实用 UNIX 和 Internet 安全技术

PRACTICAL UNIX & INTERNET SECURITY

[美]Simson Garfinkel　Gene Spafford　著

王启智　申功迈
单和平　牛大刚　译

邵钟武　审校

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书是一本对 UNIX 系统和 Internet 安全有全面系统的研究和广泛深入实践的非同一般的好书。作者通过大量数据和资料、概括而生动的语言，将 UNIX 的实用性与 Internet 的安全性讲得清楚透彻。

本书的读者对象是大学高年级学生、研究和从事 UNIX 和 Internet 安全的读者。

书　　名：实用 UNIX 和 Internet 安全技术
著　　者：[美]Simson Garfinkel　Gene Spafford
译　　者：王启智　申功迈　单和平　牛大刚
审 校 者：邵钟武
责任编辑：赵　平
特约编辑：辛再甫
排版制作：华燕实业公司
印 刷 者：北京天竺颖华印刷厂
出版发行：电子工业出版社　URL:http://www.phei.com.cn
　　北京市海淀区万寿路 173 信箱　邮编 100036
经　　销：各地新华书店
开　　本：787×1092　1/16　印张:43.5　字数:1116.8 千字
版　　次：1999 年 1 月第 1 版　1999 年 1 月第 1 次印刷
书　　号：ISBN 7-5053-5010-2/TP·2479
定　　价：72.00 元
版权贸易合同登记号　图字:01-98-0095

译者的话

《实用 UNIX 和 Internet 安全技术》一书是一本对 UNIX 系统和 Intetnet 安全有全面系统的研究和广泛深入实践的非同一般的好书，作者加芬克尔(Garfinkel)和斯帕福特(Spafford)占有大量雄辩的数据和资料，使用高度综合和概括的语言，生动而极富哲理的描述，把一个驰名全球的高级操作系统 UNIX 勾画得淋漓尽至。把复杂的 Internet 的安全问题深入浅出的说得清楚透彻，令人备受启迪。它把 UNIX 的实用性和 Internet 的安全性有机地结合起来，给人们提供了进一步发挥 UNIX 操作系统在网络时代提高 Internet 安全性的正确思路和有效途径。

我们翻译这本书的目的在于向大学高年级学生，研究生和专门从事 UNIX 系统和 Internet 安全技术工作的读者提供一本全面翔实和有一定深度的参考书。

由于这本书内容丰富，涉及面宽，篇幅较长，加上时间有限，参与翻译的人又都是在大学担任教学工作的老师，译文的质量可能存在这样或那样的不足，甚至有谬译之处，因此，我们恳切希望专家和广大读者批评指正。

参加本书翻译工作的四位老师是单和平(翻译第 1 至第 9 章和前言)，牛大刚(翻译第 10 至第 13 章和封底)，王启智(翻译第 14 至第 18 章)和申功迈(翻译第 19 至第 27 章和附录)。

在本书的翻译过程中得到了王湘英，朱德锋老师和王宏兵，王镱茗，钱峰，闵贾，苏雪晴，郭晓玉等同志的大力协助，在此一并致以深切的谢意！

全书得到了邵钟武教授严谨细致的审校。对全书的整体翻译质量起到了关键作用。

本书在翻译和出版的过程中得到了电子工业出版社的热情支持和帮助，特向社领导，审校和所有同志表示诚挚的感谢！

译　者

1997.8.25. 于北京

前　言

本书的第一版问世到现在，已经五年了。在这五年期间，计算机领域内已经发生了巨大的变化！

在1991年，大多数美国人所知道的关于UNIX系统和国际互联网（Internet）的唯一事情是：在1988年，那是一个被计算机病毒大举进攻的地方。而今天，多于1000万的美国人正使用国际互联网发送电子信件，搜寻网上信息，甚至于进行网上的商业买卖。在1991年，我们还在称国际互联网为“金色的小村庄”。而今天，它已成为信息高速公路，而且它还正变得越来越宽而且越来越拥挤。借助于它，位于七大洲的数百个国家的数百万的用户实现了电子化通迅联系。

然而，尽管我们现在更加依赖于网络计算，而Internet并不比1991年时候更安全。若稍有区别的话，则是Internet迅速地成为电子计算机化空间的“未开发的西部”。虽然学术界及工业界的人士很早就知道联到Internet上计算机的基本弱点，但现在这些弱点却都被容忍了，而不是被改正了。结果，我们已经看到，在过去的几年中，许多通过网络的大量违犯安全的事件。例如，在一个事件中，有多于30000人的用户密码被窃取，帐号被侵入。而在另一个事件中，一个非法的存取，就从一个公司一次窃取了20000多个信用卡号码。

计算机犯罪是一个日益严重的问题，一个研究分析小组（Yankee Group），在它新近的一项研究中估计，由于计算机安全问题而导致生产率，顾客信任度及竞争优势的丧失，仅美国商业界就将受到每年不低于50亿美元的损失[①]。发表在1995年的计算机安全学会刊物《当前的和将来的危险》[②]上的另一项研究指出：

