网络与信息安全技术经典丛书

继“黑客大曝光”之后的又一力作

HARDENING

Network Security 中文版

Bulletproof your systems before you are hacked!

为你的系统构筑坚固的安全堡垒

John Mallery Jason Zann Patrick Kelly Wesley Noonan Eric Seagren
Paul Love Rob Kraft Mark O'Neill 著

邓琦皓 孙学涛 许鸿飞 译

McGraw Hill Osborne

清华大学出版社

网络与信息安全技术经典丛书

Hardening Network Security 中文版

[美] John Mallery, Jason Zann
Patrick Kelly, Wesley Noonan
Eric Seagren, Paul Love
Rob Kraft, Mark O'Neill 著

邓琦皓 孙学涛 许鸿飞 译

清华大学出版社
北京

John Mallery, Jason Zann, Patrick Kelly, Wesley Noonan, Eric Seagren, Paul Love, Rob Kraft, Mark O'Neill
Hardening Network Security
EISBN 0-07-225703-2

图书在版编目（CIP）数据

Hardening Network Security 中文版/（美）麦勒瑞（Mallery, J.）等著；
邓琦皓，孙学涛，许鸿飞译. —北京：清华大学出版社，2006.5
书名原文：Hardening Network Security
ISBN 7-302-12964-9

Ⅰ.H…　Ⅱ.①麦…　②邓…③孙…　Ⅲ.计算机网络—安全技术
Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2006）第 043271 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010-82896445
组稿编辑：夏非彼
文稿编辑：刘秀青
封面设计：林陶
版式设计：科海
印 刷 者：北京市耀华印刷有限公司
发 行 者：新华书店总店北京发行所
开　　本：异 16　　**印张**：34.25　　**字数**：748 千字
版　　次：2006 年 6 月第 1 版　2006 年 6 月第 1 次印刷
书　　号：ISBN 7-302-12964-9/TP・8242
印　　数：0 001~3 000
定　　价：59.00 元

内 容 提 要

Hardening 系列是美国 McGraw-Hill 公司新近推出的又一套信息安全系列丛书，与久负盛名的“黑客大曝光”系列携手，为信息安全界奉献了一道饕餮大餐。

本书是 Hardening 系列成员之一，由数位信息安全领域的著名专家编写，通过四段式系统加固教学法，从技术和策略两方面，详细介绍网络系统的安全防护工作，并对系统管理员容易疏忽或犯错的细节进行深入探讨，旨在帮助读者把网络系统建设成信息安全堡垒。

全书共分 4 大部分 22 章。第 1 部分给出降低系统威胁的 7 个关键步骤，是系统阻止入侵的必要措施；第 2 部分则是本书的重中之重，自顶向下系统讲述加固网络系统的具体方法和措施，其中涉及了如何用深度防御、身份管理系统、加密、入侵检测与响应等方法来提高网络安全性，并详尽描述了如何加固跨平台认证、Web 服务、移动环境、数据传输、远程客户端、无线网络、混合 Unix 系统等当前人们密切关注的问题；第 3 部分告诫人们永远没有一劳永逸，需要持之以恒地对系统进行监控和评估，并及时修订管理方式和打补丁；第 4 部分就安全计划如何获得预算支持、管理层认可以及员工协作，制订出详细的策略，在同类书中少见。

本书覆盖了所有的主流平台和应用程序，是所有 IT 专业人士的必备安全工具。

谨以此书献给我的家人。没有他们的支持，我不可能顺利完成此项工作。感谢保拉、加利克和艾瑞克，在我因此书的工作而离开时你们总是十分体谅。我们一家真棒。

——约翰·麦勒瑞

谨以此书献给我的妻子谢丽尔，我们的女儿杰西卡·克拉克和艾比·海纳特，外孙欧申和艾扎克·雷德蒙；感谢布里奇特教导我认识生活的意义、休会休闲的价值和树立永不放弃的精神。

