

/THEORY/IN/PRACTICE

Beautiful Security

Leading Security Experts Explain How They Think

O'REILLY®

Andy Oram & John Viega

Beautiful Security

"This collection of thoughtful essays catapults the reader well beyond deceptively shiny security FUD toward the more subtle beauty of security done right. Beautiful Security demonstrates the yin and the yang of security, and the fundamental creative tension between the spectacularly destructive and the brilliantly constructive."

—Gary McGraw, CTO of Cigital, author of *Software Security* and nine other books

Although most people don't give security much attention until their personal or business systems are attacked, this thought-provoking anthology demonstrates that digital security is not only worth thinking about, it's also a fascinating topic. Criminals succeed by exercising enormous creativity, and those defending against them must do the same.

Beautiful Security explores this challenging subject with insightful essays and analysis on topics that include:

- The underground economy for personal information: how it works, the relationships among criminals, and some of the new ways they pounce on their prey
- How social networking, cloud computing, and other popular trends help or hurt our online security
- How metrics, requirements gathering, design, and law can take security to a higher level
- The real, little-publicized history of PGP

This book includes contributions from:

Peiter "Mudge" Zatkó

Jim Stickley

Elizabeth A. Nichols

Chenxi Wang

Ed Bellis

Benjamin Edelman

Philip Zimmermann and Jon Callas

Kathy Wang

Mark Curphey

John McManus

Jim Routh

Randy V. Sabett

Anton Chuvakin

Grant Geyer and Brian Dunphy

Peter Wayner

Michael Wood and Fernando Francisco

All royalties will be donated to the Internet Engineering Task Force (IETF).

US \$39.99

CAN \$49.99

ISBN: 978-0-596-52748-8



Safari
Books Online

Free online edition

for 45 days with purchase of this book. Details on last page.

O'REILLY[®] www.oreilly.com

Beautiful Security

Beautiful Security

Edited by Andy Oram and John Viega

O'REILLY®

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

Beautiful Security

Edited by Andy Oram and John Viega

Copyright © 2009 O'Reilly Media, Inc. All rights reserved.

Printed in the United States of America.

Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

O'Reilly books may be purchased for educational, business, or sales promotional use. Online editions are also available for most titles (<http://my.safaribooksonline.com/>). For more information, contact our corporate/institutional sales department: 800-998-9938 or corporate@oreilly.com.

Production Editor: Sarah Schneider
Copyeditor: Genevieve d'Entremont
Proofreader: Sada Preisch

Indexer: Lucie Haskins
Cover Designer: Mark Paglietti
Interior Designer: David Futato
Illustrator: Robert Romano

Printing History:

April 2009: First Edition.

O'Reilly and the O'Reilly logo are registered trademarks of O'Reilly Media, Inc. *Beautiful Security*, the image of a cactus, and related trade dress are trademarks of O'Reilly Media, Inc.

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and O'Reilly Media, Inc., was aware of a trademark claim, the designations have been printed in caps or initial caps.

While every precaution has been taken in the preparation of this book, the publisher and authors assume no responsibility for errors or omissions, or for damages resulting from the use of the information contained herein.

ISBN: 978-0-596-52748-8

[V]

1239647579

*All royalties from this book will be donated
to the Internet Engineering Task Force
(IETF).*

CONTENTS

	PREFACE	xi
1	PSYCHOLOGICAL SECURITY TRAPS <i>by Peiter “Mudge” Zatkó</i>	1
	Learned Helplessness and Naïveté	2
	Confirmation Traps	10
	Functional Fixation	14
	Summary	20
2	WIRELESS NETWORKING: FERTILE GROUND FOR SOCIAL ENGINEERING <i>by Jim Stickley</i>	21
	Easy Money	22
	Wireless Gone Wild	28
	Still, Wireless Is the Future	31
3	BEAUTIFUL SECURITY METRICS <i>by Elizabeth A. Nichols</i>	33
	Security Metrics by Analogy: Health	34
	Security Metrics by Example	38
	Summary	60
4	THE UNDERGROUND ECONOMY OF SECURITY BREACHES <i>by Chenxi Wang</i>	63
	The Makeup and Infrastructure of the Cyber Underground	64
	The Payoff	66
	How Can We Combat This Growing Underground Economy?	71
	Summary	72
5	BEAUTIFUL TRADE: RETHINKING E-COMMERCE SECURITY <i>by Ed Bellis</i>	73
	Deconstructing Commerce	74
	Weak Amelioration Attempts	76
	E-Commerce Redone: A New Security Model	83
	The New Model	86
6	SECURING ONLINE ADVERTISING: RUSTLERS AND SHERIFFS IN THE NEW WILD WEST <i>by Benjamin Edelman</i>	89
	Attacks on Users	89
	Advertisers As Victims	98

	Creating Accountability in Online Advertising	105
7	THE EVOLUTION OF PGP'S WEB OF TRUST <i>by Phil Zimmermann and Jon Callas</i>	107
	PGP and OpenPGP	108
	Trust, Validity, and Authority	108
	PGP and Crypto History	116
	Enhancements to the Original Web of Trust Model	120
	Interesting Areas for Further Research	128
	References	129
8	OPEN SOURCE HONEYCLIENT: PROACTIVE DETECTION OF CLIENT-SIDE EXPLOITS <i>by Kathy Wang</i>	131
	Enter Honeyclients	133
	Introducing the World's First Open Source Honeyclient	133
	Second-Generation Honeyclients	135
	Honeyclient Operational Results	139
	Analysis of Exploits	141
	Limitations of the Current Honeyclient Implementation	143
	Related Work	144
	The Future of Honeyclients	146
9	TOMORROW'S SECURITY COGS AND LEVERS <i>by Mark Curphey</i>	147
	Cloud Computing and Web Services: The Single Machine Is Here	150
	Connecting People, Process, and Technology: The Potential for Business Process Management	154
	Social Networking: When People Start Communicating, Big Things Change	158
	Information Security Economics: Supercrunching and the New Rules of the Grid	162
	Platforms of the Long-Tail Variety: Why the Future Will Be Different for Us All	165
	Conclusion	168
	Acknowledgments	169
10	SECURITY BY DESIGN <i>by John McManus</i>	171
	Metrics with No Meaning	172
	Time to Market or Time to Quality?	174
	How a Disciplined System Development Lifecycle Can Help	178
	Conclusion: Beautiful Security Is an Attribute of Beautiful Systems	181
11	FORCING FIRMS TO FOCUS: IS SECURE SOFTWARE IN YOUR FUTURE? <i>by Jim Routh</i>	183
	Implicit Requirements Can Still Be Powerful	184
	How One Firm Came to Demand Secure Software	185
	Enforcing Security in Off-the-Shelf Software	190
	Analysis: How to Make the World's Software More Secure	193
12	OH NO, HERE COME THE INFOSECURITY LAWYERS! <i>by Randy V. Sabett</i>	199

	Culture	200
	Balance	202
	Communication	207
	Doing the Right Thing	211
13	BEAUTIFUL LOG HANDLING	213
	<i>by Anton Chuvakin</i>	
	Logs in Security Laws and Standards	213
	Focus on Logs	214
	When Logs Are Invaluable	215
	Challenges with Logs	216
	Case Study: Behind a Trashed Server	218
	Future Logging	221
	Conclusions	223
14	INCIDENT DETECTION: FINDING THE OTHER 68%	225
	<i>by Grant Geyer and Brian Dunphy</i>	
	A Common Starting Point	226
	Improving Detection with Context	228
	Improving Perspective with Host Logging	232
	Summary	237
15	DOING REAL WORK WITHOUT REAL DATA	239
	<i>by Peter Wayner</i>	
	How Data Translucency Works	240
	A Real-Life Example	243
	Personal Data Stored As a Convenience	244
	Trade-offs	244
	Going Deeper	245
	References	246
16	CASTING SPELLS: PC SECURITY THEATER	247
	<i>by Michael Wood and Fernando Francisco</i>	
	Growing Attacks, Defenses in Retreat	248
	The Illusion Revealed	252
	Better Practices for Desktop Security	257
	Conclusion	258
	CONTRIBUTORS	259
	INDEX	269

Preface

IF ONE BELIEVES THAT NEWS HEADLINES REVEAL TRENDS, THESE ARE INTERESTING times for computer security buffs. As *Beautiful Security* went to press, I read that a piece of software capable of turning on microphones and cameras and stealing data has been discovered on more than 1,200 computers in 103 countries, particularly in embassies and other sensitive government sites. On another front, a court upheld the right of U.S. investigators to look at phone and Internet records without a warrant (so long as one end of the conversation is outside the U.S.). And this week's routine vulnerabilities include a buffer overflow in Adobe Acrobat and Adobe Reader—with known current exploits—that lets attackers execute arbitrary code on your system using your privileges after you open their PDF.

Headlines are actually not good indicators of trends, because in the long run history is driven by subtle evolutionary changes noticed only by a few—such as the leading security experts who contributed to this book. The current directions taken by security threats as well as responses can be discovered in these pages.

All the alarming news items I mentioned in the first paragraph are just business as usual in the security field. Yes, they are part of trends that should worry all of us, but we also need to look at newer and less dramatic vulnerabilities. The contributors to this book have, for decades, been on the forefront of discovering weaknesses in our working habits and suggesting unconventional ways to deal with them.

Why Security Is Beautiful

I asked security expert John Viega to help find the authors for this book out of frustration concerning the way ordinary computer users view security. Apart from the lurid descriptions of break-ins and thefts they read about in the press, average folks think of security as boring.

Security, to many, is represented by nagging reminders from system administrators to create backup folders, and by seemingly endless dialog boxes demanding passwords before a web page is displayed. Office workers roll their eyes and curse as they read the password off the notepad next to their desk (lying on top of the budget printout that an office administrator told them should be in a locked drawer). If this is security, who would want to make a career of it? Or buy a book from O'Reilly about it? Or think about it for more than 30 seconds at a time?

To people tasked with creating secure systems, the effort seems hopeless. Nobody at their site cooperates with their procedures, and the business managers refuse to allocate more than a pittance to security. Jaded from the endless instances of zero-day exploits and unpatched vulnerabilities in the tools and languages they have to work with, programmers and system administrators become lax.

This is why books on security sell poorly (although in the last year or two, sales have picked up a bit). Books on hacking into systems sell much better than books about how to protect systems, a trend that really scares me.

Well, this book should change that. It will show that security is about the most exciting career you can have. It is not tedious, not bureaucratic, and not constraining. In fact, it exercises the imagination like nothing else in technology.

Most of the programming books I've edited over the years offer a chapter on security. These chapters are certainly useful, because they allow the author to teach some general principles along with good habits, but I've been bothered by the convention because it draws a line around the topic of security. It feeds the all-too-common view of security as an add-on and an afterthought. *Beautiful Security* demolishes that conceit.

John chose for this book a range of authors who have demonstrated insight over and over in the field and who had something new to say. Some have designed systems that thousands rely on; some have taken high-level jobs in major corporations; some have testified on and worked for government bodies. All of them are looking for the problems and solutions that the rest of us know nothing about—but will be talking about a lot a few years from now.

The authors show that effective security keeps you on your toes all the time. It breaks across boundaries in technology, in cognition, and in organizational structures. The black hats in security succeed by exquisitely exercising creativity; therefore, those defending against them must do the same.

With the world's infosecurity resting on their shoulders, the authors could be chastised for taking time off to write these chapters. And indeed, many of them experienced stress trying to balance their demanding careers with the work on this book. But the time spent was worth it, because this book can advance their larger goals. If more people become intrigued with the field of security, resolve to investigate it further, and give their attention and their support to people trying to carry out organizational change in the interest of better protection, the book will have been well worth the effort.

On March 19, 2009, the Senate Committee on Commerce, Science, and Transportation held a hearing on the dearth of experts in information technology and how that hurts the country's cybersecurity. There's an urgent need to interest students and professionals in security issues; this book represents a step toward that goal.

Audience for This Book

This book is meant for people interested in computer technology who want to experience a bit of life at the cutting edge. The audience includes students exploring career possibilities, people with a bit of programming background, and those who have a modest to advanced understanding of computing.

The authors explain technology at a level where a relatively novice reader can get a sense of the workings of attacks and defenses. The expert reader can enjoy the discussions even more, as they will lend depth to his or her knowledge of security tenets and provide guidance for further research.

Donation

The authors are donating the royalties from this book to the Internet Engineering Task Force (IETF), an organization critical to the development of the Internet and a fascinating model of enlightened, self-organized governance. The Internet would not be imaginable without the scientific debates, supple standard-making, and wise compromises made by dedicated members of the IETF, described on their web page as a "large open international community of network designers, operators, vendors, and researchers." O'Reilly will send royalties to the Internet Society (ISOC), the longtime source of funding and organizational support for the IETF.

Organization of the Material

The chapters in this book are not ordered along any particular scheme, but have been arranged to provide an engaging reading experience that unfolds new perspectives in hopefully surprising ways. Chapters that deal with similar themes, however, are grouped together.

