国外计算机科学经典教材

THOMSON

Web Security for Network and System Administrators

网络和系统管理员Web安全指南

David Mackey 著

孙岩 邵良杉 等译

清华大学出版社

网络和系统管理员 Web 安全指南

David Mackey 著
孙 岩 邵良杉 等 译

清华大学出版社
北 京

David Mackey
Web Security for Network and System Administrators
EISBN: 0-619-06495-1

Copyright © 2003 by Course Technology, a division of Thomson Learning.
Original language published by Thomson Learning (a division of Thomson Learning Asia Pte Ltd). All Rights reserved.

本书原版由汤姆森学习出版集团出版。版权所有，盗印必究。
Tsinghua University Press is authorized by Thomson Learning to publish and distribute exclusively this Simplified Chinese edition. This edition is authorized for sale in the People's Republic of China only (excluding Hong Kong, Macao SAR and Taiwan). Unauthorized export of this edition is a violation of the Copyright Act. No part of this publication may be reproduced or distributed by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.
本中文简体字翻译版由汤姆森学习出版集团授权清华大学出版社独家出版发行。此版本仅限在中华人民共和国境内(不包括中国香港、澳门特别行政区及中国台湾)销售。未经授权的本书出口将被视为违反版权法的行为。未经出版者预先书面许可，不得以任何方式复制或发行本书的任何部分。
981-265-878-5
北京市版权局著作权合同登记号　图字：01-2003-8486 号

版权所有，翻印必究。举报电话：010-62782989　13501256678　13801310933
本书封面贴有清华大学出版社防伪标签，无标签者不得销售。
本书防伪标签采用特殊防伪技术，用户可通过在图案表面涂抹清水，图案消失，水干后图案复现；或将表面膜揭下，放在白纸上用彩笔涂抹，图案在白纸上再现的方法识别真伪。

图书在版编目(CIP)数据

网络和系统管理员 Web 安全指南/(美)麦基(Mackey, D.)著；孙岩，邵良杉等译. —北京：清华大学出版社，2006.5
书名原文：Web Security for Network and System Administrators
ISBN 7-302-12651-8

Ⅰ. 网…　Ⅱ. ①麦…②孙…③邵…　Ⅲ. 计算机网络－安全技术－指南　Ⅳ. TP393.08-62

中国版本图书馆 CIP 数据核字(2006)第 018472 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：010-62776969
组稿编辑：冯志强
文稿编辑：林晴佳
印 刷 者：北京市清华园胶印厂
装 订 者：三河市新茂装订有限公司
发 行 者：新华书店总店北京发行所
开　　本：185×260　印张：22.25　字数：550 千字
版　　次：2006 年 5 月第 1 版　2006 年 5 月第1 次印刷
书　　号：ISBN 7-302-12651-8/TP·8088
印　　数：1～3000
定　　价：43.00 元

前　言

如今计算机系统的现实情况是，虽然人们已经尽了最大的努力，但是，滥用的计算机用户，即滥用者，正在变得日益盛行。淘气的孩子想看看他们能够把所学的 IT（信息技术）知识应用到什么程度。公司的窃贼和破坏者通过计算机空间（cyberspace）实施对抗竞争者的邪恶活动。政府的间谍收集有关机密的军事信息和社会秘密。但是，所有滥用者的头脑中都有一个相同的目的——为其私用而暗中破坏 IT 系统。

信息安全是 IT 中发展最快的一个部分。为了应对计算机空间中日益增长的威胁，公司、组织和政府机构组织了越来越多的力量对付滥用者，保护高度机密的数据。这些安全专家通过部署阻止恶作剧所需的防御措施提供富有价值的服务，检测正在发生的攻击，并适当地进行响应，以确保高度机密的数据永远不会被窥探到。