——帕垂克·凯利

感谢我的妻子达纳，她对我编写此书提供了很多支持。感谢我的父母大卫和琼，他们给我的帮助超出他们的想象。

——杰逊·扎恩

关于丛书的编辑/作者

罗伯特·布拉格（密苏里州格瑞恩谷），持有 CISSP、Security+、ETI Client Server、Certified Technical Trainer、IBM Certified Trainer、DB2-UDB、Citrix Certified Administrator 和 MCSE: Security 等证书。6 年来一直在为 Microsoft Certified Professional Magazine（微软认证专业杂志）的 Security Advisor（安全顾问）栏目撰稿，为 Security Watch（安全观察）新闻邮件撰稿也已有 3 年历史。她是 SearchWindowsSecurity.com 的安全专家，负责为该网站的 Security Checklist（安全检查列表）栏目撰稿。罗伯特策划、设计、组织和参与了 2002 年在美国西雅图召开的首届 Windows 安全峰会。同样是在 2002 年，在 TechMentor 圣地亚哥会议上，罗伯特主持了“安全学院”为期 3 天的首次安全建网实践研讨班，该研讨班在 2003 年又重复举办了 5 次。2004 年，她代表微软公司出席了一系列安全峰会。罗伯特也是 SANs 公司和 MIS 培训中心的培训师。

罗伯特曾参加过很多次安全审计，并曾以安全传教士、网络安全顾问、评估师和培训师等身份到过世界各地。罗伯特也是西雅图太平洋大学和约翰逊县立社区学院的兼职教授，执教与信息安全设计有关的课程。罗伯特还是由 McGraw-Hill/Osborne 出版的 *Network Security:The Complete Reference*（网络安全：完全参考手册，2003）、*Hardening Windows Systems*[①]（2004）和微软出版社的 *Designing Security for a Windows Server 2003 Network*（Windows Server 2003 网络安全设计，2004）等著作的主编。

关 于 主 编

约翰·麦勒瑞是 BKD 和 LLP 的管理顾问，也是一位资深安全专家。他曾出任过 Clarence M. Kelley and Associates 股份有限公司的 CTO，该公司是由美国联邦调查局前局长创办的调查与安全咨询公司。在计算机犯罪取证与计算机安全领域，约翰是全国享有盛名的演讲人和培训师。他还为法律界开发了法律教育软件，并为法律的实施进行规划，在全国性会议上的演讲总是深受好评。

约翰善于利用自己曾当过调查员、网络安全顾问和喜剧演员的独特经历，其演讲既精深又不失娱乐性。他是 ASIS International 信息技术安全理事会的成员，是高技术犯罪调查

---

① 编者注：本书中提到的 *Hardening Windows Systems*、*Hardening Network Infrastructure*、*Hardening Linux* 等书的中文版均由科海培中公司与清华大学出版社联合出版。

联合会 Infragard 的成员，也是 *Security Technology and design*（安全技术与设计）杂志的特约编辑。

杰逊·扎恩，持有 CISSP 证书，现任 DST Systems 股份有限公司的信息安全顾问。他从事信息安全工作已有 9 年多，并一直负责全球的信息安全产品、系统、网络和流程的管理、运作和技术开发。他曾就职于企业和咨询机构，做过产品开发，先后提出了多种信息安全理念和解决方案。

帕垂克·凯利，持有 CISSP、CCSE、MCSE、MCP+I 等证书，现为 ComGlobal Systems 股份有限公司的信息保障工程师。帕垂克有 15 年多的应用开发和网络安全经验。目前，他负责企业安全规划、脆弱性和风险评估、安全部件的设计与开发等。在其职业生涯中，帕垂克一直都是负责实施和设计网络安全规划，曾开发的项目包括入侵检测与响应系统、防火墙技术设计与实现、网络安全风险和脆弱性评估、因特网安全规划等。

