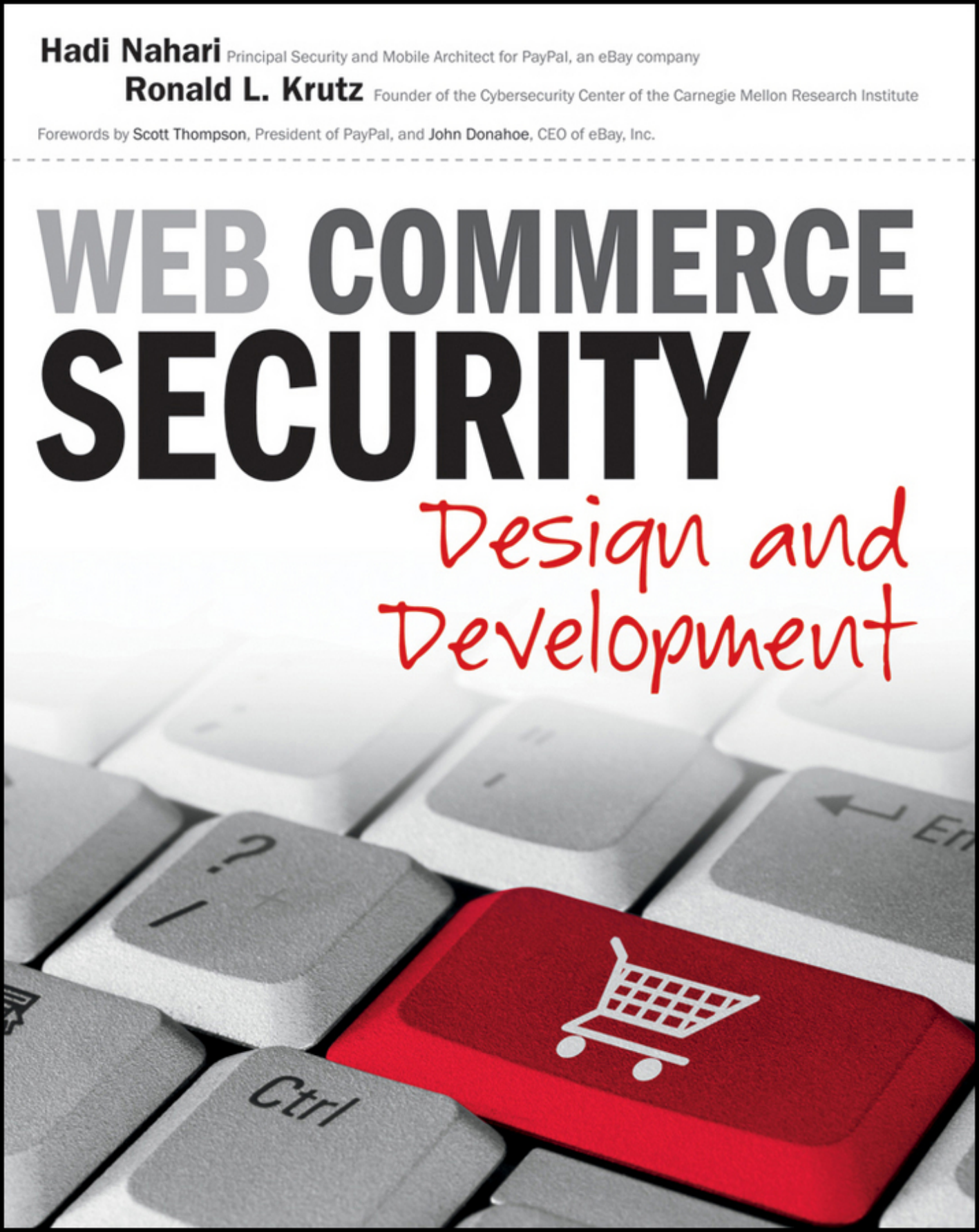
Hadi Nahari Principal Security and Mobile Architect for PayPal, an eBay company
Ronald L. Krutz Founder of the Cybersecurity Center of the Carnegie Mellon Research Institute

Forewords by **Scott Thompson**, President of PayPal, and **John Donahoe**, CEO of eBay, Inc.

