Web安全与电子商务（影印版）

2nd Edition

Expanded & Updated

Web Security, Privacy & Commerce

T U
TSINGHUA UNIVERSITY

Simson Garfinkel
with Gene Spafford 著

O'REILLY®

清华大学出版社

第二版

Web 安全与电子商务（影印版）

Web Security, Privacy, and Commerce

江苏工业学院图书馆
藏书章

Simson Garfinkel

with Gene Spafford

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Paris • Sebastopol • Taipei • Tokyo

O'Reilly & Associates, Inc. 授权清华大学出版社出版

清华大学出版社

图书在版编目（CIP）数据

Web安全与电子商务（第二版）：/（美）加芬克尔（Garfinkel, S.），（美）斯帕福德（Spafford, G.）著 — 影印版. — 北京：清华大学出版社，2002.11

书名原文：Web Security, Privacy, and Commerce, Second Edition

ISBN 7-302-05951-9

Ⅰ.W… Ⅱ.①加… ②斯… Ⅲ.①万维网－安全技术－英文 ②电子商务－英文 Ⅳ.①TP393.4 ②F713.36

中国版本图书馆CIP数据核字（2002）第077178号

北京市版权局著作权合同登记
图字：01-2002-4630号

©2002 by O'Reilly & Associates, Inc.

Reprint of the English Edition, jointly published by O'Reilly & Associates, Inc. and TsingHua University Press, 2002. Authorized reprint of the original English edition, 2002 O'Reilly & Associates, Inc., the owner of all rights to publish and sell the same.

All rights reserved including the rights of reproduction in whole or in part in any form.

英文原版由O'Reilly & Associates, Inc. 出版2002。

英文影印版由清华大学出版社出版2002。此影印版的出版和销售得到出版权和销售权的所有者 —— O'Reilly & Associates, Inc. 的许可。

版权所有，未得书面许可，本书的任何部分和全部不得以任何形式重制。

本书封面贴有清华大学出版社激光防伪标签，无标签者不得销售。

书　　名/	Web安全与电子商务（第二版）（影印版）
书　　号/	ISBN 7-302-05951-9/TP·3540
责任编辑/	冯志强
封面设计/	Edie Freedman，张健
出版发行/	清华大学出版社（www.tup.tsinghua.edu.cn）
地　　址/	北京清华大学学研大厦（邮政编码100084）
经　　销/	各地新华书店
印　　刷/	北京艺辉印刷有限公司
开　　本/	787毫米×980毫米　16开本　49.25印张
版　　次/	2002年11月第一版　2002年11月第一次印刷
印　　数/	0001-1500册
定　　价/	119.00元（册）

O'Reilly & Associates 公司介绍

O'Reilly & Associates 公司是世界上在 UNIX、X、Internet 和其他开放系统图书领域具有领导地位的出版公司，同时是联机出版的先锋。

从最畅销的*The Whole Internet User's Guide & Catalog*(被纽约公共图书馆评为20世纪最重要的50本书之一)到GNN(最早的Internet门户和商业网站),再到WebSite(第一个桌面 PC 的 Web 服务器软件)，O'Reilly & Associates 一直处于 Internet 发展的最前沿。

许多书店的反馈表明，O'Reilly & Associates 是最稳定的计算机图书出版商 —— 每一本书都一版再版。与大多数计算机图书出版商相比，O'Reilly & Associates 公司具有深厚的计算机专业背景，这使得O'Reilly & Associates形成了一个非常不同于其他出版商的出版方针。O'Reilly & Associates 所有的编辑人员以前都是程序员，或者是顶尖级的技术专家。O'Reilly & Associates 还有许多固定的作者群体 —— 他们本身是相关领域的技术专家、咨询专家，而现在编写著作，O'Reilly & Associates 依靠他们及时地推出图书。因为O'Reilly & Associates紧密地与计算机业界联系着，所以O'Reilly & Associates 知道市场上真正需要什么图书。