在本书中，你将了解安全专家如何拟定保护数据，并在威胁发生时如何制订所需要的全面安全计划。你将了解各种 IT 安全威胁，以及对付这些威胁所需的全面信息安全计划。除了执行信息安全计划所需的管理过程以外，你还将了解暗中破坏网络技术的各种方法，它们允许滥用者在数据传输过程中盗窃数据。你还将了解 UNIX 和 Windows 系统，以及为了确保所有数据的安全性，如何保护这两种系统。

目标读者

本书不仅描述了现今 IT 环境中存在的各种威胁，而且向你展示了如何通过开发必要的安全策略和过程、安全的网络和系统，以及防御措施的预先测试，使系统抵御这些威胁。为了成功地完成本书中基于任务的学习，你必须具有 UNIX 和 Windows 计算机系统的应用知识，并且必须对 Internet 有基本的了解。至于以前是否有信息安全方面的经验则不做要求。纵览本书，重点不仅放在技能的培养上，而且放在全面信息安全计划中非常重要的概念上。

本书针对两方面的读者。一方面，本书是为帮助训练有素的 IT 专业人员通过 ProsoftTraining 的 CIW（认证的 Internet Web 管理员）安全专家考试而设计的。另一方面，Course Technology 公司出版针对学术环境的图书——针对学习信息技术的个人。对于这些人来说，IT 概念解释得比较详细。虽然 IT 专业人员对其中的一些概念比较熟悉，但是这些概念中与安全有关的方面将提供许多新的见解。

学习方法

为了便于学习，本书结合帮助你理解和应用信息安全概念的示例来介绍内容和理论。每一章都包括与这一章以及这一章小结有关的 Internet 上额外资源的参考资料、CIW 安全专家考试预习题、突出和巩固所介绍的主要概念的复习题。

实习项目是一些定向活动，其目的在于让你练习和巩固在本章学习的技术和技能，它们建立在你在前面章节中学习的技术和技能的基础上。通过提供在新情况下应用所学知识的额外方法，这些项目将增强你的学习经验。在某些章中，所有实习项目都相互没有联系。有时，它们以同一章中前面的实习项目为基础，但是这样的情况始终会加以标注。

在每一章的结尾都有案例项目，它们允许你使用在本章学习的技能解决现实问题。另外还欢迎你查看 Web 站点，寻找你在本章中学习的概念和方法的示例。

本书概述

本书中的示例、步骤、项目和案例将帮助你达到下列目标：

- 定义基本的安全概念
- 开始评估安全风险
- 概述安全策略
- 查找信息安全资源
- 回顾安全教育计划的基本组件
- 了解和矫正软件漏洞
- 了解安全问题管理的需要
- 响应安全事件
- 识别对公司 IT 环境的主要攻击途径
- 学习加密技术的基础知识
- 了解网络通信的基础知识
- 了解 TCP、UDP 和 IP 协议以及它们的弱点
- 识别 TCP/IP 协议套件中的其他协议以及它们的弱点
- 了解无线网络的威胁
- 了解入侵检测的好处和问题
- 探究可用于 UNIX 和 Windows 系统的系统安全控制
- 学习各种信息安全标准
- 学习安全测试技术

第 1 章将介绍基本的安全概念以及信息安全计划的基础——安全策略。第 2 章将介绍必须伴随安全策略的安全过程。对安全教育、问题、风险、咨询和事件的管理构成了全面信息安全计划的重要部分。第 3 章介绍当今信息的各种 IT 安全威胁。第 4 章介绍各种加密

此为试读，需要完整PDF请访问：www.ertongbook.com

技术以及每种技术的安全问题。第 5 章将介绍基本的网络技术以及将数据从一个计算机系统传输到另一个计算机系统时有关的安全问题。第 6 章深入介绍通过网络传输数据所需的内在技术的细节，以及每种技术固有的弱点。第 7 章介绍入侵检测。本章将描述各种帮助检测遍历网络的恶意活动的技术，或者在计算机系统上实施各种技术。第 8 章将介绍用于保护计算机系统本身的各种方法和技术。第 9 章以第 8 章的概念为基础，具体解决有关 UNIX 系统的安全问题。为了得到完整的蓝图，第 10 章突出介绍了有关 Windows 系统的安全问题。第 11 章介绍了大量信息安全标准以及审计 IT 环境安全性的需要。最后，第 12 章介绍了如何使用各种技术模拟攻击者，从而探索你自己识别弱点的安全防御措施。