关于供稿作者

维斯·努南（德克萨斯州休斯顿市），持有 MCSE、CCNA、CCDA、NNCSS、Security+ 等证书，从事计算机行业已超过 11 年，专门研究基于 Windows 系统的网络和网络基础架构的设计与实现。他是 Collective Technologies, LLC （http://www.colltech.com）公司的高级网络顾问，该公司专门从事存储器、服务器和网络设计、架构、安全等方面的业务。维斯是在美国海军陆战队服役时开始从事计算机安全工作的，当时使用的是海军陆战队的 Banyan VINES 网络，此后便从事针对 25~25 000 用户的安全网络的构建和设计工作。维斯曾在 BMC Software 股份有限公司的研发部门工作过，当时做的是 PATROL 管理解决方案，负责网络和应用管理产品的构架和测试等工作。维斯也是一位很活跃的培训师，讲授独具特色的关于 Cisco 路由技术和交换技术的课程。他曾在很多技术会议上对用户群体发表过演讲，是 http://searchwindowssecurity.techtarget.com 网站上 Ask the Experts 栏目的成员。维斯也是 *Hardening Network Infrastructure*（McGraw-Hill/Osborne, 2004）一书的作者。

艾瑞克·西格闰（德克萨斯州密苏里市），持有 CISSP、ISSAP、SCNP、CCNA、CNE、MCP+I、MCSE 等证书，有 9 年的计算机行业从业经验，最近 6 年就职于金融服务业的某家名列《财富》100 强之中的企业。艾瑞克的计算机职业生涯开始于 Novell 服务器，当时是为总部设在休斯顿市的某家小公司做一般的网络维护。在目前的这家金融服务公司，他的职责包括服务器管理、灾难恢复、业务连续性协调和解决 2000 年问题等。最近 4 年他又以 IT 构架师的身份，从事安全、可扩展、冗余网络的设计。他的工作经验包括实现多个入侵检测系统、对网络设计和网络设备配置进行安全评估等。

鲍尔·拉乌，持有 CISSP、CISA、CISM、Security+等证书。从事 IT 行业已有 15 年的

历史，目前是某大型金融机构的安全经理。鲍尔先后获得过信息系统学士学位和网络安全硕士学位。他与别人合著了 *Hardening Linux*（McGraw-Hill/Osborne, 2004）一书，也曾做过 10 多本关于 Linux 和 Unix 的畅销书的技术编辑。在.com 风靡一时的年代，鲍尔曾开办过一个很成功的 Linux 门户网站。

罗布·克拉夫特是 KCX 股份有限公司软件开发部主任，曾做过两年的微软认证培训师，讲授过关于 SQL Server 和 Visual Basic 的课程。他也通过了 IBM 公司的认证，有资格讲授 DB2 和 WebSphere。除授课外，罗布还有 15 年的开发经验，而且使用过多种平台、多种开发语言和多种数据库管理系统。罗布与别人合编过多部与微软 SQL Server 有关的著作，并多次在会议或研讨班上讲过 SQL Server、因特网安全和 Visual Basic。在业余时间，罗布还帮助本地的非盈利机构解决 IT 或其他方面的问题。如欲联系罗布，请访问 http://www.RobKraft.org。

马克·奥尼尔是 *Web Services Security*（McGraw-Hill/Osborne, 2003）一书的主要作者。马克曾先后在 *Web Services Journal*（Web 服务）、*XML Journal*、*Java Pro*、*Enterprise Architect*（企业构架）、*Infoconomy*（信息经济）、*Technology for Finance*（金融技术）等期刊上撰文阐述关于 XML 和 Web 服务安全的问题。作为 Vordel 公司（提供 XML 安全产品的先驱）的首席技术官（CTO），马克曾接触过很多早期的 XML 使用者，并对他们的安全需求做了归纳总结。现在马克定期在伦敦、加利福尼亚和美国东海岸讲授关于 Web 服务安全的培训课程。在过去四年中，他连续被邀请在信息安全行业规模最大的 RSA 年会上就 XML 安全问题做演讲。马克居住在波士顿的罗丝林蒂（Roslindale）地区，妻子叫克里斯蒂，儿子刚两岁，叫本。

