完全手册丛书

顶级安全专家倾力之作

Network Security: The Complete Reference

网络安全完全手册

Roberta Bragg
[美] Mark Rhodes-Ousley 等著
Keith Strassberg

程代伟 路晓村
池亚平 李冬冬 等译

薛荣华 审校

安全策略的发展历程及最新安全技术介绍

Windows、Linux/UNIX、Novell及无线网络的安全技术

二十多位业界精英的集体智慧结晶

電子工業出版社
Publishing House of Electronics Industry
http://www.phei.com.cn

完全手册丛书

网络安全完全手册

Network Security: The Complete Reference

Roberta Bragg
[美] Mark Rhodes-Ousley 等著
Keith Strassberg

程代伟 路晓村 池亚平 李冬冬 等译

薛荣华 审校

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内容简介

本书由多位美国计算机网络安全专家集体编写，为读者描绘了有关网络安全领域的总体框架。全书共分6个部分30章，详细介绍了30种不同的网络安全领域的解决方案，主要包括授权与认证控制、网络设备安全、防火墙、VPN、无线网络、入侵检测、Linux/UNIX安全、Windows安全、Novell安全、J2EE安全、.NET安全、数据库安全、灾难恢复及事件响应、法律问题等。本书在内容上注重全面性，几乎涉及了与网络安全相关的所有主题，是一本完整的网络安全参考手册。

本书适合从事网络安全工作的技术人员及开发人员使用，也适合作为计算机应用专业高年级本科生和研究生的教材。

Roberta Bragg, Mark Rhodes-Ousley, Keith Strassberg: Network Security: The Complete Reference.
ISBN:0-07-222697-8

版权贸易合同登记号　图字：01-2002-5894

图书在版编目（CIP）数据

网络安全完全手册/（美）布拉格（Bragg, R.）等著；程代伟等译. -北京：电子工业出版社，2005.10
（完全手册丛书）
书名原文：Network Security: The Complete Reference
ISBN 7-121-01767-9

Ⅰ.网… Ⅱ.①布… ②程… Ⅲ.计算机网络-安全技术-技术手册 Ⅳ.TP393.08-62

中国版本图书馆CIP数据核字（2005）第107698号

责任编辑：许菊芳
印　　刷：北京天宇星印刷厂
出版发行：电子工业出版社
　　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：39.25　字数：1005千字
印　　次：2005年10月第1次印刷
定　　价：65.00元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换；若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

译 者 序

本书由多位美国计算机网络安全专家集体编写，为大家描绘有关网络安全领域的总体框架，并详细介绍了30种不同的网络安全领域的解决方案。本书所涉及的内容如下：从物理安全到最近颁布的法律；从认证、授权和审计到防御、制止和检测；从灾难恢复到在Cisco路由器上配置安全；从Windows到Linux；等等，是一本全面介绍计算机网络安全的权威参考书。

本书共分6部分，第一部分对网络安全进行了基本的描述，并定义了信息安全的主要管理问题和组织结构。此外还介绍了风险分析和安全策略，并定义了在企业中是如何组织安全管理的。第二部分介绍了如何通过控制对计算机及计算机上的数据和应用程序的访问，增强计算机的安全性。第三部分说明网络必须有一些潜在的基础设施，并在每一个结合点处将它与安全考虑一起进行设计。在这一部分中，读者会找到关于如何保障网络安全的简单定义和丰富建议，找到对安全设备（比如防火墙和IDS）的解释，以及使它们安全的步骤。第四部分介绍操作系统的安全模型。应用程序运行在连接到网络的客户端和服务器上，应用程序安全的基础则是操作系统。在考虑保证运行在网络上的应用程序的安全之前，需要加固应用程序赖以提供服务的基础程序的安全。第五部分详细介绍了编写安全软件的原理和方法。第六部分讲述当天灾人祸损害到数据或系统时，我们该如何进行应对。该部分还包括信息安全所涉及的法律问题。

参与本书翻译工作的有：程代伟（前言和第1～8章）、路晓村（第9～21章）、池亚平（第22～25章）、李冬冬（第26～30章）。全书由薛荣华审校。参加本书译录校工作并给予大力协助的还有王军素、闫慧娟、李可、郭淼、姚栋、曹汉征、许秀英、矫克民、薛姗、刘晓玉、蔡红志、刘东顺、李南平、王建成、薛亮、沈兰英、王太东等同志。电子工业出版社编辑们为此书的出版做了大量艰苦细致的工作，译者谨向他们表示衷心的感谢。

