HZ BOOKS

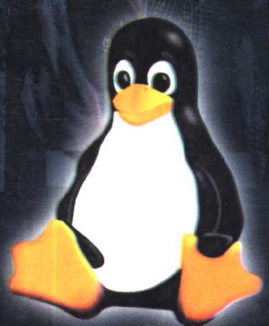
Hack Proofing Linux

A Guide to Open Source Security

网络与信息安全技术丛书

Linux黑客防范

开放源代码安全指南



附赠 CD-ROM

(美) James Stanger
Patrick T. Lane 著

钟日红 宋建才 等译

机械工业出版社
China Machine Press

SYNGRESS

网络与信息安全技术丛书

Linux 黑客防范开放源代码安全指南

（美） James Stanger
Patrick T. Lane 著

钟日红 宋建才 等译

前导工作室 审校

机械工业出版社
China Machine Press

这是开放源代码安全的完全手册，是一本极具价值的学习 Linux 安全的参考书。它从开放源代码的角度，以一个黑客的思维全面介绍了 Linux 操作系统的攻击与防御，涵盖了 Linux 的安全知识。书中不仅注重 Linux 安全基本知识的讲解，而且介绍了许多安全常识、安全技巧、安全工具、系统漏洞等知识。

本书语言生动、图文并茂，对于 Linux 安全、网络安全、系统管理等领域的从业人员具有实用价值。随书所附光盘中包括了众多实用程序。

本书版权登记号：图字：01-2001-4406

图书在版编目（CIP）数据

Linux 黑客防范：开放源代码安全指南/（美）斯坦格（Stanger, J.）等著；钟日红等译. -北京：机械工业出版社，2002.2
（网络与信息安全技术丛书）
书名原文：Hack Proofing Linux: A Guide to Open Source Security
ISBN 7-111-09529-4

Ⅰ.L... Ⅱ.①斯...②钟... Ⅲ.Linux 操作系统-安全技术 Ⅳ.TP316.81

中国版本图书馆 CIP 数据核字（2001）第 078835 号

机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码 100037）
责任编辑：李 炎 张鸿斌
北京昌平奔腾印刷厂印刷·新华书店北京发行所发行
2002 年 2 月第 1 版第 1 次印刷
787mm×1092mm 1/16·26.25 印张
印数：0 001-4 000 册
定价：49.00 元（附光盘）

译 者 序

记得5年以前，为了买一张Linux的正版光盘，我跑遍了我所在的城市，最后还是通过邮寄才获得，那时候使用Linux的人很少，卖Linux软件的商家自然也少。如今的Linux再也不是5年以前的Linux了，各行各业都希望使用不担心“后门”，能够自主修改的操作系统。Linux的版本很多，Red Hat是使用最广的版本，这与其发布的形式和宣传力度是分不开的。随着Linux使用者的增加，其安全问题也越来越显得重要了。

大家都知道，Linux是一种开放源代码的操作系统。开放源代码意味着，人们不用担心操作系统的后门。这么说网络的安全人员可以高枕无忧了吗？如果你这么认为，那就大错特错了。开放的源代码就意味着这种操作系统完全开放，不言而喻，安全问题也是相伴而生的。

与众多喜欢去“书城踏青”的朋友一样，我很喜欢书店那种新书的清新感。当我试着在漫漫书海寻找一本介绍Linux系统安全方面的书籍时，却困惑了。我发现这个方面的书很少，并且大部分都只介绍了一些理论方面的知识，而没有真正地指导我们如何去使我们的网络变得更安全，也很少有书籍能够专业地从“开放源代码”的角度来透彻地讲解这种操作系统的安全问题。当我们看到这本书时，心里真的很激动。一方面，能够在翻译的同时系统地进行学习，另一方面，能够有机会将这么好的一本书奉献给广大的读者，这对我们来说真的是一个很难得的机会。