·由于计算机诈骗和远程通迅诈骗而造成的损失，仅仅在美国就可能达到100多亿美元，而且这损失还正在增大。

·大约百分之二十五的机构，在上述调查的十二个月中，确实经历了计算机犯罪活动。

·从1988年到1993年的五年中，月报表明，对专有的商业信息的窃取增长了260%。

另一项1995年的研究：《在美国的计算机犯罪》[③]，也指出：

·98.5%的被调查过的商业公司已经是某种计算机犯罪方式的受害者。

·43.3%的公司称自己已受到多于25次的计算机犯罪的侵害。

·非法访问计算机文件的“偷看”事件（不同于直接的窃取）在过去的五年中增长了95%。

·软件盗版，即在版权侵权中的不道德的拷贝软件事件，在过去五年中增加了91%。

·跨国界的计算机病毒侵入公司网络事件在过去五年中上升了66%。

·非法访问及窃取公司信息的事件在过去五年中上升了75%。

值得注意，还有更多的计算机安全事件不曾被发现或未被报导！

---

① "Securing the LAN Envionment", Yankee Group, 1994.1, White Paper (+1-617-367-1000)。

② Power Richard, Current and Future Danger: A CSI primer on Computer Crime andInformation Warfare. Computer Security Institute, 1995.

③ Carter, David and Andra Katz. Computer Crime in Amirica. Michigan State University, 1995.

在 1995 年底,《Information Week》杂志与《Ernst & Young》会计公司对美国的大多数公司做了一个调查,发现在过去的两年当中,由于安全上的漏洞,它们中多于 20%的公司都已经失去了价值相当于 100 多万美元的信息。这项调查也发现,多于 80%的公司都设有一个专职的信息安全负责人。大约 70%的公司认为在过去的五年中,计算机安全问题增加了。

这些数字对 UNIX 系统意味着什么? 由于 UNIX 系统被广泛地采用作为 Internet 上的操作系统,并且由于它在客户机/服务器环境中的流行,毫无疑问,有很多的 UNIX 机器已经被卷入到这些安全性事故中。而且,由于它将在这些环境中继续被应用,UNIX 还会卷入到将要到来的大多数的安全性事故中,这些统计数字和未来趋势是令人忧虑的。我们希望我们的这个新版本将有助于限制这类事故发生的范围和数量。

UNIX"安全性"?

当本书的第一版在 1991 年问世时,很多人认为"UNIX 安全性"这个词是一个自相矛盾的提法——两个词看起来像是一对反义词,很像"巨大的小虾"或"国会行动"一类的词。那个时候,在计算机界,普遍流传着"一个 UNIX 行家可以轻易闯入一个系统,操纵控制并肆意破坏这个系统"这样一类故事。一些人甚至不能够想像:"一个运行 UNIX 系统的计算机可以是安全的。"

从那时以来,计算机界已经在改变。现在,很多的人认为 UNIX 是一个相对安全的操作系统……。至少,它们是将它作为相对安全的操作系统在使用。UNIX 系统正被世界上的数百万人及成千上万个机构使用着。虽然 UNIX 没有按照军事级别的安全性来设计,它仍被设计得能够抵御有限的外来攻击,及保护用户免遭偶然事故或别的用户的恶意行为的损害。多年来不间断的应用及研究已经使这个操作系统更安全,因为大多数的 UNIX 系统的安全缺陷已被公布于众且被修补了。

然而实际上,UNIX 系统并没有随着它的日益流行而变得更安全。这是因为在这个操作系统设计和使用中的基本缺陷仍然存在。UNIX 系统的超级用户(superuser)提供了被攻击点:任何入侵者或内部用户,当他成为一个 UNIX 系统的超级用户时,就可以接管这个系统,设置程序陷阱,并挟持计算机上的用户,有时这甚至不需要他们的专门知识就能够实现。

有一件事是被改善了,那就是我们更理解了应如何保持一个计算机的相对安全。在最近几年中,很多的工具和技术已经被开发,它们被用于帮助系统管理员维护他们的 UNIX 计算机的安全。另一件被改变的事情是:系统管理员对 UNIX 的了解程度提高了。现在公司和其它机构想招聘重视计算机安全的系统管理员就相对容易多了。

本书将提供这方面的帮助。

本书提供什么

这本书是一部 UNIX 系统安全方面的实用指导书。对于用户,我们解释什么是计算机安全,描述他们可能面对的一些危险,并告诉他们如何保护他们的数据安全。对于系统管理员,我们更详细地解释 UNIX 安全体系如何工作,并说明如何配置和管理他们的计算机,以便最大限度地保护计算机的安全。此外,每一位读者都可以从中学到一些关于 UNIX 的内部机理,UNIX 的历史,以及如何保护自己免于受到损害。