- Chapter 1, *Psychological Security Traps*, by Peiter “Mudge” Zatkó
- Chapter 2, *Wireless Networking: Fertile Ground for Social Engineering*, by Jim Stickley
- Chapter 3, *Beautiful Security Metrics*, by Elizabeth A. Nichols
- Chapter 4, *The Underground Economy of Security Breaches*, by Chenxi Wang
- Chapter 5, *Beautiful Trade: Rethinking E-Commerce Security*, by Ed Bellis
- Chapter 6, *Securing Online Advertising: Rustlers and Sheriffs in the New Wild West*, by Benjamin Edelman
- Chapter 7, *The Evolution of PGP’s Web of Trust*, by Phil Zimmermann and Jon Callas
- Chapter 8, *Open Source Honeyclient: Proactive Detection of Client-Side Exploits*, by Kathy Wang
- Chapter 9, *Tomorrow’s Security Cogs and Levers*, by Mark Curphey
- Chapter 10, *Security by Design*, by John McManus
- Chapter 11, *Forcing Firms to Focus: Is Secure Software in Your Future?*, by James Routh
- Chapter 12, *Oh No, Here Come the Infosecurity Lawyers!*, by Randy V. Sabett
- Chapter 13, *Beautiful Log Handling*, by Anton Chuvakin
- Chapter 14, *Incident Detection: Finding the Other 68%*, by Grant Geyer and Brian Dunphy
- Chapter 15, *Doing Real Work Without Real Data*, by Peter Wayner
- Chapter 16, *Castling Spells: PC Security Theater*, by Michael Wood and Fernando Francisco

Conventions Used in This Book

The following typographical conventions are used in this book:

Italic

Indicates new terms, URLs, filenames, and Unix utilities.

Constant width

Indicates the contents of computer files and generally anything found in programs.

Using Code Examples

This book is here to help you get your job done. In general, you may use the code in this book in your programs and documentation. You do not need to contact us for permission unless you’re reproducing a significant portion of the code. For example, writing a program that uses several chunks of code from this book does not require permission. Selling or distributing a CD-ROM of examples from O’Reilly books does require permission. Answering a question by citing this book and quoting example code does not require permission. Incorporating a

significant amount of example code from this book into your product's documentation does require permission.

We appreciate, but do not require, attribution. An attribution usually includes the title, author, publisher, and ISBN. For example: "*Beautiful Security*, edited by Andy Oram and John Viega. Copyright 2009 O'Reilly Media, Inc., 978-0-596-52748-8."

If you feel your use of code examples falls outside fair use or the permission given here, feel free to contact us at permissions@oreilly.com.

Safari® Books Online



When you see a Safari® Books Online icon on the cover of your favorite technology book, that means the book is available online through the O'Reilly Network Safari Bookshelf.

Safari offers a solution that's better than e-books. It's a virtual library that lets you easily search thousands of top tech books, cut and paste code samples, download chapters, and find quick answers when you need the most accurate, current information. Try it for free at <http://my.safaribooksonline.com/>.

How to Contact Us

Please address comments and questions concerning this book to the publisher:

O'Reilly Media, Inc.
1005 Gravenstein Highway North
Sebastopol, CA 95472
800-998-9938 (in the United States or Canada)
707-829-0515 (international or local)
707-829-0104 (fax)

We have a web page for this book, where we list errata, examples, and any additional information. You can access this page at:

<http://www.oreilly.com/catalog/9780596527488>

To comment or ask technical questions about this book, send email to:

bookquestions@oreilly.com

For more information about our books, conferences, Resource Centers, and the O'Reilly Network, see our website at:

<http://www.oreilly.com>

Tomorrow's Security Cogs and Levers

Mark Curphey

Without changing our patterns of thought, we will not be able to solve the problems that we created with our current patterns of thought.

—Albert Einstein

INFORMATION SECURITY IS NOT JUST ABOUT TECHNOLOGY. It is about people, processes, and technology, in that order—or more accurately, about connecting people, processes, and technology together so that humans and entire systems can make informed decisions. It may at first seem rather odd to start a chapter in a book about the future of security management technology with a statement that puts the role of technology firmly in third place, but I felt it was important to put that stake in the ground to provide context for the rest of this chapter.

This doesn't mean that I belittle the role of technology in security. I firmly believe that we are at the very beginnings of an information technology revolution that will affect our lives in ways few of us can imagine, let alone predict. It's easy to dismiss futuristic ideas; many of us still laugh at historical predictions from the 1970s and 1980s portraying a future where self-guided hovercars will whisk us to the office in the mornings and where clunky humanoid robots will mix us cocktails when we get home from work, yet fundamental technological breakthroughs are emerging before our eyes that will spark tomorrow's technological advances.

One such spark, which feeds my conviction that we are on the cusp of an exponential technology curve, is the development of programming languages and artificial intelligence

technology that will improve itself at rates humans can't match. Think about that for a moment: programming languages that can themselves create better languages, which in turn can create better languages, and so on. Software that can reprogram itself to be better based on what it learns about itself, designing and solving solutions to problems that we didn't even imagine were solvable (assuming we even knew about them in the first place). Many people debate ethical medical research and cry foul about how human cloning could change the planet, but they may well be focused on the wrong problem.

Information security and its relationship with technology, of course, dates back through history. The Egyptians carved obfuscated hieroglyphs into monuments; the Spartans used sticks and wound messages called *scytales* to exchange military plans; and the Romans' Caesar ciphers are well documented in school textbooks. Many historians attribute the victory in the Second World War directly to the code breakers at Bletchley Park who deciphered the famous Enigma machine, yet even this monumental technological event, which ended the World War and changed history forever, may pale into insignificance next to changes to come.

The packet switching network invented by Donald Davies in 1970 also changed the world forever when the sudden ability of computers to talk to other computers with which they previously had no relationship opened up new possibilities for previously isolated computing power. Although the early telegraph networks almost a century before may have aroused the dream of an electronically connected planet, it was only in the 1970s, 1980s, and 1990s that we started to wire the world together definitively with copper cables and later with fiber-optic technology. Today that evolution is entering a new phase. Instead of wiring physical locations together with twisted copper cables, we are wiring together software applications and data with service-oriented architectures (SOAs) and, equally importantly, wiring people into complex social networks with new types of human relationships.

While I would be foolish to think I could predict the future, I often find myself thinking about future trends in information security and about the potential effect of information security on the future—two very distinct but interrelated things. Simply put, I believe that information security in the future will be very different from the relatively crude ways in which we operate today.

The security tools and technology available to the masses today can only be described as primitive in comparison to electronic gaming, financial investment, or medical research software. Modern massive multiplayer games are built on complex physics engines that mimic real-world movement, leverage sophisticated artificial intelligence engines that provide human-like interactions, and connect hundreds of thousands of players at a time in massively complex virtual worlds. The financial management software underpinning investment banks performs "supercrunching" calculations on data sets pulled from public and private sources and builds sophisticated prediction models from petabytes of data.* Medical research systems

* One could, of course, argue that the 2008 credit crunch should have been predicted. The lapse may be the fault of prejudices fed to the programmers, rather than the sophistication of the programs.

analyze DNA for complex patterns of hereditary diseases, predicting entire populations' hereditary probability to inherit genetic traits.

In stark contrast, the information security management programs that are supposed to protect trillions of dollars of assets, keep trade secrets safe from corporate espionage, and hide military plans from the mucky paws of global terrorists are often powered by little more than Rube Goldberg machines (Heath Robinson machines if you are British) fabricated from Excel spreadsheets, Word documents, homegrown scripts, Post-It notes, email systems, notes on the backs of Starbucks cups, and hallway conversations. Is it any wonder we continue to see unprecedented security risk management failures and that most security officers feel they are operating in the dark? If information security is to keep pace (and it will), people, processes, and (the focus of this chapter) information security technology will need to evolve. The Hollywood security that security professionals snigger at today needs to become a reality tomorrow.

I am passionate about playing a part in shaping the security technology of the future, which to me involves defining and creating what I call the “security cogs of tomorrow.” This chapter discusses technology trends that I believe will have a significant influence over the security industry and explores how they can be embraced to build information security risk management systems that will help us to do things faster, better, and more cheaply than we can today. We can slice and dice technology a million ways, but advances usually boil down to those three things: faster, better, and cheaper.

I have arranged this chapter into a few core topics:

- “Cloud Computing and Web Services: The Single Machine Is Here” on page 150
- “Connecting People, Process, and Technology: The Potential for Business Process Management” on page 154
- “Social Networking: When People Start Communicating, Big Things Change” on page 158
- “Information Security Economics: Supercrunching and the New Rules of the Grid” on page 162
- “Platforms of the Long-Tail Variety: Why the Future Will Be Different for Us All” on page 165

Before I get into my narrative, let me share a few quick words said by Upton Sinclair and quoted effectively by Al Gore in his awareness campaign for climate change, *An Inconvenient Truth*, and which I put on a slide to start my public speaking events:

It's difficult to get a man to understand something when his salary depends on him not understanding it.

Challenging listeners to question the reason why they are being presented ideas serves as a timely reminder of common, subtle bias for thoughts and ideas presented as fact. For transparency, at this time of writing I work for Microsoft. My team, the Connected Information

Security Group, has a long-term focus of advancing many of the themes discussed here. This chapter represents just my perspective—maybe my bias—but my team’s performance depends on how closely the future measures up to the thoughts in this chapter!

Cloud Computing and Web Services: The Single Machine Is Here

Civilization advances by extending the number of important operations which we can perform without thinking of them.

—Alfred North Whitehead
An Introduction to Mathematics (1911)

Today, much is being made of “cloud computing” in the press. For at least the past five years, the computer industry has also expressed a lot of excitement about web services, which can range from Software as a Service (SaaS) to various web-based APIs and service-oriented architecture (SOA, pronounced “so-ah”).

Cloud computing is really nothing more than the abstraction of computing infrastructure (be it storage, processing power, or application hosting) from the hardware system or users. Just as you don’t know where your photo is stored physically after you upload it to Flickr, you can run an entire business on a service that is free to run it on any system it chooses. Thus, part or all of the software runs somewhere “in the cloud.” The system components and the system users don’t need to know and frankly don’t care where the actual machines are located or where the data physically resides. They care about the functionality of the system instead of the infrastructure that makes it possible, in the same way that average telephone users don’t care which exchanges they are routed through or what type of cable the signal travels over in order to talk to their nanas.

But even though cloud computing is a natural extension of other kinds of online services and hosting services, it’s an extremely important development in the history of the global network. Cloud computing democratizes the availability of computing power to software creators from virtually all backgrounds, giving them supercomputers on-demand that can power ideas into reality. Some may say this is a return to the old days when all users could schedule time on the mainframe and that cloud computing is nothing new, but that’s hardly the point. The point is that this very day, supercomputers are available to anyone who has access to the Internet.

Web services are standards-based architectures that expose resources (typically discrete pieces of application functionality) independently of the infrastructure that powers them. Web services allow many sites to integrate their applications and data economically by exposing functionality in standards-based formats and public APIs. SOAs are sets of web services woven together to provide sets of functionality and are the catalyst that is allowing us to connect (in the old days we may have said “wire together”) powerful computing infrastructure with software functionality, data, and users.

I'm not among the skeptics who minimize the impact of cloud computing or web services. I believe they will serve up a paradigm shift that will fundamentally change the way we all think about and use the Internet as we know it today. In no area will that have effects more profound than in security—and it is producing a contentious split in the security community.

Builders Versus Breakers

Security people fall into two main categories:

- Builders usually represent the glass as half full. While recognizing the seriousness of vulnerabilities and dangers in current practice, they are generally optimistic people who believe that by advancing the state they can change the world for the better.
- Breakers usually represent the glass as half empty, and are often so pessimistic that you wonder, when listening to some of them, why the Internet hasn't totally collapsed already and why any of us have money left unpilfered in our bank accounts. Their pessimism leads them to apply the current state of the art to exposing weaknesses and failures in current approaches.

Every few years the next big thing comes along and polarizes security people into these two philosophical camps. I think I hardly need to state that I consider myself a builder.

Virtual digital clouds of massive computing power, along with virtual pipes to suck it down and spit it back out (web services), trigger suspicions that breakers have built up through decades of experience. Hover around the water coolers of the security "old school," and you will likely see smug grins and knowing winks as they utter pat phrases such as, "You can't secure what you don't control," "You can't patch a data center you don't own," and the ultimate in cynicism, "Why would you trust something as important as security to someone else?"

I've heard it all, and of course it's all hard to argue against. These are many valid arguments against hosting and processing data in the cloud, but by applying standard arguments for older technologies, breakers forget a critical human trait that has been present throughout history: when benefits outweigh drawbacks, things almost always succeed. With the economic advantages of scalable resources on demand, the technological advantages of access to almost unlimited computing resources, and the well-documented trend of service industries, from restaurants to banking, that provide commodity goods, the benefits of cloud computing simply far outweigh the drawbacks.