关于技术述评撰稿人

里·艾迈瑞，持有 CISSP、ISA、CPP 等证书，是联邦政府信息安全专家。他负责撰写关于保护重要信息和不同级别信息的策略，并与多个政府机构合作，以实施符合这些策略要求的技术规程。此前他曾是(ISC)²的高级通信经理，曾编辑制作过(ISC)²的新闻邮件——这些邮件被发送给遍布全球的 2 万多名信息安全专业人士。他还曾是 CISSP CBK 评估研讨班的主要授课人，授课对象是全球的私营企业员工或政府职员。他曾就职于通信公司、零售企业和咨询机构，现在仍以多种方式为信息安全行业做着各种贡献，包括兼任 ASIS 信息技术安全理事会理事、ISSA 职业道德委员会主任等。

致　谢

我要感谢 Ameriquest 公司的麦克尔·维德。他是我的第一位导师，在我把 DOS 说成是“dose”时，他并没有嘲笑我。还要感谢 Fishnet Security 公司的马克·卡尼，他在无线网络安全方面给我提供了很大帮助。尤其要感谢 CMKA 的汤姆·达普瑞斯特，几乎我的所有技术培训都是在他的帮助下完成的。特别感谢罗伯特·布拉格，是她为我提供了参与本项目的机会。她的支持和鼓励让我深受感动。谢谢你，布拉格，谢谢你给我提供这样好的机会。

——约翰·麦勒瑞

必须要感谢罗伯特·布拉格。她为计算机安全领域做出了很大贡献，也为我提供了这么好的机会。要感谢保罗·鲍西克，感谢他的远见卓识和对我的鼓励。以他的才干，完全可以成为风云人物。还要感谢弗兰克·海维特、克里斯·卡斯帕肯、迈克和康尼·乌德沃德、帕垂克·克提斯、莱斯利·格瑞福斯和罗丝·莫尔为我提供这样富有挑战性的机会。

——帕垂克·凯利

我要感谢在从事此项目过程中所有为我指点迷津、提供帮助的人，其中包括卓维斯·玛露、申恩·肯斯克、奥吉·维斯克、吉姆斯·萨利文、布鲁斯·吉姆斯和 DST Systems 公司的信息安全团队。还要感谢为此项目的成功实施做出了重要贡献的罗伯特·布拉格和 McGraw-Hill/Osborne 本团队的员工们。

——杰逊·扎恩

序

网络安全不仅包括实施技术控制和防范对系统的攻击，也不仅是增强某个操作系统或确保网络基础架构的安全，其实最重要的是网络安全不会因为我们最终所用的代码完美无缺而自动实现。在尽了一切努力之后，网络安全还依赖于网络经营者和网络使用者的道德和能力。

而且，在网络安全方面，我们不会总能找到“梦之队”，不能奢望所有员工都品德高尚、所有客户都遵纪守法，更不能指望全世界的人们都与我们有着同样的信仰。因为“人无完人”，我们所构建的信息系统可能会有问题，所采用的技术防护可能被他人破坏，而且我们还可能忽视一些若及时发现并采取措施就可能免遭破坏的事件。

但应对的办法不是放弃。不能总让别人为我们解决问题，我们必须与所信任的人士共同开发解决方案，这些方案即使不算完美，但至少能使系统持续运行、能提供有效防范、能让我们比攻击者领先一步。让我们每次都取得一点儿进步，每次都多保护一台机器，每次都再赢得一天。如果愿意听，就会发现有很多宝贵经验能为我们提供帮助；如果乐意做，就会发现有很多工作是可以做的。我们需要分享知识，切磋经验，揭示真相。