这本书是否对你有用？也许有。如果你管理一个 UNIX 系统，你将能够从这本书中找到很多技巧，使你的计算机运行得更安全。即使你是一个临时的 UNIX 用户，你也应该读这本书。如果你是一个完全的 UNIX 新手，你也能够从这本书中受益，因为它包含对 UNIX 操作系统的全面概述。而且你也不希望永远只是一个 UNIX 的新手！（我们建议，你也许首先要读一些附录 D，参考书目，列出的 O'Reilly 公司的其他书籍。）

在本书中，我们所做的，是汇集了关于如何保护你的 UNIX 系统，抵御来自内部及外部两方面的威胁的有用的信息。本书中的大部分是针对 UNIX 系统管理员的。在大多数情况下，我们给出了有关的技术资料及操作命令，但是没有详细解释它们怎样工作。并且，在一些情况下，我们仅仅简单地指出所用的命令及文件的特点。因为我们考虑到，一个通常的系统管理员是熟悉这些命令和文件的，或至少有适用的技术手册供他学习参考。

本书的某些关键章节写得较详细，是针对初学者的水平而写。之所以这样做，有两个原因：确保重要的“UNIX 安全性”概念得以充分的阐述，同时使重要的章节（例如，“文件授权和口令”）能够被初学的读者阅读。因此，初学者可以凭借提示直接阅读有关章节，例如“请读第三章‘学习如何设置口令”[①]。

本书没有提供什么

本书不是作为 UNIX 系统的通用教科书而写，也不是作为系统管理的通用教科书而写——有其它合适的书可用于上述目的，并且一个好的系统管理员需要知道更多的知识，仅仅了解“安全技术”是不够的。本书可以被用作 UNIX 系统的教科书及系统管理技术手册的辅助读物。

请注意你的技术手册

也许有人认为，阅读这本关于计算机安全的书籍，就可以不去管他们的系统的技术手册。其实不然。计算机生产商更新他们的软件（并且只提供很少的注释）比出版社发行新版图书的速度快很多。因此，如果你希望你的计算机运行安全，你就有必要花费额外的时间去读你的随机技术手册，以便核对我们书中所说论述的那些。你也应该在你正运行着的系统上试验，以便证实你的系统软件的功能确实符合你的系统手册中所提到的。

因此，我们建议你每隔几个月就读一遍你的技术手册，以便保持对你的系统的熟悉了解。有时，在你有了经验以后再重读技术手册，可以增加你的视野，或者使你记起很多你未曾用过但是却很有用的技术特点。很多成功的系统管理员告诉我们，他们每隔 6 个月或 12 个月就定期重读一遍他们的全部技术手册。

这也不是一部讲述计算机安全技术的通用教科书。在本书中我们尽可能少地采用这种形式。因此，这不是一部能够帮你设计新的 UNIX 系统安全机理的书，虽然本书中有一章是在

---

① 记住要经过全书或获得另外的共享拷贝，如果你制作的几页照相拷贝，以为传播，实际就违犯了版权。这成了法律和规则范围内的坏例子，传播反对好的安全性的策略！

讲述如何编写更安全的程序。

我们在书中也尽可能地减少那些可被利用来非法闯入计算机系统的信息。如果任何人有此目的，那么这本书将不会对他有帮助。

我们也力图避免做出以下建议：

- 替换你的系统的标准命令
- 修改你的系统核心程序
- 或其它重大的保护你的系统的编程实践

这是因为本书的目的是实用性。为了使安全指标是有效的，它们必须能被普遍地应用。当前大多数商业系统的用户不能读到系统的源代码，而且很多用户甚至不能够访问他们的系统的编译器。对于替代命令的公共域信息源，不大可能得到生产商的全面支持。即使我们建议对系统做某些改动，这建议也很难适应于所有的计算机系统。

对系统进行大泛围的修改也将带来问题。不仅很多改变使系统更难于维护，而且当系统管理着数十台位于不同地方且具有不同的配置的计算机设备时，这种修改甚至是不可能实现的。这也将使生产商更难于维护他们的系统——试想，面对一个系统故障报告，而这故障又不是由他们提供的软件引起的，他们该怎样回应这个故障报告呢？

最后，我们已经发现，放在公共网络上的很多程序和修改建议是不正确的，甚至是危险的。很多商业机构和学术机构的系统管理员不具备必要的专业知识，他们很难对修改系统核心程序，系统结构或系统命令后的整体安全性能进行评估。如果有人经常性地下载和安装“第三方”提供的程序，用以改善他的系统安全性，那么它的整体安全性在以后将可能变得更糟。由于上述原因，我们主张使用原操作系统提供的工具。如果在本书中有例外，我们将给出我们的理由。

内容摘要

本书被划分为 6 个部分，共包括 27 章和 7 个附录。

第一部分，计算机安全基础，提供一个关于安全策略的基本介绍 。用户和系统第 1 章，引论，介绍 UNIX 操作系统的历史和 UNIX 系统的安全性问题，以及我们在本书中用到的一些基本术语。