One reason I deeply understand the breaker mentality springs from a section of my own career. In 2002, I joined a vulnerability management firm named Foundstone (now owned by McAfee) that sold a network vulnerability scanner. It ran as a client in the traditional model, storing all data locally on the customer's system. Our main competitor, a company called Qualys, offered a network scanner as a service on their own systems with data stored centrally at their facilities. We won customers to our product by positioning hosted security data as an

outrageous risk. Frankly, we promoted FUD (Fear, Uncertainty, and Doubt). Most customers at the time agreed, and it became a key differentiator that drove revenue and helped us sell the company to McAfee. My time at Foundstone was among the most rewarding I have had, but I also feel, looking back, that our timing was incredibly fortunate. Those inside the dust storm watched the cultural sands shift in a few short years, and we found more and more customers not only accepting an online model but demanding it.

The same is true of general consumers, of course. Over five million WordPress blog users have already voted with their virtual feet, hosting their blogs online. And an estimated 10% of the world's end-user Internet traffic comes from hosted, web-based email, such as Yahoo! Mail, Gmail, and Live Mail. Google is renowned for building megalithic data centers across the world; Microsoft is investing heavily in a cloud operating system called Azure, along with gigantic data center infrastructures to host software and services; and Amazon has started renting out parts of the infrastructure that they built as part of their own bid to dominate the online retailing space.

Clouds and Web Services to the Rescue

The question security professionals should be asking is not “Can cloud computing and web services be made secure?” but “How can we apply security to this new approach?” Even more cleverly, we should think: “How can we embrace this paradigm to our advantage?”

The good news is that applying security to web services and cloud computing is not as hard as people may think. What at first seems like a daunting task just requires a change of paradigm. The assumption that the company providing you with a service also has to guarantee your security is just not valid.

To show you how readily you can see the new services as a boon to security instead of a threat, let me focus on a real-world scenario. Over Christmas I installed a nice new Windows Home Server in our house. Suddenly, we are immersed in the digital world: our thousands of photos and videos of the kids can be watched on the TV in the living room via the Xbox, the six computers scattered around the house all get backed up to a central server, and the family at home once again feels connected. Backing up to a central server is all well and good, but what happens if we get robbed and someone steals the PCs and the server?

Enter the new world of web services and cloud computing. To mitigate the risk of catastrophic system loss, I wrote a simple plug-in (see the later section “Platforms of the Long-Tail Variety: Why the Future Will Be Different for Us All” on page 165) to the home server that makes use of the Amazon Web Services platform. At set intervals, the system copies the directories I chose onto the server and connects via web services to Amazon's S3 (Simple Storage System) cloud infrastructure. The server sends a backup copy of the data I choose to the cloud. I make use of the WS-Security specification (and a few others) for web services, ensuring the data is encrypted and not tampered with in transport, and I make use of an X.509 digital certificate to ensure I am communicating with Amazon. To further protect the data, I encrypt it locally

before it is sent to Amazon, ensuring that if Amazon is hacked, my data will not be exposed or altered. The whole solution took 30 minutes to knock up, thanks to some reusable open source code on the Internet.

So, storing your personal data on someone else's server seems scary at first, but when you think it through and apply well-known practices to new patterns, you realize that the change is not as radical as you first thought. The water cooler conversations about not being able to control security on physical servers located outside your control may be correct, but the solution is to apply security at a different point in the system.

It is also worth pointing out that the notion of using services from other computers is hardly new. We all use DNS services from someone else's servers every day. When we get over the initial shock of disruptive technologies (and leave the breaker's pessimism behind), we can move on to the important discussions about cloud computing and web services, and embrace what we can now do with these technologies.

A New Dawn

In a later section of this chapter, I discuss *supercrunching*, a term used to describe massive analysis of large sets of data to derive meaning. I think supercrunching has a significant part to play in tomorrow's systems. Today we are bound by the accepted limitations of local storage and local processing, often more than we think; if we can learn to attack our problems on the fantastically larger scale allowed by Internet-connected services, we can achieve new successes.

This principle can reap benefits in security monitoring, taking us beyond the question of how to preserve the security we had outside the cloud and turning the cloud into a source of innovation for security.

Event logs can provide an incredible amount of forensic information, allowing us to reconstruct an event. The question may be as simple as which user reset a specific account password or as complex as which system process read a user's token. Today there are, of course, log analysis tools and even a whole category of security tools called Security Event Managers (SEMs), but these don't even begin to approach the capabilities of supercrunching. Current tools run on standard servers with pretty much standard hardware performing relatively crude analysis.

A few short years ago I remember being proud of a system I helped build while working for a big financial services company in San Francisco; the system had a terabyte of data storage and some beefy Sun hardware. We thought we were cutting-edge, and at the time we were! But the power and storage that is now available to us all if we embrace the new connected computing model will let us store vast amounts of security monitoring data for analysis and use the vast amounts of processing power to perform complex analysis.

We will then be able to look for patterns and derive meaning from large data sets to *predict* security events rather than *react* to them. You read that correctly: we will be able to predict

from a certain event the probability of a tertiary event taking place. This will allow us to provide context-sensitive security or make informed decisions about measures to head off trouble.

In a later section of this chapter (“Social Networking: When People Start Communicating, Big Things Change” on page 158), I discuss social networking. Social networking will have a profound impact on security when people start to cooperate efficiently. Sharing the logfiles I mentioned earlier with peers will enable larger data sets to be analyzed and more accurate predictions to be made.

It’s also worth noting that a cloud service is independent from any of the participating parties, and therefore can be a neutral and disinterested facilitator. For a long time, companies have been able to partition their network to allow limited access to trusted third parties, or provide a proxy facility accessible to both parties. This practice was not lost on the plethora of folks trying to compete for the lucrative and crucial identity management area. Identity management services such as OpenID and Windows Live ID operate in the cloud, allowing them to bind users together across domains.

Connecting People, Process, and Technology: The Potential for Business Process Management

Virtually every company will be going out and empowering their workers with a certain set of tools, and the big difference in how much value is received from that will be how much the company steps back and really thinks through their business processes, thinking through how their business can change, how their project management, their customer feedback, their planning cycles can be quite different than they ever were before.

—Bill Gates

New York Times columnist Thomas Friedman wrote an excellent book in 2005 called *The World Is Flat* (Farrar, Straus and Giroux) in which he explored the outsourcing revolution, from call centers in India and tax form processing in China to radiography analysis in Australia. I live Friedman’s flat world today; in fact, I am sitting on a plane to Hyderabad to visit part of my development team as I write this text. My current team is based in the United States (Redmond), Europe (London and Munich), India (Hyderabad), and China (Beijing). There’s a lot of media attention today on the rise of skilled labor in China and India providing goods and services to the Western world, but when you look back at history, the phenomenon is really nothing new. Friedman’s book reveals that there has been a shift in world economic power about every 500 years throughout history, and that shift has always been catalyzed by an increase in trading.

And furthermore, what has stimulated that increase in trading? It's simple: connectivity and communication. From the Silk Road across China to the dark fiber heading out of Silicon Valley, the fundamental principle of connecting supply and demand and exchanging goods and services continues to flourish. What's interesting (Friedman goes on to say) is that in today's world workflow software has been a key "flattener," meaning that the ability to route electronic data across the Internet has enabled and accelerated these particular global market shifts (in this case, in services). Workflow software—or more accurately, Business Process Management (BPM) software, a combination of workflow design, orchestration, business rules engines, and business activity monitoring tools—will dramatically change both the ways we need to view the security of modern business software and how we approach information security management itself.

Diffuse Security in a Diffuse World

In a flat world, workforces are decentralized. Instead of being physically connected in offices or factories as in the industrial revolution, teams are combined onto projects, and in many cases individuals combined into teams, over the Internet.

Many security principles are based on the notion of a physical office or a physical or logical network. Some technologies (such as popular file-sharing protocols such as Common Internet File System [CIFS] and LAN-based synchronization protocols such as Address Resolution Protocol [ARP]) take this local environment for granted. But those foundations become irrelevant as tasks, messages, and data travel a mesh of loosely coupled nodes.

The effect is similar to the effects of global commerce, which takes away the advantage of renting storefront property on your town's busy Main Street or opening a bank office near a busy seaport or railway station. Tasks are routed by sophisticated business rules engines that determine whether a call center message should be routed to India or China, or whether the cheapest supplier for a particular good has the inventory in stock.

BPM software changes the very composition of supply chains, providing the ability to dynamically reconfigure a supply chain based on dynamic business conditions. Business transactions take place across many companies under conditions ranging from microseconds to many years. Business processes are commonly dehydrated and rehydrated as technologies evolve to automatically discover new services. The complexity and impact of this way of working will only increase.

For information security, of course, this brings significant new challenges. Over thousands of years, humans have associated security with physical location. They have climbed hills, built castles with big walls, and surrounded themselves with moats. They have worked in office buildings where there are physical controls on doors and filing cabinets, put their money in bank vaults (that seems so quaint nowadays), and locked their dossiers (including the ones on computers) in their offices or data centers. Internet security carried over this notion with firewalls and packet filters inspecting traffic as it crossed a common gateway.

Today, groups such as the Jericho Forum are championing of the idea of “deperimeterization” as companies struggle to deal with evolving business models. A company today is rarely made up of full-time employees that sit in the same physical location and are bound by the same rules. Companies today are collaborations of employees, business partners, outsourcing companies, temporary contractors (sometimes called “perma-vendors”), and any number of other unique arrangements you can think of. They’re in Beijing, Bangalore, Manhattan, and the Philippines. They are bound by different laws, cultures, politics, and, of course, real and perceived security exigencies. The corporate firewall no longer necessarily protects the PC that’s logged into the corporate network and also, incidentally, playing *World of Warcraft* 24/7. Indeed, the notion of a corporate network itself is being eroded by applications that are forging their own application networks connected via web services and messaging systems through service-oriented architectures.

When a company’s intellectual property and business data flow across such diverse boundaries and through systems that are beyond their own security control, it opens up a whole new world of problems and complexity. We can no longer have any degree of confidence that the security controls we afford our own security program are effective for the agent in a remote Indian village. Paper contracts requiring vendors to install the latest anti-malware software is of little comfort after the botnet was activated from Bulgaria, bringing the key logger alive and altering the integrity of the system’s processing. Never has the phrase “security is as only good as the weakest link” been more apt, and systems architects are being forced to operate on the premise that the weakest link can be very weak indeed.

BPM As a Guide to Multisite Security

Despite these obvious concerns, I believe the same technologies and business techniques encompassed by the term BPM will play a critical role in managing information security in the future.

For example, if we examine today’s common information security process of vulnerability management, we can easily imagine a world where a scalable system defines the business process and parcels various parts of it off to the person or company that can do it faster, better, or more cheaply. If we break a typical vulnerability management process down, we can imagine it as a sequence of steps (viewed simplistically here for illustrative purposes, of course), such as the analysis of vulnerability research, the analysis of a company’s own data and systems to determine risk, and eventual management actions, such as remediation.

Already today, many companies outsource the vulnerability research to the likes of iDefense (now a VeriSign company) or Secunia, who provide a data feed via XML that can be used by corporate analysts. When security BPM software (and a global network to support it) emerges, companies will be able to outsource this step not just to a single company, in the hope that it has the necessary skills to provide the appropriate analysis, but to a global network of analysts. The BPM software will be able to route a task to an analyst who has a track record in a specific

obscure technology (the best guy in the world at hacking system X or understanding language Y) or a company that can return an analysis within a specific time period. The analysts may be in a shack on a beach in the Maldives or in an office in London; it's largely irrelevant, unless working hours and time zones are decision criteria.

Business rules engines may analyze asset management systems and decide to take an analysis query that comes in from San Francisco and route it to China so it can be processed overnight and produce an answer for the corporate analysts first thing in the morning.

This same fundamental change to the business process of security research will likely be extended to the intelligence feeds powering security technology, such as anti-virus engines, intrusion detection systems, and code review scanners. BPM software will be able to facilitate new business models, microchunking business processes to deliver the end solution faster, better, or more cheaply. This is potentially a major paradigm shift in many of the security technologies we have come to accept, decoupling the content from the delivery mechanism. In the future, thanks to BPM software security, analysts will be able to select the best anti-virus engine and the best analysis feed to fuel it—but they will probably not come from the same vendor.

When Nicholas Carr wrote *Does IT Matter?*,[†] he argued that technology needs to be realigned to support business instead of driving it. BPM is not rocket science (although it may include rocket science in its future), but it's doing just that: realigning technology to support the business. In addition to offering radical improvements to information security by opening new markets, BPM can deliver even more powerful changes through its effects on the evolution of the science behind security. The Business Process Management Initiative (BPMI) (<http://www.bpmi.org>) has defined five tenets of effective BPM programs. These tenets are unrelated to information security, but read as a powerful catalyst. I'll list each tenet along with what I see as its most important potential effects on security:

1. Understand and Document the Process
Security effect: Implement a structured and effective information security program
2. Understand Metrics and Objectives
Security effect: Understand success criteria and track their effectiveness
3. Model and Automate Process
Security effect: Improve efficiency and reduce cost
4. Understand Operations and Implement Controls
Security effect: Improve efficiency and reduce cost
Security effect: Fast and accurate compliance and audit data (visibility)
5. Optimize and Improve

[†] *Does IT Matter?*, Nicholas Carr, Harvard Business School Press, 2004.