出版说明

计算机网络与通信技术的成熟和广泛应用，以及Internet与Web的迅速发展，为人类的工业生产、商业活动和日常生活都带来了巨大的影响。网络与通信技术在我国的很多领域也已经广泛应用，并且取得了巨大的效益。然而，该领域的技术创新的速度之快也是有目共睹的。为了帮助国内技术人员和网络管理人员在第一时间掌握国外最新的技术，清华大学出版社引进了美国O'Reilly & Associates公司的一批在计算机网络理论和应用方面代表前沿技术领域的著作，以飨读者。本套丛书采用影印版的形式，力求与国外图书“同步”出版，“原汁原味”地展现给读者各种权威技术理论和技术术语，适合于相关行业的高级技术人员、科研机构研究人员和高校教师阅读。

首批图书包括以下几种:

- 《Web安全与电子商务》
- 《无线Java入门》
- 《Web缓存》
- 《BEEP权威指南》
- 《802.11无线网络权威指南》
- 《大规模局域网设计》
- 《IP路由》
- 《DNS与BIND》

此为试读，需要完整PDF请访问: www.ertongbook.com

Preface

The World Wide Web has changed our world. More than half the people in the United States now use the Web on a regular basis. We use it to read today's news, to check tomorrow's weather, and to search for events that have happened in the distant past. And increasingly, the Web is the focus of the 21st century economy. Whether it's the purchase of a $50 radio or the consummation of a $5 million business-to-business transaction, the Web is where the action is.

But the Web is not without its risks. Hand-in-hand with stories of the Internet's gold rush are constant reminders that the 21st century Internet has all the safety and security of the U.S. Wild West of the 1860s. Consider:

- In February 2000, web sites belonging to Yahoo, Buy.com, Amazon.com, CNN, E*Trade, and others were shut down for hours, the result of a massive coordinated attack launched simultaneously from thousands of different computers. Although most of the sites were back up within hours, the attacks were quite costly. Yahoo, for instance, claimed to have lost more than a million dollars per minute in advertising revenue during the attack.
- In December 1999, an attacker identifying himself as a 19-year-old Russian named "Maxim" broke into the CDUniverse web store operated by eUniverse Inc. and copied more than 300,000 credit card numbers. Maxim then sent a fax to eUniverse threatening to post the stolen credit cards on the Internet if the store didn't pay him $100,000.* On December 25, when the company refused to bow to the blackmail attack, Maxim posted more than 25,000 of the numbers on the hacker web site "Maxus Credit Card Pipeline."† This led to instances of credit card fraud and abuse. Many of those credit card numbers were then canceled by the issuing banks, causing inconvenience to the legitimate holders of

[*] *http://www.wired.com/news/technology/0,1282,33539,00.html*

[†] *http://www.cnn.com/2000/TECH/computing/01/10/credit.card.crack.2/*

those cards.[*] Similar break-ins and credit card thefts that year affected RealNames,[†] CreditCards.com, EggHead.Com, and many other corporations.

- In October 2000, a student at Harvard University discovered that he could view the names, addresses, and phone numbers of thousands of Buy.com's customers by simply modifying a URL that the company sent to customers seeking to return merchandise. "This blatant disregard for security seems pretty inexcusable," the student, Ben Edelman, told *Wired News*.[‡]
- Attacks on the Internet aren't only limited to e-commerce sites. A significant number of high-profile web sites have had their pages rewritten during attacks. Those attacked include the U.S. Department of Justice, the U.S. Central Intelligence Agency (see Figure P-1), the U.S. Air Force, UNICEF, and the *New York Times*. An archive of more than 325 hacked home pages is online at *http://www.antionline.com/archives/pages/*.