第 2 章，方针与策略，介绍策略对于保护计算机系统的作用，以及风险，成本和效益之间的关系。

第二部分，用户的责任，提供一个关于 UNIX 主机安全的基本介绍。用户和系统管第 3 章，用户和口令，涉及到 UNIX 系统的用户帐户。它讨论口令的目的，解释如何产生好的口令及坏的口令，并描述 crypt()口令加密系统如何工作。

第 4 章，用户、用户组及超级用户，描述 UNIX 用户组如何控制对文件和设备的访问。它也讨论 UNLX 超级用户和特殊用户的作用。

第 5 章，UNIX 文件系统，讨论 UNIX 文件系统提供的安全机制，以及如何使对文件或目录的访问仅限于文件拥有者、用户组成员或该计算机系统所有人。

第 6 章，密码术，讨论加密技术和消息摘录在系统安全中的作用。它还讨论几种流行的加密方法(包括 PGP 邮件包)。

第三部分，系统安全，这一部分主要是面向 UNIX 系统管理员的。它描述应如何在你的

计算机上设置 UNLX 系统，以便减少系统被打断的机会，以及限制非授权用户获取超级用户特权的机会。

第 7 章，备份，讨论如何以及为什么制作你的存储数据的文档备份。它也包括对于不同类型机构应采用的备份策略的讨论。

第 8 章，保护你的帐户，描述计算机攻击者可能应用的攻击你的计算机系统的一些基本方法。通过了解那些“门”以及关闭那些“门”的方法，你可以增强你的系统安全度。

第 9 章，完整性管理，讨论如何监控对你的文件系统的非授权修改。这包括消息摘录和只志存储磁盘的使用，以及 Triwire 实用程序的设置和使用。

第 10 章，审查与登记，讨论 UNIX 的记录机制，它可以帮助你审计你的系统的的使用和行为。

第 11 章，抵御程序化威胁，介绍计算机病毒，计算机蠕虫(worm)，和特洛依木马，以及用于防范这些电子侵害的详细的技巧。

第 12 章，物理安全，如果有人由于不能侵入你的计算机系统而愤怒地要用大锤砸毁你的计算机，你该怎么办？这章讨论你的计算机和数据所面临的物理危险以及防范它们的方法。

第 13 章，人事安全，讨论你应该雇用什么样的人员，以及如何使他们适应你的安全体系。

第四部分，网络与 Internet 安全，是关于各个 UNIX 计算机相互之间和外界进行通信的方法。以及攻击者侵入你的计算机系统而破坏这些系统的途径。由于许多攻击者都来自外部，所以这部分内容对于任何一个计算机与外部有连接的人来说中到关重要的。

第 14 章，电话安全性，描述了调制解调器是如何工作的，以及为了检测你的计算机的调制解调器是否有潜在的安全问题的逐步说明。

第 15 章，UUCP，是关于 UNIX 到 UNIX 的复制系统，它可以使用标准电话线复制文件传递电子函件和交换新闻。本章还说明 UUCP 是如何工作的，以及告诉你如何确认它的损坏不会危及你的系统。

第 16 章，TCP/IP 网络，提供了 TCP/IP 网络程序如何工作的背景，并叙述了它们造成的安全问题。

第 17 章，TCP/IP 服务，讨论了在 UNIX 上形成的常用 IP 网络服务，以及随之而来的问题和弊病。

第 18 章，WWW 安全性，叙述了一些包含在运行一个 WWW 服务程序避免产生安全性问题的论点。这里讨论的论点还考虑到了其它类型的网络服务器运行的情况。

第 19 章，RPC，NIS，NIS + 和 kerberos，讨论了各种网络信息服务，包括某些有关它们如何工作的一些说明和一般缺陷。

第 20 章，NFS，叙述了 Sun Microsystem 的网络文件系统 (NFS)是如何工作的，以及它潜在的安全问题。

第五部分，高级课题，这一部分主要讨论组织机构的网络由 Internet 相互连接时出现的问题，还将讨论通过更好的程序增加网络的安全性的方法。

第 21 章，防火墙，主要阐述了如何建立各种类型的“防火墙”，以免内部网络遭受外来的入侵。

第 22 章，包装程序与代理程序，主要介绍一些共同的包装和代理程序帮助保护你的机器及不需要访问源代码的程序。

第 23 章，编写安全的 SUID 与网络程序，主要讨论当编写自己的软件时共同的缺陷，并提

示编写抵御恶意用户入侵的可靠的软件。

第六部分,处理安全事件,本书的这部分包括如果你的计算机的安全受到威胁时如何行动的说明。这些章节还将帮助系统管理人员保护他们的系统免受滥用其特权的授权用户的侵害。

第 24 章,发现闯入,包括一步接一步地沿着目录发现有未被允许的人使用你的计算机时你要逐步采取指示。

第 25 章,拒绝服务攻击与解决方法(Denial of Service Attack and Solutions),描述了合法的,受权的用户能够使你的系统不能操作的方法,你能够找出什么人干了些什么及有关对付的方法。

