



# Crimeware

Understanding New Attacks and Defenses

*"The biggest development in online security in the last five years has been the emergence of a criminal economy where villains specialize and trade with each other. This book provides a much-needed update on the tools that these gangsters use now and on others that they might be using in the near future."*

—Ross Anderson, Professor of Security Engineering, Cambridge University

Markus Jakobsson • Zulfikar Ramzan

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 the publisher was aware of a trademark claim, the designations have been printed with initial capital letters or in all capitals.

The authors and publisher have taken care in the preparation of this book, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: U.S. Corporate and Government Sales, (800) 382-3419, [corpsales@pearsoned.com](mailto:corpsales@pearsoned.com).

For sales outside the United States please contact: International Sales, [international@pearsoned.com](mailto:international@pearsoned.com).



---

#### **This Book Is Safari Enabled**

The Safari® Enabled icon on the cover of your favorite technology book means the book is available through Safari Bookshelf. When you buy this book, you get free access to the online edition for 45 days. Safari Bookshelf is an electronic reference library that lets you easily search thousands of technical books, find code samples, download chapters, and access technical information whenever and wherever you need it.

To gain 45-day Safari Enabled access to this book:

- Go to [www.informit.com/onlineedition](http://www.informit.com/onlineedition)
- Complete the brief registration form
- Enter the coupon code J6DM-EZRD-F2MK-NEEY-DI7S

If you have difficulty registering on Safari Bookshelf or accessing the online edition, please e-mail [customer-service@safaribooksonline.com](mailto:customer-service@safaribooksonline.com).

---

Visit us on the Web: [informit.com/aw](http://informit.com/aw)

*Library of Congress Cataloging-in-Publication Data*

Jakobsson, Markus.

Crimeware : understanding new attacks and defenses / Markus Jakobsson,  
Zulfikar Ramzan. p. cm.

Includes bibliographical references and index.

ISBN 978-0-321-50195-0 (pbk. : alk. paper) 1. Computer security.

2. Internet—Security measures. 3. Computer crimes. I. Ramzan, Zulfikar. II. Title.

QA76.9.A25J325 2008

005.8—dc22

2007050736

Copyright © 2008 Symantec Corporation

All rights reserved. Printed in the United States of America. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, write to:

Pearson Education, Inc  
Rights and Contracts Department  
501 Boylston Street, Suite 900  
Boston, MA 02116  
Fax (617) 671-3447

ISBN-13: 978-0-321-50195-0

ISBN-10: 0-321-50195-0

Text printed in the United States on recycled paper at Courier in Stoughton, Massachusetts.  
First printing, April 2008

# Preface

---

Traditionally, malware has been thought of as a purely technical threat, relying principally on technical vulnerabilities for infection. Its authors were motivated by intellectual curiosity, and sometimes by competition with other malware authors.

This book draws attention to the fact that this is all history. Infection vectors of today take advantage of social context, employ deceit, and may use data-mining techniques to tailor attacks to the intended victims. Their goal is profit or political power. Malware become *crimeware*. That is, malware has moved out of basements and college dorms, and is now a tool firmly placed in the hands of organized crime, terror organizations, and aggressive governments. This transformation comes at a time when society increasingly has come to depend on the Internet for its structure and stability, and it raises a worrisome question: *What will happen next?* This book tries to answer that question by a careful exposition of what crimeware is, how it behaves, and what trends are evident.

The book is written for readers from a wide array of backgrounds. Most sections and chapters start out describing a given angle from a bird's-eye view, using language that makes the subject approachable to readers without deep technical knowledge. The chapters and sections then delve into more detail, often concluding with a degree of technical detail that may be of interest only to security researchers. It is up to you to decide when you understand enough of a given issue and are ready to turn to another chapter.

Recognizing that today's professionals are often pressed for time, this book is written so that each chapter is relatively self-contained. Rather than having each chapter be sequentially dependent on preceding chapters, you can safely peruse a specific chapter of interest and skip back and forth as desired. Each chapter was

contributed by a different set of authors, each of whom provides a different voice and unique perspective on the issue of crimeware.

This book is meant for anyone with an interest in crimeware, computer security, and eventually, the survivability of the Internet. It is not meant only for people with a technical background. Rather, it is also appropriate for makers of laws and policies, user interface designers, and companies concerned with user education. The book is not intended as a guide to securing one's system, but rather as a guide to determining what the problem really is and what it will become.

Although we often use recent examples of attacks to highlight and explain issues of interest, focus here is on the underlying trends, principles, and techniques. When the next wave of attacks appears—undoubtedly using new technical vulnerabilities and new psychological twists—then the same principles will still hold. Thus, this book is meant to remain a useful reference for years to come, in a field characterized by change. We are proud to say that we think we have achieved this contradictory balance, and we hope that you will agree.

## Acknowledgments

We are indebted to our expert contributors, who have helped make this book what it is by offering their valuable and unique insights, and selflessly donated their time to advance the public's knowledge of crimeware. The following researchers helped us provide their view of the problem: Shane Balfe, Jeffrey Bardzell, Shaowen Bardzell, Dan Boneh, Fred H. Cate, David Cole, Vittoria Colizza, Bruno Crispo, Neil Daswani, Aaron Emigh, Peter Ferrie, Oliver Friedrichs, Eimear Gallery, Mona Gandhi, Kourosh Gharachorloo, Shuman Ghosemajumder, Minaxi Gupta, James Hoagland, Hao Hu, Andrew Kalafut, Gary McGraw, Chris J. Mitchell, John Mitchell, Steven Myers, Chris Mysen, Tyler Pace, Kenneth G. Paterson, Prashant Pathak, Vinay Rao, Jacob Ratkiewicz, Melanie Rieback, Sourabh Satish, Sukamol Srikwan, Sid Stamm, Andrew Tanenbaum, Alex Tsow, Alessandro Vespignani, Xiaofeng Wang, Stephen Weis, Susanne Wetzel, Ollie Whitehouse, Liu Yang, and the Google Ad Traffic Quality Team.

In addition, Markus wishes to thank his graduate students, who have helped with everything from performing LaTeX conversions to being experiment subjects, and many of whose research results are part of this book. Zulfikar wishes to thank Oliver Friedrichs and the rest of the Symantec Advanced Threat Research team (as well as his colleagues throughout Symantec) for affording him the opportunity to

work on this book and for engaging in countless stimulating discussions on these topics.

We also both want to acknowledge the help and guidance we have received from Jessica Goldstein and Romny French at Addison-Wesley.

Finally, we want to thank our understanding spouses and families, who have seen much too little of us in the hectic months during which we labored on getting the book ready for publication.

*Markus Jakobsson*

Palo Alto, California

January, 2008

*Zulfikar Ramzan*

Mountain View, California

January, 2008

# Chapter 10

## Cybercrime and Politics

---

*Oliver Friedrichs*

While we first saw the Internet used extensively during the 2004 U.S. presidential election, its use in future presidential elections will clearly overshadow those humble beginnings. It is important to understand the associated risks as political candidates increasingly turn to the Internet in an effort to more effectively communicate their positions, rally supporters, and seek to sway critics. These risks include, among others, the dissemination of misinformation, fraud, phishing, malicious code, and the invasion of privacy. Some of these attacks, including those involving the diversion of online campaign donations, have the potential to threaten voters' faith in the U.S. electoral system.

The analysis in this chapter focuses on the 2008 presidential election to demonstrate the risks involved, but our findings may just as well apply to any future election. Many of the same risks that we have grown accustomed to on the Internet can also manifest themselves when the Internet is expanded to the election process.

It is not difficult for one to conceive of numerous attacks that might present themselves and, to varying degrees, influence the election process. One need merely examine the attack vectors that already affect consumers and enterprises today to envision how they might be applied to this process. In this chapter, we have chosen to analyze those attack vectors that would be most likely to have an immediate and material effect on an election, affecting voters, candidates, or campaign officials.

A number of past studies have discussed a broad spectrum of election fraud possibilities, such as the casting of fraudulent votes [258] and the security, risks, and challenges of electronic voting [173]. There are many serious and important risks to consider related both to the security of the voting process and to the new

breed of electronic voting machines that have been documented by others [46]. Risks include the ability for attackers or insiders either to manipulate these machines or to alter and tamper with the end results. These concerns apply not only to electronic voting in the United States, but have also been raised by other countries, such as the United Kingdom, which is also investigating and raising similar concerns surrounding electronic voting [274]. Rather than revisit the subject of electronic voting, the discussion here focuses exclusively on Internet-borne threats, including how they have the potential to influence the election process leading up to voting day.

We first discuss domain name abuse, including typo squatting and domain speculation as it relates to candidate Internet domains. Next, we explore the potential impact of phishing on an election. We then discuss the effects of security risks and malicious code, and the potential for misinformation that may present itself using any of these vectors. Finally, we review how phishers may spoof political emails (such as false campaign contribution requests) instead of emails appearing to come from financial institutions. The goal in such attacks might still be to collect payment credentials, in which case the political aspect is just a new guise for fraud. However, political phishing emails might also be used to sow fear among potential contributors and make them less willing to contribute online—whether to spoofed campaigns or to real ones.

These sets of risks cross technical, social, and psychological boundaries. Although traditional forms of malicious code certainly play an important role in these threats, social engineering and deception provide equal potential to be exploited and might have a more ominous psychological impact on voters who are exercising their right to elect their next president, or cast their vote in any other type of election.

This chapter includes both active research conducted by the author and discussion of how current threats may be customized. To determine the impact of typo squatting and domain name speculation, for example, we performed an analysis of 2008 presidential election candidate web sites and discovered numerous examples of abuse.

In regard to the attacks discussed in this chapter, we believe and hope that candidates and their campaigns are unlikely to knowingly participate in or support these activities themselves, for two reasons. First, it would not be acting in good faith. Second, their actions would in many cases be considered a breach of either existing computer crime or federal election law.<sup>1</sup>

We conclude that perpetrators would likely fall into two categories: those with political motives and those seeking to profit from these attacks. In the end, it may

---

1. U.S. Code Title 18, Part I, Chapter 29. Available from [http://www4.law.cornell.edu/uscode/html/uscode18/usc\\_sec\\_18\\_00000594\\_---000-.html](http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00000594_---000-.html)

be difficult to identify from a given attack which one of these goals is the attacker's true motive.

## 10.1 Domain Name Abuse

To communicate with constituents and supporters, candidates have created and maintain web sites, which are identified by and navigated to via their registered domain names. All candidates for the 2008 federal election have registered, or already own, unique domain names that are used to host their respective web sites. In all cases this domain name incorporates their own name in some capacity, and in some cases has been registered specifically in support of the 2008 campaign. Domain names play one of the most important roles in accessing a web site. They are the core part of the URL that is recognized by the general population and, as such, their ownership dictates who can display content to users visiting web sites hosted on that domain name.

While users may well know the URL for their bank or favorite commerce site, voters may not readily know the URL for their political party's or chosen candidate's web site. Legitimate-sounding domain names may not be as they appear. The authors of this book, for example, were able to freely register domain names such as <http://www.democratic-party.us> and <http://www.support-gop.org> that have for some time warned visitors about the risks presented by phishing. It would be easy to use a domain name of this type for the purposes of phishing or crimeware installation.

Consider, for example, an email pointing to one of these domains that contains text suggesting it came from the Democratic Party and asking the recipient for a donation. If willing to contribute, the recipient may be offered to choose a variety of payment methods, each one of which would allow the phisher to potentially capture the user's credentials as he or she enters this data on the site (or on another, suitably named site hyperlinked from the donation page). The email might also offer the recipient a chance to download and access resources, such as campaign movies, which themselves might contain malware. Existing movies can be modified to incorporate malware [388]. Typical Internet users are also very susceptible to attacks in which self-signed certificates vouch for the security of executables as long as a person known to them has also indicated that the material is safe [388]. In one study [388], that known person was a friend; in our hypothetical case, it might be a political party or a politician.

In today's online environment, individuals and businesses must consider a number of risks posed by individuals attempting to abuse the domain name system. These involve domain speculators, bulk domain name parkers, and typo squatters.



### 10.1.1 Background

Since the early days of Internet commerce, Internet domain names have held an intrinsic value, much as real estate in the physical world has been valued for centuries. In the early 1990s, when relatively few .com domain names existed, it was highly probable that if one attempted to acquire the name of a well-known company, individual, or trademark, this name would be readily available. Many early domain name speculators did, in fact, acquire such domain names, in many cases later selling them to the legitimate trademark holder. At that point, the legal precedence for domain name disputes had not yet been set, and the speculator had a chance of profiting from this sale, in particular if it was to a well-known and well-funded corporation.

It was only a matter of time before formal dispute guidelines were created to eliminate such infringement. A formal policy was created by ICANN in 1999, which is known as the Uniform Domain Name Dispute Resolution Policy (UDRP) [127]. The UDRP is implemented in practice by the World Intellectual Property Organization's (WIPO) Arbitration and Mediation Center.

While this policy provides a framework for resolving infringement, it does not preclude the registration of an infringing domain name if that domain name is unregistered. What is in place is a policy and framework for the legitimate trademark owner to become the owner of the domain, granted the trademark owner first becomes aware of the infringing domain's existence. The policy is frequently used by legitimate business trademark holders to protect their names.<sup>2</sup>

While it is used to protect trademarked proper names, the same policy applies to unregistered, or "common law" marks, including well-known individuals' proper names, even when a formal trademark does not exist. Julia Roberts, for example, was able to obtain ownership of the `juliaroberts.com` domain name, even in the absence of a registered trademark.<sup>3</sup> This is common when a domain name is specific enough and matches a full proper name. In other examples, such as the more general domain name `sting.com`, contested by the well-known singer Sting, the transfer was not granted and the original registrant retained ownership.<sup>4</sup>

There appear to be very few cases in which either elected or hopeful political candidates have disputed the ownership of an infringing domain name. One

---

2. *The Coca-Cola Company v. Spider Webs Ltd.* <http://www.arb-forum.com/domains/decisions/102459.htm>.

3. *Julia Fiona Roberts v. Russell Boyd.* <http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0210.html>.

4. *Gordon Sumner, p/k/a Sting v. Michael Urvan.* <http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0596.html>

example that does exist is for the domain name `kennedytownsend.com` and several variations thereof. Disputed by Kathleen Kennedy Townsend, who was Lieutenant Governor of the State of Maryland at the time, the transfer was not granted, based predominantly on what appears to be a technicality of how the dispute was submitted. Central to the ruling in such dispute cases is whether the trademark or name is used to conduct commercial activity, and thus whether the infringement negatively affects the legitimate owner and, as a result, consumers:

Here, the claim for the domain names is brought by the individual politician, and not by the political action committee actively engaged in the raising of funds and promotion of Complainant's possible campaign. Had the claim been brought in the name of the Friends of Kathleen Kennedy Townsend, the result might well have been different. But it was not. The Panel finds that the protection of an individual politician's name, no matter how famous, is outside the scope of the Policy since it is not connected with commercial exploitation as set out in the Second WIPO Report.<sup>5</sup>

Within the United States, trademark owners and individuals are further protected by the Anticybersquatting Consumer Protection Act, which took effect on November 29, 1999.<sup>6</sup> The ACPA provides a legal remedy by which the legitimate trademark owner can seek monetary damages in addition to the domain name, whereas the UDRP provides for only recovery of the domain name itself.

Even today, the relatively low cost involved in registering a domain name (less than \$10 per year) continues to provide an opportunity for an individual to profit by acquiring and selling domain names. The relative scarcity of simple, recognizable "core" domain names has resulted in the development of a significant after-market for those domain names and led to the creation of a substantial amount of wealth for some speculators [377]. Today, a number of online sites and auctions exist explicitly to facilitate the resale of domain names.

In addition to engaging in domain name speculation for the purpose of its future sale, many speculators seek to benefit from advertising revenue that can be garnered during their ownership of the domain name. These individuals—and, more recently, for-profit companies such as iREIT<sup>7</sup>—may register, acquire, and own hundreds of thousands to millions of domain names explicitly for this purpose. These domains display advertisements that are, in many cases, related to the domain name itself, and their owners receive an appropriate share of the

---

5. *Kathleen Kennedy Townsend v. B. G. Birt*. <http://www.wipo.int/amc/en/domains/decisions/html/2002/d2002-0030.html>

6. Anticybersquatting Consumer Protection Act. <http://thomas.loc.gov/cgi-bin/query/z?c106:S.1255.IS:=>

7. Internet REIT. <http://www.ireit.com/>

advertising revenue much like any web site participating in CPM, CPC, or CPA<sup>8</sup> advertising campaigns.

### 10.1.2 Domain Speculation in the 2008 Federal Election

Typo squatting seeks to benefit from a mistake made by the user when entering a URL directly into the web browser's address bar. An errant keystroke can easily result in the user entering a domain name that differs from the one intended. Typo squatters seek to benefit from these mistakes by registering domain names that correspond to common typos. Whereas in the past users making typos were most likely to receive an error indicating that the site could not be found, today they are likely to be directed to a different web site. In many cases, this site may host advertisements, but the potential for more sinister behavior also exists.

