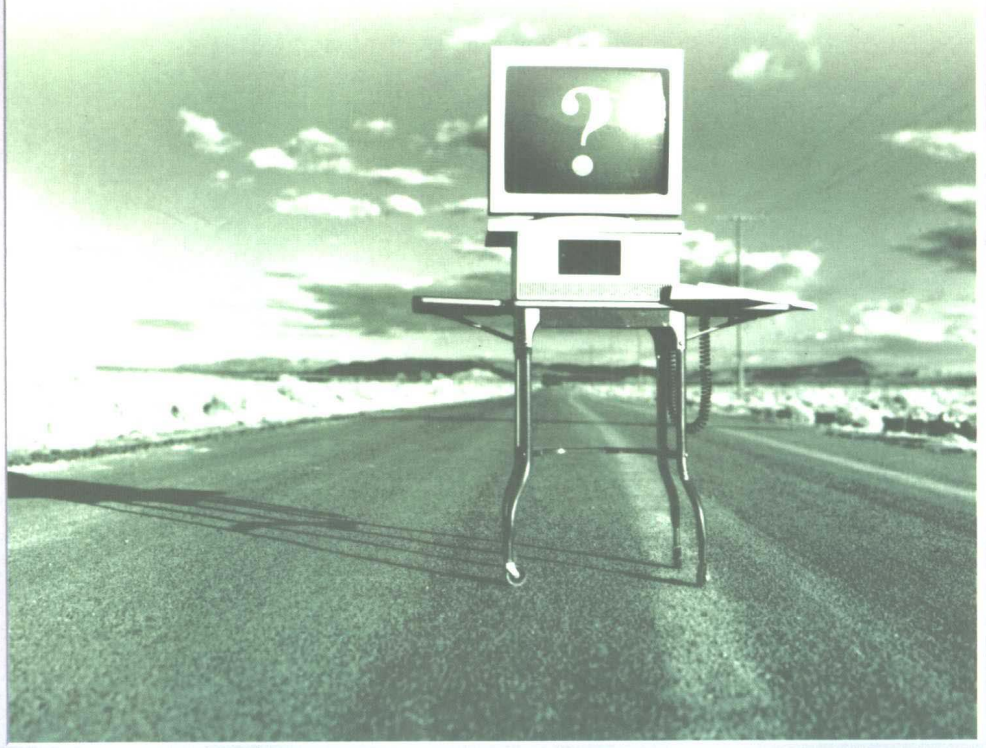
PTR PH 中国计算机学会计算机安全专业委员会推荐参考书

信息与网络安全丛书

# Solaris 安全手册



[美] Peter H. Gregory 著

潇湘工作室 译

杨智慧 刘凤昌 审校

人民邮电出版社

www.pptph.com.cn

中国计算机学会计算机安全专业委员会推荐参考书

信息与网络安全丛书

# Solaris 安全手册

[美] Peter H. Gregory 著

潇湘工作室 译

杨智慧 刘凤昌 审校

人 民 邮 电 出 版 社

中国计算机学会计算机安全专业委员会推荐参考书
信息与网络安全丛书

**Solaris 安全手册**

◆ 著 [美] Peter H.Gregory
译 潇湘工作室
审 校 杨智慧 刘凤昌
责任编辑 李 际

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街14号
邮编 100061 电子邮件 315@pptph.com.cn
网址 http://www.pptph.com.cn
北京汉魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本:787×1092 1/16
印张:18
字数:419千字 2000年10月第1版
印数:1-5 000册 2000年10月北京第1次印刷

著作权合同登记 图字:01-1999-2560号
ISBN 7-115-08728-8/TP·1779

定价:32.00元

# 内容提要

本书从各个方面介绍如何保护 Solaris 系统的安全性。全书共分为 5 部分，第一部分介绍安全性的基础知识，主要分析了安全问题的起因，并提出了系统安全的 9 大原则；第二部分介绍 Solaris 单机系统的安全保护，主要涉及到系统的启动与关闭、系统日志、用户帐号和环境、文件系统等内容；第三部分详述 Solaris 网络系统的安全保护，其主要内容有网络接口与服务、网络打印、电子邮件、网络访问控制、名称服务等；第四部分介绍灾难恢复的问题；第五部分是附录。