第 26 章,计算机安全与美国法律(Computer Security and U.S. Law)。不经常地,你能做的唯一的事是提出控告或试图将你的破坏者投入监狱。这一章描述了在有安全缺口后,你可以求助的合法手段并讨论为什么合法的手段常常是无效的。本章还包括经常接到广域网,如 Imternet 的服务器站点有关的新问题。

第 27 章,你信任谁(Who Do You Trust ?),是做结论的一章,证明了在任何地方,你需要信任一些事及人的论点。你在信任正确有结论吗?

第七部分,附录,提供了有用的对照表和参考的号码。

附录 A,UNIX 安全对照表,包含一个本书内容提出的许多建议的点对点的列。

附录 B,重要的文件,是一个在 UNIX 文件系统中重要的文件列表,以及它们的安全含义的简单的讨论。

附录 C,UNIX 进程,是一个 UNIX 系统怎样管理进程的技术讨论。还描述了进程的一些特殊属性,包括 UID,GID 及 SUID。

附录 D,电子资源,是用于 UNIX 的一些有意义的安全工具的主要列表,包括在 Internet 上如何找到它们的目录。

附录 E,组织机构,包含组织机构的名字,电话号码,及地址,这些组织机构专门从事使计算机更安全的工作。

附录 F,IP 服务表,列出共同的 TCP/IP 协议,连同它们的端口号码及所建议的防火墙处理。

哪种 UNIX 系统?

由于 UNIX 流行而带来的一个不幸的后果是,产生了许多不同版本的 UNIX;今天,几乎任何计算机制造商都有他自己的版本。由于许可权限制,直到现在,只有由美国电话电报公司(AT&T)销售的 UNIX 操作系统可以被称为 UNIX。其它的制造厂商采用其它名字,例如 SunOS(Sun Microsystems 公司),Solaris(也是 Sun 公司),A/UX(Apple 公司),DYNIX(Sequent 公司),OSF/1(Open Software Foundation),Linux(Linus Tovalds 公司),Ultrix(DEC 公司),以及 AIX(IBM 公司)等。实际上,每一个 UNIX 或准 UNIX 操作系统的提供者都将他们自己的改变加到了他们的操作系统。有些系统变动很小,然而也有些系统变动很大。这些改动中的一些带有令人激动的系统安全性的意味,然而,很不幸的是,这些暗示中的很多通常是不明显的。并不是每一个制造商在做出他们的修改以前都考虑到了对安全性的影响。

当我们写本书的第一版时,有两个主要的 UNIX 家族:AT&T 公司的 System V 以及加州

大学伯克利分校的 BSD 系统。也有一些与它们稍有不同的系统，包括 AT&T 公司的 System III，Xenix，System 8，以及一些其它的。有很多年，在 System V 和 BSD 系统间有一个尖锐的分岐。由于 System V 的地位，即它是一个被很好支持的、正宗的 UNIX 版本，因此它得到工业界及政府机构的拥护。而 BSD 系统，由于它的广度及灵活性以及额外的特点，则被学术界和开发商拥护。

如同我们在第一章，引论，中所描述，几年以前，这两个主要的 UNIX 家族，在 System V 的第 4 版（通常写作 V.4 或 SVR4）中实现了联合。BSD 4.3 系统中的很多好的特点被植入 SVR4，导致了一个组合了这两个系统中的很多最好的特点（不幸也组合了一些最糟糕的特点）的 UNIX 系统。现在它是当今最流行的 UNIX 系统的主要基础。当然还有一些例外，例如，BSD 4.4，Free BSD 和 Linux 等 UNIX 系统的自由版。

本书论述 UNIX 安全性是针对通常的 UNIX 版本。我们在书中出示的资料，均假设它是属于 SVR4 系统，同时也注释它们与其它 UNIX 系统版本的不同。由于我们对基于 BSD 版本的 UNIX 系统有较长期的经验，我们将经常用术语“基于 BSD 特点”和“基于 AT&T 特点”来提及不同的特征，即使 SVR4 可以被认为是二者的结合。当你遇到术语“基于 BSD”时可以认为是 BSD 系统，Ultrix，SunOS 3.4 和 4.4，Solaris 2.x 和 SVR4 系统。当你遇到术语“基于 AT&T”时，可认为是 System V 的第 3 版，Solaris 2.x，以及一些扩展系统，如 AIX 和 HP—UX。