为了增强学习经验，每一章都包括下列内容。

- **本章学习目标**：每一章的开始都列出了本章要掌握的重要概念。这个列表可以让你快速参看该章的内容。它还是一个有用的学习工具。
- **Elway 商业服务公司**：每一章都包含大量与一个虚构的名称为 EBS(Elway 商业服务公司)有关的轶事。这些故事的目的是将大部分基本的信息安全资料与现实世界的场景和商业需要联系起来。
- **提示**：每一章都包含大量提示，它们提供了与所讨论概念有关的实际建议和得到证明的策略。提示还提供了解决你在学习该章时可能遇到的问题的建议。
- **本章小结**：每一章的后面都对概念进行了总结。这些总结为扼要重述和重新查看每一章涉及的概念提供了一种有益的方法。
- **复习题**：章尾评估部分开始于一组大约为 15 个的复习题，它们将巩固每章中介绍的主要概念。这些问题将确保你已经掌握了概念，并且理解所介绍的信息。
- **考试复习题**：这些问题是为模拟 CIW 安全专家考试中的问题而设计的。希望通过这个考试的个人可以使用本书中的 120 个问题对考试进行准备。
- **实习项目**：除了概念性解释以及逐步展开的章节以外，每一章都提供了与每个主要主题有关的实习项目。设计它们的目的是让你对本章中介绍的概念获得实际的经验。有些实习项目包含详细的指导，而另一些实习项目则要求你在指导较少的情况下应用本章介绍的概念。
- **案例项目**：每一章的最后都介绍了几个案例。这些案例有助于你将本章学到的知识应用到现实中。它们让你有机会独立地综合与评价信息，检查潜在的解决方案以及提出建议，就像你身处实际的商业环境中那样。

致谢

首先，我想感谢我的妻子 Andrea 和儿子 Nathan，感谢他们对我的不断鼓励以及完成本书的大力支持。我还想感谢 IBM 管理安全服务机构的 Michael Walter，感谢他对本书技术资料方面所提供的大量帮助和建议。此外，如果没有 Course Technology 公司的朋友，本书就不会面世。我想特别感谢 Betsey Henkels、Tricia Boyle 和 BillLarkin 付出的所有辛勤劳动，以及让我保持正确方向所表现出来的毅力。

此外，我想感谢下列评论人员为我所付出的时间和他们的专业技术：CertificationCorner. com 的 Jeff Durham、Mercury 技术解决方案公司的 Emmett Dulaney、Davenport University——Kalamazoo 的 Michelle Hansen、Pennsylvania State University——Schuylkill Campus 的 Robert B. Lipton 博士、Gettysburg College 的 David Ozag、Peirce College 的 Denise Padavano、Frostburg State University 的 JoAnna Burley Shore、IBM 管理安全服务机构的 Michael A. Walter 以及 Susquehanna University 的 Craig L. Williams。

开始学习前请阅读下列内容

你可以使用你们学校实验室中的计算机或者你自己的计算机完成本书中的自学材料、实习项目和案例项目。使用你自己的计算机时，你需要有：

- **Red Hat Linux** 所有练习都是使用版本 7.3 和 8.0 设计和测试的。每个版本都能很好地适用于实习工作。
- **Windows Server 2003 标准版** 为了评估第 10 章中描述的各种安全技术和工具，学生应当访问这个 Windows 服务器操作系统。但是，由于这个操作系统价格昂贵，并且需要高级的计算机系统，所以学生也许不能访问它。在大多数情况下，具有 Windows 2000 的 PC 应当足以演示这一章讨论的大部分安全概念。
- **与 Internet 的连接** 许多信息安全资源都在 Web 上提供。此外，本书中提到的许多安全工具必须从 Web 站点获得。