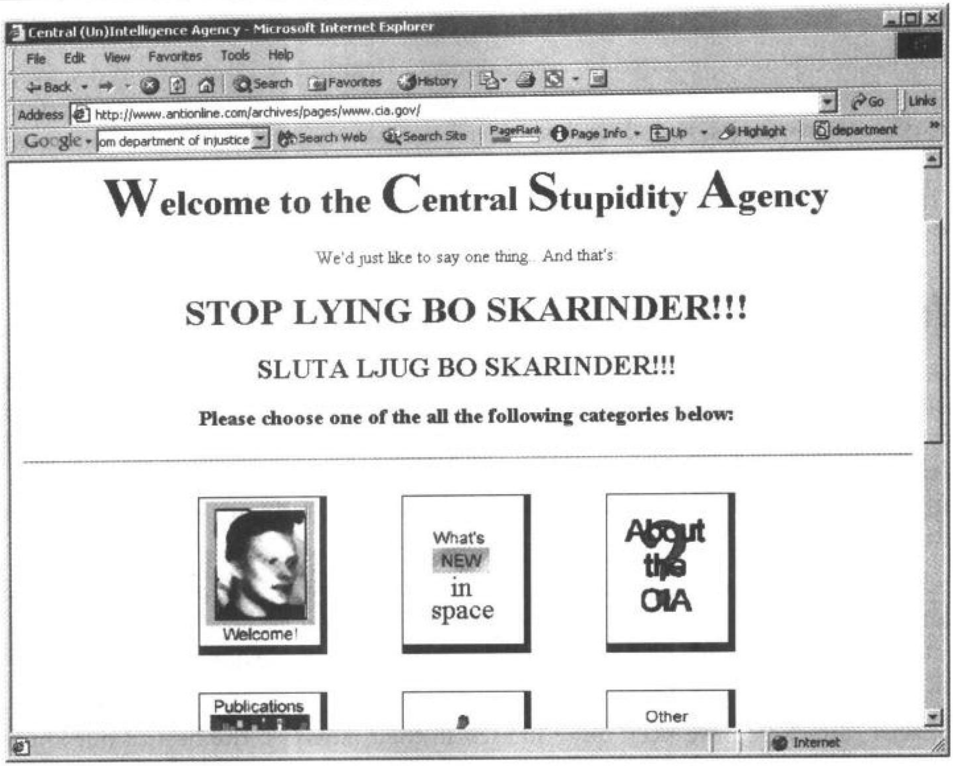
Attacks on web servers are not the only risks we face on the electronic frontier:

- On August 25, 2000, a fraudulent press release was uploaded to the computer of Internet Wire, an Internet news agency. The press release claimed to be from Emulex Corporation, a maker of computer hardware, and claimed that the company's chief executive officer had resigned and that the company would have to adjust its most recent quarterly earnings to reflect a loss, instead of a profit. The next morning, Emulex's share price plunged by more than 60%: within a few hours, the multi-billion-dollar company had lost roughly half its value. A few days later, authorities announced the Emulex caper had been pulled off by a single person—an ex-employee of the online news service, who had made a profit of nearly $250,000 by selling Emulex stock short before the release was issued.
- Within hours of its release on May 4, 2000, a fast-moving computer worm called the "Love Bug" touched tens of millions of computers throughout the Internet and caused untold damage. Written in Microsoft Visual Basic Scripting Language (VBS), the worm was spread by people running the Microsoft Outlook email program. When executed, the worm would mail copies of itself to every email address in the victim's address book, then destroy every MP3 and JPEG file that it could locate on the victim's machine.
- A growing number of computer "worms" scan the victim's hard disk for Microsoft Word and Excel files. These files are infected and then sent by email to recipients in the victim's address book. Not only are infections potentially started more often, but confidential documents may be sent to inappropriate recipients.

[*] Including one of the authors of this book.

[†] *http://www.thestandard.com/article/display/0,1151,9743,00.html*

[‡] *http://www.wired.com/news/technology/0,1282,39438,00.html*



Central (Un)Intelligence Agency - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Go Links
Google Search Web Search Site PageRank Page Info Up Highlight department
Welcome!
What's NEW in space
About the CIA
Publications
Other
Internet

Address http://www.antionline.com/archives/pages/www.cia.gov/

Google om department of injustice

Welcome to the Central Stupidity Agency

We'd just like to say one thing... And that's:

STOP LYING BO SKARINDER!!!

SLUTA LJUG BO SKARINDER!!!

Please choose one of the all the following categories below:

Figure P-1. On September 18, 1996, a group of Swedish hackers broke into the Central Intelligence Agency's web site (http://www.odci.gov/cia) and altered the home page, proclaiming that the Agency was the Central Stupidity Agency.