在本书中一些涉及特定的 UNIX 命令，选择项及副作用的细节描述是基于作者对于 System V 的 3.2 和 4.0 版，对于 BSD 系统的 4.3 和 4.4 版，对于 NEXTSTEP 系统，对于 Digital UNIX（新名字是 OSF/1），对于 SunOs 4.0 和 4.1 版，Solaris 2.3 和 2.4 版，以及对于 Ultrix 4.0 系统的实践经验。同时也得益于我们对于其它系统，例如 AIX，HP—UX 和 Linux 的长期的实践经验。由于这些系统代表当前 UNIX 系统的主流，我们的这些描述很可能适用于读者将接触到的大多数机器。

注意

在本书中，我们通常称 System V 的第 4 版为 SVR4。当我们提到 SunOs 而没有提到版本号时，可认为那是指 SunOs 4.1.x。当我们提到 Solaris 而没有提版本号时，可认为那是指 Solaris 2.x。

很多 UNIX 生产商已经修改了它们的系统命令中的基本功能，并且存在着为数众多的 UNIX 生产商。因此，我们不可能描述每个制造厂家所发表的每个版本的每条专门特性，那样做，只能使本书更长，也更难读。还使本书不准确，因为制造商经常修改它们的系统。再有，我们也不愿意去描述那些我们还不能够全面测试的系统的特殊性能。无论你是一个系统管理员或一个初级用户，你都应该阅读你的 UNIX 系统的技术资料，以便理解你正使用的系统命令的实际语法与本书所表述的之间的不同。当你根据程序的特定功能去检验或增强你的系统安全度时，这一点尤其重要。

注意

我们写这本书的目的，是希望提供有用的信息以便帮助用户及系统管理员改善它们的系统的安全性。我们力图保证书中的每一件事准确和完整。然而，正如我们先前提到的，我们不能够肯定我们已经覆盖了每一件事。而且，我们不可能全部了解那些被加到每一个 UNIX 系

统的每一个版本上的修改及警言。此外,有如此众多的生产商,以致有时很容易被那些相似而又不同的版本搞混乱。因此,我们不能够担保你的系统安全将永远不受侵害,即使你遵循了我们的全部劝告。然而我们可以肯定,这侵害将会减少。同时,如果读者发现本书展示的事例与他们的经验有明显不同,我们也鼓励读者告诉我们;这些不同将可能在将来的版本中被提及。

UNIX 系统的"安全"版本

几个生产商已经开发了 UNIX 系统的"安全"版,又称为"trusted UNIX"。这个系统体现出一些在各种政府标准文件中描述的机制,提高和限制措施。这些 UNIX 的增强版设计成在多级安全(MLS)环境和分布式工作站(CMW)环境下工作,在那里有严格的约束规则,采用不同安全等级(例如一般保密及顶级保密)的分类,防止数据和代码的混合。"可信任的"Xenix 和系统 V/MLS 是两个众所周知的"可信任的"UNIX。

"安全"UNIX 系统通常都增加了一些额外的特性,包括访问控制表,数据标号及增强审计等。它们也去除了一些 UNIX 系统的传统特性,例如超级用户专有的任意访问特权,及对一些设备文件的存取访问。然而,尽管有这些改变,这些系统仍然遭受到与标准 UNIX 相类似的情况。

这些系统并没有被广泛采用,它们仅仅被使用在一些特定的政府机构。我们甚至怀疑,这些系统是否能够最终得到公众的广泛认可,因为它们的很多特点仅仅在军事秘密的政策范围中才有意义。而在另一方面,他们的一些增强特性在商业环境中是有用的,其中 C2 安全特性已经在很多新版的 UNIX 系统被应用。

今天,"可信任的"UNIX 系统更难用于各种不同的环境,更难用于端口程序,而且价格及维持费用更昂贵。因此,在本书中我们没有再费力去描述这些系统的这些特殊的且有争议的特点。如果你有那样一个系统,我们建议你仔细且重复地阅读生产商提供的技术资料。如果这些系统将来被广泛应用了,我们将在今后的版本中再描述它们。

面对"自由 UNIX"的许许多多

本书面对的一个困难是:有太多的 UNIX 版本。所有这些版本都互不相同。有些差别微小,但有些却差别很大。我们的问题是:在两个操作系统之间,即使出现很微小的差别,也可以导致整体安全性能上的显著差别。简单地改变在一个文件中的保护性设置参数可以使一个安全的操作系统转变成为一个不安全的系统。

Linux 操作系统甚至使事情更复杂。那是因为 Linux 是一个无政府的、多变的目标。有很多不同版本的 Linux,它们中的一些有很小的差别,例如仅多安装了一个或二个修补文件。另一些却有显著的不同,例如有不同的系统内核,不同的驱动器软件,及不同的安全模式。

Linux 不是唯一的"自由"UNIX 系统。在 Berkerley 4.3 版之后,伯克利计算系统研究组(CSRG)以及一些凭借 Internet 连接的志愿者又开发了一个最终的版本:BSD 4.4,它不含有任何 AT&T 的源程序码。开发过程中,开发小组又分成了几个小部分,结果生产出了三个操作系统:BSD 4.4,NetBSD 以及 Free BSD。今天,这些操作系统中的每一个都拥有几个版本。此外,也有基于 Mach 的"自由 UNIX"系统以及利用一些源程序构成的类似 UNIX 特点的操作系统。今天,"自由 UNIX"的世界是一个大漩涡,它就如商品 UNIX 正被几千个不同的厂商推销和开发。如果你想安全地运行 Linux,或 NetBSD,或 Free BSD,或其它的类似系统,你

必须确切了解在你的计算机上正运行着什么样的软件。仅仅读你的技术手册可能是不够的!你可能不得不读它的源程序。你可能不得不检验你在读的源代码,实际编译出你在运行的二进制代码!