本书适用于安全管理员和 UNIX（特别是 Solaris）系统管理员。

## 信息与网络安全丛书 审定委员会

名誉主任：朱恩涛
主　　任：谢模乾
副 主 任：杜肤生
　　顾建国
　　徐修存
委　　员：（以下以姓氏笔划为序）
　　王亚明　冯登国　刘凤昌　吕晓春　杨智慧　屈延文
　　赵世强　赵战生　卿斯汉　高新宇　崔书昆　缪道期

# 丛书前言

随着科学技术的飞速发展，人们已经生活在信息时代。计算机技术和网络技术深入到社会的各个领域，因特网把“地球村”的居民紧密地连在了一起。如果说“天涯若比邻”在过去只是描写人们心灵上的贴近，那么今天计算机网络已使这句话变成了生活现实。近年来因特网的迅速发展，给人们的日常生活带来了全新的感受，人类社会各种活动对信息网络的依赖程度已经越来越大。

然而，凡事“有一利必有一弊”。人们在得益于信息革命所带来的新的巨大机遇的同时，也不得不面对信息安全问题的严峻考验。1999 年好莱坞推出的以网络为主题的影片《黑客帝国》风靡全球，给人们提示了这个问题的严重性。在人们对网络技术的普及叫好声尚未消失的时候，黑客攻击战在现实生活中也愈演愈烈。国内外众多的网站相继被“黑”，病毒制造者们各显其能。从 CIH 噩梦难醒，到“爱虫”病毒狂吻全球，全球“中毒”者不计其数。这些给各行各业带来了巨大的经济和其他方面损失。除此之外，“电子战”、“信息战”已成为国与国之间、商家与商家之间的一种重要的攻击与防卫手段。因此，信息安全、网络安全的问题已经引起各国、各部门、各行、各业以及每个计算机用户的充分重视。

为了提高我国各级计算机信息网络主管部门的安全意识，普及计算机安全知识，进一步提高国内计算机安全的技术水平，帮助国内技术人员汲取国外计算机安全先进技术和经验，有效保护我国信息网络安全；在公安部公共信息网络安全监察局的大力支持下，我们策划且及时推出了这套《信息与网络安全丛书》。这套丛书采用开放式选题架构，全部是从国外著名出版公司出版的有关信息与网络安全类的权威著作和畅销书中精选而成。这套丛书内容涉及计算机硬件安全、操作系统安全、工作站和服务器的系统安全、网络安全设计、网络入侵检测、网络安全理论等各方面的内容。

由于本套丛书的原版书均是由国外权威人士编写而成，因此在观念上和技术上站在了该领域的前沿。也正因为此，本套丛书受到了有关部门领导和专家的高度重视。由公安部领导和公共信息网络安全监察局及部分计算机安全专家组成的审定委员会对图书进行了审阅，从而保证了丛书的权威性和准确性。当然，由于原版图书所涉及的网络及社会环境等与我国情况不尽相同，读者定会本着批评借鉴的态度结合工作实际进行阅读、参考和分析。

我们真诚希望本套丛书能够为信息与网络安全管理和技术人员提供帮助，为我国的信息安全建设做出贡献。

编者

2000 年 7 月

# 版权声明

# 译者序

一个在某保密部门工作的人说他们的网络不与外界相连。也许这是保证网络安全最可靠的措施。但随着电子商务的发展，我们不可能将所有的业务都封闭起来。我们要对外开放，这就带来了安全上的隐患。