The Web doesn't merely represent a threat for corporations. There are cyberstalkers, who use the Web to learn personal information and harass their victims. There are pedophiles, who start relationships with children and lure them away from home. Even users of apparently anonymous chat services aren't safe: In February 1999, the defense contracting giant Raytheon filed suit against 21 unnamed individuals who made disparaging comments about the company on one of Yahoo's online chat boards. Raytheon insisted that the 21 were current employees who had leaked confidential information; the company demanded that the Yahoo company reveal the identities behind the email addresses. Yahoo complied in May 1999. A few days later, Raytheon announced that four of the identified employees had "resigned," and the lawsuit was dropped.*

* *http://www.netlitigation.com/netlitigation/cases/raytheon.html*

Even using apparently "anonymous" services on the Web may jeopardize your privacy and personal information. A study of the 21 most visited health-related web sites on the Internet (prepared for the California HealthCare Foundation) discovered that personal information provided at many of the sites was being inadvertently leaked to third-parties, including advertisers. In many cases, these data transfers were in violation of the web sites' own stated privacy policies.* A similar information leak, which sent the results of home mortgage calculations to the Internet advertising firm DoubleClick, was discovered on Intuit's Quicken.com personal finance site.†

Web Security: Is Our Luck Running Out?

We have been incredibly lucky. Despite the numerous businesses, government organizations, and individuals that have found danger lurking on the Web, there have been remarkably few large-scale electronic attacks on the systems that make up the Web. Despite the fact that credit card numbers are not properly protected, there is surprisingly little traffic in stolen financial information. We are vulnerable, yet the sky hasn't fallen.

Today most Net-based attackers seem to be satisfied with the publicity that their assaults generate. Although there have been online criminal heists, there are so few that they still make the news. Security is weak, but the vast majority of Internet users still play by the rules.

Likewise, attackers have been quite limited in their aims. To the best of our knowledge, there have been no large-scale attempts to permanently crash the Internet or to undermine fundamental trust in society, the Internet, or specific corporations. The *New York Times* had its web site hacked, but the attackers didn't plant false stories into the newspaper's web pages. Millions of credit card numbers have been stolen by hackers, but there are few cases in which these numbers have been directly used to commit large-scale credit fraud.

Indeed, despite the public humiliation resulting from the well-publicized Internet break-ins, none of the victimized organizations have suffered lasting harm. The Central Intelligence Agency, the U.S. Air Force, and UNICEF all still operate web servers, even though all of these organizations have suffered embarrassing break-ins. Even better, none of these organizations actually lost sensitive information as a result of the break-ins, because that information was stored on different machines. A few days after each organization's incident, their servers were up and running again—this time, we hope, with the security problems fixed.

* *http://admin.chcf.org/documents/ehealth/privacywebreport.pdf*

† *http://news.cnet.com/news/0-1007-200-1562341.html*

The same can be said of the dozens of security holes and design flaws that have been reported with Microsoft's Internet Explorer and Netscape Navigator. Despite attacks that could have allowed the operator of some "rogue web site" to read any file from some victim's computer—or even worse, to execute arbitrary code on that machine—surprisingly few scams or attacks make use of these failings.[*] This is true despite the fact that the majority of Internet users do not download the security patches and fixes that vendors make available.

Beyond the Point of No Return

In the world of security it is often difficult to tell the difference between actual threats and hype. There were more than 200 years of commerce in North America before Allan Pinkerton started his detective and security agency in 1850,[†] and another nine years more before Perry Brink started his armored car service.[‡] It took a while for the crooks to realize that there was a lot of unprotected money floating around.

The same is true on the Internet, but with each passing year we are witnessing larger and larger crimes. It used to be that hackers simply defaced web sites; then they started stealing credit card numbers and demanding ransom; in December 2000, a report by MSNBC detailed how thousands of consumers had been bilked of between $5 and $25 on their credit cards by a group of Russian telecommunications and Internet companies; the charges were small so most of the victims didn't recognize the fraud and didn't bother to report the theft.[§]

Many security analysts believe things are going to get much worse. In March 2001, the market research firm Gartner predicted there would be "at least one incident of economic mass victimization of thousands of Internet users . . . by the end of 2002:"[**]

> "Converging technology trends are creating economies of scale that enable a new class of cybercrimes aimed at mass victimization," explain[ed] Richard Hunter, Gartner Research Fellow. More importantly, Hunter add[ed], global law enforcement agencies are poorly positioned to combat these trends, leaving thousands of consumers vulnerable to online theft. "Using mundane, readily available technologies that have already been deployed by both legitimate and illegitimate businesses, cybercriminals can now surreptitiously steal millions of dollars, a few dollars at a time, from millions of individuals simultaneously. Moreover, they are very likely to get away with the crime."

[*] More accurately, there have been very few reported incidents. It is possible that there have been some widespread incidents, but the victims have either been unaware of them, or unwilling to report them.