WEB COMMERCE SECURITY

Design and Development



Web Commerce Security Design and Development

Hadi Nahari
Ronald L. Krutz

WILEY
Wiley Publishing, Inc.

Web Commerce Security Design and Development

Published by
Wiley Publishing, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Published by Wiley Publishing, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-0-470-62446-3
ISBN: 978-1-118-09889-9 (ebk)
ISBN: 978-1-118-09891-2 (ebk)
ISBN: 978-1-118-09898-1 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Library of Congress Control Number: 2011920900

I dedicate this book to my mom, Alieh, and to my late dad, Javad, for they brought me in this world without consulting me first, showed by example how to never give up, and trusted that I would make it.

— Hadi Nahari

To the saying, "Life is God's gift to you. What you do with it is your gift to Him."

— Ronald L. Krutz

About the Authors

Hadi Nahari is a security professional with 20 years of experience in software development, including extensive work in design, architecture, verification, proof-of-concept, and implementation of secure systems. He has designed and implemented large scale, high-end enterprise solutions, as well as resource-constrained embedded systems with the primary focus on security, cryptography, vulnerability assessment and threat analysis, and complex systems design. He is a frequent speaker in the U.S. and international security conferences and has led and contributed to various security projects for Netscape Communications, Sun Microsystems, Motorola, eBay, and PayPal, among others.

Ronald L. Krutz is a senior information system security consultant. He has over 30 years of experience in distributed computing systems, computer architectures, real-time systems, information assurance methodologies, and information security training. He holds B.S., M.S., and Ph.D. degrees in Electrical and Computer Engineering and is the author of best-selling texts in the area of information system security. Dr. Krutz is a Certified Information Systems Security Professional (CISSP) and Information Systems Security Engineering Professional (ISSEP).

He coauthored the *CISSP Prep Guide* for John Wiley & Sons and is coauthor of several books for Wiley, including the *Advanced CISSP Prep Guide*; *CISSP Prep Guide, Gold Edition*; *Security + Certification Guide*; *CISM Prep Guide*; *CISSP Prep Guide, 2nd Edition: Mastering CISSP and ISSEP*; *Network Security Bible*, *CISSP and CAP Prep Guide, Platinum Edition: Mastering CISSP and CAP*; *Certified Ethical Hacker (CEH) Prep Guide*; *Certified Secure Software Lifecycle Prep Guide*, and *Cloud Security*.

He is also the author of *Securing SCADA Systems* and of three textbooks in the areas of microcomputer system design, computer interfacing, and computer architecture. Dr. Krutz has seven patents in the area of digital systems and has published over 40 technical papers.

Dr. Krutz is a Registered Professional Engineer in Pennsylvania.

About the Technical Editor

David A. Chapa is a Senior Analyst with the Enterprise Strategy Group, a research and strategic consulting firm. He has invested more than 25 years in the computer industry, focusing specifically on data protection, data disaster recovery, and business resumption practices. He has held several senior-level technical positions with companies such as Cheyenne Software, OpenVision, ADIC, Quantum, and NetApp. He has been a featured speaker at a variety of industry events covering various topics related to disaster recovery, compliance, and the use of disk, tape, and cloud for recovery and backup strategies. He is recognized worldwide as an authority on the subject of backup and recovery. David is also a member of SNIA's Data Protection and Capacity Optimization (DPCO) Committee, whose mission is to foster the growth and success of the storage market in the areas of data protection and capacity optimization technologies.