本书就是这种共同协作的结果。去年，美国堪萨斯市的六位安全专业人士在一家星巴克咖啡店里聚首，商讨编写一本书——这本书不应是简单阐述我们各自不同的信息安全经验，而应是我们共享这些经验的结晶。我们不想在此书中罗列相互独立的事实，而是要讨论协同工作的机理。虽然我们会为帮助他人搞清如何从技术上保证系统安全而讲到一些技术问题，但不想忽视在这一过程中人的作用。

就像传奇故事中探险的勇士一样，我们怀着崇高的理想踏上了征程。在编写此书的过程中，我们遭遇了各种灾难和重大人生变故。原来的团队中有人离开了，又有新人加入进来。差不多与此书相关的每个人——从作者、审稿人到出版社的编辑们——都在本书编撰期间经历了一些改变人生的事件。有的辞职，有的被解雇；有的乔迁，有的办了婚事；有的亲属遭遇不测，危及生命的事故接二连三。作为此套丛书的编辑，有时候我觉得自己就是《幸存者》中的一员。但此书终于成功出版了。

现在，读者已经看到了我们这次探险的成果。本书并不是解决困扰当今信息安全领域的各种问题的万能药，但或许本书比其他著作有价值得多。别忘了：情况在变，人也在变，每天都有新问题。如果你想为所在机构的信息安全做贡献，如果你想为全球的信息安全做贡献，就必须在努力做好今天的防范的同时，做好适应未来变化的准备。相信我们，按本书所讲的去做，现在就尽可能做好。同时要留心本书中所讲到的或自己所想到的那些将帮助我们的信息系统在未来仍能成功抵御攻击的东西。最重要的是，你自己要为此战的胜利做出贡献——这是一场需要我们共同努力才能打赢的战争。

—— 罗伯特·布拉格，“我想我们不再是在堪萨斯了”

2004 年 12 月 15 日

前　言

约翰·麦勒瑞

我谈论计算机安全问题已有六年，也编写过一些著作。最初我的观点来源于自己做系统管理员的经验，而后则来自在安全顾问公司做首席技术官（CTO）的经验。在受聘于安全顾问公司期间，先后涉足过计算机安全的诸多方面，如策略与过程、渗透测试、补丁管理和终端用户培训等，也由此加深了对一些问题的认识。随着在这一行业阅历的增加，我认识到有很多人在提供与计算机安全有关的培训和服务。伴随着与安全问题有关的材料的增多，我想安全将成为每家公司、每个系统管理员优先考虑的问题之一。但去年的两次经历让我相信，并不是每个人都已认识到计算机安全问题的紧迫性。

第一次经历开始于我接到客户打来的电话，称“我们觉得公司会计偷了公司的一些钱。”到该客户的办公室之后，发现这位会计不仅仅是偷了“一些钱”，其数额竟是让人咋舌的300 万美元！更让我感到诧异的是，这一数额居然没有更大些，因为该客户的这个网络直接连接到因特网，没有加防火墙，也不需要认证口令。另外，每个工作站都配有调制解调器，接有电话线，有远程访问客户端，同样也不需要认证口令。真让我纳闷这家公司的所有者们在过去六年中是否一直昏迷不醒。这家公司脆弱的安全防范使它的会计能够随时访问到所有财务记录和程序，而且她的所作所为都没有日志记录可查。结果是这位会计删除了虚假交易，更改了财务报告，重新划分了各项开支。

另一次经历是我碰到一位为 6 家法律公司管理网络的计算机顾问。他告诉我说这 6 家公司都经办了大量敏感案件，但它们的网络都没有加防火墙。当问到为什么没有装防火墙时，他反问我“你觉得应该装么？”我想自己当时是小声嘀咕了一句“笨蛋”。

