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 Windows Systems 中文版

Bulletproof your systems before you are hacked!

为你的系统构筑坚固的安全堡垒

[美] Boberta Bragg 著

吴晓斌 程文俊 译

Mc Graw Hill Osborne

Mc Graw Hill

清华大学出版社

网络与信息安全技术经典丛书

Hardening Windows Systems 中文版

[美] Roberta Bragg 著

吴晓斌 程文俊 译

清华大学出版社
北京

Roberta Bragg
Hardening Windows Systems
EISBN 0-07-225354-1

北京市版权局著作权合同登记号　图字 01-2006-0350 号

图书在版编目（CIP）数据

Hardening Windows Systems 中文版/（美）布拉格（Bragg, R.）编著；
吴晓斌，程文俊译. —北京：清华大学出版社，2006.5
书名原文：Hardening Windows Systems
ISBN 7-302-13040-X

Ⅰ. H…　Ⅱ. ①布…　②吴…③程…　Ⅲ. 窗口软件，Windows
Ⅳ. TP316.7

中国版本图书馆 CIP 数据核字（2006）第 049556 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：何武
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：185×230　　**印张：**29　　**字数：**633 千字
版　　次：2006 年 6 月第 1 版　2006 年 6 月第 1 次印刷
书　　号：ISBN 7-302-13040-X/TP・8277
印　　数：0 001~3 000
定　　价：53.00 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，由安全界著名传道士 Roberta Bragg 执笔，通过四段式系统强化教学法，从技术和管理制度两方面，详细介绍 Windows 系统的安全防护工作，对系统管理员容易疏忽或犯错的细节进行深入发掘，旨在帮助读者把 Windows 系统建设成强固的信息安全堡垒。

全书共分 4 大部分 14 章，第 1 部分给出降低系统威胁的 10 项关键措施，是系统阻止入侵的必要手段；第 2 部分是本书的重中之重，自顶向下系统讲述强化 Windows 系统的各项具体方法和措施；第 3 部分告诫人们：一劳不能永逸，需要利用各种监控技术持续监控系统，教会读者创建业务连续性计划、制定安全策略以及灾难恢复策略等；第 4 部分对信息安全工作的湿件方面进行全方位讨论，同类书中少见。

本书操作平台覆盖 Windows 95/98/NT 4.0/2000/XP 以及 Windows Server 2003，是 IT 专业人士的福音。

作 者 简 介

Roberta Bragg，CISSP，M.C.S.E.：Security，Security+，在 IT 界从业 25 年，从大型主机到移动系统，从穿孔卡片到.NET，从拨号上网到 Internet，她一直是活跃人物并创造了很多神话。当前承担的项目包括高级的、短期的有关 Windows 安全方面的咨询业务，长期担任 MCP Magazine Security Advisor 杂志的安全领域专栏作者，还是 TechTarget Win2000 Security Expert Q & A 的特邀顾问。Roberta Bragg 是 McGraw-Hill/Osborne 公司出版的 Hardening 系列图书的策划人，本套图书旨在帮助读者在遭受黑客攻击之前系统地加固自己的网络。

序　言

最近三年，系统安全问题已经从发生事故后 IT 部门的事后反思，变成了决策时首先需要考虑的问题，其重要性日益凸显。系统安全越来越重要的后果是，不仅需要大量合格的安全专家，而且对几乎所有的 IT 管理员来说，是否懂得系统安全已成为一项非常重要的工作需求。但是对大多数的 IT 管理员来说，他们日常本身已没有足够的时间来完成手头现有的工作，更不必说花费时间来搜集大量的文献、书籍和网站等信息来加强他们的 Windows 操作系统，特别是如果公司的网络使用 Windows 不同版本的系统，那将更麻烦。如果你遇到了上述问题，那么这本书将是你的最好选择。此书将给你全面细致的系统安全解决方案。