Credits

Executive Editor
Carol Long

Senior Project Editor
Adaobi Obi Tulton

Technical Editor
David A. Chapa

Senior Production Editor
Debra Banninger

Copy Editor
Nancy Rapoport

Editorial Director
Robyn B. Siesky

Editorial Manager
Mary Beth Wakefield

Freelancer Editorial Manager
Rosemarie Graham

Marketing Manager
Ashley Zurcher

Production Manager
Tim Tate

Vice President and Executive Group Publisher
Richard Swadley

Vice President and Executive Publisher
Barry Pruett

Associate Publisher
Jim Minatel

Project Coordinator, Cover
Katie Crocker

Compositor
Craig Johnson,
Happenstance Type-O-Rama

Proofreader
Nancy Carrasco

Indexer
Robert Swanson

Cover Image
© Baris Onal / iStockPhoto

Cover Designer
Ryan Sneed

Acknowledgments

Acknowledging all those who directly and indirectly helped me and helped shape this book would require a book of its own. My special thanks to Carol Long for her full support and commitment, to Adaobi Obi Tulton, Nancy Rapoport, and Nancy Carrasco for their excellence and high standards, and to the rest of the team at John Wiley & Sons. I appreciate the invaluable feedback that David A. Chapa, the book's technical editor, provided to ensure the book's technical accuracy. I'm grateful to my coauthor, Dr. Ronald L. Krutz, for all that he taught me throughout the process of developing this text. The list is very long, but there's one person without whom it is certainly incomplete . . .

Without your patience and the most creative, subtle, encouraging, and smart ways that you supported me, I could not have written this book: Thank you Eva.

— Hadi Nahari

In addition to my own thanks to the Wiley team, the technical editor, and my co-author, I want to thank my wife, Hilda, for her support and encouragement during the writing of this book.

— Ronald L. Krutz

Contents

	Foreword by John Donahoe	**xxi**
	Foreword by Scott Thompson	**xxiii**
	Introduction	**xxv**
Part I	**Overview of Commerce**	**1**
Chapter 1	**Internet Era: E-Commerce**	**3**
	Evolution of Commerce	3
	Hard vs. Digital Goods	4
	Payment	5
	Money	6
	Financial Networks	6
	ACH	9
	Card Processing	10
	Mobile Payment and Commerce	14
	Distributed Computing: Adding E to Commerce	16
	Client/Server	17
	Grid Computing	18
	Cloud Computing	20
	Shared Resources	22
	Dynamic Resource Allocation	22
	Physical Abstraction	23
	Utility Model	23
	Self Service	23
	SLA-Driven Management	24
	Automation	24
	Self-Healing	24
	Service Orientation	25
	Multi-Tenancy	25

Cloud Security 25
Architecture Review 25
Centralized Authentication 26
Single Sign-On and Delegation 26
Role-Based Access Control 27
Credential Store 27
Secure Communication and Storage 28
Isolated Management 28
Regulatory Compliance 28
Distributed Trust 28
Freshness 29
Trust 29
Secure Isolation 29
Authorization 31
Threats 32
Operational Aspects 35
Governance 36
Summary 39
Notes 39

Chapter 2 Mobile Commerce 41
Consumer Electronics Devices 42
Mobile Phone and M-Commerce 42
Landscape 42
M- vs. E-commerce 46
Mobile Hardware 46
Device Manufacturer 47
Operating System 48
Stack 49
Application Model 49
State of Mobile 52
Mobile Technologies: Mosquito on Steroids 54
Carrier Networks 54
Stacks 57
Java Micro Edition 57
Android 61
BlackBerry 67
iPhone 68
Symbian 73
Other Stacks 74
Summary 75
Notes 75

Chapter 3 Important "Ilities" in Web Commerce Security 77
Confidentiality, Integrity, and Availability 77
Confidentiality 77
Integrity 78
Availability 79

Extensibility 80
Black Box Extensibility 81
White Box Extensibility (Open Box) 82
White Box Extensibility (Glass Box) 82
Gray Box Extensibility 83
Fault Tolerability 84
High Availability 85
Telecommunications Network Fault Tolerance 86
Interoperability 86
Additional Interoperability Standards 87
Testing for Interoperability 87
Maintainability 88
Manageability 89
Modularity 89
Monitorability 90
Intrusion Detection 91
Penetration Testing 92
Violation Analysis 92
Operability 93
Protection of Resources and Privileged Entities 94
Categories of Web Commerce Operability Controls 94
Portability 95
Predictability 96
Reliability 97
Ubiquity 98
Usability 99
Scalability 99
Accountability 101
Audit Ability 101
Traceability 103
Summary 104
Notes 105