To determine the current level of domain name speculation and typo squatting in the 2008 federal election, we performed an analysis of well-known candidate domain names to seek out domain speculators and typo squatters. First, we identified all candidates who had registered financial reports with the Federal Election Commission for the quarter ending March 31, 2007.<sup>9</sup> A total of 19 candidates had submitted such filings. Next, we identified each candidate's primary campaign web site through the use of popular search engines and correlated our findings with additional online resources to confirm their accuracy. This, in turn, gave us the primary registered domain name upon which the candidate's web site is hosted.

To simplify our analysis, we removed domains that were not registered under the .com top-level domain. This resulted in the removal of two candidates who had domains registered under the .us top-level domain. Our decision to focus on the .com top-level domain was driven by no other reason than our ability to access a complete database of .com registrants at the time of our research. Our final list of candidate web sites and their resulting domains appears in Table 10.1.

Once we had identified the set of candidate domain names, we conducted two tests to examine current domain name registration data. First, we determined how widespread the behavior of typo squatting was on each candidate's domain. Second, we examined domain name registration data so as to identify cousin domain names [198]. For our search, we defined a cousin domain name as one that contains

---

8. See Chapter 11 for a description of CPM, CPC, and CPA, along with a discussion of Internet advertising.

9. FEC Filing from Prospective 2008 Presidential Campaigns. <http://query.nictusa.com/pres/2007/Q1>

---

Joe Biden (Democrat)	<a href="http://www.joebiden.com">http://www.joebiden.com</a>
Sam Brownback (Republican)	<a href="http://www.brownback.com">http://www.brownback.com</a>
Hillary Clinton (Democrat)	<a href="http://www.hillaryclinton.com">http://www.hillaryclinton.com</a>
John Cox (Republican)	<a href="http://www.cox2008.com">http://www.cox2008.com</a>
Christopher Dodd (Democrat)	<a href="http://www.chrisdodd.com">http://www.chrisdodd.com</a>
John Edwards (Democrat)	<a href="http://www.johnedwards.com">http://www.johnedwards.com</a>
James Gilmore (Republican)	<a href="http://www.gilmoreforpresident.com">http://www.gilmoreforpresident.com</a>
Rudy Giuliani (Republican)	<a href="http://www.joinrudy2008.com">http://www.joinrudy2008.com</a>
Mike Huckabee (Republican)	<a href="http://www.mikehuckabee.com">http://www.mikehuckabee.com</a>
Duncun Hunter (Republican)	<a href="http://www.gohunter08.com">http://www.gohunter08.com</a>
John McCain (Republican)	<a href="http://www.johnmccain.com">http://www.johnmccain.com</a>
Barack Obama (Democrat)	<a href="http://www.barackobama.com">http://www.barackobama.com</a>
Ron Paul (Republican)	<a href="http://www.ronpaul2008.com">http://www.ronpaul2008.com</a>
Bill Richardson (Democrat)	<a href="http://www.richardsonforpresident.com">http://www.richardsonforpresident.com</a>
Mitt Romney (Republican)	<a href="http://www.mittromney.com">http://www.mittromney.com</a>
Tom Tancredo (Republican)	<a href="http://www.teamtancredo.com">http://www.teamtancredo.com</a>
Tommy Thompson (Republican)	<a href="http://www.tommy2008.com">http://www.tommy2008.com</a>

---

**Table 10.1:** The final candidate web site list, together with the domain names.

the candidate domain name in its entirety, with additional words either prefixed or appended to the candidate domain name. In this context, we would consider domain names such as `presidentbarackobama.com` or `presidentmittromney.com` as cousin domain names to the candidates' core domain names of `barackobama.com` and `mittromney.com`, respectively. One can also define a cousin name more loosely as a name that semantically or psychologically aims at being confused with another domain name. In this sense, `www.thompson-for-president.com` should be considered a cousin name domain of `www.tommy2008.com`, despite the fact that they do not share the same core. For the sake of simplicity, we did not examine cousin domains that are not fully inclusive of the original core domain name.

To generate typo domain names, we created two applications, `typo_gen` and `typo_lookup`. The `typo_gen` application allowed us to generate typo domain names based on five common mistakes that are made when entering a URL into the web browser address bar [466].

Missing the first "." delimiter:	<code>wwwmittromney.com</code>
Missing a character in the name ("t"):	<code>www.mitromney.com</code>
Hitting a surrounding character ("r"):	<code>www.mitrtromney.com</code>
Adding an additional character ("t"):	<code>www.mittttromney.com</code>
Reversing two characters ("im"):	<code>www.imttromney.com</code>

As a result of such mistakes, the potential number of typos grows in proportion to the length of the domain name itself. The sheer number of typos for even a short domain name can be large. It is rare to find that an organization has registered all potential variations of its domain name in an effort to adequately protect itself. Typo squatters take advantage of such omissions to drive additional traffic to their own web properties.

Our second application, `typo_lookup`, accepted a list of domain names as input and then performed two queries to determine whether that domain name has been registered. First, a DNS lookup was performed to determine whether the domain resolves via the Domain Name System (DNS). Second, a `whois` lookup was performed to identify the registered owner of the domain.

For the purposes of our analysis, we considered a domain to be typo squatted if it was registered in bad faith by someone other than the legitimate owner of the primary source domain name. We visited those web sites for which typos currently exist and confirmed that they were, in fact, registered in bad faith. We filtered out those that directed the visitor to the legitimate campaign web site as well as those owned by legitimate entities whose name happens to match the typo domain.

Our second test involved the analysis of domain registration data to identify cousin domain names. We obtained a snapshot of all registered domains in the `.com` top-level domain during the month of June 2007. We performed a simple text search of this data set in an effort to cull out all matching domains.

Additional techniques could be used to generate related domain names that we did not examine during our research. This may include variations on a candidate's name (`christopher` instead of `chris`), variations including only a candidate surname (`clinton2008.com`), and the introduction of hyphens into names (`mitt-romney.com`). In addition, a number of typos might be combined to create even more variations on a given domain name, although it becomes less likely that an end user will visit such a domain name as the number of mistakes increases. Nevertheless, such domain names can be very effective in phishing emails, because the delivery of the malicious information relies on spamming in these cases, and not on misspellings made by users.

Expanding our search criteria in the future may result in the discovery of an even larger number of related domains. It also has the side effect of increasing our false-positive rate, or the discovery of domains that appear related but may, in fact, be legitimate web sites used for other purposes. In addition, the amount of manual analysis required to filter out such false positives further forced us to limit our search. Our results are shown in Table 10.2.

We can draw two clear conclusions from the results of our analysis. First, a large number of both typo and cousin domain names were registered by parties other than the candidate's own campaign. We found that many of the registered

Domain Name	Registered Typo Domains	Example	Registered Cousin Domains	Example
barackobama	52 of 160	narackobama	337	notbarackobama
brownback	0 of 134		152	runagainstbrownback
chrisdodd	14 of 145	chrisdod	21	chrisdoddforpresident
cox2008	3 of 92	fox2008	50	johncox2008
gilmoreforpresident	0 of 276		20	jimgilmore2008
gohunter08	1 of 150	ohunter08	23	stopduncanhunter
hillaryclinton	58 of 191	hillaryclinton	566	blamehillaryclinton
joebiden	15 of 125	jobiden	43	firejoebiden
johnedwards	34 of 170	hohnedwards	190	goawayjohnedwards
johnmccain	20 of 137	jhnmcain	173	nojohnmccain
joinrudy2008	9 of 173	jionrudy2008	123	dontjoinrudy2008
mikehuckabee	3 of 167	mikehukabee	28	whymikehuckabee
mittromney	18 of 123	muttromney	170	donttrustmittromney
richardsonforpresident	2 of 340	richardsonforpresiden	69	nobillrichardson
ronpaul2008	11 of 143	ronpaul20008	276	whynotronpaul
teamtancredo	1 of 170	teamtrancredo	16	whytomtancredo
tommy2008	1 of 107	tommyt2008	30	notommythompson

**Table 10.2:** Typo squatting and cousin domain analysis results. Many typo domain names were already registered and being used in bad faith. In addition, even more cousin domain names were registered, both in support of a candidate and, in many cases, to detract from a candidate. Note that all domains and examples are in the .com top-level domain.

web sites, in both the typo squatting case and the cousin domain name case, were registered for the purpose of driving traffic to advertising web sites.

Second, candidates have not done a good job in protecting themselves by proactively registering typo domains to eliminate potential abuse. In fact, we were able to find only a single typo web site that had been registered by a candidate's campaign: <http://www.mittromny.com>. All typo domains were owned by third parties that appeared unrelated to the candidate's campaign.

One observation that we made is that many of the typo domains that displayed contextual advertisements were, in fact, displaying advertisements that pointed back to a candidate's legitimate campaign web site. This is best demonstrated in Figure 10.1. In such cases, a typo squatter had taken over the misspelling of a candidate's domain name and was able to profit from it. Even worse, the candidate was paying to have his or her ads displayed on the typo squatter's web site! This is a result of the way in which ad syndication on the Internet works.





**Figure 10.1:** When we visited <http://www.barackobams.com> (a typo of Barack Obama's web site, <http://www.barackobama.com>), it contained advertisements pointing to the candidate's legitimate campaign site.

Ad syndicates display advertisements on a web site by indexing its content and displaying advertisements that are appropriate given that content. They may also look at the domain name itself and display advertisements for matching keywords in the domain name. As a result, advertisements for the legitimate campaign may be displayed on a typo squatter's web site. When a user mistypes the web site name and browses to the typo domain, he or she is presented with an advertisement for the legitimate campaign's web site. If the user clicks on this advertisement, the ad syndicate generates a profit, giving a portion to the typo squatter for generating the click through and charging the advertiser, which in this case is the legitimate campaign.<sup>10</sup>

10. A more detailed discussion of how Internet advertising works can be found in Chapter 11.

Individuals who register cousin domain names may have similar motives to those of typo squatters, but they may also be speculating on the value of the domain name itself, with the intent to resell it at a later date. It is also possible that they intend to use the domain to defraud people or to make people wary of emails purportedly coming from a given candidate.

In our analysis, the majority of the identified domains, both in the typo and cousin cases, likely had been acquired in bulk, for the explicit purpose of driving traffic to advertisements. As a result, many of these domains were parked with companies that provide a framework for domain name owners to profit from the traffic that their web sites receive.

### 10.1.3 Domain Parking

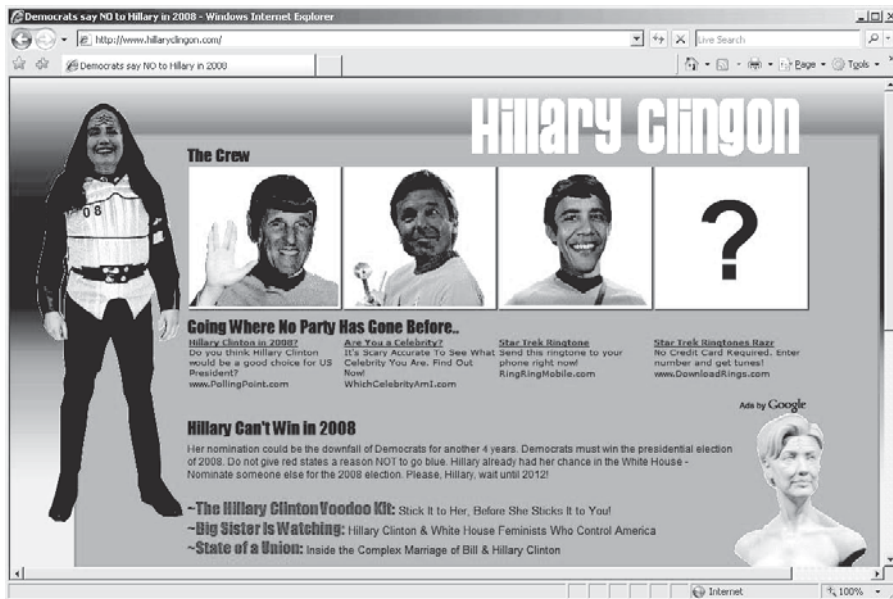
Typo squatters and domain name speculators need not host the physical web infrastructure required to display their own web content or to host their advertisements. Instead, domain name owners can rely on domain parking companies that will happily handle this task for them, for an appropriate share of the advertising revenue. Domain name parking companies will provide the required web site and leverage their preestablished relationships with advertising providers to make life as simple as possible for domain name owners. To leverage a domain name parker, the domain name owner need only configure his or her domain's primary and secondary DNS servers to that of the domain parker. This makes the acquisition and profit from the ownership of a domain name even simpler, to the extent that an individual need just register a domain name and park it at the same time.

While registering a domain name and parking that domain name put the core requirements and relationships in place for a revenue generation model, they do not guarantee that the domain owner will, in fact, profit from this setup. To generate a profit, an adequate amount of traffic and interest must be generated to draw Internet users to that domain name. As such, more emphasis is placed on domain names that are more likely to generate more interest. This is supported by our analysis in Table 10.1, which clearly demonstrates that typo squatters and speculators have favored the domain names of leading candidates.

### 10.1.4 Malicious Intent

While advertising has been the primary motive behind the registration of typo and cousin name domains to date, more measurable damage using these techniques is highly likely to occur. We have already observed a number of cases where a





**Figure 10.2:** <http://www.hillaryclinton.com> is a typo-squatted version of Hillary Clinton's real web site, <http://www.hillaryclinton.com> (the "g" key is right below the "t" key on the keyboard), but it has another meaning as well.

typo-squatted domain has been forwarded to an alternative site with differing political views, as seen in Figures 10.2, 10.3, and 10.4. This is problematic in the typo squatting case, because the end user is unknowingly being redirected to a different web site. It is even more common when analyzing cousin domains, which can be registered by anyone; the number of possible registrations can become nearly infinite. It is, however, much more difficult to drive visitors to those domains without having some way in which to attract them. As such, owners of cousin domains use other techniques to attract visitors, including manipulating search engines to increase their ranking (search engine optimization) or, in some cases, even taking out their own advertisements. It may also involve phishing-style spamming of a large number of users.

One interesting side effect of ad syndication networks as they exist today is that we frequently encounter typo domains that are hosting advertisements for a candidate's competitor. It is interesting to see how search engine optimization and keyword purchasing play roles in attracting visitors. Many search engines allow the purchasing of advertisements that are displayed only when users search for specific keywords. Google AdWords is a popular example of such a program where particular keywords can be purchased and advertisements of the purchaser's



**Figure 10.3:** <http://www.joinrudy2008.com>, a typo-squatted version of Rudy Giuliani’s campaign web site, <http://www.joinrudy2008.com>, redirects users to a detractor’s web site at <http://rudy-urbanlegend.com>.

choice will then be displayed. As shown in Figure 10.5, this may result in advertisements for one candidate being displayed when a user is searching for a particular keyword, or accidentally browsing to a typo-squatted web site.

Advertising, misdirection, and detraction aside, the real potential for future abuse of typo and cousin domains may revolve around the distribution and installation of security risks and malicious code. This attack vector is by no means new, as web sites and banner advertisements are frequently used to attack visitors who happen to browse to a malicious web site [233]. Attackers who control such web sites frequently leverage a software vulnerability in the web browser [234], or use social engineering and misleading tactics to trick the user into installing security risks [95] and malicious code. Even in the absence of a software vulnerability, we can conceive of a number of convincing scenarios that an attacker might use to convince visitors to install such software. For example, a site could easily mirror Hillary Clinton’s legitimate web site, but prominently feature an offer for a Hillary Clinton screensaver that is, in fact, spyware or malicious code.

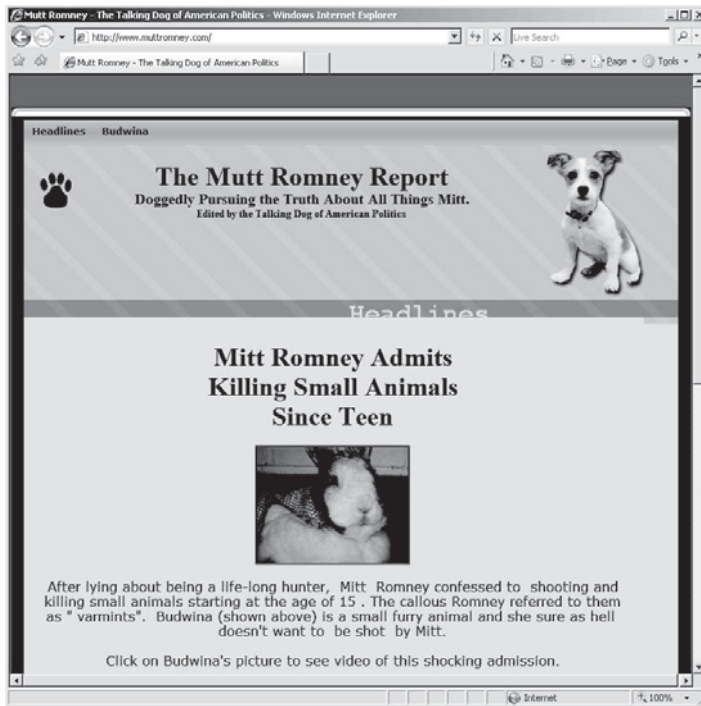


Figure 10.4: <http://www.mutttromney.com> is a typo-squatted version (the “u” key is beside the “i” key on the keyboard) of Mitt Romney’s web site, <http://www.mittromney.com>, which redirects the user to a detractor’s web site.