访问我们的 World Wide Web 站点

特别为你设计的其他资料可能会在 World Wide Web 上提供。请登录 www. course. com，并定期搜索这个站点，以获取更多的细节。

目 录

第 1 部分 一般的安全要素

第 2 部分 网络安全

第 4 部分 安全保证

此为试读，需要完整PDF请访问：www.ertongbook.com

附 录

第 1 部分

一般的安全要素

信息安全领域经常与其最有趣的方面有关，如道德剽窃和计算机侦查。信息安全专家在他们的计算机前弯着腰搜索数字入侵者的画面看起来像在玩游戏。虽然这些焦点区域确实存在，但是最重要的一些工作是以良好的老式策略和过程的形式出现的。

本书的第 1 部分涉及下列帮助公司建立防御计算机攻击的坚固架构的主题：

- 信息安全策略
- 信息安全过程
- IT 安全威胁
- 加密技术

第1章 信息安全

本章学习目标

- 定义基本的安全概念
- 开始评估安全风险
- 概括描述安全策略
- 查找信息安全资源

Elway 商业服务公司

晚餐、电影和 Web 站点丑化

Noah Atwater 和 Paige David 是 Web 管理员。他们是 Elway 商业服务公司的 IT（信息技术）部的成员，他们负责 EBS 的普通 Web 环境。Noah 负责 Windows 服务器，Paige 负责 Linux 服务器和网络设备。他们对 IT 领域都较为陌生，但是他们都是能干的管理员。

一个星期五的晚上，在进行了需要 55 小时的服务器迁移以后，他们都正在休息。Noah 正在看电影；Paige 正在郊外野营。突然，Noah 收到了一个传呼。按照寻呼机上的号码回过电话以后，Noah 感到有点意外，因为他正在和 EBS 的首席信息官 Jeff Mobley 通话。这位 CIO 的声音听起来惊恐不安，他说道："EBS 的主 Web 页面已经被一个上面写有'SM1L3Y OWNZ U!'的大笑脸替换。"这时，Noah 也惊呆了，因为他知道，EBS 的 Web 环境保存着大量财务工具、宝贵的客户数据和 EBS 的专用数据。在打完电话后，Noah 向他的妻子表示道歉，然后离开电影院，赶快回去工作。IT 人员以前几乎没有担心过安全性。由于 EBS 客户和工作人员持续不断的技术需求，两个 IT 部门勉强能够维持公司台式机、服务器、网络和应用程序的顺利运行。IT 人员没有设置阻止、检测和矫正可能攻击的过程和解决方案。面对可能出现的安全事件，Noah 进入了一个陌生的 IT 领域——信息安全。

近些年来，安全已经成为生活中方方面面需要优先考虑的问题。在个人层面上，人们对可疑活动更加了解，并且更加愿意采取措施保护自己。在社会层面上，政府正在将大量资金投入警察、军事和情报组织，以阻止有组织的安全威胁。在企业层面上，公司开始理解更大

范围的安全风险以及保护关键的公司和客户数据所需要的费用。不论好坏，老百姓、政府和企业正在采取更有效的措施来保护重要的资产。

在IT(信息技术)界中，对安全性的这种日益关注导致了保护关键数据的人员、策略、过程、服务和解决方案的爆炸性增长。IT安全更合适的叫法是信息安全，它并不是一个新领域或新概念；这个领域一直伴随着计算机。但是，信息安全正在作为一个关键的IT功能而受到越来越多的关注。部署信息安全专家、公司安全官员和各种安全技术的公司比以前任何时候都多——所有这些措施都是为了确保现在的机密业务数据不会被有意或无意地泄露。