Security effect: Do more with less

Security effect: Reduce cost

Put another way: if you understand and document your process, metrics, and objectives; model and automate your process; understand and implement your process; and optimize and improve the process, you will implement a structured and effective information security program, understand the success criteria and track effectiveness, improve efficiency and reduce cost, produce fast and accurate compliance, audit data, and ultimately do more with less and reduce the cost of security. This is significant!

While the topic of BPM for information security could of course fill a whole book—when you consider business process modeling, orchestration, business rules design, and business activity modeling—it would be remiss to leave the subject without touching upon the potential BPM technologies have for simulation. When you understand a process, including its activities, process flows, and business rules, you have a powerful blueprint describing how something should work. When you capture business activity data from real-world orchestrations of this process, you have powerful data about how it actually works.

Simulation offers us the ability to alter constraints and simulate results before we spend huge resources and time. Take for example a security incident response process in which simulation software predicts the results of a certain number or type of incidents. We could predict failure or success based on facts about processes, and then change the constraints of the actual business to obtain better results. Simulation can take place in real time, helping avoid situations that a human would be unlikely to be able to predict. I believe that business process simulation will emerge as a powerful technique to allow companies to do things better, faster, and more cheaply. Now think about the possibilities of BPM when connected to social networks, and read on!

Social Networking: When People Start Communicating, Big Things Change

Human beings who are almost unique (among animals) in having the ability to learn from the experience of others, yet are also remarkable in their apparent disinclination to do so.

—Douglas Adams

One night at sea, Horatio Hornblower, the fictional character from C. S. Forester's series of novels, is woken up by his first officer, who is alarmed to see a ship's light in his sea lane about 20 miles away, refusing to move. Horatio quickly joins the deck and commands the ship via radio communications to move starboard 20 degrees at once. The operator refuses and indignantly tells 1st Baron Horatio that it is he who should be moving his ship starboard 20 degrees at once. Incensed and enraged, Horatio Hornblower pulls rank and size on the other

ship, stating that he's a captain and that he's on a large battleship. Quietly and calmly, the operator replies, informing Captain Hornblower that his is in fact the biggest vessel, being a lighthouse on a cliff above treacherous rocks.

Each time I tell this story, it reminds me just how badly humans communicate. We are all guilty, yet communication is crucial to everything we do. When people communicate, they find common interests and form relationships.

Social networking is considered to be at the heart of Web 2.0 (a nebulous term that describes the next generation of Internet applications), yet it is really nothing new. Throughout history people have lived in tribes, clans, and communities that share a bond of race, religion, and social or economic values, and at every point, when social groups have been able to connect more easily, big things have happened. Trading increases, ideas spread, and new social, political, and economic models form.

I started a social network accidentally in 2001 called the Open Web Application Security Project (OWASP) (<http://www.owasp.org>). We initially used an email distribution list and a static website to communicate and collaborate. In the early days, the project grew at a steady rate. But it was only late in 2003, when a wiki was introduced and everyone could easily collaborate, that things really took off. Today the work of OWASP is recommended by the Federal Trade Commission, the National Institute for Standards, and the hotly debated Payment Card Industry Data Security Standard, or PCI-DSS. I learned many valuable life lessons starting OWASP, but none bigger than the importance of the type of social networking technology you use.‡

The State of the Art and the Potential in Social Networking

Today Facebook and MySpace are often held up as the leading edge of social networking software that brings together people who share a personal bond. People across the world can supposedly keep in touch better than they could before it was created. The sites are certainly prospering, with megalevels of subscribers (250 million+ users each) and their media darling status. But in my observations, the vast majority of their users spend their time digitally “poking” their friends or sending them fish for their digital aquariums. To the older kids like me, this is a bit like rock ‘n’ roll to our parents’ parents—we just don’t get it—but I am ready to accept I am just getting old.

Equally intriguing are social networks forming in virtual worlds such as Second Life. With their own virtual economy, including inflation-capped monetary systems, the ability to exchange real-world money for virtual money, and a thriving virtual real estate market, Second Life has attracted a lot of interest from big companies like IBM. Recently, researchers were able to teleport an avatar from one virtual world to another, and initiatives such as the OpenSocial

‡ I can't take credit for starting the wiki (Jeff Williams can); on the contrary, I actually opposed it because I thought it was unstructured and would lead to a deterioration in content quality. I learned a good lesson.

API indicate that interoperability of social networks is evolving. Networks of networks are soon to emerge!

Social networking platforms like these really offer little for corporations today, let alone for security professionals, but this will change. And when it changes, the implications for information security could be significant.

If social networking today is about people-to-people networking, social networking tomorrow may well be about business-to-business. For several years, investment banks in New York, government departments in the U.S., and other industry groups have shared statistical data about security among themselves in small private social networks. The intelligence community and various police forces make sensitive data available to those who “need to know,” and ad hoc networks have formed all over the world to serve more specific purposes. But in the grand scheme of things, business-to-business social networking is very limited. Information security is rarely a competitive advantage (in fact, studies of stock price trends after companies have suffered serious data breaches indicate a surprisingly low correlation, so one could argue that it’s not a disadvantage at all), and most businesses recognize that the advantages in collaborating far outweigh the perceived or real disadvantages.

This still begs the question, “Why isn’t social networking more prevalent?” I would argue that it’s largely because the right software is lacking. We know that humans don’t communicate well online without help, and we can cite cases such as the catalytic point when OWASP moved to a wiki and theorize that when the right type of social networking technology is developed and introduced, behavior similar to what we have seen throughout history will happen.

Social Networking for the Security Industry

What this may look like for the security industry is hard to predict, but if we extrapolate today’s successful social networking phenomenon to the security industry, some useful scenarios emerge.

Start with the principle of reliability behind eBay, for instance, a highly successful auction site connecting individual sellers to individual buyers across the globe. Its success is based partially on a reputation economy, where community feedback about sellers largely dictates the level of trust a buyer has in connecting.

Now imagine a business-to-business eBay-type site that deals in information security. It could list “security services wanted” ads, allowing companies to offer up service contracts and the criteria for a match, and allow service providers to bid for work based on public ratings and credentials earned from performing similar work for similar clients.

eBay-type systems not only act as conduits to connect buyers and sellers directly, but potentially can provide a central data of market information on which others can trade. Take, for example, security software. How much should you pay for a license for the next big security source code scanning technology to check your 12 million lines of code? In the future, you

may be able to consult the global database and discover that other companies like you paid an average of X .

In order for these types of social networks to succeed, they will likely have to operate on a “pay to play” model. It will be a challenge to seed them with enough data to make them enticing enough to play at the beginning, but I have no doubt the networks will emerge. Virus writers in Eastern Europe and China have long traded techniques via old-school bulletin boards, and we are starting to see the first stages of exploit exchanges and even an exploit auction site. Why shouldn't the white hats take advantage of the same powerful networks?

Actually, large social networks of security geeks already exist. They typically use email distribution lists, a surprisingly old-school, yet effective, means of communication.

Before the 2008 Black Hat Conference, a U.S.-based “researcher” named Dan Kaminsky announced he was going to discuss details of a serious vulnerability in DNS. Within days, mailing lists such as “Daily Dave” were collaborating to speculate about what the exploit was and even share code. Imagine the effectiveness of a more professional social network where security engineers could share empirical data and results from tests and experiments.

Security in Numbers

Social networking isn't just about connecting people into groups to trade. It's a medium for crowdsourcing, which exploits the wisdom of crowds to predict information. This could also play an interesting role in the future security market.

To give you a simple example of crowdsourcing, one Friday at work someone on my team sent out a simple spreadsheet containing a quiz. It was late morning on the East Coast, and therefore late on Friday afternoon in Europe and late evening in our Hyderabad office. Most people on the team were in Redmond and so were sitting in traffic; most Brits were getting ready to drink beer and eat curry on Friday evening; and most Indians were out celebrating life. Here are the stats of what happened in the next 50 minutes:

- Request started at 11:07 AM EST
- Crowd size of 70+ across multiple time zones
- Active listening crowd of probably less than 30 due to time zone differences
- Participation from 8
- Total puzzles = 30
- Initial unsolved puzzles = 21
- Total responses = 35
- Total time taken to complete all puzzles = 50 minutes

The brain is still the most powerful computer created (as of today), and when we build distributed networks of such powerful computers, we can expect great results. Networks can

support evolving peer groups who wish to share noncompetitive information in a sheltered network. For social networking to be truly useful to the security industry, it will likely need to develop a few killer applications. My money is on the mass collection, sharing, and analysis of information and benchmarking. Participants can run benchmarks of service quality in relation to software cost, corporate vulnerabilities, and threat profiles. The potential scope is enormous, as shown through the MeMe map in Figure 9-1, taken from a security industry source.

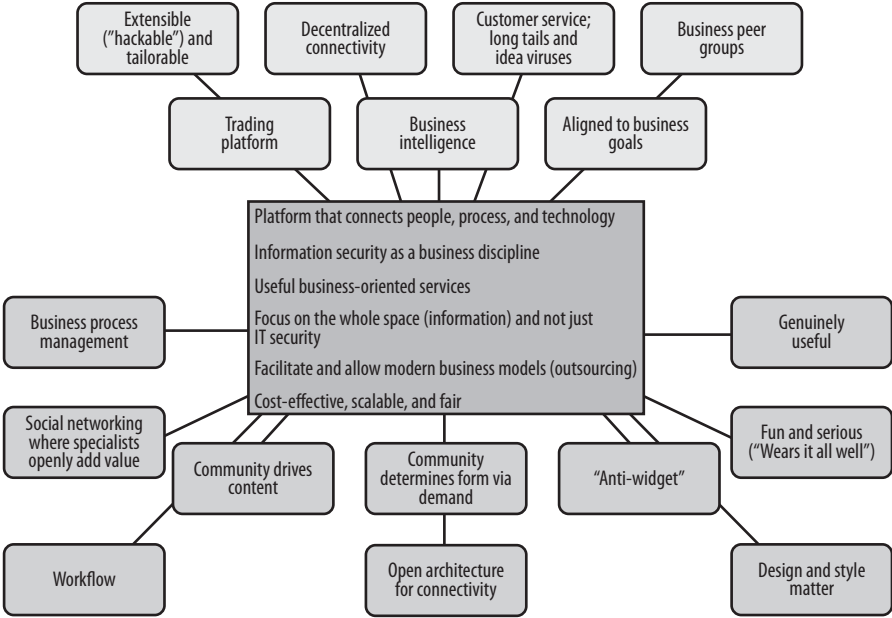


FIGURE 9-1. Possibilities of social networking for security professionals

Information Security Economics: Supercrunching and the New Rules of the Grid

Curphey turned to his friend Jeff Cave in an investment bank server room in London in the late '90s and said, "What's the time?" Cave replied, "Quite simply the measurement of distance in space, dear chap."

Scene 1: Imagine you are picnicking by a river and you notice someone in distress in the water. You jump in and pull the person out. The mayor is nearby and pins a medal on you. You return to your picnic. A few minutes later, you spy a second person in the water. You perform a second rescue and receive a second medal. A few minutes later, a third person, a third rescue, and a third medal, and so on through the day. By sunset, you are weighed down with medals and honors. You are a local hero! Of course, somewhere in the back of your mind there is a sneaking

suspicion that you should have walked upriver to find out why people were falling in all day—but then again, that wouldn't have earned you as many awards.

Scene 2: Imagine you are a software tester. You find a bug. Your manager is nearby and pins a “bug-finder” award on you. A few minutes later, you find a second bug, and so on. By the end of the day, you are weighed down with “bug-finder” awards and all your colleagues are congratulating you. You are a hero! Of course, the thought enters your mind that maybe you should help prevent those bugs from getting into the system—but you squash it. After all, bug prevention doesn't win nearly as many awards as bug hunting.

Simply put: *what you measure is what you get*. B. F. Skinner told us 50 years ago that rats and people tend to perform those actions for which they are rewarded. It's still true today. As soon as developers find out that a metric is being used to evaluate them, they strive mightily to improve their performance relative to that metric—even if their actions don't actually help the project. If your testers find out that you value finding bugs, you will end up with a team of bug-finders. If prevention is not valued, prevention will not be practiced. The same is of course true of many other security disciplines, such as tracking incidents, vulnerabilities, and intrusions.

Metrics and measurement for information security has become a trendy topic in recent years, although hardly a new one. Peter Drucker's famous dictum, “If you can't measure it, you can't manage it,” just sounds like common sense and has been touted by good security managers as long as I can remember.