在读此书的初稿时，Roberta 女士在加强 Windows NT 4.0，Windows XP，Windows 2000 和 Windows Server 2003 等系统安全方面出色的工作给我留下了深刻的印象。市面上大多数系统安全书籍只讲述一至二个 Windows 操作系统，很少像本书一样涉及全部 Windows 系统，特别是作为一点小奖励，Roberta 女士更是讲了一些 Windows 95 和 Windows 98 系统安全的小技巧。再加上她随和、轻松的写作风格，这本书将是一本独一无二的系统安全宝典。（我认识 Roberta 女士已很多年，在读此书时，字里行间仿佛都能听到她的声音。）

本书另一个突出的优点就是其方案的可操作性很强，虽然计算机安全是计算机本身的事情，但最大的安全漏洞往往是人。好消息是，一旦人们得到良好的训练，他们就是你可配置的最好安全措施；坏消息是，很显然，你无法按组策略来配置他们。本书详细阐述了计算机、用户、管理员和 IT 管理人员之间相互关联的能够引发网络攻击的一些重要领域，并介绍了一些除安全配置之外的技术措施。

我可以很有信心地说，通过阅读此书，你将能熟练出色地加强公司客户端和服务器上 Windows 操作系统的安全。

Ben Smith
Security Strategist
Microsoft Corporation

“一个优秀的系统安全领路人——我自认无法比她写得更好。一本全面、通俗易懂的 Windows 系统安全参考书。每个系统管理员必读的宝典。”

Eric Schultze
首席安全架构师，Shavlik Technologies
微软高信度计算小组前成员

前　言

生活如大多数人想的一样充满各种危险因素，如果我们想幸免于难，就必须做好信息系统的安全防范工作，必须学会如何更好地防护信息系统，以及极力阻止那些粗枝大叶，甚至用心险恶，或者口无遮拦的人可能对系统造成的任何破坏。

信息防护是一项繁重到几乎不可思议的工作。但在我们遇到大问题等待安全专家救驾时，还是可以采取一些适当的弥补措施。问题的关键是，我们不应该等待、犹豫——而是应该立马采取行动。在我们与他人合作或独自工作时，应努力营造一种安全文化，加强所有牵涉到的网络组件的安全，建造一个更安全的系统，并把此理念灌输给每个员工。如果你从事 IT 行业，那更应有此观念！本书所属的“Hardening”系列丛书，能给你提供一些帮助。此系列丛书中的每本书分别涉及信息系统的一个部分，并为每个部分提供了相应的系统强化措施。

本书为强化 Windows 系统的一些必要步骤罗列了一个主要的目录，适用于 Windows 98，Windows 95，Windows NT 4.0，Windows 2000，Windows XP 以及 Windows Server 2003 系统。本书不想成为信息安全的一个全面向导，也不可能包含理解和实践 Windows 安全所必需的全部信息。但本书叙述详尽而且简单易懂，每一强化步骤都附有一步步的详细说明。对部分读者，本书为您提供了一个开始强化信息系统安全的平台；对另一部分读者，本书所列举的措施可用于判断您目前采取的措施是否正确；对其他一些读者，本书可为您的 Windows 系统安全知识打下坚实的基础。

请您阅读、吸收，然后使用书中的知识。如果您觉得本书好，请推荐给您的朋友。如果您觉得本书不尽人意，请告诉我们。但最重要的，请强化您的 Windows 系统。

致　谢

感谢 Athena Honore 一直给我善意的提醒；感谢组稿编辑 Tracy Dunkelberger，一位出色的组稿编辑，也是我的拳击陪练；感谢文稿编辑 Bob Campbell 给本书润色不少；感谢计划编辑 Emily Rader 统筹一切事情；感谢技术编辑 Rodney R.Fournier；以及其他一些我不知名的对本书出版做出贡献的人们。

我还将感谢所有使整个世界的信息系统更加安全的读者朋友们，你们已经做了大量工作。你们将一直是我灵感和其他悲伤的来源。

目　录

第 1 部分　马上行动

第 2 部分　从顶端做起：系统地强化安全

第 3 部分　一劳不能永逸