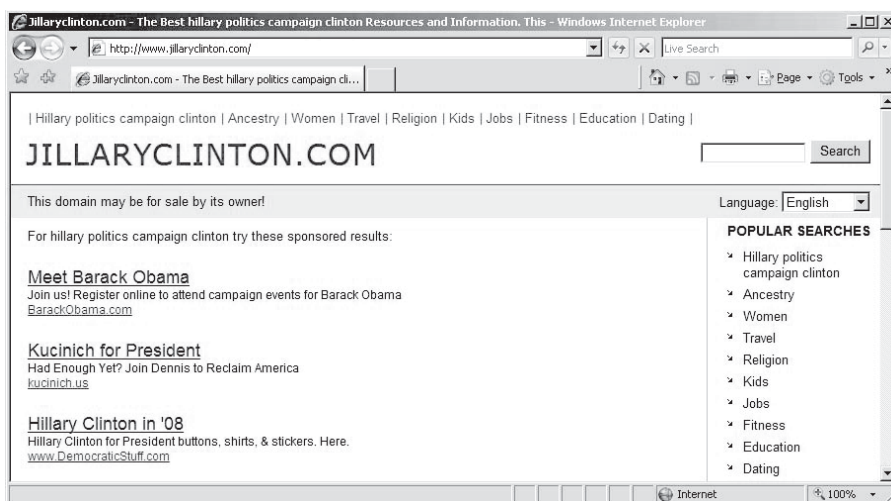


Figure 10.5: <http://www.jillaryclinton.com>, a typo-squatted version of Hillary Clinton’s web site, <http://www.hillaryclinton.com>, displays advertisements directing visitors to rival web sites.

Another site, perhaps mirroring that of Rudy Giuliani, might offer an application claiming to give instant access to his travels, speeches, and videos. Yet another site might claim that by downloading an application, the visitor can assist the candidate in fundraising; that application would, instead, monitor and steal the victim's own banking credentials. The impact of downloading such an application under false pretenses is covered in more detail later in this chapter.

## 10.2 Campaign-Targeted Phishing

Phishing has without a doubt become one of the most widespread risks affecting Internet users today. When we look at phishing and the role that it may play in an election campaign, we can readily envision several incremental risks that present themselves beyond the traditional theft of confidential information.

### 10.2.1 Profit-Motivated Phishing

Profit-motivated, event-based phishing is certainly not new. It has been seen in the past on numerous occasions leading up to and following significant events worldwide. For example, this type of attack was seen after natural disasters such as the Indian Ocean tsunami in 2004 [66] and Hurricane Katrina in 2005 [220, 251]. It was also seen in conjunction with sporting events, such as the 2006 and 2010 FIFA World Cup [275].

Election-related phishing has been observed in the past. During the 2004 federal election, phishers targeted the Kerry-Edwards campaign [370], a campaign that was acknowledged as being at the forefront of leveraging the Internet for communications. At least two distinct types of phishing were observed. In one case, phishers set up a fictitious web site to solicit online campaign contributions shortly after the Democratic National Convention; this site stole the victim's credit card number, among other information. In the second case, phishers asked recipients to call a for-fee 1-900 number, for which the victim would subsequently be charged \$1.99 per minute [417]. This is a prime example of how such attacks can cross technology boundaries to appear even more convincing. The perpetrators of these two attacks were never caught.

When considering the 2004 election as a whole, phishing presented only a marginal risk. At the time, phishing was still in its infancy, and had yet to grow into the epidemic that can be observed today. When assessing the potential risk of phishing in conjunction with the 2008 federal election, however, we find ourselves in a much different position. Candidates have flocked to the Internet, seeing it as a key means to communicate with constituents and to raise campaign contributions.

Domain Name	Redirects to
barackobama.com	<a href="https://donate.barackobama.com">https://donate.barackobama.com</a>
brownback.com	<a href="https://www.campaigncontribution.com">https://www.campaigncontribution.com</a>
chrisdodd.com	<a href="https://salsa.wiredforchange.com">https://salsa.wiredforchange.com</a>
cox2008.com	<a href="https://www.completecampaigns.com">https://www.completecampaigns.com</a>
mikehuckabee.com	<a href="https://www.mikehuckabee.com">https://www.mikehuckabee.com</a>
gilmoreforpresident.com	<a href="https://www.gilmoreforpresident.com">https://www.gilmoreforpresident.com</a>
gohunter08.com	<a href="https://contribute.gohunter08.com">https://contribute.gohunter08.com</a>
hillaryclinton.com	<a href="https://contribute.hillaryclinton.com">https://contribute.hillaryclinton.com</a>
joebiden.com	<a href="https://secure.ga3.org">https://secure.ga3.org</a>
johnedwards.com	<a href="https://secure.actblue.com">https://secure.actblue.com</a>
johnmccain.com	<a href="https://www.johnmccain.com">https://www.johnmccain.com</a>
joinrudy2008.com	<a href="https://www.joinrudy2008.com">https://www.joinrudy2008.com</a>
mittromney.com	<a href="https://www.mittromney.com">https://www.mittromney.com</a>
richardsonforpresident.com	<a href="https://secure.richardsonforpresident.com">https://secure.richardsonforpresident.com</a>
ronpaul2008.com	<a href="https://www.ronpaul2008.com">https://www.ronpaul2008.com</a>
teamtancredo.com	<a href="https://www.campaigncontribution.com">https://www.campaigncontribution.com</a>
tommy2008.com	<a href="https://secure.yourpatriot.com">https://secure.yourpatriot.com</a>

**Table 10.3:** An analysis of 2008 federal candidate web sites and the sites to which contributors are directed to. The sites to which contributors are redirected are legitimate, but the fact that they are often different from the original site increases the risk for confusion and thereby the risk that a phishing attack with a similar design would succeed.

We performed an analysis of campaign web sites in an attempt to determine to what degree they allow contributions to be made online. We discovered that every candidate provided a mechanism by which supporters could make a donation online. All of the web sites on which contributions could be made leveraged SSL as a means to secure the transaction. We also noted the domain of each contribution site. In numerous cases, would-be contributors were redirected to a third-party site, which sat on a different primary domain. Table 10.3 lists both the original domain, and the web site to which the user is redirected.

This redirection was the result of third-party consulting, media, and online advocacy firms being used to assist in the running of the campaign, including the processing of online campaign contributions. This practice does not present a security risk in and of itself, nor is it an indication that phishing is taking place; however, the change in the top-level domain may add to the confusion of potential contributors, who tend to err on the side of caution. It also indicates that additional parties may be involved in the gathering and processing of personal information on

behalf of a campaign, increasing the overall exposure of the credit card numbers processed during fundraising.

It should also be noted that the redirection used here is not necessary, and that the contribution site could just as easily remain in the same top-level domain, as a subdomain hosted by the third party for processing. To do so simply requires the appropriate configuration of the primary domain's DNS records. In fact, the majority of the remaining candidates have chosen to follow this path. Future research may also reveal whether those donation sites that do live under the campaign's domain name are, in fact, hosted on the same physical network as the campaign web site or on another third-party payment processor's network.

Figure 10.6 provides a sample of the information collected during an online contribution. We found that forms were fairly consistent in the type of information that was collected, while (not surprisingly) varying from a visual perspective.

The ability to process credit card transactions on an authentic campaign web site may provide an unexpected benefit to online identity thieves. One tactic

**MAKE AN ONLINE CONTRIBUTION**

[Click here to contribute by mail](#)

**CONTACT INFORMATION**

First Name:   
Last Name:   
Address:   
City:   
State:   
Zip:   
Phone:   
Email:

**SELECT A TYPE AND AMOUNT**

☒ One-time contribution ☐ Recurring monthly [\(what's this?\)](#)

☐ \$10 ☐ \$50 ☐ \$250 ☐ \$1000 ☐ \$4600  
☐ \$25 ☐ \$100 ☐ \$500 ☐ \$2300 ☐ Other \$

**CREDIT CARD INFORMATION**

Card Number:    
Expiration:    
Security Code:  [\(what's this?\)](#)

**EMPLOYMENT**

To comply with Federal law, we must use best efforts to obtain, maintain, and submit the name, mailing address, occupation and name of employer of individuals whose contributions exceed \$200 in an election cycle.  
If not employed, enter "none"  
Employer:   
Occupation:

**CONFIRM YOUR ELIGIBILITY**

☐ By checking this box, I confirm that the following statements are true and accurate:

1. This contribution is made from my own funds, and not those of another.
2. This contribution is not made from the general treasury funds of a corporation, labor organization or national bank.
3. I am not a Federal government contractor.
4. I am not a foreign national who lacks permanent resident status in the United States.
5. I am at least 18 years of age.
6. This contribution is made on a personal credit or debit card for which I have the legal obligation to pay, and is made neither on a corporate or business entity card nor on the card of another.

**SUBMIT**

**Figure 10.6:** A sample form from one candidate's web site allowing visitors to make contributions online. This is a legitimate site. Given that typical Internet users would not be well acquainted with the domains associated with political candidates, there is a risk that phishers might use a similarly designed web site to collect credentials from unsuspecting victims.



regularly employed by those peddling in stolen credit cards is to process a very small transaction so as to validate a credit card as legitimate [48]. Thieves began using this technique in early 2007 on online charity web sites, but it has long been used on other types of online payment sites. Such a small transaction is unlikely to be noticed by the credit card holder and is unlikely to be flagged by the party processing the transaction.

Of course, not all contributions would necessarily be helpful. Attackers might seek to disrupt a candidate's fundraising efforts by initiating illegitimate payments to create confusion. If performed en masse, the widespread contribution of small, random amounts of money, from thousands or tens of thousands of stolen credit cards, would certainly have a negative effect. While there is a slight chance such an attack might remain stealth, it is more likely that it will be noticed, making it nearly impossible to differentiate legitimate contributions from fraudulent donations. Thus a significant burden would be placed on the affected candidates by diluting legitimate contributions with those that were not initiated by the credit card owners.

The increased collection of online campaign contributions also provides a ripe opportunity for phishers to target members of the unsuspecting public. Candidates and their parties regularly communicate with voters through email, as demonstrated in Figure 10.7. Phishing involves the use of email to lure a victim to a fictitious web site that attempts to steal confidential information from the victim [91]. While it is unreasonable to expect campaigns not to solicit contributions using email as a medium, they would be well advised to follow best practices that have been set by other online entities heavily prone to phishing. (A number of excellent resources are available through the Anti-Phishing Working Group [313], including a report funded by the U.S. Department of Homeland Security [101] that discusses the problem in depth and suggests best practices for organizations to communicate safely with their constituents.) However, whether or not the candidate uses email for contribution requests, a phisher may pose as a candidate and ask the recipients of his or her email for money. The typical goal would be to steal the credentials of the victims.

Phishers can increase their success rate by registering domain names that are typos or cousin domains of their target, a tactic already discussed in some depth in this chapter. For example, a phisher targeting John Edwards might elect to register `donatejohnedwards.com`. Additionally, phishers may simply create subdomains for primary domains that they already own. A phisher who buys the domain `donatefor2008.com`, for example, might simply add DNS records for `johnedwards.donatefor2008.com` and `ronpaul.donatefor2008.com`, among others. These domain names could then be referenced in the phishing emails sent to



**Figure 10.7:** A portion of a legitimate fundraising email, which allows the recipient to click on the hyperlinked “Contribute” button to support the campaign. This approach would be very easy for a phisher to mimic in an effort to make people submit their credentials to the phisher, thinking they are contributing. Of course, phishers can use inflammatory texts (even more so than political candidates) as calls for action. The authors of this book were able to register the domain `democratic-party.us`, which would be suitable in such an attack, and found a wealth of other cousin name domains available for both parties. Thus, whereas financial institutions typically have registered cousin name domains to defend against abuse, political parties and candidates have not.

potential victims. When clicked on, the link would drive the victim to the fictitious web site.

As we have observed, a significant number of typo domain names have already been registered, or are available to be registered, by parties who are acting in bad faith. Many of these domain names appear so similar to the legitimate domain name that the unsuspecting eye of a potential victim would not notice if directed to one of these sites. Campaigns can take clear and immediate steps to purchase typo domains prior to them falling into the wrong hands. As of this writing, few have done so.

More difficult, however, is the acquisition of cousin domain names. As discussed previously, a significant number of cousin domain names have been registered for both speculative and advertising purposes. Given the near-infinite number of possible cousin domain names, it is unlikely that a campaign could acquire all possibilities. This fact of life provides phishers with the opportunity to register a domain name that may appear similar to the legitimate campaign’s web site.



Yet another type of attack might use a spoofed email that appears to come from a political party or candidate to entice recipients to open attachments, thereby infecting their machines with malicious code. Again, this may be done either with the direct goal of spreading malicious code or to deliver a below-the-belt blow to political candidates who rely heavily on the Internet for their communication with constituents.

Even without the registration of a similar domain name, phishers will undoubtedly continue to succeed in constructing emails and web sites that are obvious to detect by a trained eye, but perhaps not so obvious to those who continue to fall victim to them.

### **10.3 Malicious Code and Security Risks**

Malicious code and security risks present some of the more sinister risks to the election process. Malicious code, such as threats that leverage rootkit capabilities,<sup>11</sup> has the potential to gain complete and absolute control over a victim's computer system. Likewise, security risks such as adware and spyware pose serious concerns, both in terms of their invasiveness to a user's privacy (in the case of spyware) and their ability to present users with unexpected or undesired information and advertisements (in the case of adware).

We can consider a number of scenarios where well-known classes of malicious code may be tailored specifically to target those participating in an election. Targets may range from candidates and campaign officials to voters themselves. In discussing these risks we begin with what we consider the less serious category of security risks; we then move into the more serious, insidious category of malicious code.

#### **10.3.1 Adware**

Adware, in its truest form, may not pose an immediate and dire risk to the end user. Once installed, however, its control over a user's Internet experience places it into a strategic position on the end user's computer. Adware has the potential to manipulate a user's Internet experience by displaying unexpected or unwanted advertisements. These advertisements may be displayed on the user's desktop or shown to the user through the web browser as the user visits Internet web sites. These advertisements may appear as pop-up windows, or they may appear as content (ads) that are either overlaid or inserted into existing web pages visited by

---

11. A detailed discussion of rootkits can be found in Chapter 8.

the user. Both techniques have been used frequently by such well-known adware applications as 180Solution's Hotbar [99], Gator Corporation's Gator [96], and WhenU's Save [97]. Adware may be installed by the end user as part of another third-party application, or it may be installed surreptitiously through the exploitation of a software vulnerability in the user's web browser. Chapter 12 discusses adware in more detail.

Adware might be used in numerous ways to influence or manipulate users during the course of an election. In its most innocuous form, adware might simply present the user with advertisements promoting a particular candidate and directing the user to the candidate's web site when clicked. Taking a more deceptive angle, adware might be used to silently replace advertisements for one candidate with another. This may be done directly in the user's browser by manipulating the incoming HTML content before it is rendered or by overlaying a new advertisement on top of an existing advertisement on the user's screen.

Until it is observed in the wild, it is difficult for us to predict the real-world impact that such an adware application might have. It would be important for such an application to be silent and unobtrusive, acting clandestinely to avoid annoying the end user lest its objective backfire. In addition, such an effort may simply help to sway those voters who have not already committed to a particular party or candidate, rather than those voters who have already made their decision.

### 10.3.2 Spyware

We have frequently seen adware and spyware traits combined into a single application that both delivers advertising and monitors a user's Internet habits. For the purposes of our discussion, we chose to distinguish between the distinct behaviors of adware and spyware, discussing each separately. Spyware, with its ability to secretly profile and monitor user behavior, presents an entirely new opportunity for the widespread collection of election-related trend data and behavioral information.

When discussing the use of spyware, we can conceive of a number of behaviors that might be collected throughout the course of an election in an attempt to provide insight into voters' dispositions. The most basic tactic would be to monitor the browsing behavior of voters and to collect the party affiliations of the Internet sites most frequently visited by the end user. Even without the installation of spyware on an end user's computer, one web site may silently acquire a history of other web sites that the user has previously visited. This capability has been demonstrated by researchers in the past and can be observed at <https://www.indiana.edu/~phishing/browser-recon>. This type of data collection may also

include the tracking of online news articles that are viewed and online campaign contributions that are made by determining whether a particular URL was visited.