由于时间紧迫和水平有限，本书难免存在一些疏漏和错误之处，衷心希望广大读者批评指正。

作者简介

Roberta Bragg(CISSP,MCSE:Security; Security + ,ETI Client Server,Certified Technical Trainer,IBM Certified Trainer,DB2-UDB,Citrix Certified Administrator)已经为 *Microsoft Certified Professional* 杂志做了5年的安全顾问兼专栏作家,她也是 SearchWin2000.com 的安全专家,她还为订户超过 55 000 的 *Security Watch* 新闻列表写文章。Roberta 设计、计划、发起并参与了 2002 年在美国西雅图举行的第一届 Windows 安全峰会。同年,Roberta 在 San Diego 的 TechMentor 推出了"安全研究院"的第一项成果,这是一个为期 3 天的实际动手组建安全网络的培训班,这个培训班后来在 2003 年又举办了 5 期。在 2002 年的 9 月和 10 月,Roberta 是 4 个学期的 SANS Gold Standard Windows 2000 培训班的指导教师。Roberta 参与过众多的安全审计,她是一个安全方面的传道者,她的足迹遍布全世界,不断地进行网络和 Windows 安全方面的咨询、评估和培训工作。Roberta 是 Seattle Pacific 大学的兼职人员,她还在 Johnson County Community 学院承担 Windows 2000 安全设计和网络安全设计课程。Roberta 是微软出版社即将出版的 *MCSE* 70-298 *Designing Windows Server* 2003 *Security* 和 *Windows Server* 2003 *Security Administrators Companion* 的第一作者。她还在 QUE 和 New Riders 出版社出版过有关 SQL Server 2000、CISSP 和 Windows 安全方面的书籍。

Mark Rhodes-Ousley(CISSP)从事过 10 多年的安全实践工作,是一名资深的安全工程师。Mark 为几十家公司策划、设计并安装了安全技术和策略,包括财富 500 强的公司(比如 Clorox 和 Gap 公司)和大型的公司(比如 Sun Microsystems 和 Hitachi Data Systems),中型的公司(比如 Metricom 和 Watkins-Johnson 公司),以及许多小公司(比如 Napster 和 Internex)。Mark 经历了这些公司的不同成长阶段,所有这些经历使得他在怎样为成长中的企业处理安全问题方面具有独到的眼光——从哪里开始,下一步该做些什么,怎样为未来的发展做出考虑。

Mark 既关注战略也关注战术,他坚信商务处理比技术配置还要重要,Mark 专修的是防卫而不是破解(hacking)。Mark 在信息安全领域所做的许多工作都是开创性的,他跟业界最杰出的一些人一起工作,并培养了其他一些人,他的某些安全理念在若干由个人和公司出版的出版物里都有所体现。Mark 持有由国际信息系统安全认证联盟、Cisco Systems、Security Dynamics、Raptor Systems、Hewlett-Packard 和 Digital Equipment Corporation 所颁发的证书,他还获得了美国加州大学圣迭哥分校(UCSD)的应用数学和电气工程学士学位。

Keith Strassberg(CPA、CISSP)是一位独立的安全顾问,他在信息安全方面有 7 年多的工作经验,最近他成为了一个中等规模的技术咨询公司的高级安全工程师。在此之前,Keith 是位于 Arthur Andersen, LLP 的计算机风险管理工作组的成员,Keith 的职业经历涵盖了信息安全的所有方面,包括(但不限于)设计和部署安全基础设施、实现防火墙和入侵检测系统、执行计算机法庭调查、进行策略和规程的开发,以及进行易受攻击性(脆弱性)测试等。

他出版的著作有:*Firewalls*: *The Complete Reference*(McGraw-Hill/Osborne,2002), *Security Architecture*: *Design*, *Deployment and Operation*(McGraw-Hill/Osborne,2001)和 *Troubleshooting*, *Maintaining & Repairing Networks*(McGraw-Hill/Osborne,2002)。