在世界上，网络安全日益成为一个亟待解决的问题。在发达国家中，企业对网络安全的投资大约占网络总成本的 10%～20%，而我国还不到 1%。曾经有一家公司对国内 50 家企业的网络进行诊断，结果发现 90% 以上的网络都存在着安全隐患。

另外，安全上的威胁不仅来自企业外部，实际上，企业内部的破坏力对安全威胁更大，因为内部作案相对来说比较容易。

本书详细介绍保证网络系统安全的各种措施，全书共分为 5 部分：

- 第一部分是安全性的基础知识，主要分析了安全问题的起因，并提出了系统安全的 9 大原则；
- 第二部分介绍单机系统的安全保护，主要涉及到系统的启动与关闭、系统日志、用户帐号和环境、文件系统等内容；
- 第三部分详述网络系统的安全保护，其主要内容有网络接口与服务、网络打印、电子邮件、网络访问控制、名称服务等；
- 第四部分介绍灾难恢复的问题；
- 第五部分是附录。其中不仅补充了本书的内容，还给出了黑客攻击网络的各种方法。

通过对本书的学习，读者便能够在自己的系统中实施各种安全保护措施，并能够做到在灾难来临的时候有备无患。

参加本书翻译的人员主要有仰颢、芦宪茂、贺民，全书最后由贺军统稿。由于我们水平所限，本书如有错误和不当之处，请读者不吝指教。

潇湘工作室　2000 年 8 月

# 原书序

我们曾经听说过黑客的故事，他们闯入到美国政府的一些站点中。对于这样的事情，大多数人的观点是这两种：黑客非常棒，或者，政府软弱无能。毫无疑问，这些事件说明了信息网络空间（Cyberspace）很糟糕，在那里，没有法律的保护，任何人都不安全。

确实是这样吗？确实完全是这样吗？尽管通常是这种情况，然而并不是完全正确的，但这些情况也确实有一些真实性。

对于人们的第一种看法，我们可以很容易就解决这些问题。是的，一些黑客非常棒。他们可以采用一个新的应用程序或协议，找出设计人员忽视的漏洞。但是，这样的黑客属于凤毛麟角，人数比较少。大多数黑客不过是到处抄袭的一帮人，他们运行现成的程序，这些程序可以找出系统已知的缺陷。我们的安全系统在很大程度上是以此为基础的，我们将会看到，这是非常重要的事情。

但是，如果典型的黑客并没有那么棒，那么政府（更精确地说，是遇到各种侵入到机器中的黑客的系统管理员）是不是很糟糕呢？关于这一点，我们将会在后面明确地说明。

最后一种观点，即 Internet 本身就是相当危险的，这是最有意思的看法。将这种观点转换为技术性的说法，那便是，在 Internet 上使用的协议是有缺陷的，如果设计者对安全性予以适当关注，在今天我们就不会遇到那么多的问题了。由此得出的必然结论就是，我们需要坚定的毅力，我们应当配置更新、更好的协议，并修正这些问题。下面这段话来自一个流行网页的负责人，许多公司也开始支持这种观点：

*我们的安全服务器软件（SSL）是工业标准的，而且，对于安全的商务处理来说，它们也是最好的软件。它将所有的个人信息进行加密，包括信用卡号、名字和地址。这样，当这些信息在 Internet 上传输时，就不会被别人读取。*

这段话是在解释为什么在某个站点上购物是安全的。它还引用了大量的事实，说明许多人在此购物，而没有遇到任何问题。它的含义是，加密是必要的，而且，对于解决所有的安全性问题来说，加密的方法也是足够的。

当然，加密是必须的，这毋庸置疑。使用所谓的口令侦测器（password sniffer，这是一种“窃听”程序，它获取网络上传输的口令），另外还有一些类似的程序正在开发之中，它们可以“窃取”信用卡号码。事实上，这是一个很简单的问题，口令通常是一次一个字符发