With the addition of spyware on the end user's computer, these information-gathering efforts can be taken a step further. Emails sent and received by the user can be monitored, for example. In our study, we found that all 19 candidates allow a user to subscribe to their campaign mailing lists, from which a user receives regular frequent updates on the campaign's progress. Knowing how many voters have subscribed to a particular candidate's mailing list may provide insight into the overall support levels for that candidate.

Of course, Internet and browsing behavior alone may not be an indicator of a voter's preference, as voters may be just as likely to visit a competing candidate's web sites and subscribe to a competing candidate's mailing list so as to stay informed about that candidate's campaign. Unfortunately, we could find no prior research that examined the correlation between user Internet behavior and party or candidate affiliation. Nevertheless, spyware clearly poses a new risk in terms of the mass accumulation of election-related statistics that may be used to track election trends.

The collection of voter disposition data is certainly not new, as groups such as the Gallup Organization [137] (known for the Gallup Poll) have been collecting and analyzing user behavior since 1935. What is different in this case is spyware's ability to capture and record user behavior without consent and without the voter's knowledge. Even when a spyware application's behavior is described clearly in an end-user license agreement (EULA), few users either read or understand these complex and lengthy agreements [98]. This changes the landscape dramatically when it comes to election-related data collection.

### **10.3.3 Malicious Code: Keyloggers and Crimeware**

By far one of the most concerning attacks on voters, candidates, and campaign officials alike is that of malicious code infection. Malicious code that is targeted toward a broad spectrum of voters has the potential to cause widespread damage, confusion, and loss of confidence in the election process itself. When we consider the various types of attacks mentioned in this chapter, malicious code—in the form of keyloggers, trojans, and other forms of crimeware—has the potential to carry each of them out with unmatched efficiency. These attacks include the monitoring of user behavior, the theft of user data, the redirection of user browsing, and the delivery of misinformation.

One additional angle for crimeware is the notion of intimidation. Given a threat's presence on a voter's computer, that threat has the potential to collect personal, potentially sensitive information about that individual. This capability

may include turning on the computer's microphone and recording private conversations. It may include turning on the computer's video camera and recording activities in the room. It may include retrieving pictures, browser history documents, or copyrighted files from a voter's computer. Perhaps the individual would be turned in to the RIAA if copyrighted music was found on his or her computer. This kind of information gathering creates the potential for an entirely new form of voter intimidation. The collection of such personally sensitive or legally questionable data by a threat might, therefore, allow an attacker to intimidate that individual in an entirely new way. We would, of course, expect and hope that the number of voters who might be intimidated in such a way would be relatively low, but only time will tell whether such speculation becomes reality.

Another form of threat that we have seen in the past involves holding a victim's data hostage until a fee is paid to release it. This possibility was first discussed in [487]. An example of such a threat is Trojan.Gpcode [340], which encrypts the user's data, erasing the original information, until this fee is paid. Such a threat may present another new form of intimidation whereby the only way for a user to regain access to his or her personal data is to vote accordingly. Such an attack presents obvious logistical challenges. For example, how is the attacker to know which way the victim voted? The attacker may, however, take comfort in the belief that he or she has intimidated enough of the infected population to make a meaningful difference.

Just as the widespread infection of the populace's computers poses a risk to voters, the targeted, calculated infection of specific individuals' computers is equal cause for concern. A carefully placed targeted keylogger has the potential to cause material damage to a candidate during the election process. Such code may also be targeted toward campaign staff, family members, or others who may be deemed material to the candidate's efforts. Such an infection might potentially result in the monitoring of all communications, including email messages and web site access initiated on the infected computer. This monitoring would give the would-be attacker unparalleled insight into the progress, plans, and disposition of the candidate's campaign, perhaps including new messaging, speeches, and otherwise sensitive information critical to the candidate's campaign.

## 10.4 Denial-of-Service Attacks

Denial-of-service attacks have become increasingly common on the Internet today. These kinds of attacks seek to make a computer network—in most cases, a particular web site—unavailable and therefore unusable. Also known as distributed denial-of-service (DDoS) attacks, they are frequently launched by means of

inundating a target with an overwhelming amount of network traffic. This traffic may take the form of Internet protocol requests at the IP and TCP layers or application-level requests that target specific applications such as an organization's web server, email server, or FTP server. Denial-of-service attacks are frequently perpetrated through the use of bot networks, as discussed in more detail in Chapter 7.

A number of high-profile, wide-scale DDoS attacks have demonstrated the effects that such an effort can have. One of the best-known and largest attacks was launched against the country of Estonia in May 2007 [81]. It presented a prime example of a politically motivated attack, as it was launched by Russian patriots in retaliation for the removal of a Soviet monument by the Estonian government. Attackers disabled numerous key government systems during a series of attacks that occurred over the course of several weeks.

In 2006, Joe Lieberman's web site also fell victim to a concentrated denial-of-service attack [397]. Forcing the site offline, the attack paralyzed the joe2006.com domain, preventing campaign officials from using their official campaign email accounts and forcing them to revert to their personal accounts for communication.

The implications of such attacks are clear: They prevent voters from reaching campaign web sites, and they prevent campaign officials from communicating with voters.

## 10.5 Cognitive Election Hacking

Labeled by researchers as *cognitive hacking* [73], the potential for misinformation and subterfuge attacks using Internet-based technologies is as rich as one's imagination. We have already discussed several techniques that may be used to surreptitiously lure users to locations other than a legitimate campaign's web site. These same techniques can be used to spread misleading, inaccurate, and outright false information.

So far, we have discussed typo and cousin domain names that users may visit accidentally when attempting to browse to a legitimate web site. We have also discussed phishing and spam, which have the potential to lure users to web sites by impersonating legitimate candidate web sites. Finally, we have discussed malicious code and the role that it may play in manipulating a user's desktop experience before the user even reaches the intended destination.

The security of a campaign's web site plays another vital role in determining voters' faith in the election process. The breach of a legitimate candidate's web site,

for example, would allow an attacker to have direct control over all content viewed by visitors to that web site. This may allow for the posting of misinformation or, worse, the deployment of malicious code to unsecured visitors.

Examples of misinformation about a specific candidate might include a false report about the decision by a candidate to drop out of the race, a fake scandal, and phony legal or health issues. It might also take the form of subtle information that could be portrayed as legitimate, such as a change in a candidate's position on a particular subject, resulting in abandonment of the candidate by voters who feel strongly about that issue.

Attempts to deceive voters through the spread of misinformation are not new. In fact, numerous cases have been documented in past elections using traditional forms of communication [358]. These include campaigns aimed at intimidating minorities and individuals with criminal records, attempts to announce erroneous voting dates, and many other tactics resulting in voter confusion.

During the 2006 election, 14,000 Latino voters in Orange County, California, received misleading letters warning them that it was illegal for immigrants to vote in the election and that doing so would result in their incarceration and deportation. In his testimony before congress, John Trasviña, President and General Counsel of the Mexican American Legal Defense and Educational Fund (MALDEF), discussed this use of misinformation as an example of voter suppression:

First, the Orange County letter falsely advised prospective voters that immigrants who vote in federal elections are committing a crime that can result in incarceration and possible deportation. This is a false and deceptive statement: Naturalized immigrants who are otherwise eligible to vote are free to vote in federal elections without fear of penalties (including but not limited to incarceration and/or deportation). Second, the letter stated that "the U.S. government is installing a new computerized system to verify names of all newly registered voters who participate in the elections in October and November. Organizations against emigration will be able to request information from this new computerized system." Again, the letter adopts an intimidating tone based upon false information in an apparent attempt to undermine voter confidence within the targeted group of voters. Finally, the letter stated that "[n]ot like in Mexico, here there is no benefit to voting." This letter, representing a coordinated and extensive effort to suppress the Latino vote in the days leading up to a congressional election, has been traced to a candidate running for the congressional seat in the district in which the affected voters live.<sup>12</sup>

---

12. United States Senate Committee on the Judiciary Prevention of Deceptive Practices and Voter Intimidation in Federal Elections: S. 453 Testimony of John Trasviña. Available at [http://judiciary.senate.gov/testimony.cfm?id=2798&wit\\_id=6514](http://judiciary.senate.gov/testimony.cfm?id=2798&wit_id=6514)



Another case of deception was targeted at college students in Pittsburgh, Pennsylvania, in 2004 [355]. Canvassers, posing as petitioners for such topics as medical marijuana and auto insurance rates, gathered signatures from students that, unknown to them, resulted in a change to their party affiliation and polling location.

Push polling is one technique that lends itself extremely well to Internet-based technologies. In push polling, an individual or organization attempts to influence or alter the views of voters under the guise of conducting a poll. The poll, in many cases, poses a question by stating inaccurate or false information as part of the question. One well-known push poll occurred in the 2000 Republican Party primary.<sup>13</sup> Voters in South Carolina were asked, "Would you be more likely or less likely to vote for John McCain for president if you knew he had fathered an illegitimate black child?" In this case, the poll's allegation had no substance, but was heard by thousands of primary voters. McCain and his wife had, in fact, adopted a Bangladeshi girl.

A bill known as the Deceptive Practices and Voter Intimidation Prevention Act of 2007<sup>14</sup> seeks to make these attacks illegal. Currently waiting to be heard in the Senate, it is possible that this bill might be in place for the 2008 federal election, making deceptive tactics such as these illegal, and introducing a maximum penalty of up to 5 years in prison for offenders. This legislation is likely to apply to deceptive practices whether they are performed using traditional communication mechanisms or Internet-based technologies.

While the introduction of such policies is important and provides a well-defined guideline under which to prosecute offenders, only time will tell to what extent legislation will succeed in controlling these acts. As we have seen in some areas, such as the policies developed to outlaw the transmission of spam email, regulations have only marginal effectiveness in reducing the problem. Even today, more than 50% of all email sent on the Internet is purported to consist of spam [401]. There is no reason to doubt that the type of deception and intimidation discussed will be equally successful on the Internet.

The challenge with Internet-based technologies is the ease with which such an attack may be perpetrated. Whereas traditional communication media may have required an organized effort to commit an attack, the Internet allows a single attacker to realize the benefits of automation and scale that previously did not

---

13. SourceWatch. [http://www.sourcewatch.org/index.php?title=Push\\_poll](http://www.sourcewatch.org/index.php?title=Push_poll)

14. Deceptive Practices and Voter Intimidation Prevention Act of 2007. <http://www.govtrack.us/congress/billtext.xpd?bill=h110-1281>

exist. As such, one person has the potential to cause widespread disruption, with comparably little effort.

Historically, some of the most successful misinformation attacks on the Internet have been motivated by profit. Pump-and-dump schemes [369], for example, have become an extremely common form of spam. These schemes involve the promotion of a company's stock through the issuance of false and misleading statements. After the stock price rises owing to renewed interest from the message's recipients, the perpetrators sell their own stock for a substantial profit.

One significant surge of pump-and-dump emails that was observed in 2006 was attributed to a bot network, operated by Russian fraudsters [268]. In this attack, 70,000 infected computers spread across 166 countries were organized into a bot network that was used to send out unsolicited stock-promoting spam. Such a network could easily be directed to send any form of email, including disinformation and fallacies related to a candidate, voters, and the election itself. Chapter 7 discusses botnets and their applications in more detail.

## 10.6 Public Voter Information Sources: FEC Databases

The Federal Election Commission [62] was created both to track campaign contributions and to enforce federal regulations that surround them.

In 1975, Congress created the Federal Election Commission (FEC) to administer and enforce the Federal Election Campaign Act (FECA)—the statute that governs the financing of federal elections. The duties of the FEC, which is an independent regulatory agency, are to disclose campaign finance information, to enforce the provisions of the law such as the limits and prohibitions on contributions, and to oversee the public funding of Presidential elections.

To provide a public record of campaign contributions, the FEC must maintain, and provide to the public, a full record of all campaign contributions. Many web sites that allow online contributions clearly indicate their requirement to report those contributions to the Federal Election Commission. The following text, taken from one candidate's web site exemplifies this kind of disclaimer:

We are required by federal law to collect and report to the Federal Election Commission the name, mailing address, occupation, and employer of individuals whose contributions exceed \$200 in an election cycle. These records are available to the public. However, they cannot be used by other organizations for fundraising. We also make a note of your telephone number and email address, which helps us to contact you quickly if follow-up on your contribution is necessary under Federal election law. For additional information, visit the FEC website at <http://www.fec.gov>.



The FEC's role is to make this data available to the public. The information is available as raw data files, via FTP, and through online web interfaces on the FEC web site.

Numerous third-party web sites, such as <http://www.opensecrets.org>, also use this data to provide regular high-level reports on candidate funding. Consumers of the data are restricted by a policy that regulates how the data can be used [64]. The policy is surprisingly lenient, as it is primarily intended to prevent the use of contributors' names for commercial purposes or further solicitation of contributions.

The information provided in this database consists of each contributor's full name, city, ZIP code, and particulars of the contribution, such as the receiving candidate or party, the amount, and the date of the contribution. While limited, this information does allow one to build a history of political contributions for any U.S. citizen who appears in the database.

Contributors of record may be more likely to become victims of the other attacks already discussed in this chapter. Appearing in this database may expose high-net-worth contributors to targeted phishing (spear phishing) or malicious code attacks if the individual's name can be connected to his or her email address (no longer a difficult feat).

## 10.7 Intercepting Voice Communications

While this chapter has focused primarily on Internet-based risks, we would be remiss if we did not discuss at least one additional risk given a recent particularly noteworthy and sophisticated attack against a foreign nation's communication infrastructure. Labeled the *Athens Affair* by authors Vassilis Prevelakis and Diomidis Spinellis [320], this well-coordinated attack highlighted the increased role that common technologies play in all forms of our daily communications. In their paper, the authors retrace the alarming events related to the interception of cell phone communications from high-ranking Greek government officials:

On 9 March 2005, a 38-year-old Greek electrical engineer named Costas Tsalikidis was found hanged in his Athens loft apartment, an apparent suicide. It would prove to be merely the first public news of a scandal that would roil Greece for months.

The next day, the prime minister of Greece was told that his cell phone was being bugged, as were those of the mayor of Athens and at least 100 other high-ranking dignitaries, including an employee of the U.S. embassy.

The victims were customers of Athens-based Vodafone-Panafon, generally known as Vodafone Greece, the country's largest cellular service provider; Tsalikidis was in charge of network planning at the company. A connection seemed obvious. Given the

list of people and their positions at the time of the tapping, we can only imagine the sensitive political and diplomatic discussions, high-stakes business deals, or even marital indiscretions that may have been routinely overheard and, quite possibly, recorded.




















Even before Tsalikidis's death, investigators had found rogue software installed on the Vodafone Greece phone network by parties unknown. Some extraordinarily knowledgeable people either penetrated the network from outside or subverted it from within, aided by an agent or mole. In either case, the software at the heart of the phone system, investigators later discovered, was reprogrammed with a finesse and sophistication rarely seen before or since.

In this attack, perpetrators used rootkit techniques, like those discussed in Chapter 8, on the cellular provider's phone switch to remain hidden. Over the past two decades, the basic communications systems that we rely on for both our traditional land-line telephones and our cellular phone communications have increasingly moved to commodity-based hardware and software [108]. In the past, would-be attackers were forced to learn complex and proprietary embedded systems, making the introduction of malicious code on these systems difficult, if not impossible. Today's commoditization simplifies this effort, as witnessed by the attack discussed here, and greatly increases the likelihood that an attacker might gain a similar foothold on communications systems in the future.

Central switching networks are not the only target. Mobile devices themselves remain even more likely candidates for interception of communications. Today's mobile devices, an increasing number of which can be considered smartphones, provide ripe opportunities for the introduction of malicious code. While traditional threats such as viruses, worms, and trojans have yet to gain widespread prominence on mobile devices (although they do exist), the potential for targeted customized mobile threats has existed for some time.

One particular application, known as FlexiSpy and sold by Bangkok, Thailand-based software vendor Vervata, allows listening to a remote phone's surrounding while it is not in use (Figure 10.8). It also allows retrieval of the phone's personal data and monitoring of all email and SMS messages sent by the phone. The software itself is available in "Pro," "Light," "Alert," and "Bug" versions. The vendor prides itself on its software's ability to remain hidden and unnoticeable on an infected device.