[†] *http://www.pinkertons.com/companyinfo/history/pinkerton/index.asp*

[‡] *http://www.brinksireland.com/history/history.htm*

[§] *http://www.zdnet.com/zdnn/stories/news/0,4586,2668427,00.html*

[**] *http://www.businesswire.com/webbox/bw.033001/210892234.htm*

Despite these obvious risks, our society and economy has likely passed a point of no return: having some presence on the World Wide Web now seems to have become a fundamental requirement for businesses, governments, and other organizations.

Building in Security

It's difficult for many Bostonians to get to the Massachusetts Registry of Motor Vehicles to renew their car registrations; it's easy to click into the RMV's web site, type a registration number and a credit card number, and have the registration automatically processed. And it's easier for the RMV as well: their web site is connected to the RMV computers, eliminating the need to have the information typed by RMV employees. That's why the Massachusetts RMV gives a $5 discount to registrations made over the Internet.

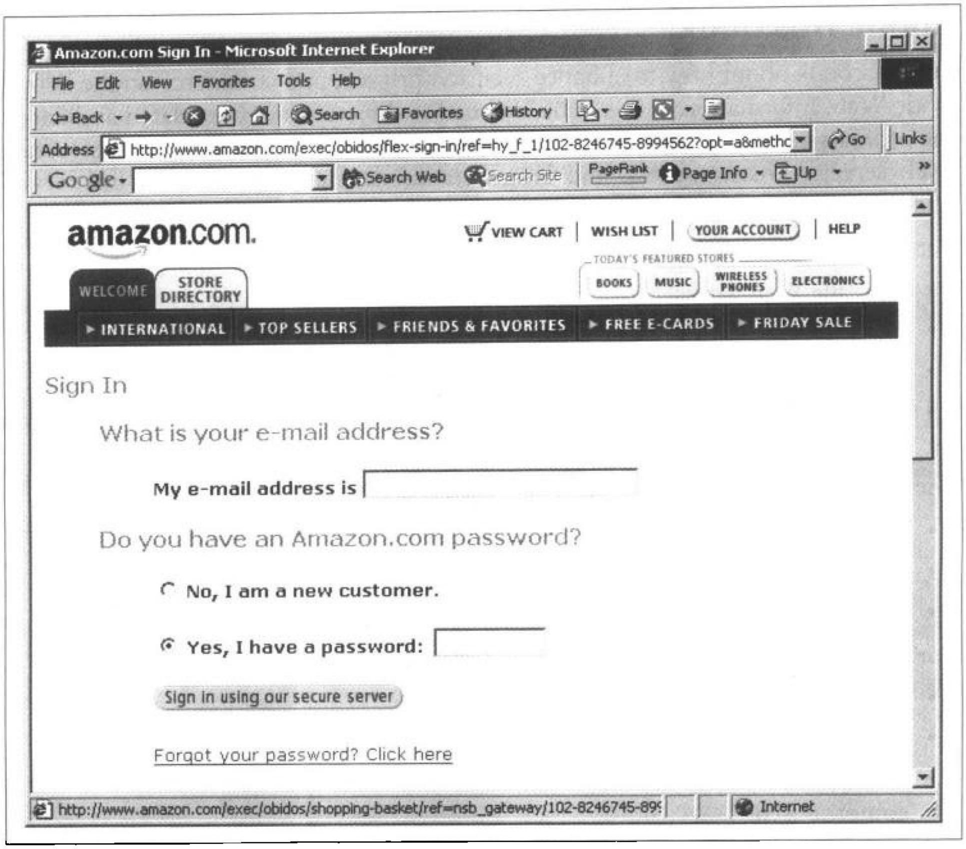
Likewise, we have found that the amount of money we spend on buying books has increased dramatically since Amazon.com and other online booksellers have opened their web sites for business. The reason is obvious: it's much easier for us to type the name of a book on our keyboards and have it delivered than it is for us to make a special trip to the nearest bookstore. Thus, we've been purchasing many more books on impulse—for example, after hearing an interview with an author or reading about the book in a magazine.

Are the web sites operated by the Massachusetts RMV and Amazon.com really *secure*? Answering this question depends both on your definition of the word "secure," and on a careful analysis of the computers involved in the entire renewal or purchasing process.