Determining the Return on Investment (ROI) for security practices has become something of a Holy Grail, sought by security experts in an attempt to appeal to the managers of firms (all of whom have read Drucker or absorbed similar ideas through exposure to their peers). The problem with ROI is that security is in one respect like gold mining. You find an enormous variance in the success rates of different miners (one could finish a season as a millionaire while another is still living in a shack 20 years later), but their successes cannot be attributed to their tools. Metrics about shovels and shifters will only confuse you. In short, ROI measures have trouble computing return on these kinds of high-risk investments. In my opinion, security ROI today is touted by shovel salesmen.

I have high hopes for metrics, but I think the current mania fails to appreciate the subtleties we need to understand. I prefer the term Economics to Metrics or Measurement, and I think that Information Security Economics will emerge as a discipline that could have a profound impact on how we manage risk.

Information Security Economics is about understanding the factors and relationships that affect security at a micro and macro level, a topic that has tremendous depth and could have a tremendous impact. If we compare the best efforts happening in the security industry today against the complex supercrunching in financial or insurance markets, we may be somewhat disillusioned, yet the same advanced techniques and technology can probably be applied to the new security discipline with equally effective results.

I recently read a wonderful story in the book *Super Crunchers: Why Thinking-by-Numbers Is the New Way to Be Smart* by Ian Ayres (Bantam Press) about a wine economist called Orley Ashenfelter. Ashenfelter is a statistician at Princeton who loves wine but is perplexed by the pomp and circumstance around valuing and rating wine in much the same way I am perplexed by the pomp and circumstance surrounding risk management today. In the 1980s, wine critics dominated the market with predictions based on their own reputations, palate, and frankly very little more. Ashenfelter, in contrast, studied the Bordeaux region of France and developed a statistic model about the quality of wine.

His model was based on the average rainfall in the winter before the growing season (the rain that makes the grapes plump) and the average sunshine during the growing season (the rays that make the grapes ripe), resulting in simple formula:

$$\begin{aligned} \text{quality} = & 12.145 + (0.00117 * \text{winter rainfall}) \\ & + (0.0614 * \text{average growing season temperature}) \\ & (0.00386 * \text{harvest rainfall}) \end{aligned}$$

Of course he was chastised and lampooned by the stuffy wine critics who dominated the industry, but after several years of producing valuable results, his methods are now widely accepted as providing important valuation criteria for wine. In fact, as it turned out, the same techniques were used by the French in the late 19th century during a wine census.

It's clear that from understanding the factors that affect an outcome, we can build economic models. And the same principles—applying sound economic models based on science—can be applied to many information security areas.

For the field of security, the most salient aspect of Orley Ashenfelter's work is the timing of his information. Most wine has to age for at least 18 months before you can taste it to ascertain its quality. This is of course a problem for both vineyards and investors. But with Ashenfelter's formula, you can predict the wine's quality on the day the grapes are harvested. This approach could be applied in security to answer simple questions such as, "If I train the software developers by X amount, how will that affect the security of the resulting system?" or "If we deploy this system in the country Hackistanovia with the following factors, what will be the resulting system characteristics?"

Of course, we can use this sort of security economics only if we have a suitably large set of prior data to crunch in the first place, as Ashenfelter did. The current phase, where the field is adopting metrics and measurement may be generating the data, and the upcoming supercrunching phase will be able to analyze it, but social networking will probably be the catalyst to prompt practitioners to share resources and create vast data warehouses from which we can analyze information and build models. Security economics may well provide a platform on which companies can demonstrate the cost-benefit ratios of various kinds of security and derive a competitive advantage implementing them.

Platforms of the Long-Tail Variety: Why the Future Will Be Different for Us All

A “platform” is a system that can be programmed and therefore customized by outside developers—users—and in that way, adapted to countless needs and niches that the platform’s original developers could not have possibly contemplated, much less had time to accommodate.

—Marc Andreessen, founder of Netscape

In October 2004, Chris Anderson, the editor in chief of the popular *Wired Magazine*, wrote an article about technology economics.[§] The article spawned a book called *The Long Tail* (Hyperion) that attempts to explain economic phenomena in the digital age and provide insight into opportunities for future product and service strategies.

The theory suggests that the distribution curve for products and services is altering to a skewed shape that concentrates a large portion of the demand in a “long tail”: many different products or service offerings that each enjoy a small consumer base. In many industries, there is a greater total demand for products and services the industries consider to be “niches” than for the products and services considered to be mainstays. Companies that exploit niche products and services previously thought to be uneconomical include iTunes, WordPress, YouTube, Facebook, and many other Internet economy trends.

I fundamentally believe that information security is a long-tail market, and I offer three criteria to support this statement:

- Every business has multiple processes.
- Processes that are similar in name between businesses are actually highly customized (i.e., no two businesses are the same).
- Many processes are unique to small clusters of users.

To understand the possible implications of the long-tail theory for the information security industry, we can look to other long-tail markets and three key forces that drive change.

Democratization of Tools for Production

A long time ago, I stopped reading articles in the popular technology press (especially the security press). I sense that these journals generally write articles with the goal of selling more advertising, while bloggers generally write articles so people will read them. That is a subtle but important difference. If I read an article in the press, chances are that it includes commentary from a so-called “industry insider.” Usually, these are people who tell the reporter

[§] See <http://www.wired.com/wired/archive/12.10/tail.html>.

what they want to hear to get their names in print, and they're rarely the people I trust and want to hear from. I read blogs because I listen to individuals with honest opinions. This trend is, of course, prevalent throughout the new economy and will become more and more important to information security. A practitioner at the heart of the industry is better at reporting (more knowledgeable and more in tune) than an observer.

Much as blogging tools have democratized publishing and GarageBand has democratized music production, tools will democratize information security. In fact, blogging has already had a significant effect, allowing thousands of security professionals to offer opinions and data.

The most far-reaching change will be the evolution of tools into *platforms*. In software terms, a platform is a system that can be reprogrammed and therefore customized by outside developers and users for countless needs and niches that the platform's original developers could not have possibly contemplated, much less had time to accommodate. (This is the point behind the Andreessen quote that started this section.) When Google offered an API to access its search and mapping capabilities, it drove the service to a new level of use; the same occurred when Facebook offered a plug-in facility for applications.

As I'll describe in the following section, a security platform will allow people to build the tools they want to solve the problems they are facing.

When we talk about platforms, we of course need to be careful. Any term that has the potential to sell more technology is hijacked by the media and its essence often becomes diluted. Quite a few tools are already advertised as security platforms, but few really are.

Democratization of Channels for Distribution

There's no shortage of security information. Mailing lists, BBSs (yes, I am old), blogs, and community sites abound, along with professionally authored content. There's also no shortage of technology, both open source and commercial. But in today's economy, making information relevant is paramount, and is one of the key reasons for the success of Google, iTunes, and Amazon.com. Their rise has been attributed largely to their ability to aggregate massive amounts of data and filter it to make it relevant to the user. Filtering and ordering become especially critical in a world that blurs the distinction between what was traditionally called "professionally authored" and "amateur created." This, in essence, is a better information distribution model.

Another characteristic that has democratized distribution in other long-tail markets is *microchunking*, a marketing strategy for delivering to each user exactly the product she wants—and no more. Microchunking also facilitates the use of new channels to reach customers.

The Long Tail uses the example of music, which for a couple decades was delivered in CD form only. These days, delivery options also include online downloads, cell phone ringtones, and materials for remix.

The security field, like much of the rest of the software industry, already offers one type of flexibility: you can install monitoring tools on your own systems or outsource them. In tomorrow's world, security users will also want to remix offerings. They may want the best scanning engine from vendor A combined with the best set of signatures from Vendor B. In Boolean terminology, customers are looking for "And," not "Or."

The underlying consideration for security tools is that one size doesn't fit all. Almost all corporate security people I talk to repeat this theme, sharing their own version for the 80/20 rule: 80% of the tool's behavior meets your requirements, and you live with the 20% that doesn't—but that 20% causes you 80% of your pain!

Let's take threat-modeling tools for software. The key to mass appeal in the future will be to support all types of threat-modeling methodologies, including the users' own twists and tweaks. Overlaying geodata on your own data concerning vulnerabilities and processing the mix with someone else's visualization tools might help you see hotspots in a complex virtual world and distinguish the wood from the trees. These types of overlays may help us make better risk decisions based on business performance data. In an industry with a notoriously high noise-to-signal ratio, we will likely see tools emerge that produce higher signal quality faster, cheaper, and more efficiently than ever before.

Connection of Supply and Demand

Perhaps the biggest changes will take place in how the next generation connects people, process, and technology. Search, ontology (information architecture), and communities will all play important roles.

The advice from *The Long Tail* is this: people will tell you what they like and don't like, so don't try to predict—just measure and respond. Recommendations, reviews, and rankings are key components of what is called the *reputation economy*. These filters help people find things and present them in a contextually useful way.

Few information security tools today attempt to provide contextually useful information. What we will likely see are tools that merge their particular contributions with reputation mechanisms. A code review tool that finds a potential vulnerability may match it to crowdsourced advice, which is itself ranked by the crowd and then provides contextual information like "50% of people who found this vulnerability also had vulnerability X." Ratings and ranking will help connect the mass supply of information with the demand.

To summarize the three trends in the democratization of security tools, I believe that real platforms will emerge in the security field that connect people, processes, and technology. They will be driven by the democratization of tools for production, the democratization of tools for distribution, and the connection of supply and demand. No two businesses are the same, and a true security platform will adapt to solving problems the original designers could have never anticipated.

Conclusion

I was fortunate enough to have been educated by the Information Security Group (<http://isg.rhul.ac.uk>) of Royal Holloway, University of London. They are the best in the business, period. Readers of *The Da Vinci Code* will recognize the name as the school where Sophie Neveu, the French cryptographer in the book, was educated.

Several years before I worked for Microsoft, Professor Fred Piper at the Information Security Group approached me for an opinion on the day that he was to speak at the British Computer Society. He posed to me a straightforward question: “Would Microsoft have been so successful if security was prominent in Windows from day one?” At this point, I should refer you back to my Upton Sinclair quote earlier in this chapter; but it does leave an interesting thought about the role security will have in the overall landscape of information technology evolution.

I was once accused of trivializing the importance of security when I put up a slide at a conference with the text “Security is less important than performance, which is less important than functionality,” followed by a slide with the text “Operational security is a business support function; get over your ego and accept it.” As a security expert, of course, I would never diminish the importance of security; rather, I create better systems by understanding the pressures that other user requirements place on experts and how we have to fit our solutions into place.

I started the chapter by saying that anyone would be foolish to predict the future, but I hope you will agree with me that the next several years in security are an interesting time to think about, and an even more interesting time to influence and shape. I hope that when I look back on this text and my blog in years to come, I’ll cringe at their resemblance to the cocktail-mixing house robots from movies of the 1970s. I believe the right elements are really coming together where technology can create better technology.

Advances in technology have been used to both arm and disarm the planet, to empower and oppress populations, and to attack and defend the global community and all it will have become. The areas I’ve pulled together in this chapter—from business process management, number crunching and statistical modeling, visualization, and long-tail technology—provide fertile ground for security management systems in the future that archive today’s best efforts in the annals of history. At least I hope so, for I hate mediocrity with a passion and I think security management systems today are mediocre at best!

Acknowledgments

This chapter is dedicated to my mother, Margaret Curphey, who passed away after an epileptic fit in 2004 at her house in the south of France. When I was growing up (a lot of time frankly off the rails), she always encouraged me to think big and helped me understand that there is nothing in life you can't achieve if you put your mind to it. She made many personal sacrifices that led me to eventually find my calling (albeit later in life than she would have hoped) in the field of information security. She always used to say that it's all good and well thinking big, but you have to do something about it as well. I am on the case, dear. I also, of course, owe a debt of gratitude for the continued support and patience of my wife, Cara, and the young hackers, Jack, Hana, and Gabe.

Numbers

- 3-D Secure protocol
 - account holder domain, 76
 - acquirer domain, 76
 - e-commerce security and, 76–78
 - evaluation of, 77
 - issuer domain, 76
 - transaction process, 76
- 802.11b standard, 51, 52
- 802.11i standard, 51

A

- ABA (American Bar Association), 203
- Access Control Server (ACS), 77
- accountability, 213, 214
- ACS (Access Control Server), 77
- ActionScript, 93
- ad banners (see banner ads)
- Adams, Douglas, 158
- Advanced Monitor System (AMS), 254, 256
- advertising (see online advertising)
- adware (see spyware)
- Aegenis Group, 66
- Agriculture, Department of, 196
- AHS (Authentication History Server), 77
- AI (artificial intelligence), 254, 257
- AllowScriptAccess tag, 94
- Amazon Web Services platform, 152
- Amazon.com, 102
- American Bar Association (ABA), 203
- AMS (Advanced Monitor System), 254, 256
- analyst confirmation traps, 12
- Anderson, Chris, 165
- Andreessen, Marc, 165, 166
- Anna Carroll (barge), 206
- anti-executables, 253
- anti-spyware software
 - evolution of, 251
 - initial implementation, 251
 - intrusive performance, 254
 - strict scrutiny, 252
- anti-virus software
 - diminished effectiveness, 249
 - functional fixation, 15
 - functionality, 232
 - historical review, 248–249
 - honeyclients and, 141
 - intrusive performance, 254
 - malware signature recognition, 251
 - need for new strategies, 248
 - strict scrutiny, 252
 - zero-day exploits and, 252
- Apgar score, 37
- Apgar, Virginia, 37
- Apple Computer, 8
- artificial intelligence (AI), 254, 257
- Ascom-Tech AG, 117
- Ashenfelter, Orley, 164
- Aspect Security, 188
- Atkins, Derek, 119
- ATMs, early security flaws, 36
- attacks (see malicious attacks)
- attribute certificates, 111
- Attrition.org, 55
- authentication
 - 3-D Secure protocol, 77
 - auto-update and, 15
 - CV2 security code, 76
 - e-commerce security, 83, 84
 - federated programs, 210
 - NTLM, 6
 - password security, 7
 - PGP Global Directory and, 127
 - portability of, 85
 - security pitfall in, 71
 - SET protocol, 78
 - WEP support, 52
- Authentication History Server (AHS), 77
- authoritative keys, 123
- authorization

We'd like to hear your suggestions for improving our indexes. Send email to index@oreilly.com.