有了这些经历之后，我认识到在向机构和个人普及计算机安全知识方面还有很多工作要做，本书就是我为之不懈努力的部分成果。与很多计算机安全著作不同的是，本书由此

领域的多位专家共同编写，这就意味着每位作者都有机会奉献自己的专长。他们根据自己的知识和专长撰写相关内容，而不是简单地重复一些常见的安全观点。另外，此书全部为“实质内容”。读者不会看到多个章节的理论阐述或因特网历史回顾，而是能很快读到可以立即用于系统和网络安全防护的内容。本书是对 Hardening 系列丛书中其他著作的非常有益的补充。如果你是计算机安全方面的新手，本书第 1 章为你提供了手把手的指导，可让你立即开始加固所在机构的网络安全。如果你对安全领域有所了解，正在寻求关于某个特定问题的新成果、新观点，也将会通过阅读本书而如愿得偿。

所以，现在就该开始加强你的网络安全。这不仅刻不容缓，而且任重道远。

内容安排

本书旨在向系统管理员传授实践知识，提供手把手的指导。这些系统管理员负责保证配有多种设备、多个操作系统的网络的安全。我们假定读者已经具备扎实的知识和技术，但可能只精通某一种操作系统或平台。本书将会让受过有限安全培训的系统管理员能立即着手“加固”所负责的网络或系统。就像所有与安全有关的著作一样，本书并不是一个完整的安全解决方案，但我们希望它成为评估企业信息安全的最佳起点。对认为所负责的系统十分安全的系统管理员来说，本书可以为你的工作做出验证，但同时也将提供一些不同的观点和其他解决方案，使你能够进一步加强安全防范。

第 1 篇：现在就做！

第 1 章：“做好开门七件事”

约翰·麦勒瑞

第 1 章的目的是给出一些可以立即用于网络及计算机系统的解决方案。对于那些不知从何入手的读者来说，第 1 章的内容可让你快速、有效地减少网络安全漏洞。本章不仅仅是给出建议，还告知具体该做什么以及如何做。我们还要给出一些重要内容，这些内容连经验丰富的系统管理员看了之后也会说“哇，我当年要能看到这些该多好”。

第 2 篇：从顶层开始：系统地加固你的公司

第 2 章：“为了安全，把网络划分成若干公共区”

约翰·麦勒瑞

计算机安全的重要思想之一是“深度防御（defense in depth）”。本章开始讨论分层次保障安全的方法，用一些具体标准对网络进行划分。本章所讲的一些标准将是很多系统管理员从未听说过的。

第 3 章：　“用身份管理系统加固安全”

杰逊·扎恩

人们对身份管理（identity management）有着很多不同的解释。但是，各种解释都强调用户管理的问题。本章探讨开发全公司范围的身份管理系统的公共基础，包括从符合法律要求和内部责任问题到如何降低成本并提高生产效率。本章还阐述了当前的基于目录的服务如何满足组织机构管理雇员、客户、签约方和厂商等不同身份的需要，并给出了如何对现有身份管理方案进行评估的建议。

第 4 章：“加固跨平台认证”

杰逊·扎恩

在访问信息系统时，用户通常必须提供账户名等信息，证明自己是合法用户，有权以此账户访问该系统。这种证实用户自称的身份的过程就叫身份认证，证实身份所用的凭证可能是口令、智能卡、令牌、生物特征或其他某种凭据。通常，安全专业人员的工作就是保证所采用的身份认证方法是最健壮的。本章讨论了在配有多种操作系统和多种平台且用户必须访问不止一个系统的情况下，应怎样做好身份认证。

第 5 章：“加固 Web 服务”

马克·奥尼尔

提供 Web 服务的系统总是面临遭受攻击的威胁。这是因为较之于其他系统，提供 Web 服务的系统更多地处于待访问状态，并且它们的漏洞也更广为人知。消除这些漏洞可保证 Web 服务的正常运行，而这经常决定着许多公司的成败。