送的，信用卡号码可以很容易地被识别，而且很可能包含在一个大信息包中。这样，说加密方法足够了的观点是夸大其词的。

我们且先不管典型的 Web 加密方法的缺陷（在使用 Web 时，这些缺陷是人类交互方式所固有的），设计人员实际上是可以做得更好些，真正的威胁来自公司：公司有许多信用卡号码，这些号码在公司的站点中存储着。能够成功进入公司站点的任何人都可以窃取大量的信用卡号码。换句话说，加密和鉴别方法的使用——这便是网络协议可以为我们做的一切事情——可以保护传输中的数据，但是，却没有管目标主机上的数据。如果有其他形式的加密方法可以防止进入主机的各种途径，那么，我们就可以说，这个网络协议更好，它所做的事情比其他协议更胜一筹。换句话说，从安全性的角度来看，我们设计的 Internet 协议应当符合我们的要求，其他网络功能与安全性问题极为相似。

但如果 Internet 是危险场所，问题并不在它的设计，问题是什么？我们的网络安全到底有什么问题？这是很难回答的问题，实际上，我们应当问的是，我们的主机有什么问题？网络本身可能会有许多问题，大多数这些问题可以容易地通过加密方法来解决，但是，我们通常看到的问题是，使用 Internet 会造成主机的安全性问题。通过回答下面有关安全性的问题，我们就可以看到其中的区别何在：如果 Internet 不存在，为了获得特权，本地用户会找出系统漏洞吗？在大多数情况下，回答是肯定的。换句话说，Internet 已经提供了这些访问，它并不是安全问题的本质。

现实是这样的，主机的安全性是实际问题，它是在 Internet 上实现安全性的关键。在这个世界上，所有的加密方法都无法保护不安全的机器。这里的窍门是知道如何保护主机，而这并不是简单的事情。

当然，一个解决方案是限制主机可以做的事情。如果程序不可用，它也就没有安全的风险。但是，在给定的计算机上，决定程序应当做什么和不应当做什么是非常棘手的。人们必须要在功能和安全性这二者之间权衡利弊。确实，在现代操作系统中，各种服务之间有着错综复杂的关系，对于我们需要的许多程序来说，可能没有其他程序就不能运行，这给我们带来了更多的不确定因素。在对系统进行权衡时，需要考虑到方方面面。

防火墙（它是当今在 Internet 上使用的主要安全设备）的目的现在已经很明确了。防火墙把危险的服务与外面的世界隔离开来，同时，允许内部值得信任的人使用。换句话说，通过限制访问，它解决了一些问题，因而在危险和好处之间取得了平衡。防火墙不仅仅和网络安全性有关，而且还是人们进行通信的阻止者。它们限制了对危险主机服务的访问。

现在，我们看到了防火墙的基本局限性：由于它并不能提供各种安全性，所以，任何人都可以绕过它，不管是内部人员，还是外部人员，都可以找到绕过或通过防火墙的一些途径，这个问题仍然威胁着被保护的机器。防火墙颇具价值，但是，它并不是医治百病的良方，它们必须被适当地使用。

在我们可以回答本讨论开始提出的问题之际，还要说明一个要点：这些安全性漏洞的

本质是什么？不管是代码中，还是系统配置中，所有这些漏洞均是些错误。如果我们可以消除这些错误，就能够消除几乎所有的安全性问题，而且，余下的大多数问题可以通过加密方法来解决。

当然，我们不可能防止出错误，特别是在其他人提供给我们的代码中。但是，我们可以使用补丁程序来进行修补。大多数成功的系统入侵都是针对已知的漏洞，补丁程序可以修复这些漏洞。当然，这种方法是针对那些不十分高明的黑客。

除此之外，系统配置的不同也会给安全性带来很大的差异。对于曾经遭遇黑客入侵的系统来说，尤其如此。例如，假定有一个入侵者访问了系统。在发生进一步的损害之前，他会停止自己的入侵行为吗？通常，这取决于入侵者是否获得了 root 特权，在本地系统配置中，这是相当重要的。