本书重点讲述如何通过一些安全工具来使你的主机和网络安全化。作者将主机和网络的安全化工作分为三步：锁定你的网络；安全化网络数据传输；建立防火墙，保护网络边界。书中内容丰富，它告诉你如何以一个黑客的思维来预防黑客的进攻。通过演示，本书讲述了强化服务器、使用扫描工具、IDS的利用、如何截获网络流量、实现网络层加密和认证、如何创建防火墙等方面的防黑方案。同时本书也是一个很好的资源库，介绍了很多下载各种网络安全工具及源代码程序的网址。通过这些网址，你可以获得更多的有关网络安全方面的工具，并且参与到网络安全方面的讨论中去。另外，本书还配有光盘，光盘中不但有书中用到的程序及实例，还有本书内容的电子版，通过电子版的超级链接，你可以很方便地直接连接到相关网页，而无需再为寻找相关知识的网址而烦恼。

这本书最主要的特点就是“所从即所得”（What you following is What Your Get）。因为在讲述每一个使网络安全化的步骤中，都有实现该步骤的实例以及练习。你只要跟着书中实例和练习一步一步地在你的服务器主机上操作，就可以轻松地掌握书中的方案。无论你现在是一个有经验的网络管理者，还是一个刚刚对网络安全产生兴趣的新手，只要你想成为一名优秀的网络管理者，或者想使你的个人服务器更加安全，这本书都是一个很好的选择。

全书由钟日红、宋建才、庄振运、张建军、张旭东、钱芳、李炎、孟萧、赵国峰、蔡强、曾庆、周文波、董涛、杨鸿、古宇、常欣、江立云，郭星平、李二勇、陈松、卢毅然等翻译，梁静统稿。前导工作室全体工作人员为本书的翻译、校对、录排等工作付出了辛勤的劳动。由于时间仓促，且译者的水平有限，在翻译过程中难免会出现一些错误，敬请读者批评指正。

如果你在阅读中碰到了什么问题，请同前导工作室联系：qiandao@263.net。我们会尽力解决你的问题。

2001 年 9 月

前　言

本书的目的是告诉你如何根据 Internet 上不同层次的安全级别配置 Linux 系统。本书提供了一些实用的命令以及常用开放源代码安全工具的使用指南。

本书首先告诉你如何获得这些软件，然后教你如何用 Bastille 应用程序来加固你的 Linux 操作系统，以使其安全运转完成你交给它的任务（比如，作为 Web 服务器，作为电子邮件服务器等等）。你还可以学习到如何让 Linux 系统为你扫描系统漏洞，就像创建一个入侵检测系统（Intrusion Detection System）一样，使你的 Linux 系统记录可疑行为并对其做出反应。使用 Gnu Privacy Guard 和 FreeSWAN，从病毒防护到加密传输，你既可以使本地数据安全化，也可以使网络数据传输安全化。读完这本书以后，你就知道哪些开放源代码以及收费工具可以使你的 Linux 系统更加安全了。

我们还用一些章节介绍了怎样嗅探和排除网络连接中的故障，怎样使用一次性密码（One Time Passwords，OTP）和 Kerberos 建立可靠认证。有了 Squid 代理服务器和 Ipchains/ Iptables，Linux 系统就可以用作防火墙；有了附带光盘上的软件工具加上书中的建议和提示，你就可以自信地在你的 Linux 系统上实现各种功能。

我们集中介绍 Linux 平台上普遍使用的安全工具。重点放在这些工具的实际配置，而不是概念上的简单介绍。最后介绍出现错误的时候该怎么做。因此，这本书是一个宝贵的资源，能教你最高效地使用你的 Linux 系统。

这本书最让人激动的地方在于它提供了非常实用的指导，帮你建立安全应用程序。从 Gnu Privacy Guard（GPG）、Bastille 到 FreeSWAN、Kerberos 和防水墙故障检测工具，这本书告诉你怎样使用 Linux 的技巧来提供最重要的安全服务，包括加密、认证、连接控制和日志。