Keith 获得了伯明翰大学的会计学位,他的 E-mail 地址为:kstrassberg@yahoo.com。

致　谢

感谢 Athena Honore，没有她的贡献，这本书就会散乱如麻，我真的不知道她是如何将 28 位作者及评论家的稿件有条不紊地组合在一起的。感谢 Tracy Dunkelberger，是她克服了不可逾越的困难才使得本书得以出版。感谢本书的其他作者，他们容忍了 Tracy 这位“怪癖”老妇人的挑剔要求：“更多一些”、“更好一些”、“更明确一些”。感谢 Internet，没有它的便利，我们可能还在采用传统的邮递方式互寄手稿，并埋怨着这种机制的效率（同时也是逾期交稿的托辞）。

Roberta Bragg

我要感谢那些建立、开发并文档化了信息安全产业以及为此做出贡献的人：Bruce Schneier、Bill Cheswick、Steve Bellovin、Winn Schwartau、Simson Garfinkel、Gene Spafford、Sun Tze、Miyamoto Musashi、Cliff Stoll、Ben Rothke、Charles Cresson Wood、Brent Chapman、Elizabeth Zwichy、William Stallings、Phil Zimmerman，以及为此贡献了智慧的其他同行们。

Mark Rhodes-Ousley

借此机会，我要感谢多年来在信息安全领域给我教诲的所有良师益友，不管他是名正言顺的导师还是曾经指点过我的人。还要感谢那些使得本书得以出版的人：Roberta、Mark、McGraw-Hill/Osborne 出版社勤勉的工作人员、Tracy Dunkelberger、Athena Honore 以及其他编辑人员，是他们细心地编辑了本书。

Keith Strassberg

前　言

网络安全是一个涉及面很广，同时又相当复杂的研究领域，实在难以想像仅靠本书的三位主要作者就能够把与网络安全有关的所有关键问题都描述清楚。我们尽了自己最大的努力，搜罗了业界最好的、最有智慧的头脑，以帮助我们创作出网络安全方面最权威的指南：你最先读到的书，就是你信赖的书。我们把握了这个机会，给大家呈现了 IT 从业人员每天都急需获取的实际而有用的信息。希望通过我们的努力能够给大家传授我们所获得的所有知识，这些知识是我们通过研究和试验而获得的，并且融入了我们在保卫真实世界中的网络时所获得的实际经验，我们知道，所有这些信息也许并不可能在一本 30 章的专著中全部表达出来。

这并不是一本用荒唐而恐怖的故事来吓唬大家的书，它也不会告诉大家保证网络安全、加固服务器或摆脱蠕虫和垃圾邮件的 10 种魔法。本书要做的是为大家描绘有关网络安全领域的总体框架，并详细介绍 30 种不同的网络安全领域的解决方案。本书所涉及的内容如下：从物理安全到最近颁布的法律；从认证、授权和审计到防御、制止和检测；从灾难恢复到在 Cisco 路由器上配置安全；从 Windows 到 Linux 系统的安全。本书的每一位作者都是相关领域中的专家，他们为本书的编写尽了最大的努力。他们都希望你也能成为专家。

本书共分 6 部分，这些部分囊括了网络安全的各个方面。

第一部分：网络安全基础

本书的第一部分对网络安全进行了概述，并定义了信息安全的主要管理问题和组织结构。如果读者是一位受过教育或有实践经验的技术人员，一开始也许会觉得自己可以跳过这一部分或者放在最后再读它。请不要这样。正如为了编写出好的代码而需要理解计算机是如何工作的以及程序指令是如何执行的；正如你为了理解联网技术而需要知道 OSI 的 7 层模型；也正如需要了解一些技术基础一样，读者需要知道信息安全的基础知识，以便应用它们。

这一部分还介绍了风险分析和安全策略，并定义了在企业中是如何组织安全管理的。

风险分析用来识别应首先保护哪一个系统，以及哪一个方案能够获得预算资金来开展工作。你有通过购买设备来改进安全的想法吗？或者应如何通过在口令策略中实行改变来增进安全性？该怎样通过对 IT 专业人员提供安全培训来保障安全？也许公司的风险分析可以为你提供所需要的信息，以获得资金支持。

安全策略用来指示在信息系统的使用中和在管理它们时可以做些什么和不能做什么。你愿意对口令数据库进行审计并找出在选择口令时没有使用好的方法的用户吗？最好应该让自己明白口令策略是什么，并遵守已制订好的安全策略，还要注意检查你是否具有对数据库进行审计的权限。

在众多机构中，安全组织是一种正式的机构。你所在的公司有这个机构吗？你希望它是什么样的？

第二部分：访问控制

如果任何人都无法对计算系统进行访问的话，就不存在任何安全问题了。然而，我们需要能够读取和操纵数据、访问远程站点、运行应用程序；我们需要使用计算机来工作，我们必须坐