主机安全性依赖于 4 个方面：无错的代码和应用程序设计，最新的系统补丁程序，良好的配置，功能与安全性之间适当的权衡。这 4 个方面中的 3 个都取决于系统管理员。如果没有良好的系统管理，就不可能有一个安全的系统。

然而，系统管理除了内部的压力之外，还有一些永久的压力，如安全性和功能的权衡，以及系统的易用性，这是因为获得可靠的信息是不容易的事情。我们可能会有太多模糊不清的引用，或者，我们可能要包括太多不同的平台。但是，给我们带来麻烦的魔鬼就藏在那些细枝末节之中，而且，供应商提供的程序升级也可能会覆盖我们已经精心调整好的安全机制。

系统管理员抱怨那些闯入者了吗？我们不知道。但是，如果他们抱怨的话，也是理所应当的。因为优秀的系统管理要保证机器的安全性，这是相当费时费力的，而且，即使仅仅进行良好的系统管理也相当不容易。

Steven M. Bellovin
AT&T Labs Research

# 前 言

## 本书的读者

本书适于两类读者：IS/IT 和安全管理人员以及 UNIX 系统管理员。

IS/IT 和安全管理人员应该阅读的内容主要是：

- 第 1 章：“安全问题”。
- 第 2 章：“安全策略”。
- 第 10 章：“网络/系统体系结构”。
- 第 16 章：“系统恢复的准备工作”。

本书的其他章节主要是技术性的，他们适合于 UNIX 系统管理员。但任何需要了解更多的 UNIX 技术（在网络安全领域）的 IS/IT 或安全管理人员都会发现，所有的技术章节都很容易读懂。在很多章的开始部分都有“本章主要内容”和“本章的重要性”。通过这些内容，你可以选择立即看这一章的内容，还是以后再阅读它。

## 本书主要内容

本书针对 Sun Microsystems 的 Solaris 2.X 和 Solaris 7 系统，讨论计算机和网络安全在物理、逻辑以及人为因素方面的问题。它包括五个部分。

- 第一部分 “安全性简介” 第 1 章以一个生动的例子描述计算机安全的问题。第 2 章为所有的 UNIX 系统管理员推荐了一些原则，这些原则同样也适用于其他计算机的管理员。

- 第二部分“独立的系统” 本部分主要讨论计算机本身，它的内容涉及计算机安全性的各个方面。对于每个系统，不管它是否连接到了网络上，这个系统同样还是一个独立的系统。第 3 章讨论 Solaris 系统中最不为人所知的一个缺陷，并提供了有效地保护桌面系统或数据中心中的 Sun 系统的方法。第 4 章全面回顾了文件和目录的安全性，介绍检查文

件系统的工具，并为UNIX 系统管理员提供了一些建议。有关用户帐号的所有问题都在第5章中讨论。在第 6 章中，你将看到系统启动的复杂性。第 7 章和第 8 章分别深入介绍各自相关的问题。

- 第三部分“网络连接系统” 本部分介绍Sun 系统在网络上的作用和地位。系统的许多严重缺陷都与它连接到网络上有关。第 9 章讨论 Sun 系统连接到网络的逻辑方式，以及它容易遭受攻击的服务。第 10 章包括网络和系统体系结构的一些原则。第 11 章的主题是电子邮件。第 12 章揭示了与打印有关的系统弱点。第 13 章介绍控制以网络方式访问系统的最佳方法。第14 章讨论 DNS、NIS 和 NIS+。第15 章详细研究了这些服务，并给出了提高它们的安全性的方法。

- 第四部分“事故和恢复” 无论是人为错误、蓄意破坏，还是正常事件，都有可能造成故障。第 16 章详细说明需要在故障发生之前采取哪些措施才能保证快速、准确、全面地恢复系统。