借助于 XML 和 Web 服务（WS）安全等技术，Web 服务为我们提供了跨计算机系统的集成解决方案。本章探讨为支持 Web 服务和 WS 安全而开发的标准，并为 Web 服务开发者和评估者提供了关于安全实践和安全陷阱的信息。无论是乐意开发和部署 Web 服务的人还是必须对是否采用 Web 服务做出决策的人，都会从本章清晰的概念和解释中获益匪浅。

第 6 章：“加固移动环境”

杰逊·扎恩

本章讨论用于 PDA、智能电话等移动设备的安全解决方案，包括身份认证、病毒防护和加密技术。还讨论了如何应对红外技术和蓝牙技术的安全漏洞，因为这两种技术广泛应用于移动设备与 PC 机、移动设备与耳机、相机和打印机等其他无线设备之间的通信。

第 7 章：“超越访问控制：保护所存储的数据”

杰逊·扎恩

密码学和数据加密传统上一直被认为是数学博士们所研究的领域。但现在，在计算机网络中采用加密算法被认为是最安全的防护手段。本章扼要介绍了如何快速而实用地搞清与某机构需求相关的密码学知识，讨论了加密算法、密钥管理、如何选择具体算法及产品等问题，还给出了如何最恰当地利用加密技术的一些具体指导。

第 8 章：“加固来自 Web 的数据库访问”

罗布·克拉夫特

现在，关键、敏感数据都是存放在数据库中的，而且这些数据库可以用基于 Web 的程序经因特网而访问到。如果这种访问不安全，公司就可能在不经意间为竞争对手或攻击者提供了访问途径。所以除了要增强因特网服务器之外，还要更多地考虑如何为这些服务器上的数据提供最佳的保护。微软、Oracle、IBM 等几大数据库厂商都为此提供了一些工具。本章阐述如何利用这些工具保护数据库，以及在同时配有多个厂商的数据库产品时该如何处理问题。本章给出了针对使用数据库时各个阶段的建议，包括安全安装数据库、设置访问权限、使用应用分区、遵循软件开发的最佳做法、监控和审核数据库行为以及保护备份等。

第 9 章： “加固跨平台访问控制”

鲍尔·拉乌和罗伯特·布拉格

Windows 和基于 Unix 的操作系统都提供有针对文件系统的访问控制，但这些控制方法并不等效。要想为跨平台访问控制提供健壮的解决方案，首先要了解它们之间的差异，并从安全的角度总体考虑集成解决方案。本章剖析了这两大类系统的访问控制方法，并对 Samba、SANs、Microsoft Services for UNIX 等多种集成解决方案的加固选项做了说明。

第 10 章：“利用加密加固数据传输”

维斯·努南

“静止”数据（即存放在某一系统中的数据）容易受到攻击，“传送中”的数据（即在系统之间传输的数据）也容易遭受破坏。本章讨论了可应用于传送中的数据的各种加密机制，包括 VPN、SSL 和 IPSec。但是，采用未能很好实现的安全解决方案会带来虚假的安全感，因此可能还不如根本没有安全解决方案。了解这些问题并遵循最佳做法可以保证通信的健壮与安全。

第 11 章：“加固远程客户端”

艾瑞克·西格闰

很多公司都非常关注加固远程访问服务器的问题，它们为网络配备了强大的边界控制措施，但却让员工带着毫无保护的便携机赶赴世界各地，允许他们从遥远的城市远程访问公司网络。正如本章所述，公司需要制订全面规划，以保证远程客户端的安全。无论客户端是传统的台式 PC 机、便携机、PDA 还是智能电话，遵循本章所讲的最佳做法将使远程访问解决方案更为安全。这些措施包括保护远程访问服务、保护远程访问的传输和保护客户端，此外还有使用安全的远程访问方法、配置客户端防火墙、限制访问权限、使用防病毒产品、及时给客户端和服务器打补丁、就如何安全地进行远程访问而对最终用户进行培训等。

第 12 章：“加固无线网络”