Part II E-Commerce Security 107

Chapter 4 E-Commerce Basics 109
Why E-Commerce Security Matters 109
What Makes a System Secure 110
Risk-Driven Security 112
Security and Usability 114
Usability of Passwords 114
Practical Notes 115
Scalable Security 116
Securing Your Transactions 117
How Secure Is Secure? 118
Summary 118
Notes 118

Chapter 5 Building Blocks: Your Tools 119
Cryptography 119
The Role of Cryptography 119
Symmetric Cryptosystems 120
Stream Ciphers 120
Block Ciphers 121
Initialization Vector 123
Some Classical Ciphers 123
Symmetric Key Cryptography Fundamentals 127
Asymmetric Cryptosystems 131
One-Way Functions 132
Public Key Algorithms 132
Public Key Cryptosystems Algorithm Categories 135
Asymmetric and Symmetric Key Length Strength Comparisons 135
Digital Signatures 136
Message Digest 136
Hash Function Characteristics 138
Digital Signature Standard and Secure Hash Standard 138
Hashed Message Authentication Code 139
Random Number Generation 140
NIST SP 800-90 140
Other PRN Generators 141
FIPS 140-2 141
Public Key Certification Systems-Digital Certificates 142
Public Key Infrastructure 142
Digital Certificates 143
Directories and X.500 143
The Lightweight Directory Access Protocol 144
X.509 Certificates 144
Certificate Revocation Lists 145
Certificate Extensions 146
Key Management 147
Distributed versus Centralized Key Management 149
Data Protection 149
Data Loss Prevention 150
Database Security 150
Access Control 152
Controls 152
Models for Controlling Access 153
Mandatory Access Control 153
Discretionary Access Control 154
Non-Discretionary Access Control 154
System Hardening 155
Service Level Security 155
Web Servers 155

Web Server Security 156
Web Services 163
Web Applications 166
Host Level Security 170
Operating Systems 170
Browser Clients 172
Native Client 173
Network Security 173
Firewalls 174
Protocols 176
E-Mail 184
Malware Issues 186
Anti-Phishing 189
Network Utility Programs 190
Summary 191
Notes 191

Chapter 6 System Components: What You Should Implement 193
Authentication 193
User Authentication 193
Passwords 194
Biometrics 196
Network Authentication 197
Device Authentication 200
API Authentication 201
HTTP Basic Authentication 201
HTTP Digest Access Authentication 201
Microsoft Windows Challenge/Response (NTLM) Authentication 202
AuthSub 203
The OAuth 1.0 Protocol 203
Process Authentication 204
Authorization 205
Non-Repudiation 206
Privacy 206
Privacy Policy 207
Privacy-Related Legislation and Guidelines 208
European Union Principles 208
Health Care-Related Privacy Issues 209
The Platform for Privacy Preferences 210
Electronic Monitoring 211
Information Security 213
Security Management Concepts 213
System Security Life Cycle 213
Confidentiality, Integrity, and Availability 214
Layered Security Architecture 214
Security Controls 215

Data and Information Classification 215
Information Classification Benefits 216
Information Classification Concepts 216
Classification Terms 217
Classification Criteria 218
Information Classification Procedures 218
Distribution of Classified Information 219
Information Classification Roles 219
Data Categorization 222
Bell-LaPadula Model 223
System and Data Audit 224
Syslog 226
SIEM 228
Defense in Depth 229
Principle of Least Privilege 232
Trust 234
Isolation 235
Virtualization 236
Sandbox 236
IPSec Domain Isolation 236
Security Policy 237
Senior Management Policy Statement 238
Advisory Policies 238
Regulatory Policies 238
Informative Policies 238
NIST Policy Categories 238
Communications Security 239
Inter-Network Security 239
Homogenous Networks 241
Heterogeneous networks 242
Summary 243
Notes 243