The infection of a candidate, campaign staff, or candidate's family's cell phone with such a freely available application could have dire consequences. All back-room and hallway conversations engaged in by the candidate could be monitored at all times and intercepted by the attacker. Worse, opinions—perhaps including those not shared with the public or outsiders—could be recorded and

This page helps you understand what all the spyphone features mean					
	PRO	LIGHT	ALERT	BUG	
<b>Application Features</b>					
 <a href="#">Remote Listening</a>					
Make a spy call to the target phone running FlexiSPY and listen in to the phones surroundings. <b>This does not allow you to listen to the phone conversation in progress.</b> Call Tapping will be available very shortly. Please sign up to our mailing list of you are interested in this feature					
 <a href="#">Control Phone By SMS</a>					
Send secret SMS to the target phone to control all functions. No need to physically access the phone for any feature not related to installation					
 <a href="#">SMS and Email Logging</a>					
All SMS and EMAIL contents are sent to your FlexiSPY web account. Support all languages					
 <a href="#">Call History Logging</a>					
The time, duration and number of all voice calls are sent to your web account. If the phone number is in the phones address book, then the name will be available also					
 <a href="#">Location Tracking</a>					
See the CELL ID and CELL name that the mobile is physically located in. Read more about <a href="#">mobile location tracking by cell id</a>					
 <a href="#">Private Data Deleting</a>					
Delete your videos, pictures, SMS, and application with one SMS					

**Figure 10.8:** FlexiSpy, developed and sold by Bangkok, Thailand's Vervata, allows for monitoring and tapping of cell phone communications. It is supported on Windows Mobile, Symbian OS, and Blackberry devices. Today installation requires physical access to the device. Much like desktop operating systems, however, future versions might be installed through software vulnerabilities or messaging applications.

made available for later playback, introducing the potential for widespread exposure and damage.

We have already seen examples of unexpected recordings accidentally made public for other political figures, including those involving California Governor Arnold Schwarzenegger in 2006 and 2007 [308]. In that case, the recordings were unintentionally exposed through the governor's web site and resulted in criticism of a number of his comments that were made without the intent of them becoming public.

## Conclusion

As campaigns increasingly look to the online medium to gather support, it is important to consider the inherent risks that will follow. In this chapter, we discussed a number of risks that may present themselves in any election campaign; however, it is important to acknowledge that many more remain that we have not discussed.

It is apparent both from past events and from our findings that candidates and their campaigns are just beginning to understand the risks of online advocacy and have yet to take the necessary precautions to protect themselves. Our fear is that a true appreciation of the required countermeasures will not be realized until these attacks do, in fact, manifest themselves.

Many of these individual risks, when combined, would result in increasingly sophisticated attacks. While we have discussed many of these risks independently, the combination of these threats creates complex new variations that are already being seen in the wild in other areas such as online banking and ecommerce.

Our goal in writing this chapter was not to sow seeds in the minds of would-be attackers or to spread fear, uncertainty, and doubt, but rather to discuss real-world risks that already exist. None of the attacks discussed here are new or novel; we have simply applied them to a specific recurring event, the election process. Our hope is to raise awareness of the potential risks before they are able to manifest themselves in the upcoming 2008 federal election, or any election that follows.

One thing is clear: It is impossible for us to predict how successful any one of these attacks might be in making a material impact on the election process. Given our experiences with previous widespread Internet-borne risks, we certainly do have an appreciation and respect for the potential that they present. While that is not to be discounted lightly, only time will tell how dangerous they become.

In addition, if a successful widespread attack were to occur (one that was recognized to have swayed the vote), what recourse is there? What if intimidation, misinformation, and infectious election-targeted malicious code become the norm?

## Acknowledgments

The author wishes to thank Markus Jakobsson for providing a political fundraising email sample, for pointing out additional political-sounding URLs that he had registered, and for contributing helpful discussions, feedback, and comments on earlier drafts. In addition, the author would like to thank Zulfikar Ramzan for his advice, feedback, and recommendations during the writing of this chapter, and Kevin Haley for his recommendation on the addition of push polling.

# Index

---

## Numbers

180Solutions  
  adware techniques for evading law enforcement, 364  
  trends in adware business, 366  
2wire, WAP default settings, 115  
3G mobile technologies, 469  
802.11 standard, wireless routers, 110–113

## A

A records, DNS, 203  
Access control  
  J2EE environment problems, 52  
  as security feature, 43, 49  
  standards for network access, 111  
  WLANs and, 110–111  
Access Control Lists (ACLs), 259  
Access Device Fraud Act, 437, 445  
Accessibility of material, education principles, 397, 410–411  
ACLs (Access Control Lists), 259  
ACPA (Anticybersquatting Consumer Protection Act), 297  
ACPI (Advanced Configuration and Power Interface), 264  
Action-based model, advertising revenues, 329–330  
Active bot-infected computers, Symantec statistics regarding, 186  
ActiveX, 77  
ActiveX, web browser vulnerabilities, 23  
Ad impressions, 327–328  
Ad-provider evasion, hiding click fraud attacks, 174–177  
Adaptability to changing threats, education principles, 397, 412  
Add/Remove Programs  
  adware programs bypassing registration with, 362  
  difficulty in removal of surreptitious software, 417  
Address verification service (AVS), credit card security, 468  
Administrative access, in wireless routers, 111–112  
Adobe Acrobat plug-ins, web browser vulnerabilities, 23  
Adobe Flash, web browser vulnerabilities, 24  
AdSense, Google, 334  
Advanced Configuration and Power Interface (ACPI), 264  
Advertising, 325–353  
  action-based model, 329–330  
  attack types, 335  
  botmasters exploiting click fraud, 379  
  click-based model, 328–329  
  click fraud auditing, 347  
  click spam, 333–334  
  coercion, 336–337  
  containment of abuses, 346–347  
  conversion spam, 334–335  
  countermeasures, 342–343  
  detection of abuses, 344–346  
  domain speculation in politics and, 302–303  
  history of, 325–326  
  human clickers, 335–336  
  impression-based model, 327–328  
  impression spam, 332–333  
  malicious intent in politics, 304–305  
  malicious side of, 391–395  
  manual clickers, 337–339

- Advertising (*contd.*)
  - metrics, 387
  - overview of, 325
  - platform, 387–391
  - prevention of abuses, 343–344
  - referral deals, 331–332
  - revenue models, 326–327
  - robotic clicking, 339–342
  - spam types, 332
  - syndication, 330–331
- Advice, security-related
  - hard to follow and unimportant, 406
  - not absorbed, 407
  - potentially dangerous, 406–407
- Adware, 357–367
  - botnets installing, 214
  - criminal applications of botnets, 383
  - evolution of industry, 366–367
  - industry-wide problems, 360–363
  - law enforcement evasion, 363–365
  - legitimate uses, 357–358
  - malicious side of advertising, 391–395
  - online advertising platform, 387–391
  - overview of, 357–359
  - players in, 359–360
  - political uses of malicious code, 312–313
  - pros/cons of, 386–387, 395
  - revenues/profits from, 365–366
- AdWatcher, preventing click fraud, 179
- AdWords, Google, 328–329
- Affiliate IDs, malware and, 394
- Affiliate marketing, as distribution technique, 24–25
- AGIS, automatic infection signature generation, 478, 481–482
- Agobot, 381
- Airsnort, WEP defeated by, 122–123
- Alt + F4 scams, 289
- AMD Pacifica, 233
- AMD Presidio, 464–466
- AND-based filters
  - composite filters across networks, 74–75
  - composite filters for individual networks, 74
  - overview of, 63
- Anomaly detection systems
  - click fraud detection, 344–345
  - for game scripts, 282
  - IDS (intrusion detection systems), 127
- Anonymizing services, botnets, 205
- Antennas, Warkitting attacks and, 122
- Anti-Phishing Working Group, 3
- Anti-spyware laws, 449–456
  - provisions of, 425–430
- Anticybersquatting Consumer Protection Act (ACPA), 297
- Antivirus programs
  - bots installing, 207
  - ClamAV, 59
  - countermeasures applied at chokepoints, 27
  - limitations as countermeasure to WiFi
    - attacks, 126
  - malicious code disarming, 44
  - shortcomings in protecting P2P networks against malware, 57
  - virus signatures and, 473
- ANYONE role, J2EE environment problems, 52
- API abuse, in Seven Pernicious Kingdoms taxonomy, 43, 48–49
- APIs (application programming interfaces)
  - API abuse, 43, 48–49
  - game security and, 291
- AppInit\_Dlls registry, loading user-mode rootkits, 236
- Apple QuickTime plug-ins, web browser vulnerabilities, 23
- Application-level keyloggers, 9–10
- Applications
  - crimeware run as application program, 30–31
  - future of crimeware and, 517
  - misleading applications, 284–285
  - RFID, 90
- APWG, 399
- Archieveus, 466
- Architecture, MMOGs, 280–283
- ASP.NET, environment problems, 52
- AT&T, education resources for understanding security risks, 403
- Athens Affair, 320
- Attachments
  - distribution techniques, 20
  - political uses of malicious code, 312
- Attack anatomy, in trusted computing, 458–460
- Attack phases, malware, 459–460
- Attack surface, 23
- Attack types, advertising
  - coercion, 336–337
  - human clickers, 335–336
  - manual clickers, 337–339
  - overview of, 335
  - robotic clicking, 339–342
- Attack types, RFID, 92–93
- Attack vectors, wireless routers, 121–122
- Attacker model, RFID, 93–94
- AttentionTrust, 395
- Attestation, in trusted computing, 462
- Auction sites, future of crimeware and, 517–519
- Audience, security goals, 408
- Auditing
  - click fraud, 347–348
  - countermeasures for RFID, 98

## Authentication

- API abuse problems, 48
- authenticated commands in botnets, 222
- countermeasures applied at chokepoints, 27–28
- credit card security, 468
- game security, 291
- identity theft and, 276
- as security feature, 43
- TGs and, 156
- time and state problems and, 49
- Authentication, crimeware resistant, 484–509
  - assumed adversary, 485–486
  - characteristics of good life questions, 497–498
  - economy and security of, 484
  - error rate determination, 499–501
  - finding good life questions, 498–499
  - good vs. bad questions, 502–503
  - human-oriented challenge-response protocols, 492–494
  - life questions, 485
  - on-screen input measures, 487
  - OTP tokens and, 484–485
  - password hashing, 490–491
  - preference-based life questions, 494–497
  - Spyblock system, 491–492
  - SSL with client-side certificates, 488
  - text passwords as authentication mechanism, 486–487
  - two-factor authentication, 488–490
- Authorization, credit card security, 468
- Auto-configuration tools, server-compromise attacks, 24
- Auto-tagging feature, Google, 350
- Automated click-throughs, in click fraud attacks, 168
- Automated scripts, malware attacks and, 179
- Automobiles, future of crimeware and, 519–520
- AVS (address verification service), credit card security, 468

## B

- Back-end analytic tools, anti-phishing, 155
- Backdoor.Ryknos, 230
- Backdoors
  - malicious software installed via, 6
  - remote control via, 29
  - rootkits installed as, 229
- Badvertisements
  - creating with JavaScript, 171–172
  - delivery component, 169–170
  - execution component, 170
  - hiding attacks, 174–177
  - revenue extraction scheme, 394
  - unawareness of, 168
- Banner ads
  - DoubleClick, 328
  - overview of, 387–388
  - revenue models, 326
- Basic Input/Output System (BIOS), 264
- Behavior-based technologies, antivirus programs, 473
- Behaviors, code quality problem, 51
- Beneficial grouping, error rates and, 499–500
- Better Business Bureau, 398
- BHOs (browser help objects), 8, 29, 483
- Bi-directional communication, in bot networks, 192
- Bidder's Edge, 423–424
- Big Ad, 77–78
- Binding, protected storage and, 463
- BIOS (Basic Input/Output System), 264
- BIOS rootkits, 264–265
- BitTorrent, 58, 359
- Blizzard, 39
- BluePill, 269
- Bluetooth devices, as targets of malware, 103
- Booting
  - secure boot, 463–464
  - social networks for bootstrap attacks, 520
- Bot-initiated commands, 191
- Bot networks/bots, 183–228
  - alternative communication channels, 202–203
  - applications of, 210–215
  - bi-directional communication, 192
  - Botnets 2.0 (browser-based botnets), 216–217
  - browser-based bots, 199–200
  - command initiation and response, 191–192
  - communication protocols, 193
  - communication topology, 188–191
  - countermeasures, 224–227
  - criminal uses of, 379, 381–384
  - denial-of-service attacks and, 204
  - DNS rebinding attacks, 217–221
  - eliminating use of bots in games, 289–290
  - estimating size of botnet problem, 184–186
  - future of, 222–224
  - general software features, 206
  - HTTP bots, 199–200
  - information harvesting, 223–224
  - IRC bots, 193–199
  - legitimate uses, 340
  - network-level resilience, 203–205
  - overview of, 183–184
  - P2P protocols, 200–202
  - player treatment violations in games and, 289
  - proof-of-concept study, 221
  - robot delegate (zombie) attacks, 121
  - robotic clicking. *See* Robotic clicking

- Bot networks/bots (*contd.*)
    - rootkits and, 207
    - same-origin policy, 217
    - size metrics, 186–188
    - spam transmission via, 33
    - techniques for resilience, 207–210
  - Botherder. *See* Botmasters
  - Botmasters
    - black market value of botnets, 378
    - changing IP address of C&C servers, 204
    - DNS used for resilience, 203–205
    - overview of, 184
    - players in bots/botnets business, 380–381
    - pushing commands to botnets, 191
    - spam used by, 379
  - Botnet 2.0 (browser-based botnets), 216–217
  - Botnets. *See* Bot networks/Bots
  - Bots/botnets, as business model, 378–384
    - criminal applications of, 381–384
    - overview of, 378–379
    - players in, 380–381
  - BREW, code execution environment, 99
  - Bricking, routers, 109–110
  - Bridges
    - wireless bridging attacks, 116–117
    - wireless to wired networks, 108
  - Browser-bots, 199–200
  - Browser help objects (BHOs), 8, 29, 483
  - Browsers. *See* Web browsers
  - Buffer overflow
    - attacking third party applications, 521
    - free() and, 50
    - input validation and representation problems, 46
  - Business models, for crimeware, 355–395
    - adware and. *See* Adware
    - bots/botnets. *See* Bots/botnets, as business model
    - overview of, 355–357
    - spyware and trojans. *See* Spyware/trojans, as business model
- ## C
- C&C (command and control) networks
    - botnet topology and, 189
    - controlling botnets, 184–185
    - covert C&C channels, 222–223
    - overview of, 183–184
  - C&C servers
    - changing IP address of, 204
    - HTTP bots and, 200
    - IRC and, 193
    - number of in U.S., 186
    - “rallying box,” 188
  - Call gates, loading kernel drivers without SCM, 259
  - Call sites, infection signatures and, 481
  - Campaign-targeted phishing
    - overview of, 307
    - profit-motivation for, 307–312
  - Campaigns. *See* Elections; Politics, cybercrime in
  - CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing) Act, 434–435, 442
  - Canon EOS digital camera, firmware hacking
    - example, 105
  - Cantenna, Warkitting attacks and, 122
  - CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart)
    - eliminating use of bots in games, 289–290
    - human clickers and, 355
    - TG mitigation techniques, 158
  - Card not present (CNP), credit card security, 467–468
  - Card security code (CSC), credit card security, 467
  - CardSpace, identity system, 159
  - Cars, future of crimeware and, 519–520
  - Cartoons, use in education, 404
  - Castlecops, 205
  - Castranova, Edward, 280
  - Catch blocks, error handling problems, 50
  - CCM (click cost multiplier), 346
  - Cell phones, malicious alteration of embedded control systems, 106
  - Centralized P2P networks, 56
  - Cerf, Vint, 187
  - Certificates
    - self-signed, 79
    - SSL with client-side certificates, 488
  - Challenge-response protocols, human-oriented, 492–494
  - Cheat codes, 280
  - Cheating, 276–278
    - classifying types of, 277–278
    - defined, 276
    - fraud compared with, 285
    - incentive to cheat in online games, 286
  - Chipsets, hardware-enforced isolation and, 464
  - Chokepoints, countermeasures applied at, 26–29
  - Chord, 201
  - Chord, P2P protocols, 201
  - chroot, 43, 48–49, 510
  - ClamAV antivirus program, 59
  - Claria
    - profitability of adware business, 365–366
    - trends in adware business, 366
  - Classes, encapsulation problems, 51
  - Clean responses, in malware filtering, 63
  - Click-based model, advertising revenue, 328–329
  - Click cost multiplier (CCM), 346
  - Click fraud
    - botnets used for, 211–212
    - cost of, 275
    - criminal applications of botnets, 384