- 3-D Secure protocol, 77
- e-commerce security, 84
- security pitfall in, 71
- Ayres, Ian, 164
- Azure cloud operating system, 152

B

- B.J.'s Wholesale Club, 50
- backend control systems, 18–20
- backward compatibility
 - LANMAN password encoding, 6
 - learned helplessness and, 2
 - legacy systems, 7
 - PGP issues, 117
- balance in information security, 202–207
- banking industry (see financial institutions)
- banking trojans, 141, 249
- banner ads
 - exploit-laden, 89–92, 143
 - honeyclients and, 143
- banner farms, 98, 99
- Barings Bank security breach, 38–49
- Barnes & Noble, 50
- Bass-O-Matic cipher, 117
- behavioral analytics, 254
- Bell Labs
 - background, 171, 173
 - software development lifecycle, 174–178
- Bellis, Ed, 73–86
- Bernstein, Peter, 33
- Bidzos, Jim, 117, 118
- Biham, Eli, 117
- biometrics, 37–38
- BITS Common Criteria for Software, 193
- Black Hat Conference, 161
- blacklisting, 252, 254
- Blaster virus, 248
- blogging, 166
- BoA Factory site, 65
- Bork, Robert, 241
- Boston Market, 50
- botnets
 - army building software, 67
 - attack infrastructure, 66
 - challenges in detecting, 231
 - client-side vulnerability, 131
 - CPC advertising, 100, 101
 - cyber underground and, 64
 - functionality, 64, 69, 230
 - peer-to-peer structure, 66
- BPM (Business Process Management)
 - levels of effective programs, 157
 - multisite security, 156–158
 - potential for, 154–158
 - supply chain composition and, 155

- BPMI (Business Process Management Initiative), 157
- breaches (see security breaches)
- bridge CAs, 111
- Briggs, Matt, 140
- brute-force attacks, 28, 251
- buffer overflows
 - security vulnerability, 15, 131
 - SQL Slammer worm, 225
- Business Process Management (see BPM)
- Business Process Management Initiative (BPMI), 157
- business rules engines, 157

C

- California AB 1950, 207
- California SB 1386
 - balance in information security, 203–205
 - on data sharing, 36, 38
 - on reporting breaches, 55
 - passage of, 207
- call options, 40
- Callas, Jon, 107–130
- Capture-HPC honeyclient, 138, 145
- CardSystems security breach, 211
- Carnegie Mellon CMMI process, 185
- Carr, Nicholas, 157
- Carter Doctrine, 201
- CAs (see certificate authorities)
- cashiers (cyber underground)
 - defined, 65
 - drop accounts, 70
- CDC (Centers for Disease Control and Prevention), 36
- Center for Internet Security (CIS), 45
- Center for Strategic and International Studies (CSIS), 201
- Centers for Disease Control and Prevention (CDC), 36
- certificate authorities, 112
 - (see also introducers in PGP)
 - certification support, 111
 - DSG support, 203
 - establishing trust relationships, 27
 - hierarchical trust, 109
 - SET requirements, 78
- certificates, 109
 - (see also specific types of certificates)
 - defined, 111
 - revoking, 120–122
 - self-signed, 109
 - verifying, 109
 - Web of Trust support, 113
- certification
 - defined, 111

- OpenPGP colloquialism for, 112
- OpenPGP support, 111
- CFAA (Computer Fraud and Abuse Act), 207
- Charney, Scott, 201
- Chuvakin, Anton, 213–224, 226
- Cigital, 171, 188
- Citi, 79
- CLASP methodology, 187, 188
- click fraud
 - botnet support, 66, 101
 - CPA advertising, 102
 - federal litigation, 102
- client-side vulnerabilities, 133
 - (see also honeyclients)
 - background, 131–132
 - malware exploitation, 15, 132, 141–143
 - naïveté about, 8–9
- Clinton, Bill, 17
- cloud computing
 - applying security to, 152
 - builders versus breakers, 151
 - defined, 150
 - identity management services, 154
- CNCI (Comprehensive National Cybersecurity Initiative), 202
- CNN network, 16
- COBIT regulation, 214
- Code Red virus, 248
- Commerce, Department of, 180
- commercial software (see software acquisition)
- Commission Junction affiliate network, 102
- Commission on Cyber Security for the 44th Presidency, 201
- Common Vulnerabilities and Exposures (CVE) database, 131
- communication
 - cyber underground infrastructure, 65, 66
 - information security and, 207–211
- Comprehensive National Cybersecurity Initiative (CNCI), 202
- Computer Fraud and Abuse Act (CFAA), 207
- confidentiality of data, 85
- confirmation traps
 - defined, 10
 - intelligence analysts, 12
 - overview, 10–11
 - rationalizing capabilities, 13
 - stale threat modeling, 12
- contagion worm exploit, 131
- cookies, stuffed, 102
- cost per action (see CPA advertising)
- cost per click (see CPC advertising)
- Cost Per Thousand Impressions (see CPM advertising)
- COTS (see software acquisition)
- coverage metrics, 46
- CPA advertising
 - functionality, 100
 - inflating costs, 102–103
 - stuffed cookies, 102
- CPC advertising
 - click-fraud detection services, 101
 - functionality, 100–101
 - syndication partnerships, 100
- CPM advertising
 - basis of, 98
 - fraud-prone, 100–103
- credit card information
 - as shared secret, 75–76, 85
 - card associations and, 82
 - checking site authenticity, 26
 - consumers and, 81, 83
 - current market value, 66
 - CV2 security code, 76
 - cyber underground and, 65
 - devaluing data, 71
 - e-commerce security, 73–75
 - financial institutions, 82
 - identity theft, 23–25
 - merchants and service providers, 81, 83
 - PCI protection, 44
 - proposed payment model, 86
 - spyware stealing, 69
 - SQL injection attacks, 69
 - TJX security breach, 50
 - virtual cards, 79
- cross-certification, 111
- cross-site scripting, 188
- crowdsourcing, 161
- Crypto Wars, 118
- CSIS (Center for Strategic and International Studies), 201
- culture, organizational, 200–202
- cumulative trust, 110
- Curphey, Margaret, 169
- Curphey, Mark, 147–169
- CV2 security code, 76
- CVE (Common Vulnerabilities and Exposures) database, 131
- cyber underground
 - attack infrastructure, 66
 - attack methods, 68–70
 - cashiers, 65
 - combating, 71–72
 - communication infrastructure, 65
 - CSI-FBI Study, 63
 - data exchange example, 67
 - fraudsters and attack launchers, 65
 - goals of attacks, 63, 226, 230
 - information dealers, 64

- information sources, 68
- makeup and infrastructure, 64–66
- malware producers, 64
- money laundering and, 70
- payoffs, 66–71
- resource dealers, 64
- Cydoor ad network, 90

D

- Danford, Robert, 144
- Data Encryption Standard (DES), 4
- data integrity, 85
- Data Loss Database (DataLossDB), 36, 55–58
- data responsibility
 - incentive/reward structure, 72
 - social metric for, 72
- data theft
 - as cottage industry, 67
 - botnet support, 66
 - combating, 71
 - from merchant stores, 68
 - incident detection considerations, 237
 - spyware and, 69
- data translucency
 - additional suggestions, 245
 - advantages, 244
 - disadvantages, 245
 - overview, 239–242
 - personal data and, 244
 - real-life example, 243
- data-sharing mechanisms
 - DHS support, 36
 - security flaws in, 35
- databases
 - data translucency in, 239–246
 - logging support, 221
 - security breaches and, 239
- Dave & Buster's, 50
- Davies, Donald, 148
- DCS systems, 18
- DDoS (distributed denial of service)
 - attacks on major ISPs, 16
 - botnet support, 66, 231
 - client-side vulnerability, 131
 - honeyclients and, 138
 - LANs and, 28
- deceptive advertisements, 94–98
- Defense, Department of, 213
- Dell computers, 131
- Deloitte & Touche, LLP, 201
- denial of service (see DDoS)
- Department of Agriculture, 196
- Department of Commerce, 180
- Department of Defense, 213
- Department of Homeland Security, 36

- deperimeterization, 156
- DES (Data Encryption Standard), 4
- designated revokers, 121
- DHCP lease logs, 237
- DHS (Department of Homeland Security), 36
- Diffie, Whitfield, 112
- digital certificates (see certificates)
- Digital Point Systems, 102
- Digital Signature Guidelines (DSG), 202–203
- direct trust
 - defined, 109
 - root certificates, 110
- directionality, 227
- distributed denial of service (see DDoS)
- distribution channels, 166
- DKIM email-authentication, 124
- Dobbertin, Hans, 119
- doing the right thing in information security, 211–212
- drop accounts, 70
- Drucker, Peter, 163
- DSG (Digital Signature Guidelines), 202–203
- DSW Shoe Warehouse, 50
- Dublin City University, 144
- Dunphy, Brian, 225–237
- Durick, J.D., 138
- dynamic testing, 190

E

- e-commerce security
 - 3-D Secure protocol, 76–78
 - analyzing current practices, 74–75
 - authorizing transactions, 84
 - broken incentives, 80–83
 - confidentiality of data, 85
 - consumer authentication, 83
 - data integrity, 85
 - exploiting website vulnerabilities, 68
 - friendly fraud and, 84
 - merchant authentication, 83
 - new security model, 83–86
 - not sharing authentication data, 84
 - portability of authentication, 85
 - primary challenges, 73
 - proposed payment model, 86
 - SET protocol, 78
 - shared secrets and, 75–76, 85
 - virtual cards, 79
- EAP (Extensible Authentication Protocol), 51
- Earned Value Management (EVM), 173
- eBay
 - CPA advertising, 102
 - DDoS attacks on, 16
 - principle of reliability, 160

ECPA (Electronic Communications Privacy Act), 207
Edelman, Benjamin, 89–105, 210, 250
Edwards, Betsy, 178
Einstein, Albert, 147
Electronic Communications Privacy Act (ECPA), 207
email
 log handling, 221
 malware exploits, 248
EMBED tag, 94
encryption
 LAN Manager sequence, 4
 PGP support, 107, 116–120
 security certificates and, 22, 24
 SET support, 78
Encyclopædia Britannica, 94–98
event logs (see logs)
EVM (Earned Value Management), 173
executables, malware exploits and, 143
exportable signatures, 125
extended introducers, 123
Extensible Authentication Protocol (EAP), 51

F

Facebook social network, 159, 165, 166
failing closed, 8
failing open, 8
false negatives, 236
false positives, 217, 236
Federal Sentencing Guidelines, 209
Federal Trade Commission (see FTC)
financial institutions
 banking trojans, 141, 249
 credit card information, 82
 cyber attacks on, 68
 drop accounts, 70
 exploiting website vulnerabilities, 68, 187
 federated authentication programs, 210
 infosecurity and, 208
Finjan security firm, 65
Finney, Hal, 117
firewalls
 energy company vulnerabilities, 18
 host logging, 232
 log handling, 216, 221
 need for new strategies, 248
 SQL Slammer worm, 225
 watch lists, 231
Flash ActionScript, 93
Forester, C. S., 158
Forever 21, 50
forums, online, 250
Foundstone vulnerability management, 151
Francisco, Fernando, 247–258

fraudsters (cyber underground)
 combating, 71
 defined, 65
 information sources, 68
Friedman, Thomas, 154
friendly fraud, 84
FTC (Federal Trade Commission)
 challenging deceptive ads, 96, 97
 deceptive door opener prohibition, 95
 Encyclopædia Britannica and, 95
 exploit-laden banner ads and, 91
 OWASP recommendation, 159
FTP server security breach, 218–221
functional fixation
 costs versus profits examples, 16–20
 defined, 14
 overview, 15
fuzzing technique, 10