Chapter 7 Trust but Verify: Checking Security 245
Tools to Verify Security 246
Vulnerability Assessment and Threat Analysis 247
Intrusion Detection and Prevention Using Snort 249
Network Scanning Using Nmap 251
Web Application Survey 252
Lynx 252
Wget 253
Teleport Pro 254
BlackWidow 255
BrownRecluse Pro 255
Vulnerability Scanning 257
Nessus 257
Nikto 258
Wireshark 259

Penetration Testing 260
Metasploit 260
Aircrack-ng 261
Wireless Reconnaissance 262
NetStumbler 262
Kismet 263
AirMagnet Wi-Fi Analyzer 264
Summary 266
Notes 266

Chapter 8 Threats and Attacks: What Your Adversaries Do 267
Basic Definitions 268
Target 268
Threat 269
Threat Modeling 269
Attack 269
Attack Tree 269
Zero-Day Attack 270
Control 270
Same-Origin Policy 270
Common Web Commerce Attacks 271
Broken Authentication and Session Management Attack 271
Control 272
Cross-Site Request Forgery Attack 272
Control 275
Cross-Site Scripting Attack 276
Stored or Persistent XSS 276
Reflected or Non-Persistent XSS 277
DOM-Based XSS 277
Control 278
DNS Hijacking Attack 280
Control 281
Failure to Restrict URL Access Attack 281
Control 281
Injection Flaws 282
Attacks 282
Control 285
Insufficient Transport Layer Protection Attack 285
Control 285
Insecure Cryptographic Storage Attack 286
Control 286
Insecure Direct Object Reference Attack 287
Control 287
Phishing and Spamming Attack 287
Control 288
Rootkits and Their Related Attacks 288
Control 288

Security Misconfiguration Attack 289
Control 289
Unvalidated Redirects and Forwards Attack 289
Control 290
Summary 290
Notes 290

Chapter 9 Certification: Your Assurance 293
Certification and Accreditation 293
The Certification Process 294
Security Control Assessment 294
Standards and Related Guidance 296
Trusted Computer System Evaluation Criteria 296
Common Criteria ISO/IEC 15408 297
Defense Information Assurance Certification and Accreditation Process 297
The DIACAP Phases 298
Office of Management and Budget Circular A-130 299
The National Information Assurance Certification and Accreditation Process 300
NIACAP Accreditation Types 302
The Four Phases of NIACAP 302
Roles of NIACAP 303
Federal Information Security Management Act 303
Federal Information Technology Security Assessment Framework 303
FIPS 199 304
FIPS 200 305
Additional Guidance 306
Related Standards Bodies and Organizations 306
Jericho Forum 307
The Distributed Management Task Force 307
The DMTF Open Virtualization Format 307
International Organization for Standardization/ International Electrotechnical Commission 308
ISO 27001 308
ISO 27002 309
ISO 27004 310
ISO 27006 310
ISO/IEC 29361, ISO/IEC 29362, and ISO/IEC 29363 Standards 310
Distributed Application Platforms and Services 311
The European Telecommunications Standards Institute 311
Storage Networking Industry Association 311

The Open Web Application Security Project 312
OWASP Top Ten Project 313
OWASP Development Guide 313
NIST SP 800-30 314
Risk Assessment 315
Risk Mitigation 316
Evaluation and Assessment 316
Residual Risk 316
Certification Laboratories 316
The Software Engineering Center Software Assurance Laboratory 317
SAIC 317
ICSA Labs 317
The Systems Security Engineering Capability Maturity Model 318
Value of Certification 321
When It Matters 322
When It Does Not 322
Certification Types 323
Common Criteria 323
MasterCard CAST 323
EMV 324
VSDC – VISA 324
M/Chip 325
GlobalPlatform Composition Model 325
Other Evaluation Criteria 325
NSA 327
The IAM Process 328
FIPS 140 Certification and NIST 328
Summary 329
Notes 330