这本书的结构分以下三个主要部分：

- 锁定网络（第 1 章～第 4 章）。
- 保证数据在网上安全传输（第 5 章～第 8 章）。
- 用防火墙保护网络周边（第 9 章～第 11 章）。

每一部分都有对特殊情况的最佳解决办法。虽然这本书的章节划分不是很明显，但这种粗糙的划分能帮助你在你的环境中实施安全措施。

第 1 章探讨了开放源代码的概念，包括 GNU 通用公共许可证（General Public License，GPL），由 www.gnu.org（自由软件基金会）提供，然后是怎样用 GPG 和 PGP（Pretty Good Privacy）来加密传输或检验你从 Web 上下载文件的签名。还有如何监测网络的步骤。

第 2 章介绍如何锁定操作系统，使之只具备你所希望得到的 Internet 服务。第 3 章介绍如何使用应用程序（如 AntiVir、Gnome ServiceScan、Nmap、Rnmap 和 Nessus）来扫描系统漏

洞。第4章介绍主机和基于网络的入侵监测器应用程序，包括 Sonrt、Tripwire 和 PortSentry。第5章解释如何很好地使用网络嗅探器，包括 Tcpdump、Ethereal 和 EtherApe。使用这些知识监测网络并知道表面现象的本质，你会成为一个优秀的网络安全管理员。

第6章，介绍怎样使用一次性密码（One Time Passwords）和 Kerberos。第7章，介绍怎样防止嗅探攻击。第8章，介绍通过配置 FreeSWAN 来创建 IPSec。第9章介绍如何使用 Ipchains 或者 Iptables 创建自己的防火墙或包过滤器防火墙。第10章，介绍如何配置 Squid 来更加详细地监测和处理数据包。最后，第11章提供了检测你的防火墙配置的工具。

开放源代码组织满足了对免费且功能强大的系统的需求，使你可以进行监测，提供网页，提供电子邮件服务，或者任何其他你想提供的 Internet 服务。如果可以很好地使用这些开放源代码组织提供的安全软件，就会感受到很多开发者是在为你工作。你会拥有更大的自由，因为可以从很多由经验丰富的开发者开发的经过广泛测试的安全工具中选择。你甚至可以选用（自己冒险）那些刚刚开发的还不太明确的工具。这就由你自己决定了。

开放源代码操作系统和安全工具是一把双刃剑，虽然它是免费的，但是你必须花很多时间来处理软件的不兼容问题。就像以前说的，通过对本书的学习，配置工具和练习，你应该能把它的不方便最小化。也希望你在读了本书以后更加积极地加入到开放源代码软件的运动中，共同实现创建强大而好用软件的愿望。

——James Stanger 博士、MCSE、MCT

关于本书作者

Patrick T. Lane（MCSE、MCP＋I、MCT、Network＋、I-Net＋、CIW）是一流的 Internet 技术培训及课程开发公司 ProsoftTraining.com 的内容设置师，是二十多门技术课程的作者，也是 CIW Foundations 及 CIW Internetworking Professional 系列的董事。在 ProsoftTraining.com 时，Patrick 帮助创建了 Internet Web 管理者认证（Certified Internet Webmaster，CIW）项目以及为 Intel、Novell 及 Microsoft 专家讲 i-Accelerate 课程。

James Stanger（Ph.D.、MCSE、MCT）在 ProsoftTraining.com 负责 Linux、Security 及 Server Administrator 认证。自从1977年获得博士学位以来，他致力于审计 Internet 服务器并编写关于 Internet 服务器管理和安全方面的课件、书籍及杂志。James 是 IBM、Symantec、Evinci（www.evinci.org）、Pomeroy（www.pomeroy.com）、Securify（www.securify.com）、Brigham Young University，以及 California State、San Bernardino 的顾问。他专门研究棘手的防火墙、入侵检测、DNS、e-mail 以及 Web 服务器实现方面的问题。