In the early days of the World Wide Web, the word "secure" was promoted by Netscape Communications to denote any web site that used Netscape's proprietary encryption protocols. Security was equated with encryption—an equation that's remained foremost in many people's minds. Indeed, as Figure P-2 clearly demonstrates, web sites such as Amazon.com haven't changed their language very much. Amazon.com invites people to "Sign in using our secure server," but is their server really "secure"? Amazon uses the word "secure" because the company's web server uses the SSL (Secure Sockets Layer) encryption protocol. But if you click the link that says "Forgot your password? Click here," Amazon will create a new password for your account and send it to your email address. Does this policy make Amazon's web site more secure or less?

Over the Web's brief history, we've learned that security is more than simply another word for cryptographic data protection. Today we know that to be protected, an organization needs to adopt an holistic approach to guarding both its computer systems and the data that those systems collect. Using encryption is clearly important, but it's equally important to verify the identity of a customer before showing that customer his purchase history and financial information. If you send out email, it's

此为试读，需要完整PDF请访问：www.ertongbook.com



Amazon.com Sign In - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://www.amazon.com/exec/obidos/flex-sign-in/ref=hy_f_1/102-8246745-8994562?opt=a&methc
Go Links
Google Search Web Search Site PageRank Page Info Up
amazon.com.
VIEW CART | WISH LIST | YOUR ACCOUNT | HELP
TODAY'S FEATURED STORES
BOOKS MUSIC WIRELESS PHONES ELECTRONICS
WELCOME STORE DIRECTORY
INTERNATIONAL TOP SELLERS FRIENDS & FAVORITES FREE E-CARDS FRIDAY SALE
http://www.amazon.com/exec/obidos/shopping-basket/ref=nsb_gateway/102-8246745-89
Internet

Sign In

What is your e-mail address?

My e-mail address is

Do you have an Amazon.com password?

○ No, I am a new customer.

● Yes, I have a password:

Sign in using our secure server

Forgot your password? Click here

Figure P-2. Amazon.com describes their server as "secure," but the practice of emailing forgotten passwords to customers is hardly a secure one.

important to make sure that the email doesn't contain viruses—but it is equally important to make sure that you are not sending the email to the wrong person, or sending it out against the recipient's wishes. It's important to make sure that credit card numbers are encrypted before they are sent over the Internet, but it's equally important to make sure that the numbers are kept secure *after* they are decrypted at the other end.

The World Wide Web has both promises and dangers. The promise is that the Web can dramatically lower costs to organizations for distributing information, products, and services. The danger is that the computers that make up the Web are vulnerable. These computers have been compromised in the past, and they will be compromised in the future. Even worse, as more commerce is conducted in the online world, as more value flows over the Internet, as more people use the network for more of their daily financial activities, the more inviting a target these computers all become.

About This Book

This is a book about how to enhance security, privacy, and commerce on the World Wide Web. Information in this book is aimed at three distinct but related audiences: the ordinary users of the Web, the individuals who operate the Web's infrastructure (web servers, hosts, routers, and long-distance data communications links), and finally, the people who publish information on the Web.

For users, this book explains:

- How the Web works
- The threats to your privacy and your computer that await you on the Web
- How you can protect yourself against these threats
- How encryption works, and why a web server that you access might demand that you use this technique

For people who are operating the Web's infrastructure, this book discusses:

- How to lessen the chances that your server will be compromised
- How you can use encryption to protect your data and your web site's visitors
- Selected legal issues

For web content providers, this book discusses:

- The risks and threats facing your data
- How to control access to information on your web server
- Procedures that you should institute so you can recover quickly if your server is compromised
- Security issues arising from the use of Java, JavaScript, ActiveX, and Netscape plug-ins

This book covers the fundamentals of web security, but it is not designed to be a primer on computer security, operating systems, or the World Wide Web. For that, we have many recommendations.

Some especially good O'Reilly books on security- and web-related topics include the following: Æleen Frisch's *Essential System Administration*, Chuck Musciano and Bill Kennedy's *HTML & XHTML: The Definitive Guide*, Shishir Gundavaram's *CGI Programming on the World Wide Web*, Elizabeth Zwicky, Simon Cooper, and Brent Chapman's *Building Internet Firewalls*, and finally our own book, *Practical Unix & Internet Security*.