维斯·努南

无线网络几乎已成为公司甚至家庭用户的标准操作环境。关于如何保证单访问点无线网络或仅覆盖少数几个用户的无线网络的安全，已经有了很多建议。但是，大型机构使用无线网络或无线广域网的安全问题，则鲜有人注意。若保证无线网络的安全，其基本思想总是类似的：采用无线安全策略、保证身份认证和数据传输的安全、提供密钥管理、检测并取消非正常的无线网络、把无线网络看作不可信网络。但是，无线广域网为我们提出了更多的挑战，这些内容都在本章讨论。

第 13 章：“加固混合的 Unix 网络”

鲍尔·拉乌

Unix 操作系统是诸多公司和开发人员历经 30 多年不断开发和改进的成果。在这一过程中，Unix 演变成了多种版本，每个版本在协议和系统过程的实现上都有所不同。虽然所有 Unix 系统现在仍沿用 Unix 的核心思想，但它们在安全机制的实现方面已有很大差异，而且这种差异已足以让未受过培训的人混淆。本章就是要让读者彻底了解异构环境中各种版本的 Unix 和 Windows 在安全实现方面的异同，并特别强调了 Linux 在工作环境中的日益流行以及当 Linux 与 Unix 和 Windows 同处一网时应注意的问题。

第 14 章：“入侵检测与响应”

帕垂克·凯利

了解防线何时被突破是网络安全最重要的方面之一，而入侵检测系统（IDS）可以对某机构的网络和主机访问行为进行持续监控。经过适当配置，这种监控系统可以识别出恶意

行为或未经授权的行为，并可提供具体审计信息。如果处理得当，这些审计信息可以在识别攻击及确定如何补救方面提供非常有价值的证据。但很多管理员都未受过恰当培训，在IDS发出入侵告警时不能做出有效的响应。IDS的告警可能是攻击引发的，也可能是误警，管理员必须要能对此做出鉴别，这很重要。IT专业人员需要了解IDS的框架，搞清这种系统能在多大程度上帮助维护可靠、安全、富有效率的技术环境。本章将对这些内容做出阐述。

第15章："管理恶意代码"

杰迪·扎恩

现在，病毒、木马、间谍软件等恶意代码非常多，从未听说过"恶意代码"这个词的人肯定是生活在没有计算机的地方。分层的方法，或者说提供深度防御的方法，也适用于对恶意代码的防范。因为不可能仅靠安装一个产品或一个程序而实现完全的防护，所以必须对防范体系划分层次，要有边界防护，也要有对服务器和客户机的防护。恶意代码不容易检测到，这是因为在很多情况下，恶意代码是把原有的系统设置应用到了本来不包括的范围内，从而产生不良后果。这些不良后果可能是对隐私性构成威胁、对系统造成破坏，也可能就是典型的恶作剧。本章介绍了各种恶意代码，并对如何检测、报告和阻止恶意代码做了阐述。

第16章："增强湿件"

约翰·麦勒瑞

安全专业人士经常哀叹：如果不让人使用，他们的系统就会安全了。有些人甚至说安全防护最薄弱的环节就是人。可以采取一些措施对安全所涉及到的"人"进行教育和培训，但诚如本章所述，这需要付出努力，需要妥善规划，需要得到管理层的持久支持。

第3篇：永远没有一劳永逸

第17章："混合网络的安全审核与测试"

艾瑞克·西格闰

创建和实现牢固而全面的安全策略仅是加固网络的第一步，下一步就是要保证最终确实实现了安全。正如本章所述，信息系统审计可帮我们搞清自己的网络在多大程度上实现了安全规划，以及自己的安全防范在多大程度上与当前公认的安全实践相符合。审计会根据预先确定的范围对当前的安全配置与安全策略的相符程度进行评估，并可能对网络进行测试，搞清安全防护的实际效果。但审计不仅是渗透测试，也不仅是对照列表进行检查，而应指导我们如何改进。