关于本书光盘

本书附带光盘一张，盘中包括书中要用到的文件和程序。这些文件包含了配置举例、包截获以及附加资源。还包括了本书中要用到的特定开放源代码程序，因此就可以在你自己的系统上一步一步地跟着每章的范例练习。

光盘中的每一个文件都在书中有详细讨论，并且在有光盘图标时被引用。当需要一个特定文件或程序时，会指示你到光盘中去找。本书也告诉你可以下载最新软件版本以及可以找到程序相关资源的网址。比如，你可以从www.freeswan.org 下载 Free Secure Wide Area Network (FreeS/WAN)，或使用 CD 中的版本。建议使用 CD 中的版本，这会提高范例的成功率，因为本书出版后，有些程序做了改变。

本书基于 Red Hat Linux 7.x 平台编写，因此，CD 中的大部分文件都是 Red Hat Package Manager (.rpm)文件。也有很多的 Tape Archive(.tar)文件和 GNU Zip(.gzip)文件。解压缩和安装这些文件的命令包含在它们的相关目录。为了挂接 CD 到你的 Linux 系统，请输入以下命令（对于 Red Hat 系统）：

```
mount-t iso9660/ dev/ cdrom/ mnt/ cdrom
```

如果要卸载 CD，请输入：

```
umount/ mnt/ cdrom
```

建议你在使用 CD 中的文件前，将文件拷贝到硬盘。如果你使用了其他版本的 Linux，你需要修正书中范例，或者下载一个与所用版本的 Linux 兼容的开放源代码的可移植版本。

当要获取书中范例文件时，应该先找到这个光盘图标。

目　录

第 1 章　开放源代码安全简介

本章中涵盖的解决方案包括：

- 使用 GNU 通用公共许可证（General Public License）
- 处理开放源代码怪问题的技巧
- 应该选用 RPM 还是 Tarball
- 获得开放源代码软件
- 加密的简短回顾
- 公钥和信任关系
- 监测过程

1.1　简　介

虽然网络业发展跌宕起伏，但是开放源代码软件却已经成为商业公司如 Microsoft、Sun 和 IBM 之外的另一可行的选择。尽管开放源代码软件有它自己的个性和问题，但开放源代码运动还是在网络市场上占有一席之地。作为一个网络专业人员，你一定非常有兴趣了解一些很容易得到的而且很重要的安全应用和服务。

本书的目的是为经验丰富的网络管理员提供开放源代码安全方面的工具。我们尽力满足尽可能多的读者，介绍尽可能多的技巧，本书假定你对 Linux 已经有基本的认识。本书主要介绍开放源代码的 Linux 应用程序，监控程序和系统修复工具。本书第 1 章介绍如何锁定网络，第 2 章介绍如何监测操作系统以保证安全，如何扫描本机或远端网络的漏洞，具体介绍了有关保证系统服务和根用户安全的详细信息。

第 3 章介绍了如何配置本机上的反病毒和扫描程序。使用这些扫描程序能降低危险，更多地了解网络服务。扫描工具如 nmap、nessus 可以帮助你知道网络上的开放端口，以及这些开放端口如何威胁着系统。第 4 章详细地介绍了在本机或网络上配置入侵监测器的方法，使用诸如 Tripwire、Portsentry 或 Snort，可以准确地识别系统异常或检测非法登录。第 5 章介绍了如何使用开放源代码工具如 tcpdump、Ethereal、EtherApe 和 Ntop 来检查网络和得到网络的通信进度。

本书第二部分集中介绍使用开放源代码软件加强认证。第 6 章介绍一次性密码（OTP）和 Kerberos，还有防止恶意用户从网上截获你密码的方法。第 7 章讨论了使用 Secure Shell（SSH）和安全套接层（SSL）快速加密以保护数据的方法。第 8 章介绍了如何在 Linux 系统上建立 IPSec 来配置虚拟专用网（VPN）。了解了更多虚拟专用网的主要产品，称做免费安全广域网（FreeS/WAN），你会看到它是如何在你自己的网络上或是 Internet 上保护