Appendix A Computing Fundamentals 331
Introduction 331
Hardware 334
Central Processing Unit 334
Instruction Execution Cycle 338
A Bit about Bytes 345
Memory and Storage 345
Input and Output 350
Popular Architectures 351
ARM 351
MIPS 352
PowerPC 353
X86 353
XScale 354

Software 355
Underware 357
Firmware 357
Virtualization 357
Operating System 359
Middleware 362
Applications 363
Programming Languages 363
Summary 364

Appendix B Standardization and Regulatory Bodies 365
ANSI 366
COBIT 366
COSO 367
CSA 367
Ecma 368
ETSI 368
FIPS 369
GlobalPlatform 370
IANA 371
IEC 372
IETF 372
ISO 372
Kantara 373
NIST 373
OASIS 376
OAuth 377
OpenID 377
OpenSAF 378
PCI 379
SAF 380
SOX 380
The Open Group 381
W3C 382
WASC 382
Notes 383

Appendix C Glossary of Terms 385

Appendix D Bibliography 449

Index 457

Foreword

Technology-driven innovation is changing the way consumers around the world shop and pay. E-commerce is evolving rapidly and traditional distinctions between online and offline shopping are blurring. Four trends are helping to shape new ways people shop: the emergence of mobile commerce, the influence of social media, the growth of digital goods, and the potential of technology to create more convenient and accessible local shopping options. Increasingly, we can find whatever we want, whenever we want, wherever we are.

In this extraordinarily exciting and dynamic global commerce environment, Hadi Nahari and Ron Krutz's book is both timely and topical. Web commerce security is fundamental to the future of how we will shop and pay. The Web is becoming integral to more aspects of our lives. In a world where consumers will move seamlessly across screens and devices to shop, pay, and connect, security is paramount.

At eBay, how we design, manage and scale our global commerce and payment platforms to ensure that security is embedded in a compelling user experience is critical to our success. And it should be top of mind for any company competing in today's wired, digital world.

Our global platforms at eBay and PayPal support nearly 190 million active accounts and users. Buyers and sellers transact $60 billion of gross merchandise volume on eBay worldwide each year. In 2010, consumers transacted nearly $2 billion of gross merchandise volume through our eBay mobile applications. And we expect that number to double to $4 billion in 2011. PayPal processes more than $92 billion of payment volume annually around the world. And PayPal handled more than $750 million of mobile payment volume in 2010; we expect that to double in 2011.

At that global scale and volume, security is something we take very seriously. Entrepreneurs, merchants, and consumers around the world rely every day on the security of our platforms. Scalability and security go hand-in-hand, data protection and privacy are critical, and ensuring reliability is paramount. All of this complexity has to be managed while delivering highly interactive, real-time 24/7 global commerce and payment experiences in a convenient, easy-to-use environment.

To compete and grow, companies must deeply understand and manage Web commerce security. Hadi Nahari and Ron Krutz are two of the best in this space, and they are sharing their knowledge and insight in this book. That's a gift, and this is a must-read for anyone serious about playing and winning in today's global e-commerce world.

John Donahoe
President and CEO
eBay, Inc.

Foreword

The Internet has been changing our lives at a staggering pace. Thanks to the continuous stream of innovations in software the changes are only accelerating. In this era of global connectivity the new generation can hardly imagine the wide world without the Web.

The ubiquity of the Web has also enabled us to deliver services in ways inconceivable in the past. The breadth of what can be accomplished on the Web makes it the perfect and the most convenient platform to carry out commerce, pay, and get paid. The scale of electronic commerce growth is astonishing: PayPal transacted $3,380 every single second of the fourth quarter in 2010, a 28 percent yearly increase from the previous year!

With this growth comes the uncompromising consumer expectation for convenience, availability, and security of the services that they receive. It is the core mandate of any responsible company to facilitate a viable, reliable, and secure user experience: Hadi Nahari and Ron Krutz's book shows you how to create such a system.

