Table of Contents

Preface .... *ix*

I. Introduction *1*

1. The Web Security Landscape *3*
Web Security in a Nutshell *3*
The Web Security Problem *9*
Credit Cards, Encryption, and the Web *14*
Firewalls: Part of the Solution *20*
Risk Management *24*

II. User Safety *25*

2. The Buggy Browser: Evolution of Risk *27*
Browser History *27*
Data-Driven Attacks *33*
Implementation Flaws: A Litany of Bugs *36*

3. Java and JavaScript *39*
Java *39*
JavaScript *54*
Denial-of-Service Attacks *56*
JavaScript-Enabled Spoofing Attacks *62*
Conclusion *66*

4. *Downloading Machine Code with ActiveX and Plug-Ins* *67*
When Good Browsers Go Bad *67*
Netscape Plug-Ins *69*
ActiveX and Authenticode *73*
The Risks of Downloaded Code *77*
Is Authenticode a Solution? *81*
Improving the Security of Downloaded Code *85*

5. *Privacy* *87*
Log Files *87*
Cookies *90*
Personally Identifiable Information *94*
Anonymizers *96*
Unanticipated Disclosure *98*

III. *Digital Certificates* *99*

6. *Digital Identification Techniques* *101*
Identification *101*
Public Key Infrastructure *112*
Problems Building a Public Key Infrastructure *119*
Ten Policy Questions *126*

7. *Certification Authorities and Server Certificates* *132*
Certificates Today *132*
Certification Authority Certificates *134*
Server Certificates *137*
Conclusion *150*

8. *Client-Side Digital Certificates* *151*
Client Certificates *151*
A Tour of the VeriSign Digital ID Center *153*

9. *Code Signing and Microsoft's Authenticode* *169*
Why Code Signing? *169*
Microsoft's Authenticode Technology *172*
Obtaining a Software Publisher's Certificate *181*

IV. *Cryptography* 185

10. *Cryptography Basics* 187
Understanding Cryptography 187
Symmetric Key Algorithms 193
Public Key Algorithms 200
Message Digest Functions 202
Public Key Infrastructure 207

11. *Cryptography and the Web* 209
Cryptography and Web Security 209
Today's Working Encryption Systems 212
U.S. Restrictions on Cryptography 219
Foreign Restrictions on Cryptography 229

12. *Understanding SSL and TLS* 233
What Is SSL? 233
TLS Standards Activities 243
SSL: The User's Point of View 243

V. *Web Server Security* 251

13. *Host and Site Security* 253
Historically Unsecure Hosts 253
Current Major Host Security Problems 255
Minimizing Risk by Minimizing Services 268
Secure Content Updating 270
Back-End Databases 272
Physical Security 273

14. *Controlling Access to Your Web Server* 275
Access Control Strategies 275
Implementing Access Controls with <Limit> Blocks 280
A Simple User Management System 286

15. *Secure CGI/API Programming* 293
The Danger of Extensibility 293
Rules To Code By 300
Specific Rules for Specific Programming Languages 305
Tips on Writing CGI Scripts That Run with Additional Privileges 308
Conclusion 309

VI. *Commerce and Society* 311

16. *Digital Payments* 313
Charga-Plates, Diners Club, and Credit Cards 313
Internet-Based Payment Systems 322
How to Evaluate a Credit Card Payment System 332

17. *Blocking Software and Censorship Technology* 335
Blocking Software 335
PICS 338
RSACi 346

18. *Legal Issues: Civil* 349
Intellectual Property 350
Torts 359

19. *Legal Issues: Criminal* 362
Your Legal Options After a Break-In 362
Criminal Hazards That May Await You 367
Criminal Subject Matter 370
Play it Safe 372
Laws and Activism 374

VII. *Appendixes* 377

A. *Lessons from Vineyard.NET* 379

B. *Creating and Installing Web Server Certificates* 402

C. *The SSL 3.0 Protocol* 417

D. *The PICS Specification* 442

E. *References* 450

Index 471