网络通信的。

本书的最后一部分集中在如何建立高效的网络周边。第 9 章介绍如何在 Linux 系统上安装和配置 Ipchains 和 Iptables。低于 2.3 版本的内核可以用 Ipchains，2.3 或者高于 2.3 版本的使用 Iptables。不管怎样，你都将知道如何使用这两个包过滤工具来过滤数据。

第 10 章介绍代理服务器是怎样加强控制网络周边的。特别介绍了怎样使用 Squid 代理服务器控制用户访问 Internet，还介绍了如何指定 Linux 客户端访问代理服务器。最后，第 11 章，介绍怎样处理和排除网络周边出现的问题和故障，介绍如何维护、检查、记录防火墙，以及在外界和你的网络间建立一个屏障。

我们的目的是写这样一本书，提供有关常用开放源代码安全工具的实用信息和建议。

本书中用到的工具

本书是在 Red Hat Linux 7.0 上写的，它不是世界上最好的 Linux 版本（世界上至少有 100 个版本），但它是最流行的。我们尽力让本书的工具和技巧适用于其他的 Linux 版本和开放源代码操作系统，如 FreeBSD（www.freebsd.org）。然而，每个 Linux 版本都有自己独特的个性，可能本书的建议会有所偏差。

1.2 使用 GNU 通用公共许可证

GNU 通用公共许可证（General Public License，GPL）是开放源代码运动的基础。这个许可协议是由 GNU（Gnu is Not Unix）组织提供的，它们开发了很多软件包。GNC 是 Richard Stallman在 1984 年发起的，是为确保开放源代码运动的一直繁荣而特别创造的许可证。在 www.gnu.org 的网页上有更多的关于 GNU 的信息，如图 1-1 所示。

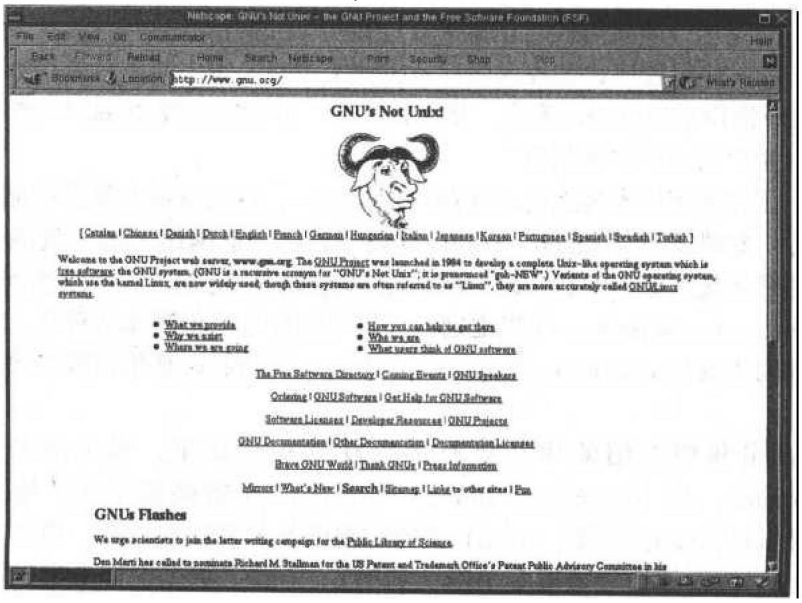


图 1-1 GNU 网页

这个许可证最重要的要素不是保护个别人或个别公司，而是保护创建应用程序的源代码。传统的，是保护个人对软件的著作权，以及通过销售软件来盈利。另外，在其他人使用源代码生成类似的应用程序时，原作者有权采取行动予以制止。不管是好是坏，Richard Stallman、Eric Raymond 和其他人帮助建立开放软件许可证的概念——GNU 通用公共许可证（经常简写为 GPL），并使之流行。www.gnu.org/copyleft/gpl.html 上有 GPL 的内容。