At PayPal, we believe that in this highly integrated world our services must be provided the same way and irrespective of access channels: Whether it is a personal computer, mobile phone, tablet computer, Internet-connected television, or any other consumer electronic device, PayPal users are guaranteed an impeccable, easy, and safe experience. We design our solutions and deliver our services with those core values in mind: We believe our users deserve nothing less.

In 2010, PayPal's net Total Payment Volume, the total value of transactions, was about 18 percent of global e-commerce. With an annual revenue of $3.4 billion, our cross-border trade now accounts for approximately 25 percent of the total transactions. Mobile commerce is another area of explosive growth: By 2014, the mobile payment market across the world is expected to reach $633 billion.

This is an exciting time and we are fully prepared to grow our business to support e-commerce and m-commerce the PayPal way: easy, usable, and secure.

We delight global consumers by empowering them to control their money — securely and easily. We do it by providing a scalable, reliable, and secure infrastructure that is simple and secure for our consumers and merchants to use. In this book, Hadi Nahari and Ron Krutz, internationally recognized experts in e-commerce and m-commerce security, show you how to do it the right way.

Scott Thompson
President
PayPal

Introduction

Performing electronic or e-commerce activities online is ubiquitous; we all engage in it on a daily basis whether or not we are aware of it. Consumer electronics devices in general and mobile phones in particular are also becoming an integral part of our lives. Devices are becoming more powerful, extensively interconnected, much easier to use, and therefore capable of performing more and more tasks better, faster, and more reliably. Devices are becoming gatekeepers for our interaction with the digital world; they are entrusted to be the de facto means to live our digital life. Now if we combine the two trends mentioned, you will see the next digital wave that is taking place: interacting with our social networks, performing electronic commerce activities such as banking, ordering goods online, and so on, all using our consumer electronics devices. All these activities have one important element in common: They touch and use our identity. In other words, our digital security now depends on the security of our devices and the systems that they interact with. When there is identity, there must be reliable mechanisms in place to manage it safely and securely.

From the system designers' vantage point, the task of securing such a complex system is overwhelming, to say the least. There are different elements of this ecosystem that need to operate in synchrony, although many of them have not been originally designed to work together. From the end user's perspective, however, the need is much simpler; it must be safe and secure to use the system! In this book, we describe what it means to make such a system secure and thus safe for consumers to use, with a specific focus on e-commerce and its various forms, such as mobile commerce.

Even though the fundamental information system security principles are applicable across a variety of domains, e-commerce security provides special challenges to the information security professional. The technologies involved are advancing at a breakneck pace, both in terms of hardware and software. The hackers as well as the service providers have large amounts of computing power available to them at lower and lower costs. For example, with the availability of cloud computing, an individual can utilize tremendous computer resources at rates around a dollar per hour or less. This capability can be used for beneficial activities or for malicious purposes such as discovering encryption keys used to protect critical personal and financial transaction information stored in e-commerce databases. Also, in many countries today, cell phones provide credit card functionality that is used in hands-free scanning transactions. RFID reading capability in mobile devices opens the door to a variety of e-commerce paradigms in addition to novel attack methods. Therefore, understanding the e-commerce approach to information system security is necessary to appreciate the security threats and countermeasures associated with this business sector.

This book explains the steps necessary to analyze and understand system security from both holistic and atomic perspectives. It defines risk-driven security, protection mechanisms and how to best deploy them, and presents ways to implement security in a usable and user-friendly manner. The theme of all topics will be e-commerce, although they apply to m-commerce as well. The following are some important topics covered in this book:

- Users, users, users. Security that is difficult to use, albeit bullet-proof, will not be adopted by users, so it's important to know how to design and implement a strong security that is also user-friendly.
- What makes e- and m-commerce (electronic and mobile, respectively) secure; how to design and implement it.
- Techniques to implement an adaptive, risk-driven, and scalable security infrastructure.
- Fundamentals of architecting e- and m-commerce security infrastructure with high availability and large transactional capacity in mind.
- How to identify weak security in a large-scale, transactional system.