We also have some recommendations for books from other publishers. For in-depth information on cryptography, we heartily recommend Bruce Schneier's excellent book *Applied Cryptography*. For detailed information on configuring the Apache web server, we recommend Lincoln Stein's *Web Security*. And for a general overview of security engineering and practices, we recommend Ross Anderson's *Security Engineering*.

These books and other helpful references are listed Appendix E.

Organization of This Book

This book is divided into five parts; it includes 27 chapters and 5 appendixes:

Part I, *Web Technology*, examines the underlying technology that makes up today's World Wide Web and the Internet in general.

Chapter 1, *The Web Security Landscape*, examines the basics of web security—the risks inherent in running a web server, in using the Web to distribute information or services, and finally, the risks of being a user on the Internet.

Chapter 2, *The Architecture of the World Wide Web*, is a detailed exploration of computers, communications links, and protocols that make up the Web. It provides a technical introduction to the systems that will be discussed throughout the rest of the book and that underlie web security concepts.

Chapter 3, *Cryptography Basics*, introduces the science and mathematics of cryptography, with a particular emphasis on public key encryption.

Chapter 4, *Cryptography and the Web*, specifically looks at the encryption algorithms that are used on the Web today.

Chapter 5, *Understanding SSL and TLS*, looks more closely at the Secure Sockets Layer (SSL) and the Transport Layer Security (TLS) system that are used by "secure" web servers.

Chapter 6, *Digital Identification I: Passwords, Biometrics, and Digital Signatures*, introduces the topic of authentication and gives an overview of several classes of authentication systems in use on the Internet.

Chapter 7, *Digital Identification II: Digital Certificates, CAs, and PKI*, focuses on the use of digital certificates for authentication and introduces certification authorities (CAs) and the public key infrastructure (PKI).

Part II, *Privacy and Security for Users*, looks at the concerns of people using the Web to access information—that is, anybody who runs a web browser.

Chapter 8, *The Web's War on Your Privacy*, discusses the technical means by which personal information can be compromised on the Web.

Chapter 9, *Privacy-Protecting Techniques*, explores techniques that you can follow to increase your privacy while using the Web.

Chapter 10, *Privacy-Protecting Technologies*, continues the discussion of privacy self-help, by exploring programs and services that can further enhance your privacy.

Chapter 11, *Backups and Antitheft*, shows you how to protect against data loss and theft of both data and equipment.

Chapter 12, *Mobile Code I: Plug-Ins, ActiveX, and Visual Basic*, explores how programs that travel over the Web can threaten your computer system and your personal information. This chapter focuses on the most dangerous programs that can be downloaded with email or through web pages.

Chapter 13, *Mobile Code II: Java, JavaScript, Flash, and Shockwave*, continues the discussion of mobile programs that can threaten computer users. This chapter focuses on the "safer" technologies that, it turns out, still have some security implications.

Part III, *Web Server Security*, is addressed to people and organizations that are operating servers attached to the Internet. The chapters in this part focus on the mechanics of web server operation. They are particularly relevant to corporations that operate their own web servers, administrators at Internet service providers (ISPs), and home users who run their own servers at the end of cable modems or DSL lines.

Chapter 14, *Physical Security for Servers*, addresses one of the most important but frequently overlooked topics—how to protect your computer's physical well-being.

Chapter 15, *Host Security for Servers*, explores security having to do with your computer's operating system.

Chapter 16, *Securing Web Applications*, discusses the added security issues that arise when running web servers that can execute programs or scripts.

Chapter 17, *Deploying SSL Server Certificates*, gives step-by-step instructions for enabling SSL on the Apache and Internet Information Services (IIS) web servers.

Chapter 18, *Securing Your Web Service*, broadens the security discussion to show how to defend your service against problems resulting from your ISP or the Internet's Domain Name Service (DNS).

Chapter 19, *Computer Crime*, explores the specific legal options available to you after your computer system has been broken into, as well as other legal issues of concern to administrators.

Part IV, *Security for Content Providers*, focuses on issues surrounding the content of the web server, rather than the mechanics of the web server's operation.

Chapter 20, *Controlling Access to Your Web Content*, looks at techniques for controlling information to "private" areas of your web server.

Chapter 21, *Client-Side Digital Certificates*, expands on the access control techniques described in Chapter 20 by discussing how you can use digital certificates for access control and secure messaging.

