受「這本書」的折磨，以及許多夜晚與週末的編輯工作。Kathy 也幫忙作校對工作。

在本書的第一版與第二版之間，Simson 嫁給了 Elisabeth C. Rosenberg。特別感謝她的原因，是她能了解這個計畫所花的時間有多少。

線上資訊

與本書有關的線上資訊（譬如，勘誤、範例程式碼），可以到 <http://www.oreilly.com/catalog/puis/> 取得；台灣的讀者亦可到 <http://www.oreilly.com.tw/chinese/Security/puis/> 取得。

批評與建議

我們永遠樂意聽到讀者對出版品的意見，包括如何讓本書更好的建議、指正本書的錯誤或是建議本書往後改版時，應該再加進來的其它主題。以下是本公司的聯絡資料：

美商歐萊禮股份有限公司台灣分公司

電話：(02) 2709-9669

傳真：(02) 2703-8802

網頁：<http://www.oreilly.com.tw>

電子郵件：

market@oreilly.com.tw (行銷部)

editor@oreilly.com.tw (編輯部)

bookquestion@oreilly.com.tw (讀者疑難雜症解答)

請以電子郵件的方式與我們聯絡，這會比電話和傳統郵件方便。有興趣為本公司翻譯書籍的眾家高手，可與編輯部聯絡；如果您買到的書有印刷品質上的問題，可以寫信到行銷部；若您對書籍內容有疑義，或是發現錯字，請寫信到 bookquestion@oreilly.com.tw 與我們聯絡，謝謝您！

給電腦怪客的幾句話

在寫作方式上，我們嘗試不讓這本書成為潛在系統怪客的「指導」(how-to)手冊。如果你在尋找如何侵入系統的提示，不要買這本書。如果你是系統「怪客」(cracker)，試試將你的精力與創造力放在解決某些對我們更急迫的問題上，而不要為精疲力竭的電腦使用者與管理者製造新問題。侵入系統並不能證明什麼特殊能力，而侵入他人的機器來展示安全問題，即使只是到處看看，都是很糟糕，並具破壞性的。

本書中系統的名稱與帳號都只是範例而已，並不代表任何特定的機器或使用者。我們在這裡明確地表示，絕無任何邀請人們侵入作者或出版商的電腦，或內文中提到的系統之意。任何這樣的嘗試，如果可能的話，都會以最嚴重的罪名告發。我們了解大部分的讀者連這種念頭都不會有，因此在這裡先對你致歉。