- defined, 2
- detection, 344–345
- uses of crimeware, 34
- WAPKit attacks, 120–121
- Click fraud, in advertising
  - auditing, 347–348
  - confidentiality of signals and, 348–349
  - data limitations and, 349–351
  - economics of, 352–353
  - privacy and, 351–352
- Click fraud, using JavaScript, 167–182
  - badvertisement, 171–172
  - delivery component, 169–170
  - detecting/preventing abuse, 179–180
  - economics and implications of, 180–182
  - execution component, 170
  - hiding the attack, 174–177
  - JavaScript code snippets, 172–174
  - luring visitors to site, 178–179
  - overview of, 167–168
  - terms and definitions, 168–169
- Click spam, 333–334
- Click-through rates. *See* CTR (click-through rates)
- Clickbot.A, 341
- Clickbots
  - defined, 340
  - For-Sale clickbots, 341
  - malware-type clickbots, 341
- ClickProtector, preventing click fraud, 179
- Client containment, as wireless countermeasure, 129
- Client evasion, hiding click fraud attacks, 174
- Client/server networks, 281
- Client-side certificates, SSL, 488
- Client-side vulnerabilities, auto-configuration tools and, 24
- CNP (card not present), credit card security, 467–468
- Code injection attacks, 479
- Code quality, in Seven Pernicious Kingdoms
  - taxonomy, 45, 50–51
- Code Red II exploit, 480
- Code snippets, JavaScript, 172–174
- Codes of conduct, abuses of adware, 362–363
- Coding errors. *See* Seven Pernicious Kingdoms (taxonomy of coding errors)
- Coercion, advertising attacks, 336–337
- Cognitive hacking, elections, 316–319
- Command initiation and response, bot network communication, 191–192
- Command injections, input validation and representation problems, 47
- Commercial web sites, CPA advertising and, 330
- Communication, bot networks
  - alternative channels for, 202–203
  - bi-directional, 192
  - command initiation and response, 191–192
  - HTTP and, 199–200
  - IRC and, 193–199
  - multiple protocols, 223
  - P2P and, 200–202
  - protocols, 193
  - topology, 188–191
- Communication, intercepting voice communication, 320–322
- Competitor clicking, 334
- Competitor clicking, invalid clicks, 334
- Completely Automated Public Turing Test to Tell Computers and Humans Apart. *See* CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart)
- Complexity, in Trinity of Trouble, 39
- Composite filters
  - for individual networks, 73–74
  - used across networks, 74–75
- Computer Fraud and Abuse Act
  - federal laws regarding surreptitious code, 443–444
  - provisions of, 418, 419–420
- Computer operation, surreptitious code interfering with, 416–417
- ComScore's Market Score, 367
- ConferenceRoom, popular IRC servers, 194
- Confidential data. *See also* Theft of sensitive information
  - countermeasures applied at chokepoints, 26–27
  - data theft, 16–17
- Confidentiality, as security feature, 43
- Confidentiality of signals, click fraud, 348–349
- Configuration management, home routers, 163
- Confirmation agents, TG mitigation techniques, 158–159
- Connectivity, in Trinity of Trouble, 38–39
- Consent to install, abuses of adware, 363
- Constellations, RFID tracking and, 92
- Consumers
  - company role in consumer security, 385
  - security education and, 398
- Containment
  - botnet countermeasures, 226
  - defense-in-depth and, 476–477
  - SpyShield for, 478, 482–483
- Content injection attacks, web browsers
  - exploits, 22–23
- Content, luring visitors to site for click fraud attack, 178
- Content protection, trusted computing, 469–472
- Context-aware phishing, 284
- Contextual advertisements, 388
- Contributions, political
  - abuses of requests, 309–310
  - FEC role in tracking, 319–320

- Control flow, unsafe reflection as input and representation problem, 48
- Control register zero (CR0), accessing service tables, 244
- Controlling the Assault of Non-solicited Pornography and Marketing (CAN-SPAM) Act, 434–435, 442
- Controls, countermeasures for RFID, 98
- Conversion spam, advertising, 334–335
- Copy machines, early target for malicious code, 38
- Copyrights, rootkits for protecting, 230
- Corporate espionage
  - data theft, 16
  - email and instant messaging redirectors, 10–11
  - trojans for, 370–372
- Cost per action. *See* CPA (cost per action)
- Cost per click. *See* CPC (cost per click)
- Cost per mille, impression-based model and. *See* CPM (cost per mille)
- Countermeasures
  - applied at chokepoints, 26–29
  - click fraud attacks, 179–181
  - drive-by pharming, 166–167
  - MMOG fraud, 291–292
  - RFID crimeware, 97–99
  - transaction generators, 158–160
  - USB-based malware, 89
  - WiFi firmware, 126–129
- Countermeasures, advertising
  - containment of abuses, 346–347
  - detection of abuses, 344–346
  - overview of, 342–343
  - prevention of abuses, 343–344
- Countermeasures, bot networks, 224–227
  - containment, 226
  - detection, 225–226
  - eradication, 226–227
  - prevention, 224–225
- Countermeasures, kernel-mode rootkits
  - detection, 272–273
  - prevention, 271–272
- Countermeasures, WiFi
  - antivirus programs, 126
  - client containment, 129
  - hacking own computer, 126–127
  - host scanning, 127
  - IDS (intrusion detection systems), 127–128
  - security settings, 126
  - wireless honeypots, 128–129
- Cousin-domain phishing attacks, 79
- Cousin domains, 298
- CPA (cost per action)
  - ad revenue models, 327, 329–330
  - conversion spam and, 334
  - hosting advertisements and, 389
- CPC (cost per click)
  - ad revenue models, 327, 328–329
  - coercion and, 336
  - hosting advertisements and, 389
  - manual clickers and, 337
  - referral deals, 331–332
  - smart pricing and, 346
  - as special case of CPA, 329
  - syndication deals, 330–331
- CPM (cost per mille)
  - ad revenue models, 326
  - hosting advertisements and, 389
  - impression-based model and, 327–328
  - manual clickers and, 337
  - metric for online advertising, 394
- CR0 (control register zero), accessing service tables, 244
- CreateRemoteThread, 334
- Credentials
  - trojans for stealing, 373
  - web trojans for collecting, 12
- Credit Card (or “Access Device”) Fraud Act, 437, 445
- Credit cards
  - protecting sensitive information in online games, 286
  - securing transactions, 467–468
  - security education and, 400
  - tips for beating thieves, 405
- Credit reports, 405
- Crimeware, future of, 515–523
  - big picture, 522–523
  - infrastructure control, 520
  - new applications and platforms, 517
  - overview of, 515
  - phones, cars, and wearable computers, 519–520
  - reputation systems, auction sites, and gambling applications, 517–519
  - social networks for bootstrap attacks, 520
  - terrorware, vandalware, and ransomware, 515–517
  - vulnerability of e-society, 521–522
- Crimeware, introduction
  - affiliate marketing as distribution technique, 24–25
  - attachment-based distribution, 20
  - attack stages, 6–7
  - click fraud as use of, 34
  - data ransomware as use of, 34–35
  - data theft, 16–17
  - denial-of-service attacks as use of, 33–34
  - distribution techniques, 19
  - email and instant messaging redirectors, 10–11
  - infection and data compromise points, 25–29
  - information compromise as use of, 31–33
  - information consolidation as use of, 35
  - installation stages, 29–31
  - Internet worms as distribution technique, 21

- keyloggers and screen scrapers, 8–10
- man-in-the-middle attacks, 17–19
- overview of, 1–2
- P2P distribution, 20
- piggybacking distribution technique, 20–21
- prevalence, 4–5
- propagation techniques, 3–4
- rootkits, 19
- scope of, 2–3
- server-compromise as distribution technique, 24
- session hijackers, 11–12
- spam transmission as use of, 33
- summary, 35–36
- system reconfiguration attacks, 13–15
- theft of sensitive information, 2
- threat model and taxonomy, 5–7
- transaction generators, 12–13
- uses of, 31
- variations, 8
- web browsers exploits as distribution technique, 22–24
- web trojans, 12
- Criterion
  - composite filters. *See* Composite filters
  - in malware filtering, 63
  - single criteria filters. *See* Single criteria filters
- Cross-site request forgery. *See* CSRF (cross-site request forgery)
- Cross-site scripting
  - input validation and representation problems, 47
  - web browsers exploits, 22–23
- Cross-view detection, rootkit detection, 272
- Crypto-viruses, 35
- Cryptography. *See also* Encryption
  - integrity measurement and storage, 461–462
  - as security feature, 44
  - in TPM specification, 460
- CSC (card security code), credit card security, 467
- CSRF (cross-site request forgery)
  - attack flow in drive-by pharming, 161
  - configuring home routers, 163
  - router protection, 166–167
  - TGs compared with, 156
- CTR (click-through rates)
  - impression-based ad model, 327–328
  - impression spam and, 332–333
  - smart pricing and, 346
- curl, open-source utilities for building bots, 340
- Currencies, crimeware targeting, 518
- Custom bots, 340
- Cybercrime, defined, 458
- Cybercriminals, convictions and punishment, 386
- D**
  - Data compromise points, 25–29
    - chokepoints and, 26–29
    - overview of, 25–26
  - Data isolation, virtual machines and, 510
  - Data leaks (encapsulation problems),
    - between users, 51
  - Data limitations, click fraud and, 349–351
  - Data loss (confidentiality), information security, 285
  - Data mining, 284, 494
  - Data modification (integrity), information security, 285
  - Data ransomware. *See* Ransomware
  - Data theft
    - crimeware run as application program, 30–31
    - overview of, 16–17
    - spyware for extracting sensitive data, 101
  - DDoS (Distributed Denial of Service) attacks
    - botmasters using, 204, 379
    - criminal applications of botnets, 381
    - political uses of, 315–316
    - robot delegates (zombies), 121
    - uses of crimeware, 33–34
  - Dead-drop, trojans delivering data to, 372–373
  - Deadlocks, time and state problems, 49
  - Deauthenticate frames, 129
  - Debug code, encapsulation problems, 51
  - Debugging, botnets installing antidebugging techniques, 208
  - Debugging messages, environment problems in ASP.NET, 52
  - Decentralized P2P networks, 56
  - Deceptive Practices and Voter Intimidation Prevention Act, 318
  - Defense-in-depth
    - advertising countermeasures, 342
    - lines of defense in, 476–477
    - spyware case study, 476–478
  - Defense techniques
    - crimeware resistant authentication. *See* Authentication, crimeware resistant
    - overview of, 473–475
    - spyware case study. *See* Spyware case study
    - virtual machines, 510–514
  - Denial-of-service attacks
    - botnets mounting, 213–214
    - bots use in, 204
    - classes of RFID attacks, 93
    - client containment and, 129
    - political uses of, 315–316
    - uses of crimeware, 33–34
  - Denial-of-service (availability), information security and, 285
  - Desynchronizing the split translation look-aside buffer approach, 255

- Detection
  - botnet countermeasures, 225–226
  - malicious behavior detection in AGIS, 481
  - rootkits, 272–273
- detours (inline function patching)
  - modifying execution path of user-mode rootkits, 238–240
  - system call code patching compared with, 247
- Device drives, kernel-level device drivers in keylogger implementation, 8
- Device fingerprinting, in drive-by pharming attack, 164
- Devices, mobile. *See* Mobile devices
- Devices, small. *See* Small devices
- Dictionary attacks, credit card security, 468
- digg, 520
- Digital rights management (DRM). *See* OMA DRM (Open Mobile Alliance Digital Rights Management)
- Digital Signal Transponder (TI-DST), Texas Instruments, 97
- Direct compromise and reselling, WiFi firmware, 125–126
- Direct kernel object manipulation (DKOM), 253–254
- Direct memory access (DMA), 87
- Direct Revenue
  - adware company, 362
  - profitability of, 365–366
  - trends in adware business, 366
- Directories, API abuse problems, 48
- Disassembly skills, application, 371
- Disinfection, defense-in-depth and, 476–477
- Distributed computing, time and state and, 44
- Distributed Denial of Service. *See* DDoS (Distributed Denial of Service) attacks
- Distribution phase, of malware attacks, 459
- Distribution techniques
  - adware techniques for evading law enforcement, 364
  - affiliate marketing, 24–25
  - attachment-based, 20
  - Internet worms, 21
  - overview of, 19
  - P2P, 20
  - piggybacking, 20–21
  - server-compromise, 24
  - stages of crimeware attacks and, 7
  - web browsers exploits, 22–24
- DKOM (direct kernel object manipulation), 253–254
- DLL injection, 234
- DMA (direct memory access), 87
- DNS cache, hostname lookup attacks and, 14
- DNS (Domain Name System)
  - botnet resilience and, 203–205
  - hostname lookup attacks and, 13–15
  - pharming attacks and, 116, 284
  - pinning, 219–220
- DNS rebinding attacks, 217–221
  - applications of, 220–221
  - defending against, 219–220
  - at high level, 218–219
  - overview of, 217–218
- DNS servers
  - drive-by pharming attacks, 160–161
  - hostname lookup attacks, 14–15
  - server-compromise attacks, 24
- Domain name abuses, 295–307
  - domain parking, 303
  - domain speculation and typo squatting in 2008 federal election, 298–303
  - malicious intent in politics, 303–307
  - overview of, 295–296
  - registration and infringement, 296–297
  - security education and, 401
- Domain parking, 303
- Domain speculation, in 2008 federal election, 298–303
  - advertisements and, 302–303
  - analysis conclusions, 300–301
  - analysis process, 298–300
  - overview of, 297–298
  - typo squatting and, 298
- DoubleClick, 328
- Download phase, file sharing, 56
- Downloader, trojan authors writing, 376–377
- Downloads, surreptitious code and, 415
- Downtime, environmental stability in games, 290
- Draught, Carlton, 77–78
- Drive-by downloader, 101
- Drive-by pharming attacks, 160–167
  - attack details, 162–163
  - attack flow, 161–162
  - configuring home routers, 163–164
  - countermeasures, 166–167
  - device fingerprinting, 164
  - IP address determination and JavaScript host scanning, 164
  - overview of, 160
  - visiting attacker's web page, 165
- DriverObject list, unlinking drivers from, 254
- Drivers
  - file system filter driver rootkit, 248–249
  - IRP patching, 251–252
  - keyboard filter driver rootkit, 249–251
  - layered model (WDM) for, 247–248
  - loading kernel drivers without SCM, 258–260
  - unlinking from DriverObject list, 254

DRM (digital rights management). *See* OMA DRM (Open Mobile Alliance Digital Rights Management)

Dual-personality page, 169

Dynamic DNS, 203–204

Dynamic Link Library (DLL) injection, 234

## E

E-society, vulnerability of, 521–522

Eavesdropping, 485–486

eBay

  Spoof Email Tutorial, 403

  Trespass to Chattels tort, 423–424

Economy servers, underground for selling sensitive information, 210

eCPM (expected CPM), 330

Education. *See also* Security education

  approaches to improved security, 398

  combating crimeware, 385

EEPROM (erasable programmable readonly memory)

  BIOS contained on, 264

  embedded control systems and, 104

Egg-drop, trojans delivering data to, 372–373

Elections. *See also* Politics, cybercrime in

  abuses of political contribution requests, 309–310

  cognitive hacking, 316–319

  federal regulations, 319–320

  malicious code and security risks, 312

  overview of election fraud, 293

  phishing and, 307

  TGs and, 157

Electronic Communications Privacy Act, 430–433

  federal laws regarding surreptitious code, 445–446

  Pen Register Act (Title III), 470–471

  Stored Communications Act (Title II), 469–470

  Wiretap Act (Title I), 468–469

Electronic fraud

  misleading applications, 284–285

  MMOGs. *See* MMOGs (massively multiplayer online games)

  overview of, 283

  phishing and pharming, 283–284

Electronic Product Code (EPC), RFID and, 91

Email

  attachment-based distribution of crimeware, 20

  botnets for harvesting, 211

  dangers of hyperlinks in, 400

  domain name abuse in politics and, 295

  luring visitors to site for click fraud attack, 178

  protecting sensitive information in online games, 286

  redirectors, 10–11

  tips for beating thieves, 405

Embedded computers, as targets of malware, 103

Embedded control systems, 104–106

  firmware updates for, 104–105

  list of targets, 106

  types of, 104

  uses of, 105–106

Embedded software, 104. *See also* Firmware abuses

EMV (Europay Mastercard and Visa), credit card security, 467

Encapsulation, in Seven Pernicious Kingdoms taxonomy, 45, 51

Encryption. *See also* WEP (wired equivalent privacy); WPA (WiFi protected access)

  botnets use of, 205

  countermeasures applied at chokepoints, 27–28

  game security and, 291

  WAP default settings, 115

  WiFi and, 126

  wireless access and, 110

  wireless networking, 111

End-user license agreements. *See* EULAs (end-user license agreements)

Enemy, security goal of knowing enemy, 408

Entity beans, environment problems in J2EE, 52

Environment, in Seven Pernicious Kingdoms taxonomy, 45, 52

Environmental stability, MMOGs, 290–291

EPC (Electronic Product Code), RFID and, 91

EPCIS (EPC Information Service), 91

Epidemic model, WiFi malware, 139–145

Epidemic spread, WiFi malware, 145–151

Eradication, botnet countermeasures, 226–227

Erasable programmable readonly memory (EEPROM)  
  BIOS contained on. *See* EEPROM (erasable programmable readonly memory)