- 第五部分“附录” 附录 A 全面介绍一些相关的 Web 站点、FTP 站点以及邮件列表。同样，在附录 B 中，可以找到这些安全工具来源的详细列表。附录 C 中是关于 Solaris 补丁程序的全部资料。附录 D 向读者推荐一些在线资料和出版物。Sun 公司的 Solaris 安全产品将在附录 E 中讨论。附录 F 中介绍了安装和管理 C2 安全措施所需要的步骤。附录 G 中说明了如何验证公众域软件的完整性。附录 H 是有关攻击的术语。附录 I 是安全系统的检查清单。

## 专业人员的技术要求

本书适用于需要从安全的角度深入理解 Solaris 操作系统的 UNIX 中高级系统管理员。如果你是一位技术人员，就必须具备下面提到的工具和经验。

- C 编译器——使用 Sun 公司提供的编译器，或者是 Gnu C 编译器。这是因为多数公众域工具是仅以源代码的形式打包的，且需要对它们进行编译。

- 在UNIX 系统上编译公众域工具的经验。现在，这一点并不像UNIX 开始推广的10年中那样是一个严格的必备条件，那时公众域工具还不是可移植的，在编译它们之前需要做大量的修改（应该说现在要做的工作少得多了）。同时，由于伴随公众域工具包一起的配置工具的发展，那些对 C 语言知之甚少或毫无经验的人也能够安装和运行多数复杂的公众域工具了。

## 本书约定

文件内容和脚本

Shell 脚本和计算机文件的内容将被设置为 Courier 字体以和段落区分开来。下面的例子表示用户的.profile 文件：

```
#.profile file for application users
trap exit 1 2 3 15
PATH=/export/app/bin
exec /export/app/bin/application
exit
```

下面是/etc/default/passwd 文件的例子：

```
#ident "@(#)passwd.dfl 1.3 92/07/14 SMI"
MAXWEEKS=4
MINWEEKS=1
WARNWEEKS=3
PASSLENGTH=6
```

计算机会话

在与计算机之间进行的会话中，用户的输入下面将加下划线，这样就可以和计算机的输出区分开来。下面是一个会话的例子。

```
% id
uid=1001(jim) gid=101(users)
% su bob
Password: ********
% id
uid=1004(bob) gid=102(cust)
% lp -d localprinter /home/bob/eom.prt
request-id is localprinter-87 (1 file (s))
```

另外请注意，在这个例子中，用户输入的口令由带下划线的星号组成的字符串表示。实际上，在用户输入口令的时候，Solaris 并不会回显任何字符。带下划线的星号意味着用户输入了非回显的文本。

**注意：**

有一些命令中会包含下划线字符（_），它将和带下划线的文本混淆在一起，因此在本书中原来包含下划线字符的命令将不再带下划线，而且所有的这种例子都会加上脚注。下面是一个包含下划线的命令的例子。

```
#ndd -set /dev/ip ip_forwarding 0
```

注意和警告

特殊的注意和警告信息将像下面这样与段落区分开来。

**警告：**

/usr/bin/su 将设置 SetUID 位。如果关闭这个位，那么 Su 将不能运行。

## 信息来源

本书引用了一此信息来源。在每一章的结尾处都有一节叫做“补充信息”，在这一节里将会引用下面类型的参考资料。

- AnswerBook。这是Sun公司提供的在线参考资料，Solaris 2.x发布介质中也包含它。利用AnswerBook的超链接可以快速检索到其他文档中引用的文档。任何用户都可以用answerbook命令(在web技术出现之前Sun公司自己的浏览器)或者answerbook2命令(web浏览器界面）来开始一个本地的AnswerBook会话。
- 手册页。这是原始的UNIX命令参考资料，如果需要了解某个命令或者希望了解文件名称的更多信息，那么，手册页将会非常有用。

**注意：**

*本书所引用的手册页中包括手册页的节号，它将帮助你区分那些出现在多个节中的条目的不同实例。例如，在引用passwd手册页的时候，它可能是“passwd(1M)”（passwd命令）或者“passwd(4)”（passwd文件）。要查看“passwd(1M)”手册页应该键入man -s 1M passwd命令，要查看“passwd(4)”手册页，则应该键入man -s 4 passwd命令。*

