

SECOND EDITION

# Web Security, Privacy, and Commerce

*Simson Garfinkel*  
*with Gene Spafford*

O'REILLY

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

# Table of Contents

<b>Preface</b> .....	<b>.xi</b>
----------------------	------------

## **Part I. Web Technology**

<b>1. The Web Security Landscape</b> .....	<b>3</b>
The Web Security Problem	3
Risk Analysis and Best Practices	10
<b>2. The Architecture of the World Wide Web</b> .....	<b>13</b>
History and Terminology	13
A Packet's Tour of the Web	20
Who Owns the Internet?	33
<b>3. Cryptography Basics</b> .....	<b>46</b>
Understanding Cryptography	46
Symmetric Key Algorithms	53
Public Key Algorithms	65
Message Digest Functions	71
<b>4. Cryptography and the Web</b> .....	<b>78</b>
Cryptography and Web Security	78
Working Cryptographic Systems and Protocols	81
What Cryptography Can't Do	88
Legal Restrictions on Cryptography	90
<b>5. Understanding SSL and TLS</b> .....	<b>107</b>
What Is SSL?	107
SSL: The User's Point of View	115

<b>6. Digital Identification I: Passwords, Biometrics, and Digital Signatures</b>	<b>119</b>
Physical Identification	119
Using Public Keys for Identification	130
Real-World Public Key Examples	140
<b>7. Digital Identification II: Digital Certificates, CAs, and PKI. . . . .</b>	<b>153</b>
Understanding Digital Certificates with PGP	153
Certification Authorities: Third-Party Registrars	160
Public Key Infrastructure	174
Open Policy Issues	187

## Part II. Privacy and Security for Users

<b>8. The Web's War on Your Privacy. . . . .</b>	<b>203</b>
Understanding Privacy	204
User-Provided Information	207
Log Files	210
Understanding Cookies	216
Web Bugs	225
Conclusion	229
<b>9. Privacy-Protecting Techniques. . . . .</b>	<b>230</b>
Choosing a Good Service Provider	230
Picking a Great Password	231
Cleaning Up After Yourself	242
Avoiding Spam and Junk Email	252
Identity Theft	256
<b>10. Privacy-Protecting Technologies. . . . .</b>	<b>262</b>
Blocking Ads and Crushing Cookies	262
Anonymous Browsing	268
Secure Email	275
<b>•11. Backups and Antitheft. . . . .</b>	<b>284</b>
Using Backups to Protect Your Data	284
Preventing Theft	295
<b>12. Mobile Code I: Plug-Ins, ActiveX, and Visual Basic. . . . .</b>	<b>298</b>
When Good Browsers Go Bad	299
Helper Applications and Plug-ins	304

Microsoft's ActiveX	308
The Risks of Downloaded Code	318
Conclusion	326
<b>13. Mobile Code II: Java, JavaScript, Flash, and Shockwave . . . . .</b>	<b>327</b>
Java	327
JavaScript	346
Flash and Shockwave	358
Conclusion	359

## Part III. Web Server Security

<b>14. Physical Security for Servers. . . . .</b>	<b>363</b>
Planning for the Forgotten Threats	363
Protecting Computer Hardware	366
Protecting Your Data	381
Personnel	392
Story: A Failed Site Inspection	392
<b>15. Host Security for Servers. . . . .</b>	<b>396</b>
Current Host Security Problems	397
Securing the Host Computer	405
Minimizing Risk by Minimizing Services	411
Operating Securely	413
Secure Remote Access and Content Updating	423
Firewalls and the Web	431
Conclusion	433
<b>16. Securing Web Applications. . . . .</b>	<b>435</b>
A Legacy of Extensibility and Risk	435
Rules to Code By	443
Securely Using Fields, Hidden Fields, and Cookies	448
Rules for Programming Languages	454
Using PHP Securely	457
Writing Scripts That Run with Additional Privileges	467
Connecting to Databases	468
Conclusion	471

<b>17. Deploying SSL Server Certificates. . . . .</b>	<b>472</b>
Planning for Your SSL Server	472
Creating SSL Servers with FreeBSD	477
Installing an SSL Certificate on Microsoft IIS	501
Obtaining a Certificate from a Commercial CA	503
When Things Go Wrong	506
<b>18. Securing Your Web Service. . . . .</b>	<b>510</b>
Protecting Via Redundancy	510
Protecting Your DNS	514
Protecting Your Domain Registration	515
<b>19. Computer Crime. . . . .</b>	<b>517</b>
Your Legal Options After a Break-In	517
Criminal Hazards	523
Criminal Subject Matter	526

## Part IV. Security for Content Providers

<b>20. Controlling Access to Your Web Content = . . . . .</b>	<b>533</b>
Access Control Strategies	533
Controlling Access with Apache	538
Controlling Access with Microsoft IIS	545
<b>21. Client-Side Digital Certificates . . . . .</b>	<b>550</b>
Client Certificates	550
A Tour of the VeriSign Digital ID Center	553
<b>22. Code Signing and Microsoft's Authenticode. . . . .</b>	<b>560</b>
Why Code Signing?	560
Microsoft's Authenticode Technology	564
Obtaining a Software Publishing Certificate	577
Other Code Signing Methods	577
<b>23. Pornography, Filtering Software, and Censorship. . . . .</b>	<b>579</b>
Pornography Filtering	579
PICS	582
RSACi	589
Conclusion	591

<b>24. Privacy Policies, Legislation, and P3P. . . . .</b>	<b>592</b>
Policies That Protect Privacy and Privacy Policies	592
Children's Online Privacy Protection Act	601
P3P	606
Conclusion	609
<b>25. Digital Payments. . . . .</b>	<b>610</b>
Charga-Plates, Diners Club, and Credit Cards	610
Internet-Based Payment Systems	620
How to Evaluate a Credit Card Payment System	640
<b>26. Intellectual Property and Actionable Content . . . . .</b>	<b>642</b>
Copyright	642
Patents	645
Trademarks	646
Actionable Content	650

## Part V. Appendixes

<b>A. Lessons from Vineyard.NET. . . . .</b>	<b>655</b>
<b>B. The SSL/TLS Protocol. . . . .</b>	<b>688</b>
<b>C. P3P: The Platform for Privacy Preferences Project. . . . .</b>	<b>699</b>
<b>D. The PICS Specification. . . . .</b>	<b>708</b>
<b>E. References. . . . .</b>	<b>716</b>
<b>Index. . . . .</b>	<b>735</b>