Error handling

  environment problems in ASP.NET, 52

  environment problems in J2EE, 52

  in Seven Pernicious Kingdoms taxonomy, 44–45, 50

Error rate determination, authentication and, 499–501

Espionage

  data theft, 16

  email and instant messaging redirectors and, 10–11

  trojan authors, 370–372

Ethernet Media, 366

EULAs (end-user license agreements)

  abuses of, 393

  abuses of adware, 360–361

  confusing nature of, 21

  regulations regarding, 414

  spyware and, 314

Europay Mastercard and Visa (EMV), credit card security, 467

Event hooks, Windows OSs, 235–236

Exception handling, API abuse problems, 48

Executable replacement rootkits, Linux, 260–261

Execution of attacks, stages of crimeware attacks, 7  
 Execution phase, of malware attacks, 459–460  
 Existing code attacks, 479  
 Exploit signatures, 479  
 Exploitation of intercepted information, surreptitious code, 418  
 Exploiters, cheating in games and, 277  
 Exploits, automatic detection of, 477–480  
 Extended Copy Protection (XCP), 230  
 Extensibility, in Trinity of Trouble, 40  
 Extensible platforms, 99  
 Extortion  
   criminal applications of botnets, 381–382  
   ransomware programs, 374–376  
 Extra-mechanic rules, in game play, 279

## F

Fads, infection vectors, 77  
 False-negatives/false positives  
   error rates and, 499–500  
   file-size-based filters, 67  
   in malware filtering, 63  
 Fast flux technique, for updating IP addresses, 204  
 FBCS (R28's Botnet Control System), 200  
 FEC (Federal Election Commission), public voter information sources, 319–320  
 FECA (Federal Election Campaign Act), 319  
 Federal Election Commission (FEC), public voter information sources, 319–320  
 Federal laws, surreptitious code, 418–425  
 Federal Trade Commission Act  
   federal laws regarding surreptitious code, 446–447  
   provisions of, 458–461  
 Federal Trade Commission (FTC)  
   security education and, 399  
   spyware defined by, 475  
 Federal Trademark Act of 1946 (Lanham Act)  
   federal laws regarding surreptitious code, 447  
   provisions of, 435–436  
 Federated two-factor authentication solution, 490  
 File extensions, nonmedia, 60  
 File name-based filters  
   composite filters for individual networks, 73–74  
   single criteria filters, 68–69  
 File sharing  
   P2P distribution and, 20  
   P2P networks and, 55  
   P2P protocols and, 200  
 File-size-based filters  
   composite filters for individual networks, 73–74  
   single criteria filters, 64–68  
 File system filter driver rootkit, kernel-mode rootkits, 248–249

Filter performance  
   file name-based filters, 69  
   file size-based filters, 66  
   host IP-based filters, 70–71  
   query string-based filters, 72  
   single criteria filters across network, 72–73  
 Filtering malware, composite  
   for individual networks, 73–74  
   used across networks, 74–75  
 Filtering malware, generally, 61–64  
 Filtering malware, single criteria  
   file name-based filters, 68–69  
   file size-based filters, 64–68  
   host IP-based filters, 69–71  
   query string-based filters, 71–72  
   used across networks, 72–73  
 Filters  
   detecting click fraud, 344–345  
   protecting P2P networks against malware, 57  
 Financial theft, TGs and, 157  
 Firewalls  
   HTTP and, 199  
   router management and, 166  
   virtual machines and, 513  
 Firmware abuses, 103–153  
   attack vectors, 121–122  
   Canon EOS digital camera example, 105  
   countermeasures, 126–129  
   direct compromise and reselling, 125–126  
   embedded control systems, 104–106  
   malicious alteration, 106–107  
   modeling malware epidemics. *See* WiFi malware epidemics, modeling  
   overview of, 103  
   propagation by updates, 103–104  
   router configuration, 109–110  
   router-to-router attacks, 123–124  
   security measures for wireless routers, 110–113  
   WAP case study, 107–108  
   WAPJack attacks, 116  
   WAPKit attacks, 117–121  
   Warkitting attacks, 122–123  
   weak security configuration and, 113–115  
   web scripting attacks, 124–125  
 Flash drives. *See* USB flash drives, malware propagation  
 Flash, Macromedia, 337  
 Flash memory  
   embedded control systems and, 104  
   writing BIOS to, 264  
 FlexiSpy, intercepting voice communication for political advantage, 321–322  
 Footprint, bot networks, 185  
 For-Sale clickbots, robotic clicking, 341  
 Forced browser clicks, robotic clicking, 341–342

Format strings, input validation and representation problems, 47

Fraud

- click fraud. *See* Click fraud
- compared with cheating, 285
- election fraud, 293
- electronic. *See* Electronic fraud
- games and, 276
- MMOGs. *See* MMOGs (massively multiplayer online games)

Fraudulent clicks, 333. *See also* Click fraud

free( ), buffer overflows and, 50

FTC (Federal Trade Commission)

- security education and, 399
- spyware defined by, 475

Functions

- dangerous functions in API abuse, 48
- obsolete functions as code quality problem, 51

Fund transfer, misleading applications and, 284–285

Fuzzing, application, 371

## G

Gallup Poll, 314

Gambling applications, future of crimeware, 517–519

Games

- cheating and, 276–278
- environmental stability and, 290–291
- fraud and, 276
- infection vectors, 77
- malicious alteration of embedded control systems, 107
- MMOGs. *See* MMOGs (massively multiplayer online games)
- patches, 281
- player ability, 287–288
- player treatment, 288–290
- ranking systems, 288
- RMT (real money trade), 280
- targets for malicious code, 39

Gaobot, IRC botnets, 193

Gateways, wireless access and, 108

Gator, adware application, 313

Giant component, 137–139

GNU Public License (GPL), 105–106

Gnutella protocol. *See also* Limewire

- file-sharing, 200
- filters for protecting against malware, 57
- mode options, 58

Goals, security education, 407–408

Google

- Ad Traffic Quality Team, 338
- AdSense, 334
- AdWords, 328–329
- auto-tagging feature, 350
- contextual advertisements, 388

- CPM-based advertising, 328
- smart pricing for advertising, 346

Google Desktop, security implications of web server running on desktop, 522

Google dorks, 206

Google Video, viral videos, 77

Goto.com, click-based ad model, 328

GPL (GNU Public License), 105–106

Gramm-Leach-Bliley Financial Services Modernization Act

- federal laws regarding surreptitious code, 447
- laws applicable to misrepresentation, 439

Graphical passwords, 493

Griefing, player treatment violations, 288–289

Grossman, Jeremiah, 161

GTBot, IRC botnets, 193

Guilds, game players, 279

## H

Hacking toolkits, 357

Haephrati, Michael, 372

Hardware-enforced isolation, trusted computing, 464–465

Hashes

- password hashing, 490–491
- two-factor authentication, 489

Heap injection, as API abuse problem, 48

Hector's World, education resources for

- understanding security risks, 403

Heuristics technologies, antivirus programs and, 473

High-stakes attacks, RFID attacker model, 94

Honeypots, wireless, 128–129

Hooking mechanisms

- IAT hooks, 236–238
- IDT hooks, 240–242
- keylogger implementation techniques, 8–9
- SSDT hooks, 243–245
- system call hooks, 242–243
- Windows hooks, 235–236

Hopcount, decentralized file sharing and, 56

Host IP-based filters, 69–71

Host scanning

- JavaScript, 162, 164
- as WiFi counter measure, 127

Hostname lookup attacks, 13–15, 18

Hosts file, 5, 7, 14, 30–31, 207

Hotbar, adware application, 313

HTTP (Hypertext Transfer Protocol)

- bot network communication protocols, 199–200
- click spam and, 333–334
- conversion spam and, 334
- HTTPS compared with, 112
- impression spam and, 332
- invalid clicks, 333
- list of popular HTTP bots, 200



- HTTP (Hypertext Transfer Protocol) (*contd.*)  
 manual clickers and, 337–338  
 HTTP response splitting, input validation and representation problems, 47  
 HTTPS (Secure HTTP), compared with HTTP, 112  
 Human clickers, advertising attacks, 335–336  
 Human-oriented challenge-response protocols, 492–494  
 Human-propagated crimeware  
 experimental evidence, 80–82  
 infection vectors and, 76–77  
 overview of, 76–77  
 problem statement, 76  
 signed applet case study, 77–82  
 viral marketing and, 77–80  
 Human visitors, click fraud attacks and response to, 176–177  
 Hyperlinks, dangers of hyperlinks in email, 400  
 Hypertext Transfer Protocol. *See* HTTP (Hypertext Transfer Protocol)
- ## I
- I/O request packets (IRR), kernel-level keyloggers and, 10  
 IAT hooks, 236–238  
 ICANN, Uniform Domain Name Dispute Resolution Policy (UDRP), 296  
 Identity system, CardSpace, 159  
 Identity theft  
 book resources for, 402  
 consumer education and, 398  
 cost of, 275  
 criminal applications of botnets, 382  
 Identity Theft and Assumption Deterrence Act, 436–439  
 online gaming and, 276  
 rapid growth in, 2  
 RFID-enabled, 95–96  
 ShadowCrew and, 356  
 uses of crimeware, 31  
 Identity Theft and Assumption Deterrence Act  
 federal laws regarding surreptitious code, 447–448  
 surreptitious code, 436–439  
 IDS (intrusion detection systems), as WiFi counter measure, 127  
 IDT (interrupt descriptor table)  
 IDT hooks, 240–241  
 keyboard hook example, 241–242  
 overview of, 240  
 IE7 (Internet Explorer 7), privileges, 199  
 IEEE 802.11 wireless standard, 107–108  
 iFrameCash.biz, 363  
 ILL (illegal instruction fault), 479  
 Illegal pointer values, input validation and representation problems, 47  
 IM (instant messaging), redirectors, 10–11  
 Immersion, principles of educational approaches, 397, 411  
 Impersonation strategies, surreptitious code, 415–416  
 Impression-based model, advertising revenue models, 327–328  
 Impression spam  
 causes of, 327  
 types of spam in advertising, 332–333  
 Index node, OpenFT, 58  
 Infection duration, traditional botnets compared with browser-based botnets, 216  
 Infection graphs, AGIS, 481  
 Infection phase, of malware attacks, 459  
 Infection points, 25–29  
 countermeasures applied at chokepoints, 26–29  
 overview of, 25–26  
 stages of crimeware attacks and, 7, 26  
 Infection signatures, automatic generation of, 478, 481–482  
 Infection vectors, traditional botnets compared with browser-based botnets, 216  
 Infectious, SIR epidemic model, 140  
 Infiltration, techniques for measuring botnets, 185  
 Information compromise, uses of crimeware, 31–33  
 Information consolidation, uses of crimeware, 35  
 Information security, foundations of, 285  
 Information theft  
 spyware and trojans and, 367  
 trojan authors, 372–374  
 Infosec Research Council Science and Technology Study Group (ISTSG), 37  
 Infostealer.Banker.D, 29, 415  
 Infostealer.Gampass, 9  
 Infostealer.Lineage, 9  
 Infrastructure control, future of crimeware, 520  
 Infringement, domain name abuse in politics, 296–297  
 Inline function patching (detours)  
 modifying execution path of user-mode rootkits, 238–240  
 system call code patching compared with, 247  
 Input devices, games, 281  
 Input validation problems, in Seven Pernicious Kingdoms taxonomy, 43, 46–48  
 Installation stages, crimeware, 29–31  
 Instant messaging (IM), redirectors, 10–11  
 INT 0x2E hooks, 242–243  
 Integer overflow, 47  
 Integer overflows, input validation and representation problems, 47  
 Integrity measurement and storage  
 secure boot and, 463–464  
 in trusted computing, 461–462

Intel LaGrande, 464–466  
 Intel SecureFlash, 264, 272  
 Intel VT-x (Vanderpool), 233  
 Intellectual property rights, Federal Trademark Act of 1946 (Lanham Act), 435–436  
 Interception, of communications, 320–321, 430–431, 433  
 Interfaces  
   human factors in UI design, 114–115  
   MMOGs, 281  
 Internet, 2004 presidential election and, 293  
 Internet Explorer 7 (IE7), privileges, 199  
 Internet Relay Chat. *See* IRC (Internet Relay Chat)  
 Internet Security Threat Report. *See* ISTR (Symantec Internet Security Threat Report)  
 Internet-side administration, WAPJack attacks, 116  
 Internet worms, as distribution technique, 21  
 Interrupt descriptor table. *See* IDT (interrupt descriptor table)  
 Interrupt requests, ISR (interrupt service routine) and, 240  
 Interrupt service routine (ISR), 240  
 Intra-mechanic rules, in game play, 279  
 Intrusion detection systems (IDS), as WiFi counter measure, 127  
 Invalid clicks, HTTP (Hypertext Transfer Protocol), 333–334  
 IP addresses  
   DNS A record and, 203  
   drive-by phishing attacks determining, 164  
   fast flux technique, 204  
   host IP-based filters, 69–71  
   hostname lookup attacks and, 14  
   phishing attacks and, 284  
 iPods  
   firmware updates for, 105  
   malicious alteration of embedded control systems, 107  
   vulnerabilities, 85  
 IPsec, security standards for network access, 110  
 IRC (Internet Relay Chat), 193–199  
   C&C servers communicating via, 193  
   clients and servers, 194  
   commanding botnets with, 185  
   ease of detection of IRC bots, 197–198  
   as vehicle for botnets, 193–194  
 IRP patching  
   address of IRP function table, 252  
   kernel-mode rootkits, 251–252  
   modifying return parameters, 252  
 IRR (I/O request packets), kernel-level keyloggers and, 10  
 Isolation technologies, hardware-enforced isolation, 464–465

ISR (interrupt service routine), 240  
 ISTR (Symantec Internet Security Threat Report)  
   on bot resilience, 209–210  
   on P2P distribution, 20  
   SMTP as vehicle for crimeware propagation, 3  
   web browsers exploits, 23  
 ISTSG (Infosec Research Council Science and Technology Study Group), 37

## J

J2EE  
   API abuse problems, 48  
   environment problems, 52  
   time and state problems, 50  
 J2ME, code execution environment, 99  
 Java applets, 77–78, 81, 125  
 Java LiveConnect, 219–220  
 Java Native Interface (JNI), 48  
 Java, web browser vulnerabilities, 23  
 JavaScript. *See also* Click fraud, using JavaScript  
   badvertisements, 171–172  
   for click fraud, 172–174  
   code snippets, 172–174  
   defined, 168  
   host scanning, 164  
 JNI (Java Native Interface), 48

## K

Kademlia, P2P protocols, 201  
 Kernel-level keyloggers, 10  
 Kernel-mode hooks, 232  
 Kernel-mode rootkits  
   direct kernel object manipulation, 253–254  
   file system filter driver rootkit, 248–249  
   hiding threads from Scheduler, 254–255  
   interrupt descriptor table hooks, 240–242  
   IRP patching, 251–252  
   keyboard filter driver rootkit, 249–251  
   layered drivers, 247–248  
   loading kernel drivers without SCM, 258–260  
   overview of, 240  
   redirecting virtual memory access, 255–258  
   system call code patching, 247  
   system call hooks, 242–243  
   system service descriptor table hooks, 243–245  
   thread-based SSDT hooks, 246–247  
   uses of crimeware, 31  
 Keyboard filter driver rootkit, kernel-mode rootkits, 249–251  
 Keyboards  
   kernel-level keyloggers and, 10  
   keyboard hooks used by application-level keyloggers, 9

Keyloggers, 8–10  
   application-level, 9–10  
   implementation techniques, 8  
   installed by misleading applications, 284  
   kernel-level, 10  
   on-screen input measures and, 487  
   political uses of malicious code, 314–315  
   as spyware application, 367  
   white hat, 27  
 Keywords, decentralized file sharing and, 56  
 Kinderman, Lars, 164  
 Kingdoms  
   in Seven Pernicious Kingdoms taxonomy, 42–43  
   in taxonomies, 42  
 Kismet, network sniffer, 122–123  
 Kiyashinku, 337–338  
 kmem device, 262

## L

Lag, network latency in games, 291  
 LaGrande, Intel, 464–466  
 Lanham Act (Federal Trademark Act of 1946)  
   federal laws regarding surreptitious code, 447  
   provisions of, 435–436  
 LANs (local area networks), wireless routing and, 108  
 Law enforcement  
   adware techniques for evading, 363–365  
   approaches to improved security, 398  
   conviction and punishment of cybercriminals, 386  
   downloaders and, 376  
   finding boundaries of what is legal, 414  
   global cooperation in, 385  
   penalties for violating Computer Fraud and Abuse Act, 419  
   ShadowCrew shut down by, 356  
   spammer trojans and, 378  
   spyware and, 370  
 LCP password recovery tool, 85–87  
 Leaf mode, Gnutella protocol, 58  
 Least privilege violation, 48  
 Life questions  
   characteristics of good, 497–498  
   finding good, 498–499  
   good vs. bad questions, 502–503  
   overview of, 485, 494–497  
 Likert scale, 494  
 Limewire  
   as decentralized file sharing network, 56  
   file name–based filters, 68–69  
   file size–based filters, 64–68  
   filters for protecting against malware, 57  
   identifying malware, 59–60  
   modifying for data collection, 59  
   overview of, 58  
   prevalence of malware on during test period, 60–62