- docs.sun.com。Sun把它所有的AnswerBook和手册页都放在Internet上，它位于http://docs.sun.com/。
- SunSolve。这是为Sun公司的客户提供的信息服务，这些客户具有当前维护和支持合同。SunSolve定期以CD-ROM的形式发放给客户，并可以通过http://sunsolve.sun.com/在线得到。使用这个站点的时候需要用户帐号和口令。
- 网站。这些站点中收集和组织了很多对安全性专家有用的信息。
- 出版物。包括的内容从论文、电子杂志到书籍和文章等。

## 安全补救措施和公众域软件

本书介绍Solaris操作系统中存在的安全缺陷，并针对这些缺陷提出了补救措施。补救措施的形式包括：

- 改变系统配置。安全上的缺陷经常通过简单地改变一个配置就可以得到缓解。
- 使用Sun提供的软件。本书将会介绍这些软件包的名称、在哪里可以找到它们以及在哪里可以找到安装指导。
- 使用商业软件。在某些情况下，只有商业软件包才可以作为安全补救措施。本书将介绍这些安全程序以及在哪里可以找到它们。
- 改变过程和步骤。通常，系统的薄弱环节取决于用户和系统管理员所采取的行动(或者不行动)。本书将对他们的行为提出一些建议，这些改变将会提高他们的系统安全意识。

**警告：**

对于配置的更改、公众域软件或者商业软件，本书不做任何担保和认可。最终应该由 UNIX 系统管理员或其他本地专家决定需要采取哪种措施来补救安全缺陷。

所有公众域软件工具都必须验证其完整性。曾经出现过这样的情况，一个众所周知的安全工具在一段不长的时间内被破坏了（在它上面装了一个后门），然后被散发给毫无戒心的公众。UNIX 系统管理员不应该仅仅因为安全工具是位于有名的站点上就把安全工具的完整性视为理所当然的事情。附录 G 中包含了如何验证从 Internet 上得到的软件完整性的信息。

公众域这个术语并不意味着任何个人、组织或者在任何情况下都有合法的使用权。对于任何一个公众域软件包，首先应该检查它的许可协议，确认它的条款和条件不会与你预期的用途发生冲突。每个站点的 UNIX 系统管理员或者其他本地站点的专家都必须进行合理的判断。

## 关于Web站点

本书中许多地方给出了 URL 地址，其中包含了最新的工具以及其他信息。但是，从另一个角度来看，在本书出版之后，就可能会有 URL 过时、改变或者不起作用，这便是书的特点之一。就在本书终稿和出版之间很短的一段时间内，肯定会有一些 URL 会过时，或者会重建一些站点，从而导致复杂的URL 不起作用。

请看下面的URL：

```
ftp://ftp.win.tue.nl/pub/security/tcp_wrappers_7.6.tar.gz
```

由于它包含了一个工具的版本号，因此这个 URL 很有可能会过时。如果这个工具升级了，那么这个 URL 可能会失效。在这种情况下可以像下面这样，将 URL 的最后一部分去掉，然后再试：

```
ftp://ftp.win.tue.nl/pub/security/
```

检查这个页面的内容以确定应该检索什么内容。接下来，如果前面的URL 也是无效的，则再去掉最后一部分：

```
ftp://ftp.win.tue.nl/pub/
```

然后这样继续下去，直到可以找到一些能够说明你所需要的内容发生了什么变化的信息为止。很多认真负责的Web 站点和 ftp 站点都会保存一个 README 文件，其中声明某些工具或者其他信息现在位于另一个站点上，或者已经不再提供它们。

即使上面所有的尝试都失败了，在附录 A 或附录 B 中列出的安全领域的其他某个 Web 站点中，也可能找到需要的工具或者出版物的信息。