G

gaming trojans, 141, 249
Gartner Group, 187
Gates, Bill, 154
Geer, Daniel E., Jr., 34, 35, 60
Geyer, Grant, 225–237
Gibson, Steve, 251
GLBA (Gramm-Leach-Bliley Financial Services Modernization Act), 80, 214
GoDaddy, 109
Gonzalez, Albert, 50
Google
 AdSense service, 104
 CPC advertising, 100, 101
 democratization of production tools, 166
 false ads lawsuit, 97
 honeyclient support, 145
 on malware distribution, 69
 Safe Browsing API, 145
 testing ads, 94
Gore, Al, 149
Gramm-Leach-Bliley Financial Services Modernization Act (GLBA), 80, 214
GRC.com, 251
grep utility, 216
Guin v. Brazos, 206
Gutmann, Peter, 117

H

handshakes, 28
Hannaford Brothers security breach, 67, 68, 211
hash algorithms
 data translucency and, 241
 LAN Manager, 4
 SET procedure, 78

- Windows NT, 5
- Hasselbacher, Kyle, 127
- health care field
 - infosecurity and, 208
 - security metrics, 34–38
- Health Insurance Portability and Accountability Act (HIPAA), 80, 214
- hierarchical trust
 - cumulative trust comparison, 110
 - defined, 109
- HijackThis change tracker, 92
- HIPAA (Health Insurance Portability and Accountability Act), 80, 214
- HIPS (Host-based Intrusion Prevention Systems), 253
- Holz, Thorsten, 145
- Homeland Security, Department of, 36
- honeyclients
 - defined, 133
 - future of, 146
 - implementation limitations, 143
 - open source, 133–135
 - operational results, 139–140
 - operational steps, 134, 137
 - related work, 144–145
 - second-generation, 135–138
 - storing and correlating data, 140
- honeymonkeys, 144
- Honeynet Project, 138, 145
- honeypot systems
 - defined, 133
 - proliferation of malware, 252
- Honeywall, 138
- host logging, 232–237
- Host-based Intrusion Prevention Systems (HIPS), 253
- hostile environments
 - confirmation traps and, 10
 - specialization in, 249
- hotspot services, 22
- House Committee on Homeland Security, 201
- Howard, Michael, 195
- HTTPS protocol, 66
- Hubbard, Dan, 144
- Hula Direct ad broker, 98, 99

I

- IBM, social networking and, 159
- IDEA (International Data Encryption Algorithm), 117, 118
- iDefense Labs, 59, 156
- identity certificates, 111
- identity management services, 154
- identity theft
 - devaluing credit card information, 71
 - wireless networking, 23–25
- IDS (intrusion detection system)
 - building a resilient model, 233–237
 - challenges detecting botnets, 231
 - false positives, 217
 - functionality, 226
 - honeyclient support, 133, 144
 - host logging, 232–237
 - host-based, 253
 - improving detection with context, 228–231
 - limitations, 227, 229
 - log handling considerations, 218
- Iframedollars.biz, 132
- incident detection, 233
 - (see also malicious attacks)
 - building a resilient model, 233–237
 - host logging and, 232–237
 - improving with context, 228–231
 - percentage identified, 226, 227
 - SQL Slammer worm, 225
- InCtrl change tracker, 92
- information dealers
 - defined, 64
 - IRC data exchange, 67
 - malware producers and, 64
 - sources of information, 68
- information security
 - as long tail market, 165–167
 - balance in, 202–207
 - basic concepts, 200
 - cloud computing, 150–154
 - communication considerations, 207–211
 - connecting people and processes, 154–158
 - doing the right thing, 211–212
 - historical review, 248–251
 - host logging, 232
 - need for new strategies, 247
 - organizational culture, 200–202
 - overview, 147–150
 - September 11, 2001 and, 249
 - social networking and, 158–162
 - strict scrutiny, 252–254
 - suggested practices, 257
 - supercrunching, 153, 162–164
 - taking a security history, 44–46
 - web services, 150–154
- Information Security Economics, 162–164
- Information Security Group, 168
- injected iFrames, 69
- International Data Encryption Algorithm (IDEA), 117, 118
- International Tariff on Arms Regulations (ITAR), 3
- Internet Explorer
 - exploit-based installs and, 92

- open source honeyclients, 134
 - recent vulnerabilities, 131
- Internet Relay Chat (see IRC)
- intranets, security flaws, 25
- introducers in PGP, 113
 - (see also certificate authorities)
 - defined, 109, 112
 - extended, 123
 - Web of Trust process, 113
- intrusion detection system (see IDS)
- investment metrics, 47
- IRC (Internet Relay Chat)
 - botnet communication, 66
 - cyber underground communication, 65, 67
- ISO 2700x standard, 214
- ISPs, costs versus profits, 16–17
- ITAR (International Tariff on Arms Regulations), 3
- ITIL regulation, 214
- iTunes, 165

J

- J/Secure, 76
- JCB International, 76
- Jericho Forum, 156
- Jerusalem virus, 248

K

- Kaminsky, Dan, 161
- KBA (knowledge-based authentication), 68
- key loggers
 - as information source, 68
 - specialization in, 249
- key signatures
 - bloat and harassment, 124
 - certificate support, 111
 - exportable, 125
 - freshness considerations, 122
 - in-certificate preferences, 126
 - Web of Trust, 113, 115, 120
- keyrings, 112
- keys (see certificates; public key cryptography)
- keyservers
 - defined, 112
 - key-editing policies, 126
 - PGP Global Directory, 127
- Klez virus, 248
- knowledge-based authentication (KBA), 68
- Kovah, Xen0, 138

L

- L0phtCrack
 - government interest in, 13
 - learned helplessness example, 3–6

- Lai, Xuejia, 117
- LAN Manager, 4
- Lancaster, Branko, 117
- Langevin, Jim, 201
- LANs, physical security inherent in, 28
- Lansky, Jared, 90–92
- learned helplessness
 - backward compatibility and, 2
 - defined, 2, 7
 - L0phtCrack example, 3–6
 - overview, 2–7
- Leeson, Nick, 38–49
- legacy systems
 - backward compatibility, 7
 - e-commerce security and, 74
 - end-of-life upgrades, 2, 7
 - password security and, 4–6
- legal considerations
 - balance in information security, 202–207
 - communication and information security, 207–211
 - doing the right thing, 211–212
 - information security concepts, 200
 - log handling, 223
 - organizational culture, 200–202
 - value of logs, 214
- Levy, Steven, 119
- LinkShare affiliate network, 102
- Linux systems, 221
- log management tools, 222–223
- log messages, 215
- logs
 - case study, 218–221
 - challenges with, 216–218
 - classifying, 214
 - database, 221
 - defined, 215
 - email tracking, 221
 - future possibilities, 221–223
 - host logging, 232–237
 - incident detection and, 226, 228
 - regulatory compliance and, 214
 - universal standard considerations, 217
 - usefulness of, 153, 214, 215
- long straddle trading strategy, 40
- Lucent (see Bell Labs)
- Lynch, Aidan, 144

M

- machine learning, 254
- malicious attacks, 228
 - (see also cyber underground; incident detection)
 - attack indicators, 233–237
 - Blaster, 248

- Code Red, 248
- confirmation traps, 10
- directionality of, 227
- energy companies vulnerabilities, 18
- identity theft, 22–28
- Jerusalem, 248
- Klez, 248
- Melissa, 248
- Michelangelo, 248
- Morris, 248
- MyDoom, 248
- Nimda, 248
- Pakistani Flu, 248
- Slammer, 248
- Snort signatures, 228
- Sober, 248
- Sobig, 248
- SQL Slammer worm, 225–227, 229
- Symantec reports on, 229
- VBS/Loveletter—“I Love you”, 248
- W32.Gaobot worm, 229
- malvertisements, 92–94
- malware
 - anti-virus software and, 251
 - as cyber attack method, 69
 - banking trojans, 141, 249
 - client-side exploitation, 15, 132, 141–143
 - common distribution methods, 69
 - current market values, 67
 - directionality of attacks, 227
 - gaming trojans, 141, 249
 - historical review, 248–249
 - polymorphic, 70
 - production cycle, 64
 - streamlining identification of, 254
 - targeted advertising, 250
 - testing, 65
 - zero-day exploits, 252
- malware producers
 - defined, 64
 - information dealers and, 64
 - polymorphic malware, 70
 - testing code, 65
- man-in-the-middle attacks, 25
- manual penetration testing, 190
- Massey, James, 117
- MasterCard
 - 3-D Secure protocol, 76
 - SET protocol, 78
- Maurer, Ueli, 128
- MBNA, 79
- McAfee
 - online safety survey, 187
 - SiteAdvisor, 97
 - vulnerability management, 152
- McBurnett, Neal, 128
- McCabe, Jim, 178, 179
- McCaul, Mike, 201
- McDougle, John, 178
- McGraw, Gary, 186
- McManus, John, 171–182
- Mean Time Between Security Incidents (MTBSI), 48
- Mean Time to Repair (MTTR), 58
- Mean Time to Repair Security Incidents (MTTRSI), 48
- Media Guard product, 94
- medical field
 - infosecurity and, 208
 - security metrics, 34–38
- Melissa virus, 248
- Merchant Server Plug-in (MPI), 77
- meta-introducers, 123
- metrician, 34
- metrics
 - Barings Bank security breach, 38–49
 - coverage, 46
 - for data responsibility, 72
 - health care field, 34–38
 - investment, 47
 - measuring ROI, 163
 - scan coverage, 58
 - software development lifecycle and, 172–174, 189
 - TJX security breach, 49–59
 - treatment effect, 48
- MetricsCenter technology, 45
- MetricsCenter.org, 54
- Michelangelo virus, 248
- microchunking, 166
- Microsoft, 134
 - (see also Internet Explorer)
 - Authenticode, 110
 - Azure cloud operating system, 152
 - Commission on Cyber Security, 201
 - CPC advertising, 100
 - hierarchical trust, 110
 - honeymonkeys, 144
 - L0phtCrack example, 3–6
 - security controls in SDLC, 194
 - SQL Server, 225
 - supporting legacy systems, 7
 - testing approach, 10
 - Unix systems and, 8
- MITRE Corporation, 135, 222
- money, 44, 70, 141
 - (see also financial institutions; PCI)
- Monroe Doctrine, 201
- Morris virus, 248
- mothership systems, 230

Motorola Corporation, 31
Mozilla Firefox
 honeyclient support, 140, 145
 malware exploits and, 141
MPI (Merchant Server Plug-in), 77
MTBSI (Mean Time Between Security Incidents),
 48
MTTR (Mean Time to Repair), 58
MTRRSI (Mean Time to Repair Security Incidents),
 48
Murray, Daragh, 144
MyDoom virus, 248
MySpace social network, 159

N

naïveté
 client counterpart of, 8–9
 learned helplessness and, 2–7
NASA
 background, 171
 perception of closed systems, 172
 software development lifecycle, 172–174, 178–
 181
National Institute for Standards, 159
National Office for Cyberspace (NOC), 201, 202
Nazario, Jose, 145
newsgroups, 250
Nichols, Elizabeth, 33–61
Nichols, Elizabeth A., 30
Nimda virus, 248
NOC (National Office for Cyberspace), 201, 202
NTLM authentication, 6

O

OCC, 191
off-the-shelf software (see software acquisition)
Office Max, 50
online advertising
 advertisers as victims, 98–105
 attacks on users, 89–98
 CPA advertising, 102–103
 CPC advertising, 100–101
 CPM advertising, 100–103
 creating accountability, 105
 deceptive ads, 94–98
 exploit-laden banner ads, 89–92
 false impressions, 98–99
 fighting fraud, 103–104
 malvertisements, 92–94
 special procurement challenges, 104
 targeted, 250
online advertising, targeted, 249
online forums, 250
Open Security Foundation, 55

open source honeyclients, 133–135
Open Web Application Security Project (see
 OWASP)
OpenID identity management, 154
OpenPGP standard/protocol
 background, 108
 certification support, 111, 112
 designated revokers, 122
 direct trust, 109
 exportable signatures, 125
 extended introducers, 123
 in-certificate preferences, 126
 key support, 112
 key-editing policies, 126
 revoking certificates, 122
OpenSocial API, 159
operating systems, host logging, 232, 236
OptOut spyware removal tool, 251
Orange Book, 213
organizational culture, 200–202
outsourcing
 extending security initiative to, 190
 trends in, 154
 vulnerability research, 156
OWASP (Open Web Application Security Project)
 background, 159
 CLASP methodology, 187
 Top 10 list, 187

P

P2P (peer-to-peer) networks
 botnet communication, 66
 honeyclient considerations, 146
packet sniffers, 92
packets
 handshake, 28
 SQL Slammer worm, 227
Pakistani Flu virus, 248
PAN (Primary Account Number), 77
Panda Labs, 69
PAR (Payer Authentication Request), 77
PARAM tag, 94
passive sniffing, 9
passphrases, 29
password grinding, 28
password-cracking tools
 LOphtCrack example, 3–6
 passphrases and, 29
passwords
 authentication security, 7
 identity theft and, 24
 NTLM authentication and, 6
PATHSERVER, 129
Payer Authentication Request (PAR), 77
Payment Card Industry (see PCI)