此外,请记住我们不可能描述(或知道)全部可能的不同及隐含现象。因此,不要假定我们已经论述了你的系统的全部特征。当你对它有任何疑问时,你应该对它检查、核实。

本书中的约定

本书采用了如下约定:

斜体被用于表示 UNIX 文件,目录名,用户名,命令字,用户群组名,系统调用,口令,以及 URLs。它也被用于强调新引入的专业术语及概念。

小字体被用于表示代码程序举例及系统的输出。

斜体小字被用于表示变量(例如一个文件名)的输入和输出。

黑体小字被用于表示用户输入的内容。

Stike through 被用于表示那些(实际上)不被计算机显示的输入。这主要被用于表示用户键入的口令。

call()被用于表示系统调用,而不是系统命令。在本书的第一版中,我们用 command (1)表示一个系统命令,用 call (2)或 call (3)表示系统调用。括号中的数字指出这个系统命令或系统调用在《UNIX 编程手册》中被解释在哪个部分。现在由于不同的生产商的技术手册中章节标号各不相同,本书已不采用这种约定。(用户可参阅他的技术手册中的索引)。采用 call ()约定可有助于区分命令和库函数,例如,对于 crypt 命令和 crypt ()库函数调用。

% 是 UNIX 系统的 C shell 的提示符。

$ 是 UNIX 系统的 Bourne shell 或 Korn shell 的提示符。

是 UNIX 系统的超级用户提示符 (Korn ,Bourne ,或 Cshell)。

通常,在我们的举例中,我们使用 Korn shell 或 Bourne shell,除非这例子只适用于 C shell。

[] 在一个程序语法描述中表示一个可选择项。(括号本身决不能键入。)

CTRL - X 或^X 表示控制字符的应用。即:按住控制键,同时敲 X 字符键。

全部系统命令举例都用回车键 (RETURN)结束,除非另有说明。

在线信息

本书中的例子及其它一些与本书有关的在线信息均可经 WWW 或经 FTP 获取。请在本书的插页寻找关于 O'Reilly 出版社的全部在线服务。

答谢

有很多的人为本书的出版给予了很大的帮助,我们在此向他们表示衷心的感谢。

第一版

本书的第一版在 O'Reilly & Associates 出版社的 Victor Oppenheimer, Deborah Russell 和 Tim O'Reilly 的建议下开始编写。

我们衷心地感谢那些帮助我们审阅了第一版手稿的人：Matt Bishop（UC Davis），Bill Cheswick，Andrew Odlyzko 和 Jim Reeds（AT&T Bell Labs），Paul Clark（Trusted Information Systems），Tom Cristiansen（Convex 计算机公司），Brian Kantor（UV San Diego），Laurie Sefton（Apple），Daniel Trinkle（Purdue 大学计算机科学系），Beverlt Ulbrich（Sun 公司），以及 Tim O'Reilly 和 Jerry Peek（O'Reilly & Associates）。也感谢 Chuck Mcmanis 和 Hal stem（Sun 公司），他们审阅了与 NFS 和 NIS 有关的那些章节。我们也感谢 William Cook 和 Mike Godwin（电子边界基金会）对本书给予的评论，他们审阅了与法律有关的那些章节。Fnz Juntfgnss（Purdue）对与加密有关的那些章节提供了很有帮助的反馈意见！Steve Bellovin（AT&T），Cliff Stoll（Smithsonian），和 Dan Farmer（CERT）都给予了很好的支持和有帮助的评论。感谢 Jan Wortelboer，Mike Sullivan，John Kinyon，Nelson Fernandez，Mark Eichin，Belden Menkus，和 mark Hanson，他们帮助找到了那么多的排字工人！也感谢 Barry Z. Shein（软件工具，已故），他是一个优秀的 UNIX 历史学家。Steven Wadlow 提供了 Lazlo Hollyfeld 的线索。Dennis Ritchie 的引语来自于 1990 年夏季与 Simson Garfinkel 的一次会面。

在 O'Reilly & Associates 出版社的很多人都对本书第一版的出版给予了帮助。Debby Russell 编辑了这本书，Rossane Wagger 和 Kismet McDonough 也从事了本书的编辑和出版。Chris Reilly 制作了本书的插图。Edie Freedman 设计了本书的封面以及内部结构。Ellie Cutler 制作了本书的索引。