这个许可证是“逆版权运动”的一部分，它们把自己当成传统版权法规的补充。GPL 基本上是允许任何人开发源代码并保证代码开放，意味着 GPL 许可的代码可以让任何人拿去而且可以进行改进，只不过改进后的代码要交还源代码开发者或软件开发组织。因此，任何人想得到和修改 GPL 保护的开放源代码都是允许的。如果没有 GPL 许可协议，有的人就可能拿去代码，把它完善，然后就私有化不再公开了。

GNU GPL 不是现存的惟一的自由软件许可协议。图 1-2 是 GNU 网页上关于其他许可协议的网页。如果想了解其他类似 GPL 的许可协议可以浏览网页 www.gnu.org/philosophy/license-list.html。

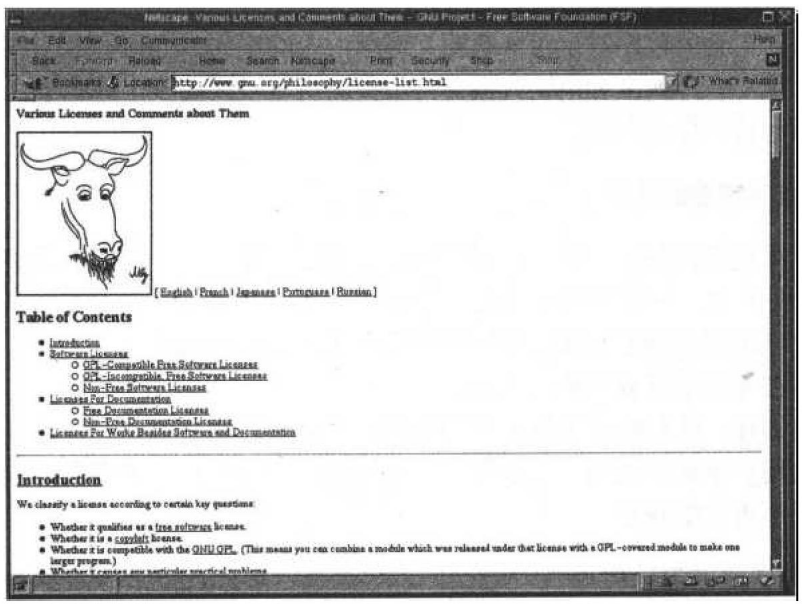


图 1-2　浏览 GNU 许可协议的目录部分

有关开放源代码运动的更多信息，最详尽的一本书是 Erik Raymond 的《The Cathedral and the Bazaar》（O'Reilly& Associates，2001）。虽然有点言过其实，但它对了解许多开发源代码开发者的心理是很有帮助的。

1.2.1　收费的 GPL 软件

和通常认为的不同，GPL 保护的开放源代码不一定是免费的。就 GPL 而言，任何人或任

何组织都可以使用GPL软件，修改它，然后包装销售，但是，这个人或组织也必须保证任何人都可以免费得到这个软件，并可以阅读或修改它。

1.2.2 在公司可以使用GPL软件吗

GNU GPL不需要使用GPL软件的公司提供许可协议或者注册这个软件。但是，其他一些许可协议在你安装它的软件时就不得不考虑一些限制，那些协议都在GPL相应的论坛里。本书所涉及的软件都是可以免费得到的，任何组织都可以用。

1.3 处理开放源代码怪问题的技巧

然而，你必须清楚，开放源代码软件也是带有挑战性的。在开始钻研开放源代码之前一定要考虑清楚。使用开放源代码软件经常是需要技巧的，如怎样消除不匹配的问题、处理经常性的变化等等。下面几节讨论了几个棘手但是很重要的问题。