- PayPal, 79
 - PCI (Payment Card Industry)
 - Data Security Standard, 75, 82, 159, 211, 214, 237
 - protecting credit card data, 44
 - peer-to-peer networks (see P2P networks)
 - PEM (Privacy Enhanced Mail), 117
 - perma-vendors, 156
 - Personally Identifiable Information (PII), 180
 - Pezzonavante honeyclient, 144
 - PGP (Pretty Good Privacy), 111
 - (see also Web of Trust)
 - background, 107, 108, 116
 - backward compatibility issues, 117
 - Crypto Wars, 118
 - designated revokers, 122
 - encryption support, 107, 116–120
 - key validity, 108
 - patent and export problems, 117
 - source download, 116
 - trust models, 109–116
 - trust relationships, 108
 - PGP Corporation, 108
 - PGP Global Directory, 127
 - pharmware, 68
 - phishing
 - 3-D Secure protocol, 77
 - as information source, 68
 - botnet support, 66
 - challenges detecting, 231
 - spam and, 70
 - specialization in, 249
 - PhoneyC website, 145
 - PII (Personally Identifiable Information), 180
 - Piper, Fred, 168
 - PKI (Public Key Infrastructure)
 - authoritative keys, 123
 - defined, 111
 - DSG support, 203
 - revoking certificates, 120
 - SET considerations, 79
 - PlexLogic, 45
 - Plumb, Colin, 119
 - port scanning, 231
 - pragmatic security, 200, 209
 - Pre-Shared Key (PSK), 28
 - Pretty Good Privacy (see PGP)
 - Price, Will, 127
 - Primary Account Number (PAN), 77
 - Privacy Enhanced Mail (PEM), 117
 - proof-of-concept project, 191–193
 - Provos, Niels, 145
 - PSK (Pre-Shared Key), 28
 - psychological traps
 - confirmation traps, 10–14
 - functional fixation, 14–20
 - learned helplessness, 2
 - public key cryptography
 - cumulative trust systems, 111
 - key revocation, 121
 - PGP support, 107
 - RSA algorithm, 117
 - SET support, 78
 - steganographic applications, 245
 - validity, 108
 - Public Key Infrastructure (see PKI)
 - Public Key Partners, 118
 - put options, 39
- ## Q
- Qualys vulnerability management, 151
- ## R
- Raduege, Harry, 201
 - Regular, Bob, 90
 - regulatory compliance (see legal considerations)
 - Reiter, Mark, 129
 - Reliable Software Technologies, 171, 173
 - reputation economy, 167
 - resource dealers, 64
 - Return on Investment (ROI), 163, 205–207
 - Return on Security Investment (ROSI), 206
 - Returnil, 254, 255, 256, 257
 - revoking certificates, 120–122
 - RFC 1991, 108, 119
 - RFC 3156, 108
 - RFC 4880, 108
 - Right Media, 94
 - ROI (Return on Investment), 163, 205–207
 - root certificates
 - defined, 109
 - direct trust, 110
 - rootkits
 - example investigating, 220
 - Rustock.C, 252
 - specialization in, 249
 - ROSI (Return on Security Investment), 206
 - routers
 - DDoS attacks on, 16
 - host logging, 232
 - watch lists, 231
 - Routh, Jim, 183–197
 - RSA Data Security Incorporated, 117
 - RSA public-key algorithm, 117
 - RSAREF library, 117
 - Rustock.C rootkit, 252
- ## S
- Sabett, Randy V., 199–212

- sandboxing
 - functionality, 254
 - HIPS support, 253
 - need for new strategies, 248
- Santa Fe Group, 44
- Sarbanes-Oxley Act (SOX), 80, 214
- SCADA systems, 18
- Schoen, Seth, 127
- SDLC (see software development lifecycle)
- Second Life virtual world, 159
- Secret Service
 - Shadowcrew network and, 65
 - TJX security breach and, 50
- Secunia, 156
- Secure Electronic Transaction (see SET)
- security breaches
 - attorney involvement in investigating, 211
 - Barings Bank, 38–49
 - California data privacy law, 203–205
 - cyber underground and, 63–72
 - databases and, 239
 - impact of, 208
 - logs in investigating, 218–221
 - public data sources, 59
 - tiger team responses, 210–211
 - TJX, 49–59
- security certificates
 - defined, 22
 - encryption and, 22, 24
 - fundamental flaw, 25
 - paying attention to, 26
 - wireless access points, 26, 27
- Security Event Managers (SEMs), 153
- security metrics (see metrics)
- Security Metrics Catalog project, 54
- security traps (see psychological traps)
- SecurityFocus database, 132
- SecurityMetrics.org, 54
- SEI (Software Engineering Institute), 176
- Seifert, Christian, 138, 145
- self-signed certificates, 109
- SEMs (Security Event Managers), 153
- separation of duties, 39
- September 11, 2001, 249
- server applications, host logging, 232
- Service Set Identifier (SSID), 52
- service-oriented architecture (SOA), 150
- SET (Secure Electronic Transaction)
 - background, 78
 - evaluation of, 79
 - protections supported, 78
 - transaction process, 79
- SHA256 hash algorithm, 241
- Shadowcrew network, 65
- short straddle trading strategy, 39, 40
- signature harassment, 125
- Sinclair, Upton, 149
- Skinner, B. F., 163
- Slammer virus, 248
- SMTP protocol
 - botnet communication, 66
 - incident detection considerations, 236
- SOA (service-oriented architecture), 150
- Sober virus, 248
- Sobig virus, 248
- social networking
 - crowdsourcing, 161
 - impact on security, 154, 158, 160–162
 - interoperability, 160
 - malware distribution and, 69
 - PGP and, 107
 - potential in, 159
 - state of the art in, 159
 - Web of Trust and, 128
- Social Security numbers
 - incident detection considerations, 237
 - spyware stealing, 69
- software acquisition
 - enforcing security, 190–193, 195–197
 - implicit requirements in, 184–185
- software development lifecycle
 - Bell Labs example, 174–178
 - business model evolution, 183
 - CLASP methodology, 187, 188
 - designing security, 171–172, 181–182, 193
 - developer training, 188
 - fixing security problems, 189
 - formal quality processes for security, 187
 - improving software security, 185–190
 - instituting security plan, 186–188
 - NASA examples, 172–174, 178–181
 - outsourcing considerations, 190
 - proof-of-concept project, 190–193
 - static code analysis tool, 188, 189, 194
- Software Engineering Institute (SEI), 176
- Sophos, 69
- SOX (Sarbanes-Oxley Act), 80, 214
- spam
 - botnet support, 66
 - challenges detecting, 231
 - client-side vulnerability, 131
 - phishing and, 70
 - specialization in, 249
 - targeted, 70
 - traffic analysis, 230
- Sports Authority, 50
- SpyBye honeyclient, 145
- spyware
 - as information source, 68
 - CPA advertising, 102

- Dell estimates, 131
- functionality, 69
- malvertisements and, 92
- OptOut removal tool, 251
- specialization in, 249
- SQL injection attacks, 69, 131
- SQL Server (Microsoft), 225
- SQL Slammer worm
 - background, 226
 - IDS challenges, 227
 - port 1434/udp, 225, 229
 - signatures, 227
- SSID (Service Set Identifier), 52
- stale threat modeling, 12
- static code analysis tool
 - context-sensitive help, 194
 - developer training, 188
 - threshold of quality, 188
 - vulnerability information, 188, 189
- steganographic applications, 245
- Stickley, Jim, 21–31
- storing data
 - honeyclients, 140
 - logs, 222
- strict scrutiny
 - blacklisting, 252, 254
 - whitelisting, 253
- Stubblebine, Stuart, 129
- stuffed cookies, 102
- supercrunching, 153, 162–164
- supervalidity, 114, 128
- switches, failing open, 8
- Symantec
 - DeepSight Threat Management Service, 59
 - Internet Security Threat Reports, 60, 229
 - Managed Security Services, 231
 - on botnets, 231
 - on malware distribution, 69
 - SQL Slammer worm, 225
- SYSLOG format, 221
- system development lifecycle (see software development lifecycle)

T

- targeted advertising, 249, 250
- technology economics, 165
- testing
 - ads, 94
 - confirmation traps in, 11
 - dynamic, 190
 - fuzzing technique, 10
 - malware code, 65
 - manual penetration, 190
 - Microsoft approach, 10
- Thomson, William (Lord Kelvin), 33

- time-to-market, 174–178
- time-to-quality, 174–178
- TJX security breach, 30, 49–59, 211
- traffic analysis, improving coverage with, 229–230
- treatment effect metrics, 48
- Truman Doctrine, 201
- trust models
 - cumulative trust, 110
 - defined, 109
 - direct trust, 109
 - hierarchical trust, 109
 - users as certification authorities, 112
- trust relationship
 - defined, 108, 114
 - establishing for wireless networks, 26–28
 - PGP support, 107
 - validity comparison, 108

U

- Unified Compliance Framework, 44
- University of London, 168
- Unix systems
 - grep utility, 216
 - log handling, 221
 - security vulnerabilities, 8
- usernames, identity theft and, 24

V

- validity
 - defined, 114
 - supervalidity, 114, 128
 - trust comparison, 108
- ValueClick, 97, 103, 105
- VBS/Loveletter—“I Love you” virus, 248
- VeriSign
 - hierarchical trust, 109, 110
 - iDefense Labs, 59, 156
- Viacrypt, 119
- Viega, John, 187
- virtual cards
 - defined, 79
 - functionality, 79
 - multiple-use, 80
 - single-use, 80
- virtual machines, 255
 - honeyclient support, 136
 - malware detection of, 141
- virtualization, 255–256, 257
- viruses (see malicious attacks)
- VirusTotal.com, 142
- Visa, Inc.
 - 3-D Secure protocol, 76
 - SET protocol, 78
 - transaction statistics, 75

- VMware, 136, 141, 255
- VMware Workstation, 92
- vulnerability scanners
 - breaker mentality and, 151
 - false positives/negatives, 236
 - functional fixation, 15
 - proliferation of malware and, 252

W

- W32.Gaobot worm, 229
- Wallace, Sanford, 89–92
- Wang, Chenxi, 63–72, 210, 250
- Wang, Kathy, 131–146
- warchalking, 29
- wardriving technique, 51
- Wason, Peter, 11
- watch lists, 230–231
- Wayner, Peter, 239–246
- Web 2.0, 159
- web applications
 - exploiting vulnerabilities, 68, 187
 - log handling support, 221
 - risk of exploits, 193
 - trends in exploits, 186, 187
 - uncovering vulnerabilities, 188
- Web of Trust
 - areas for further research, 128
 - background, 107
 - cumulative trust support, 111
 - enhancements to original model, 120–128
 - functionality, 112–114
 - implications of signing keys, 114–116
 - in-certificate preferences, 126
 - PGP Global Directory, 127
 - revoking certificates, 120–122
 - rough edges in original, 114–116
 - scaling issues, 123–124
 - signature bloat/harassment, 124
 - social networking and, 128
 - supervalidity, 114, 128
 - variable trust ratings, 128
- web services
 - applying security to, 152
 - builders versus breakers, 151
 - defined, 150
- Websense, 144
- WEP (Wired Equivalent Privacy), 21
 - authentication support, 52
 - security flaws, 28
- Western Union, 65
- wget tool, 134
- Whitehead, Alfred North, 150
- whitelisting, 253
- Whois website, 97
- Wi-Fi Protected Access (WPA), 21, 28

- Windows Home Server, 152
- Windows Live ID, 154
- Windows NT
 - hash function, 5
 - Internet security and, 8
- Windows Vista
 - Internet security and, 8
 - security warnings, 26
 - strict scrutiny and, 253
- Windows XP
 - exploit-based installs and, 92
 - honeyclient support, 137, 139
- Wired Equivalent Privacy (WEP), 21
- wireless access points
 - identity theft and, 25
 - scan coverage, 58
 - security certificates, 26, 27
 - SSID support, 52
 - WEP support, 28
- wireless networking
 - future of, 31
 - identity theft, 22–28
 - role at TJX, 49–59
 - security flaws, 28–31
 - wardriving technique, 51
- Wireshark packet sniffer, 92
- Wood, Michael, 247–258
- WordPress, 165
- worms
 - SQL Slammer, 225–227, 229
 - W32.Gaobot worm, 229
- WPA (Wi-Fi Protected Access), 21, 28
- WS-Security specification, 152

X

- X.509 certificates
 - authoritative keys, 124
 - certification support, 111
 - hierarchical trust, 110
 - revoking, 120
 - SET support, 78
 - web services and, 152

Y

- Yahoo!
 - CPC advertising, 101
 - DDoS attacks on, 16
- YouTube, 165

Z

- Zatko, Peiter “Mudge”, 1–20, 205
- zero-day exploits, 252
- Zimmermann, Phil, 107–130

COLOPHON

The cover image is a cactus from Photos.com. The cover fonts are Akzidenz Grotesk and Orator. The text font is Adobe's Meridien; the heading font is ITC Bailey.