数据保护在任何地方的重要性都没有在Web环境中大。利用Internet的能力，大多数公司都有了Web站点，数以百万计的计算机用户可以访问这些Web站点，查看公司信息，与专家进行交流，以及购买产品。利用Internet的能力，大多数公司还有了可以由Web破坏者、自动病毒程序和窃贼访问的Web站点。Internet世界的这种两面性需要采取严格的安全和保密措施，以确保正确地保护所有信息。

术语"信息安全"经常引来安全问题更有名的方面，如道德剽窃、战争拨号或入侵检测。实际上，信息安全是构成保护数据的耐用墙的决策、策略和过程的广泛结构基础。本章将介绍信息安全的基本构件。

1.1 基本的安全概念

为什么在保护信息上花费时间、资源和资金是非常重要的呢？在大多数情况下，信息代表比公司产品和服务更为宝贵的资产。例如，如果快餐集团公司的烹饪设备或食物被盗，那么它通常可以弥补其损失。但是，如果它的招牌配方或被保护的烹饪过程被盗，那么这个快餐连锁店很可能就会停业。就此而言，任何公司都不能忽视保护信息的重要性。

开始时，Web管理员和他们IT同事必须评估其公司的总体安全状况。当前受到保护的资产是什么？正在如何保护它们？这些安全措施花费了多少钱？在检查总体安全状况时，必须解决所有这些问题以及其他的问题。

1.1.1 CIA三元组

如图1-1所示，有效的安全措施应当达到包含在CIA三元组——机密性、完整性和可用性——中的目标。下面将解释CIA三元组，并定义公司的全面安全方法的范围和目标。

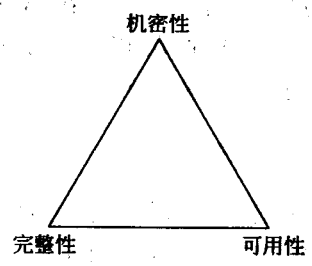

图1-1 包括信息安全的3个传统焦点的CIA三元组

1. 机密性

基本上，数据的机密性确保只允许授权的个人或组织进行访问。总的来说，保护机密性的安全措施易于向管理层进行解释。毕竟，没有人希望把重要的公司信息泄露给竞争对手或其他未经授权的个人。大部分公司已经做到了使公司员工以外的其他人不能访问专用信息。

滥用者是滥用计算机系统或者他们自己对系统的权限的计算机用户。由于滥用者可以在公司内部，所以对于IT人员来说，重要的是采取额外的措施，以确保所有员工一般不能得到某些信息（如特定员工的工资信息只能由他的经理使用）。

但是，数据的机密性经常是安全保护的惟一焦点。CIA三元组的重要性在于说明了机密性仅仅是安全体系的一部分，因此，它不能成为建立安全环境的惟一目标。

2. 完整性

数据完整性是指确保能够跟踪和正确控制数据修改的保护机制。就安全性而言，完整性的概念马上让人想到了防止滥用者操纵机密数据。但是，加强数据完整性还涉及到确保在不进行不必要修改的情况下传输数据的过程或技术机制——无论传输是从人到系统，从系统到系统，还是从系统到人。例如，数据库应用程序将执行数据完整性检验，以确保终端用户不将错误数据输入一个数据库。

3. 可用性

可用性是指在需要时可以使用IT资源的概念。总的来说，大部分IT组织都密切关注系统和网络可用性。毕竟，IT部门的主要任务就是确保网络基础设施和计算机系统可以在需要时和需要的地方供用户使用。

但是，大部分IT组织忽视了可以影响可用性的安全问题。例如，如果滥用者利用很多请求淹没了Web站点，从而实际阻止了合法用户以后怎么办？如今已臭名昭著的1999年的DDoS（分布式拒绝服务攻击）涉及几十个独立的系统，它们通过利用无用的通信淹没目标，从而使合法用户无法使用目标Web站点。由于可用性可以直接转化为货币值，所以应当利用安全策略和过程对它进行解决。