1.3.1 普遍地缺少安装程序和配置支持

虽然很多你要用到的程序都是由既聪明又博学的人编写的，但他们大多数是利用自己的休息时间。因此，很多软件就没有很正式的支持结构。所以必须找一个知识丰富的人来帮你安装和维护你的开放源代码应用程序。

1.3.2 较少的或不定期的升级

许多不开放源代码的公司会定期地升级自己的产品。盈利的公司通常希望通过收费的升级来保持产品稳定的声誉——使用的方便性和持久性，并维持较高的销售额，因此会定期升级。而开放源代码组织则不是基于对金钱的渴望。通常软件会频繁地升级。因此，你经常要花很多时间来升级你正在使用的开放源代码产品。

没有人会通知你，你的版本又发现新的漏洞了。而盈利的公司则会公布一个安全隐患问题或者联系注册的用户来通知他们。如果使用开放源代码，这个担子就压在你自己肩上了。建议你随时关注你所用版本的发展。

1.3.3 命令行方式占统治地位

很多开放源代码程序都用命令行方式的接口。在过去的几年的趋势却是图形用户接口（GUI）正在逐步取代命令行方式的应用程序。但是图形用户接口在操作系统间的可移植性却不如命令行方式。有些情况，除了那些特别编写的程序，图形用户接口的程序在功能上也不能和命令行方式的相比（就是说，在命令行方式程序上能实现的功能在图形用户接口的程序上不能完成）。

1.3.4 缺乏向后的兼容性和没有正规的发布版本

升级了操作系统后，有些经常使用的程序可能就不能用了或者工作不正常。虽然开放源代

码组织工作异常出色，还是该考虑这种可能。

而且一直使用的软件可能再也得不到或者改成收费的了，就像发现一个网址变了一样不方便。当发现喜欢的程序升级要收费，想继续使用就会出现许多问题。

1.3.5　升级途径不方便

许多开放源代码的程序在升级的时候改动很大。可能以前的版本不能升级，那只有重装。还可能简简单单地重装又不行。很多开放源代码程序都有一个窗口化的安装向导，但升级的时候可能要自己手工安装新文件。

1.3.6　供应库文件的冲突和有限的平台支持

可能发现一个非常感兴趣的软件，但是你可能要做很多繁杂工作才能让它在你的系统上运行。这些步骤中包含升级系统库文件，就是一系列的常规程序和辅助程序。库文件的例子如工具命令语言/工具箱（tcl/tk）和 Gnome 库（gnome-lib）。

经常，有关升级这些库的步骤很少被证明过，而且很难操作。另外，像 Linux 这样的系统集成很松散，没有“控制中枢”（比如 Windows 2000 的注册表，用来协调库文件的使用）。即使你能让你的系统接受很酷的新程序，但可能别的程序又不能用了。

软件的另一个问题——不通用，可能一个应用程序是针对一个风格的 Linux 而设计的，或者只是针对一个风格中的一个特殊版本而设计的。升级系统以后这个程序就不能再用了。

1.3.7　接口的改变

无论是代码编写者还是用户都不愿意图形用户接口发生很大的变化，改变接口需要编写者更多的工作量，还可能导致应用程序的不再受欢迎。然而由于开放源代码的库文件和实际编程的变化，两个版本在接口和命令上都会发生很大的变化。

1.3.8　未开发完的解决方案

有时候，自己想用的代码不能实现承诺的功能，找不到希望的或者宣传的所具有的特性，或者根本就不能安装。开放源代码应用程序的开发团队总是带着良好的愿望，或许项目还没完成。有些情况是开发团队没了经费，这个程序就不可能具有它应该具有的功能了。

在这种情况下，你的选择余地就很有限，除非按你的想法组建开发团队，完成别人没有完成的愿望。

开发和配置

开放源代码和怀有恶意的软件一样吗?

到现在你已经了解了开放源代码的有关技术问题，还有商业和安全的问题。如果