在计算机前面，连接、登录到系统，对系统进行修理、添加新的特性、安装新的软件、给它们打上补丁程序、将它们带在身旁、并将它们放在旅店的房间中。

该怎样保护它们呢？通过控制对计算机及计算机上的数据和应用程序的访问，就可以增强计算机的安全性。访问控制对于许多人来说意味着许多事情，但大多数人会同意它包含了物理安全、认证（证明你就是你所说的那个人）、授权（一旦通过了认证，判断你能做什么）以及数据和安全管理架构。这一部分的几章中包含了实际的技巧和由专家提炼的用于数据中心和传统桌面部署的方法学，此外还介绍了如何应对信息的快速积累以及使用移动计算设备时的访问控制方法。在安全架构中，很早就考虑到了访问控制，本书的作者为大家展示了他们对访问控制的见解。

第三部分：网络体系结构

将系统通过线缆连接起来并在系统和因特网之间设置防火墙，这并不是保证网络安全的方式——它只是一个开始。为了保证安全，网络必须有一种潜在的基础设施，并在每一个结合点处将它与安全因素一起进行设计。应该在哪里放置设备布线柜？怎样保障它们的安全？交换机比路由器更安全吗？使用哪一种类型的防火墙？新的入侵防范设备使得入侵检测系统过时了吗？根据什么样的设计和设备能确定一个网络是安全的，而另一个网络则无法使用？

在这一部分中，读者将找到关于如何保障网络安全的简单定义和丰富建议，找到对安全设备（比如防火墙和 IDS）的解释以及使它们安全的步骤。读者会发现使用并保障 VPN 安全、设计安全网络和将无线网络安全地集成在一起的最好的实践方案。读者还会发现如何最佳地保障网络及其所支持的数据的完整性以及支持冗余和可恢复性的需要。

如果没有涉及到怎样保障计算机所扮演的各种角色的安全的信息，任何有关网络基础设施安全的讨论就将是不完整的。邮件服务器、传真服务器、文件和打印服务器及其他设备，是网络整体设备中不可缺少的部分，需要保证它们不受到攻击，防止它们变成攻击的对象。

第四部分：操作系统安全

应用程序运行在连接到网络的客户端和服务器上，应用安全的基础则是操作系统。在考虑保证运行在网络上的应用程序的安全之前，需要加固应用程序赖以提供服务的基本程序的安全。关于操作系统的安全，首先需要理解的是：正如有定义服务的原理和模型一样（比如联网、文件系统、用户接口等），操作系统也有其安全模型。这部分的开头一章对此进行了解释，在后面的章节中，探讨了 UNIX、Linux、Windows 和 Novell 等操作系统的安全问题。

第五部分：应用系统安全

对于大多数人来说，应用程序就是计算机，他们并不关心操作系统、网络或诸如此类的事情。对于他们来说，重要的是能够收发 E-mail、玩游戏、写报告、使用电子表格、输入命令或打印工资清单等功能。对于许多网络专家来说，应用程序则是二等公民。在他们的心目中，应用程序只是比终端用户高一等。然而，应用程序以及用来创建、运行它们并管理其数据的进程，才是当今信息安全的症结所在。普通的人跟应用程序打交道，杰出的人创建应用程序，邪恶的人试图破坏应用程序。

应用程序是我们了解并使用的 E-mail 客户端、游戏和数据录入系统，但在某种程度上，它们也是操作系统、服务器和网络设备的构成部分。所有这些程序使用同样的工具、同样的语言和同样不完美的人类大脑来构建。日复一日，我们希望这些由人类所创建的复杂系统没有缺陷，而且永远不会被毁坏。当它们无法满足我们的期望时，我们就特别失望。

怎样改变这种状况呢？许多年以来，计算机科学家始终在宣扬可以编写出更好的程序的方法学，但商业软件公司并没有遵循这些方法。情况正在得到改变。本书的这一部分详细介绍了编写安全软件的原理和实践，而无需顾及所使用的特定技术，也无需顾及程序的类型。在这一部分中还包含了使用 Windows .NET 和 J2EE 的内容。这一部分以讲述保障数据库的安全的一章而结束——数据的存储及其应用。