Chapter 22, *Code Signing and Microsoft's Authenticode*, shows how you can sign Windows binaries, including ActiveX controls and *.EXE* files, using Microsoft's Authenticode technology.

Chapter 23, *Pornography, Filtering Software, and Censorship*, discusses the politics and the technology of controlling pornography on the Internet.

Chapter 24, *Privacy Policies; Legislation, and P3P*, explores the concept of data protection and discusses legislative and self-regulatory techniques for controlling the use of personal information.

Chapter 25, *Digital Payments*, is a how-to guide for sending and receiving money over the Internet. For those interested in e-commerce history, this chapter also discusses a number of failed digital payment systems.

Chapter 26, *Intellectual Property and Actionable Content*, discusses trademarks, copyright, and patents—all legal structures that can be used to protect information.

Part V, *Appendixes*, is filled with lists and nitty-gritty technical information that is too detailed for the main body of this book.

Appendix A, *Lessons from Vineyard.NET*, is a first-person account of the first five years of operation of Vineyard.NET, the oldest, largest, and currently only ISP that offers service exclusively on Martha's Vineyard.

Appendix B, *The SSL/TLS Protocol*, contains more detailed information about the SSL and TLS protocols. This chapter won't give you enough information to write your own SSL or TLS implementation, but it will give you an understanding of what is happening on the wire.

Appendix C, *P3P: The Platform for Privacy Preferences Project*, is a detailed introduction to the P3P specification. This chapter, written by Lorrie Faith Cranor and included with permission, includes information on how to write your own P3P policy.

Appendix D, *The PICS Specification*, provides detailed information on the PICS specification. Although PICS appears largely dead today, an implementation is included in Microsoft's Internet Explorer, so PICS is still there for anybody who wants to use it.

Appendix E, *References*, lists books, articles, and web sites containing further helpful information about web security, privacy, and commerce.

What You Should Know

Web security is a complex topic that touches on many aspects of traditional computer security, computer architecture, system design, software engineering, Internet technology, mathematics, and the law. To keep the size of this book under control, we have focused on conveying information and techniques that are not readily found elsewhere.

To get the most out of this book, you should already be familiar with the operation and management of a networked computer. You should know how to connect your computer to the Internet; how to obtain, install, and maintain computer software; and how to perform routine system management tasks, such as backups. You should have a working knowledge of the World Wide Web, and know how to install and maintain your organization's web server.

That is not to say that this is a book written solely for "propeller-heads" and security geeks. Great effort has been made to make this book useful for people who have a working familiarity with computers and the Web, but who are not familiar with the nitty-gritty details of computer security. That's why we have included introductory chapters on such topics as cryptography and SSL.

Web Software Covered by This Book

A major difficulty in writing a book on web security is that the field moves incredibly quickly. Configuration information and screen shots that look up-to-date one month seem antiquated and obsolete a few months later. This is partially the result of the steady release of new software versions, and the integration of new features into commonly-used software. The difficulty in keeping current is complicated by the steady drumbeat of warnings from vendors and organizations such as SANS and CERT/CC, announcing a significant new security vulnerability every few days—often caused by the vendors' rush to deliver all those new features without carefully testing them for security flaws!

But in fact, the field of web security is not moving as fast as it may seem. Although new vulnerabilities have been created and discovered, the underlying concepts of web security have changed little since the first edition of this book was published in the spring of 1997. We have therefore refrained from updating all of our screenshots and code examples simply to match the latest revisions of Microsoft and Netscape's offerings. If a point is well made by a screenshot that featured an older version of a product, we have generally opted to leave the screenshot in place.

To avoid the planned obsolescence that seems to beset many computer books, this book concentrates on teaching concepts and principles, rather than specific sequences of commands and keystrokes.

In writing this book, we used a wide variety of software. Examples in this book are drawn primarily from two web servers:

Apache
: Apache is one of the most popular web servers currently in use. Apache runs on a wide variety of computers, including most versions of Unix and Windows NT. When combined with the *mod_ssl* encryption module, Apache can be the basis for creating an extremely sophisticated web publishing system. Apache is freely available in both source code and precompiled form; it is even preinstalled on many computer systems.

Microsoft Internet Information Server
: IIS is Microsoft's cryptographically enabled web server that is bundled with the Windows NT Server and Windows 2000 operating systems.

此为试读，需要完整PDF请访问：www.ertongbook.com