1.1.2　PPP三元组

但是，在评估一个组织的总体安全状况时，只关注机密性、完整性和可用性是不够的。另外还必须处理物理安全、隐私和市场感知。虽然它们不直接是传统CIA三元组的组成部分，但是这3个方面也是在处理公司的安全需要时必须建立的关键目标，特别是在Web领域。如图1-2所示，这些目标将在PPP三元组（物理安全、隐私和市场感知）中被捕捉。

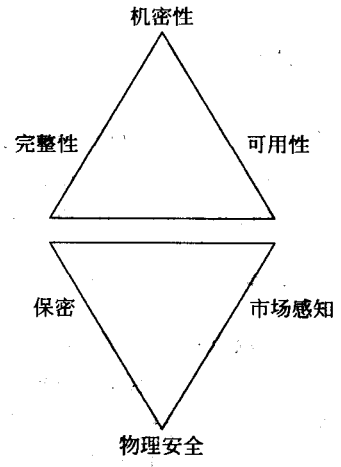

图1-2　处理信息安全问题的PPP三元组

1. 物理安全

物理安全包括对公司的所有重要的有形资产（人员、设备和设施）的保护。重要的是，每个公司不仅要保护它的数据，而且要保护支持这些数据的人员、基础设施和系统。这意味着要实现达到下列目标的措施：

- 防止个人进入禁区
- 防止盗窃
- 为员工开发安全计划和规程

在保护公司的重要资源时，需要使用这些措施以及大量其他的措施。

2. 隐私

对安全策略的传统讨论经常忽视公司员工、供应商和外部客户的隐私权。在匆忙防止数据被盗或被损坏时，组织经常践踏个人的权限。例如，客户可能不想让公司将他们的名字和地址用于销售目的，客户肯定不想让他们的财务信息透露给未知的组织。全面的安全策略应当考虑到员工、客户和商业伙伴的隐私。

3. 市场感知

在连接日益增强的信息世界中，新闻将快速扩散好事和坏事。由于 Web 的速度，公司的胜利可以使公司迅速成名。但是，同样的速度也会使公司因失败而很快声名狼藉。公司显然想避免这种消极的传播——特别是那些需要个人和其他公司信任的公司。例如，如果一个信用卡公司的 Web 站点受到攻击，它的客户在继续使用这个站点存储个人信息和财务信息时如何能感到安全呢？管理市场感知对于具有 Web 站点的公司是非常重要的，正是这种感知应当作为宝贵的资产看待。

1.2 评估风险

CIA 和 PPP 三元组概述了全面安全计划的主要目标。如果一个公司没有有效地达到这些目标，它就应当拟定一个详尽的安全策略。安全策略是一种文档，它反映构成组织所采取的每个措施的基础的全面安全概念、标准和过程。最起码，一个组织的安全策略应当包括下列内容：

- 保护人员、设备、设施和计算机资产的物理安全
- 确保只有授权人员可以访问必要系统和网络设备的用户 ID 和权限管理
- 保护网络设备和传输中的数据的网络安全
- 部署必要的防御措施以保护计算机系统免遭破坏的系统安全
- 特定计算机环境所需要的授权安全工具和测试
- 定期检查安全遵守的审计规程

安全策略中需要什么呢？这是信息安全专家或管理人员必须面对的最困难的问题之一。比较容易的答案是对企业有意义的任何事物。比较严谨和比较现实的答案是安全策略有各种各样的输入，如：

- 地方法律、规章和商业合同
- 内部的业务目标、原则和指导原则
- 通过安全评估认为必要的安全措施

前两个输入可能最容易识别和评估。第 3 个输入需要进行分析，以对照已觉察威胁的成本和可能性确定实现特定安全措施的成本。这种比较称为风险评估。

此为试读，需要完整PDF请访问：www.ertongbook.com