还要特别感谢 Kathy Heaphy（Gene Spafford 的妻子）以及 Georgia Conarroe（Gene Spafford 在 Purdue 大学计算机系的秘书）在此期间给予我们的支持。

第二版

我们要感谢每一个帮助我们完成本书的第二版的人。第二版的工作量远远超过了我们最初的预料。我们于 1995 年 1 月开始再写这本书；但是直到 1996 年的 3 月我们才将它完成，比我们最初的计划晚了几个月。

我们感谢那些阅读并审阅了本书最初的草稿的在 Purdue 大学计算机系和 COAST 研究室的人们：Mark Crosbie，Bryn Dole，Adam Hammer，Ivan Krsul，Steve Lodin，Dan trinkle，Keith A. Watson，和 Sam Wagstaff。

感谢我们的技术审校：Fred Blonder（NASA），Brent Chapman（Great Sircle 协会），Michele Grabb（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（Amsterdam 大学），David Waitzmann（BBN），和 Kevin Ziese（USAF）。我们也要感谢我们的产品审校，他们仔细地审校有关的文本并加入一些特殊的 UNIX 版本或产品的内容。他们是：C. S. Lin（HP），Carolyn Godfrey（HP），Casper Dik（Sun），Andreas Siegert（IBM/AIX），和 Grant Taylor（Linux）。

一些人审校了一些特定章节。Peter Salus 审校了《引言》章节；Ed Haven（NASA）审校了《UUCP》章节；Adam Stein 和 Matthew Howard（Cisco）审校了《网络》章节；Lincoln Stein（MIT）审校了《WWW》章节；Wietse Venema 审校了《Wrappers》章节。

"Essential System Administration"（O'Reilly & Associates，1995）的作者（leen Frisch 友好地允许我们引用了她书中的"访问控制表"部分。

感谢 O'Reilly & Associates 出版社的工作人员，他们使我们的草稿成为一个被完成的产品。Debby Russell 又一次组织了本书的编辑和审校，Mike Sierra 和 Norman Walse 在帮助我们将本书从第一版的 troff 文件格式转变为 FrameMaker 文件格式，以及在帮助我们管理日愈增大且日愈复杂的 Frame 和 SGML 工具集合方面提供了巨大的帮助。Nicole Gipson Arigo 出色地执行了生产管理的工作。Claremarie Fisher O'leary 也参与了生产过程并管理承包商们的工作。Kismet McDonough - Chan 对本书进行了高质量的审校。Cory Willing 校对了本书的手稿。Nancy Priest 完成了本书的内部设计。Chris Reilly 为本书制作了新的插图。Edie Freedman 重新设计了本书的封面。Seth Maislin 为本书制作了极有用的索引。

还要感谢 Gene Spafford 的妻子 Kathy 和女儿 Elizabeth，她们容忍他继续工作在这本书并且还占用了很多个夜晚和周末。Kathy 也帮助校对了这本书。

在本书第一版和第二版的编辑之间，Simson 与 Elisabeth C. Rosenberg 结婚了。我们感谢她对于这项工作所花费的时间量的理解。

问题和建议

我们已经尽可能地测试和核对了本书中的全部信息。但是你可能会发现某些事物已经改变，或发现某些印刷问题，或某些我们在本书的错误，请让我们知道你所发现的，及告诉我们你的建议。联系地址是：

O'Reilly & Associates, Inc.
103 Morris Street, Suite A
Sebastopal, CA 95472
1 - 800 - 998 - 9938（美国或加拿大）
1 - 707 - 829 - 0515（国际或本地）
1 - 707 - 829 - 0104（Fax）

你也可以发送电子信件给我们，请从本书插页中寻找有关 O'Reilly & Associates 的全部在线服务信息。

对计算机攻击者们的警告

我们以这样的一种方式编写此书，使它不易被潜在的系统攻击者们用作指导手册。如果你正在寻找非法闯入计算机系统的技巧，那请不要购买此书。如果你是一个计算机系统攻击者，请考虑发挥你的精力及创造力去解决我们共同面对的一些更紧迫的问题，而不是去给本已过度工作的系统管理员及计算机用户制造新的麻烦。破坏计算机系统，并不能证明你的能力，以及破坏某些用户的机器，去证明有安全的问题，即使你所做的仅仅是"浏览"，也是肮脏的以及破坏性的。

本书中用到的系统名及用户帐号仅仅是为举例而用。它们并不表示任何一个特定的计算机或用户。我们声明，我们没有邀请任何人去试图非法闯入作者的或出版商的计算机，或非法闯入书中提到的任何系统。任何那样的尝试在可能的时候将受到法律起诉。我们认为绝大多数我们的读者将不会那样去做，因此我们在这里向读者道歉，为了我们不得不在此做出的这个声明。

目　录