This book provides a systems architect or a developer with the information needed to design and implement a secure e-commerce or m-commerce solution that satisfies consumers' needs. Familiarity with security technologies, vulnerability assessment and threat analysis, transactional and scalable systems design, development, maintenance, as well as payment and commerce systems by the reader is a plus.

How This Book Is Organized

The book is organized into nine chapters and four appendices, with the chapters sequentially developing the important background information and detailed knowledge of e-commerce and e-commerce security issues. The appendices provide a review of important technical and compliance topics to support the material in the chapters.

The material in the chapters begins with the introduction of the era of e-commerce and its effect on consumer buying habits and norms. The subsequent chapters focus on the important qualities a robust and secure e-commerce system must possess and then lead into the fundamental building blocks of e-commerce. Using this information as a foundation, the middle chapters provide a detailed look at the tools available to implement a robust e-commerce environment and the means to secure such an environment. The final chapters explore methods and approaches to certify the assurance posture of e-commerce implementations.

Chapter 1 reviews the basic concepts of distributed computing and explains the unique characteristics of e-commerce as opposed to "conventional" commerce. It also covers digital goods, hard goods, payment methods, and introduces mobile or m-commerce.

Chapter 2 discusses consumer electronic devices and delves into the differences between e-commerce and m-commerce. The chapter then goes into great detail about mobile hardware, operating systems, and stacks. It also explores thin versus thick clients, application warehousing, and the characteristics of different mobile carrier networks.

In Chapter 3, the important "ilities" such as availability, interoperability, reliability, scalability, and so on are defined and developed in the context of their applicability to e-commerce systems.

With the background provided by the previous chapters, Chapter 4 focuses on e-commerce security, including what makes an e-commerce system secure, risk management, and the scalability of computing systems and corresponding security measures. It concludes with valuable material on how to secure e-commerce transactions.

Chapter 5 discusses a variety of e-commerce protection measures including cryptography, access control types and mechanisms, system hardening, and Web server security. It further explores host-level and network-level security measures applicable to e-commerce systems.

Chapter 6 describes the critical e-commerce system security components and principles that have to be applied to support secure and reliable transactions. These topics include authentication types, authorization, privacy, data classification, and system and data audit. Then, the chapter explores the principles of defense in depth, least privilege, trust, and communication security.

In order to implement the proper security controls, it is important to understand the vulnerabilities extant in an e-commerce implementation. Chapter 7 covers vulnerability assessment, intrusion detection and prevention, scanning tools, reconnaissance software, and penetration testing.

The threats to e-commerce systems are discussed in Chapter 8 through the topics of Web applications, attack trees, spamming, phishing, data harvesting, cross-site scripting, Web services attacks, rootkits, and a variety of other critical threat topics.

The book chapters conclude with Chapter 9, which presents certification issues, such as evaluation types, standards, assurance, documentation, and certification types such as MasterCard CAST, the Common Criteria, the GlobalPlatform Card Composition Model, and so on.

Appendix A presents an overview of e-commerce history and fundamental e-commerce concepts. Hardware, software and virtualization issues are explored as well as the importance of secure isolation. Operating system, networking, storage, and middleware topics are discussed in terms of their application in e-commerce systems.

Appendix B provides explanatory material on e-commerce standardization and regulatory bodies.

Appendix C is a glossary of important terms.

Appendix D is a bibliography of resources that we consulted for this book and recommend you read as well.

Who Should Read This Book

The primary audience for this book are architects and developers, systems engineers, project managers, senior technical managers, corporate strategists, and technical marketing staff.

The ideal reader for this book would be a systems architect or a developer who requires technical understanding of how to design and implement a secure e-commerce or m-commerce solution that satisfies the consumers' needs. The reader should have moderate knowledge of security technologies, vulnerability assessment and threat analysis, transactional and scalable systems design, development, maintenance, as well as payment and commerce systems. No special tools are needed.