第六部分：响应

安全不只是保证不出事，安全还包括当加固后的技术并不有效，或者当天灾人祸损害到数据或系统时该如何应对的问题。当灾难降临时，如何保证业务能继续正常进行，每个人必须对此有所准备。每一个人还应当有一个计划能回答以下三个问题：

- 当面临攻击时该怎样应对？
- 怎样防止大多数攻击的成功实施？
- 如果攻击成功了，该做些什么？

此外，信息安全的复杂世界并不会对现实世界产生免疫力。现实世界中的法律正在不断增强对隐私和知识产权的保护。并不只是邪恶的破解者会被送进监狱，任何负责数据或系统的安全性和完整性的雇员都有可能因失职而被起诉。聪明的信息安全从业者将会找到法律背后的含义。我们将帮助你从现在开始做起。

结束语

本书能够回答网络安全中遇到的所有问题吗？我可不敢保证。但我可以告诉你，本书中有许多好材料——容易理解的材料，它们是你可以应用的实际原理、细节、情节和开阔的想像。我为我们能够完成此书的写作而自豪。

Roberta Bragg

目　录

第一部分　网络安全基础

第二部分　访问控制

第三部分　网络体系结构

第四部分 操作系统安全

第五部分 应用系统安全

第六部分　响应

第一部分

网络安全基础

第1章　网络安全概述

撰稿人：Mark Rhodes-Ousley，CISSP，BSEE

安全并不是让人们无法访问网络，安全还可以按你所希望的方式让人们接入到网络中，以便让人们能一起工作。高强度的网络安全为人们访问你的业务打开了一条通路，而无需顾及他们的物理位置和连接方式。安全控制越紧，你为外部可信伙伴所提供的安全访问级别就越高，同样，他们提供给你的安全级别也高。信任程度越高，你能提供给外部伙伴的安全访问就越多，这些外部伙伴包括客户、供应商、商业合作伙伴、销售商、顾问、雇员和联系人等。这样的安全访问能够激励业务合作，并通过业务流程的并行处理来降低成本。更重要的是，许多客户和商业合作伙伴在他们同意开展业务之前，都要求很高级别的信任。

安全性使得业务能够正常开展。好的信息安全实践方案不仅能降低成本，而且还能带来新的财富机会。过去人们提到安全，想到的只是对内容（上下文）的保护，现在，这种观念已经进化为通过使用新的通信方式，使得人们能够在全球范围内开展业务。通过改进对驱动业务所需信息的访问，每个公司都可以将它的业务影响扩展到全球范围，而无需顾及公司的规模或地理位置。现代化的安全实践方案能将信息提供给那些需要它的人，而不会将信息暴露给那些不该得到的人。当信息在那些被授权拥有的人之间共享时，信息的价值就更大了。分发信息的工具越好，可以访问信息的客户群就越大。一个安全的数据网络能允许公司很快地将信息传遍组织，并分发给业务合作伙伴和客户。

不同的公司有不同的信息。公司可能有一些需要保密的信息，比如客户清单、信用卡账号、股东的名字和地址等。特殊的信息可能还包括商业秘密，比如配方、产品细节和其他一些知识产权等。服务组织可能有一些关于其客户的信息，这些信息不能向公众开放。专利方法学及其实践描述了怎样提供服务及市场销售数据。

这些宝贵的信息大都驻留在公司内部网络中，使得网络成了公司业务的关键部分。一个数据网络并不只是简单地增加产量，它还使得公司能促进销售并为客户提供服务。

1.1　好的安全实践方案的益处

经过集思广益而提出的安全实践方案能解决特定的业务问题，并能产生可预见的良好结果。这些方案的成本应当是可控的，并能适当地进行分配。安全战略的成功实施应当以可控的方式进行，采用自顶向下的方法来保证与预期的计划相一致的连贯的结果。成功的安全方案应当是经过精心策划的，用来解决特定的业务问题，并给实施者带来实实在在的好处。

防范水平高的安全方案所带来的一个特殊好处是商业灵活性。好的安全实践方案能允许公司以一种更加集成化的方式来实现其业务操作，尤其是对其客户的处理。通过精心控制提供给每个客户的访问级别，公司就可以扩展其客户群，并为每个客户扩充它所能提供的服务级别，而不会损害到相关业务的安全和完整，也不会损害到其声誉和客户的资产。好的安全方案的另一个益处在于，人们的投资能够得到回报。安全性不仅仅是以成本为中心，它还是能够在很多方面得到回报的有用工具。下一节将详细描述这些好处。