Linux  
   GPL (GNU Public License), 105–106  
   network services, 108  
   WRT54G router, 105  
 Linux rootkits. *See also* Kernel-mode rootkits  
   evolution of rootkits and, 231  
   executable replacement, 260–261  
   loadable kernel module, 261–262  
   overview of, 260  
   runtime kernel patching, 262–263  
   VFS, 263–264  
 Live population, bot networks, 185  
 LKMs (loadable kernel modules)  
   Linux rootkits, 261–262  
   rootkits accessing kernel via, 231  
   runtime kernel patching and, 262–263  
 Local area networks (LANs), wireless routing and, 108  
 Log forging, input validation and representation problems, 47  
 Login windows, web trojans for collecting credentials from, 12  
 LoverSpy, 370  
 Low-stakes attacks, RFID attacker model, 93–94. *See also* Script kiddies

## M

MAC (media access control) addresses  
   filtering, 111  
   WAP default settings for MAC filtering, 115  
   weak security configuration and, 113  
   wireless access and, 110  
 MAC (message authentication code), 222  
 Macromedia Flash, 337  
 Malicious behavior detection, AGIS, 481  
 Malicious code  
   botnets hosting, 213  
   criminal uses of, 356  
 Malicious code, political uses  
   advertisements and redirection, 303–307  
   adware and, 312–313  
   keyloggers and crimeware, 314–315  
   overview of, 312  
   spyware and, 313–314  
 Malicious code taxonomy  
   API abuse, 43, 48–49  
   code quality, 45, 50–51  
   complexity and, 39  
   connectivity and, 38–39  
   encapsulation, 45, 51  
   environment, 45, 52  
   error handling, 44–45, 50  
   extensibility and, 40  
   input validation and representation problems, 43, 46–48  
   more phyla needed, 52–53

- security features, 43–44, 49
  - Seven Pernicious Kingdoms (taxonomy of coding errors), 40–42
  - time and state, 44, 49–50
  - Trinity of Trouble, 37–38
- Malware
- affiliate IDs and, 394
  - attack phases, 459–460
  - classes of RFID attacks, 93
  - crimeware as subclass of, 2
  - defined, 1
  - determining malicious nature of, 414
  - identifying with Limewire and OpenFT, 59–60
  - in P2P networks, 55–56
  - P2P options for defending against, 57
  - prevalence of malware on Limewire and OpenFT during test period, 60–62
  - security education and, 401
- Malware-type clickbots, robotic clicking, 341
- Man-in-the-middle attacks, 17–19
- difficulty of detecting, 18–19
  - examples of, 18
  - illustration of, 17
  - WAPKit attacks, 117–119
- Mandragore worm, 57
- Manual clickers, advertising attacks, 337–339
- Market Score, ComScore, 367
- MarketScore program, from ComScore, 368
- Massively multiplayer online games. *See* MMOGs (massively multiplayer online games)
- Massively multiplayer online role-playing games (MMORPGs), 39
- MBR (master boot record), BIOS rootkits and, 264
- MDL (memory descriptor list), 245
- Media access control addresses. *See* MAC (media access control) addresses
- Media players
- malicious alteration of embedded control systems, 107
  - PMPs (portable media players), 84–85
- Memory
- denying write access to physical memory, 271
  - leaks as code quality problem, 50
  - ROM (readonly memory), 104, 272
  - use after free referencing as code quality problem, 51
  - writing to physical memory, 259
- Memory descriptor list (MDL), 245
- Merchant operator guidelines (MOGs), credit card security, 467–468
- Message authentication code (MAC), 222
- Metacharacters, input validation and representation problems, 43
- Metrics, advertising success, 387
- Microcontrollers
- hardware-enforced isolation and, 464
  - TCG specification for microcontroller design, 460
- Microsoft Windows Malicious Software Removal Tool (MSRT), 231
- Misleading applications
- defined, 21
  - electronic fraud, 284–285
- Misrepresentation (authenticity), information security, 285
- Misrepresentation strategies
- laws applicable to misrepresentation, 454
  - surreptitious code, 415–416
- Misuse detection schemes, for game scripts, 282
- Mitigation techniques, transaction generators, 158–160
- MLS (multilevel security) model, 483
- MMOGs (massively multiplayer online games)
- architectural overview, 280–283
  - countermeasures, 291–292
  - environmental stability, 290–291
  - fraud in, 285
  - player ability, 287–288
  - player treatment, 288–290
  - rules, 278–280
  - security guidelines for, 286–287
  - security model for, 285–286
- MMORPGs (massively multiplayer online role-playing games), 39
- Mobile code, encapsulation problems, 51
- Mobile devices, 99–102
- intercepting voice communication for political advantage, 321
  - overview of, 99
  - RedBrowser trojan, 100
  - spyware, 101
  - targets of crimeware, 458
  - vulnerabilities, 99–100
  - Windows Mobile, 101
- Mobile Linux, extensible platforms, 99
- Mobile platforms, TCG specifications, 460
- Mobs, gold harvesting in games and, 289
- Mods (modifications), game security and, 291
- Modular malicious code, for crimeware installation, 29
- MOGs (merchant operator guidelines), credit card security, 467–468
- Mozilla, web browser vulnerabilities, 23
- MPack, hacking toolkits, 357
- MSRT (Microsoft Windows Malicious Software Removal Tool), 231
- Multilevel security (MLS) model, 483

## N

Napster  
 as centralized file sharing network, 56  
 P2P protocols and, 200  
 NAT (network address translation), wireless routing and, 108  
 Necklace problem, two-factor authentication, 490  
 NetSmartKids, education resources for understanding security risks, 403  
 Network access, security standards, 110  
 Network address translation (NAT), wireless routing and, 108  
 Network architecture, MMOGs, 281  
 Network latency (lag), in games, 291  
 Network-level resilience, bot networks, 203–205  
 Network-oriented features, of botnets, 188  
 Network sniffers, 122–123  
 Networks  
   human and robotic attacks, 335  
   TCG specifications, 460  
 Next Generation Secure Computing Base (NGSCB), 464  
 ngrep, 197  
 NGSCB (Next Generation Secure Computing Base), 464  
 Nonmedia file extensions, 60  
 Nontraditional attacks, RFID attacker model, 94  
 Nugache, 205  
 NullPointerException  
   code quality problems, 50  
   error handling problems, 50

## O

Object name resolvers (ONS), RFID and, 91  
 OMA DRM (Open Mobile Alliance Digital Rights Management)  
   content protection in mobile environment, 469–471  
   trusted computing and, 466  
 On-screen input measures, authentication and, 487  
 One-time passwords (OTP), 484–485  
 Online advertising. *See* Advertising  
 Online business, threats faced by, 275  
 Online fraud. *See* Fraud  
 Online games. *See* Games  
 Online reputation, botnets for inflating, 215  
 ONS (object name resolvers), RFID and, 91  
 Open Mobile Alliance Digital Rights Management (OMA DRM). *See* OMA DRM (Open Mobile Alliance Digital Rights Management)  
 Open-source firmware, 105  
 OpenFT  
   file name–based filters, 68–69  
   file size–based filters, 64–68  
   identifying malware, 59–60

    modifying for data collection, 59  
   node options, 58  
   overview of, 58  
   prevalence of malware on during test period, 60–62  
 Opera, 504–505  
 Opera Widgets, 24  
 OR-based filters  
   composite filters across networks, 74–75  
   composite filters for individual networks, 73  
   overview of, 63  
 Organized crime, 5  
 OSPM (OS-controlled power management and advanced configuration), 264  
 OTP (one-time password) tokens, authentication and, 484–485  
 Overnet protocol, 202  
 Overture, click-based ad model, 328

## P

P2P (peer-to-peer) networks, 55–82  
   bot network communication protocols, 200–202  
   centralized vs. decentralized, 56  
   composite filters for individual networks, 73–74  
   distribution techniques, 20  
   file name–based filters, 68–69  
   file size–based filters, 64–68  
   host IP–based filters, 69–71  
   human-propagated crimeware, 76–77  
   identifying malware in, 59–60  
   Limewire vs. OpenFT, 58  
   malware in, 55–56  
   MMOGs and, 281  
   modifying Limewire and OpenFT for data collection, 59  
   options for defending against malware, 57  
   prevalence of malware on Limewire and OpenFT during test period, 60–62  
   query string–based filters, 71–72  
   signed applet case study, 77–82  
   single criteria filters for individual networks, 61–64  
   single criteria filters used across networks, 72–73  
 Pacifica, AMD, 233  
 Packet vaccine, for automatic detection of exploit attempts, 477–480  
 PAKE (password-authenticated key exchange), in Spyblock system, 492  
 Password hashing  
   authentication and, 490–491  
   in Spyblock system, 492  
 Passwords  
   applications/code for stealing, 4  
   botnets cracking, 214–215  
   changing router password to prevent drive-by pharming attacks, 166  
   countermeasures applied at chokepoints, 27–28

- data theft and, 16
- environment problems in ASP.NET, 52
- graphical passwords, 493
- password recovery tools, 85–87
- security feature problems, 49
- stealing Windows passwords, 85–86
- text passwords in authentication, 486–487
- Patches
  - firmware, 104
  - online games, 281
  - tips for beating thieves, 405
- PatchGuard protection, rootkit prevention and, 271
- Path manipulation, API abuse problems, 49
- Path traversal, input validation and representation problems, 47
- Pay per click (PPC), 328–329, 394. *See also* CPC (cost per click)
- Pay to click (PTC), human clickers, 338–339
- Pay to read (PTR), human clickers, 338–339
- PayPal, education resources for understanding security risks, 403
- PCI (Peripheral Component Interconnect) bus, 265
- PCI rootkits, 265–267
- PCRs (Platform Configuration Registers), 461
- PCs (personal computers), TCG specifications, 460
- PDAs (personal digital assistants), targets of crimeware, 458
- Pen Register Act (Title III), Electronic Communications Privacy Act, 432–433
- Peripheral Component Interconnect (PCI) bus, 265
- Permissions, ACLs and, 259
- Permutation and search, for finding beneficial grouping, 500
- Personal computers (PCs), TCG specifications, 460
- Personal data, collecting/transmitting, 416
- Personal digital assistants (PDAs), targets of crimeware, 458
- Pharming. *See also* Drive-by pharming attacks;  
  Hostname lookup attacks
  - electronic fraud and, 283–284
  - race pharming attacks, 119–120
  - WAPJack attacks, 116
- Phatbot, 208
- Phishing
  - anti-phishing tools, 155
  - botnets hosting, 212–213
  - criminal applications of botnets, 383
  - defined, 168
  - domain name abuse in politics and, 295
  - education resources for understanding dangers of, 402–403
  - electronic fraud and, 283–284
  - losses due to, 2
  - security education and, 400, 402
  - trawler phishing, 18, 119
  - Phishing IQ test, education resources for understanding security risks, 403
- Phones, future of crimeware, 519–520
- Phyla, Seven Kingdoms
  - API abuse, 48–49
  - code quality, 50–51
  - encapsulation, 51
  - environment, 52
  - error handling, 50
  - input validation and representation problems, 46–48
  - more need, 52–53
  - security features, 49
  - time and state, 49–50
- Phylum, in taxonomies, 42
- Physical machines, virtual machines compared with, 511
- Physical memory
  - denying write access to, 271
  - writing to, 259
- Physical theft, RFID-enabled, 96–97
- Piggybacking, distribution techniques, 20–21
- Platform Configuration Registers (PCRs), 461
- Platforms
  - extensible, 99
  - future of crimeware, 517
  - for online advertising, 387–391
- Player ability, MMOGs and, 287–288
- Player-player treatment, player treatment violations, 289
- Player treatment, MMOGs and, 288–290
- Players
  - in adware business model, 359–360
  - in bots/botnets business models, 380–381
  - in spyware/trojan business model, 368
- Plug-ins
  - Adobe Acrobat, 23
  - Apple QuickTime plug-ins, 23
  - web browsers exploits, 23
- PMPs (portable media players), vulnerabilities, 84–85
- Policy-level controls, countermeasures for RFID, 98
- Politics, cybercrime in, 293–323
  - campaign-targeted phishing, 307–312
  - cognitive hacking, in elections, 316–319
  - denial-of-service attacks, 315–316
  - domain name abuse. *See* Domain name abuses
  - overview of, 293–295
  - public voter information sources (FEC databases) and, 319–320
  - voice communication, intercepting for political advantage, 320–322
- Polybot, 208
- Polymorphic code, botnets use of, 208
- Polymorphically packed software, 31

- Pop-ups/popunders
    - abuses of adware, 361
    - means of displaying ads, 389
    - tips for beating thieves, 405
  - Port scanners, server-side vulnerabilities and, 24
  - Portable media players (PMPs), vulnerabilities, 84–85
  - Possible failures, cheating in games and, 277
  - POST (power-on self-test)
    - BIOS rootkits and, 264
    - PCI devices and, 265
  - PPC (pay per click), 328–329, 394. *See also* CPC (cost per click)
  - Preference-based life questions, 485, 494–497, 504–509
  - Presidio, AMD, 464–466
  - Pretexts, laws applicable to misrepresentation, 439
  - Prevention
    - botnet countermeasures, 224–225
    - defense-in-depth and, 476–477
    - rootkits, 271–272
  - Principles, security education, 397
  - Privacy
    - click fraud, in advertising, 351–352
    - security feature problems, 49
  - Private arrays, encapsulation problems, 51
  - Private methods, encapsulation problems, 51
  - Privileges
    - API abuse problems, 49
    - IE7 (Internet Explorer 7), 199
    - least privilege violations as security feature problem, 49
    - as security feature, 44
  - Procedural controls, countermeasures for RFID, 98
  - Process address space, denying write access to, 271
  - Process control, input validation and representation problems, 47
  - Processes, thread-based scheduling, 253–254
  - Propagation techniques, crimeware, 3–4
  - Protected storage, secure boot and, 463–464
  - Protocols, bot networks
    - HTTP, 199–200
    - IRC, 193–199
    - multiple, 223
    - overview of, 193
    - P2P, 200–202
  - Proxy attacks
    - man-in-the-middle attacks, 18
    - overview of, 15
  - Pseudo-random number generators, 49
  - PspCidTable, unlinking process from, 254
  - PTC (pay to click), human clickers, 338–339
  - PTR (pay to read), human clickers, 338–339
  - Public voter information sources, FEC databases, 319–320
  - Publisher click inflation
    - economics of click fraud and, 352–353
    - invalid clicks, 334
    - preventing, 343
  - Publishers, CPA advertising and, 330
  - Pump-and-dump stock schemes
    - spam and, 319
    - TGs and, 156
  - Purchases of goods, TGs and, 157
  - Push method, command initiation and response, 191
  - Push polling, 318
  - PwdHash, 491
- Q**
- Query phase, file sharing, 56
  - Query string-based filters, 71–72
  - QuickTime, Apple, 23
- R**
- R28's Botnet Control System (FBCS), 200
  - Race conditions, time and state problems, 50
  - Race phishing, WAPKit attacks, 119–120
  - Radio frequency ID. *See* RFID (Radio frequency ID)
  - Rake-back calculators, 20–21, 517–518
  - "Rallying box," C&C networks, 188
  - Ranking systems, games, 288
  - Ransomware
    - abuse of TPM sealing mechanism, 466
    - botnets installing, 214
    - defined, 2
    - future of crimeware, 515–517
    - trojan authors, 374–376
    - uses of crimeware, 34–35
  - RavMonE.exe, 85
  - RBID (rule-based intrusion detection), 127–128
  - ReadNotify, 371
  - Readonly memory (ROM). *See* ROM (readonly memory)
  - Real money trade (RMT), in online games, 280
  - Recovered, SIR epidemic model, 140
  - RedBrowser trojan, 100
  - Redirection
    - campaign-related phishing and, 308–309
    - political uses of malicious code, 314
    - techniques for measuring botnets, 185
    - to web sites with different political viewpoint, 304–305
  - Redirectors, email and instant messaging, 10–11
  - REFERER
    - click fraud attacks and response to, 177
    - defined, 168–169
  - Referral deals, advertising, 331–332
  - Registration, domain name abuse in politics, 296–297



- Regulatory systems, 398. *See also* Law enforcement
- Reliability, code quality and, 45
- Remote code injection, loading user-mode rootkits, 236
- Replay attacks, RFID, 92–93
- Representation problems, in Seven Pernicious Kingdoms taxonomy, 43, 46–48
- Reputation systems, future of crimeware, 517–519
- Research-driven content selection, principles of educational approaches, 397, 409
- Resident crimeware
  - overview of, 31–32
  - receiving component, 32–33
  - sending component, 32
- Resilience
  - ISTR on bot resilience, 209–210
  - network-level resilience in bot networks, 203–205
  - repacking well-known clients, 209
  - techniques for resilience in bot networks, 207–210
- Resource injection, input validation and representation problems, 47
- Resources, failure to release as code quality problem, 51
- Response, in bot network communication, 191–192
- Return on investment. *See* ROI (return on investment)
- Return values
  - unchecked values as API abuse problem, 49
  - unchecked values as error handling problem, 50
- Revenue models, advertising
  - action-based model, 329–330
  - click-based model, 328–329
  - impression-based model, 327–328
  - overview of, 326–327
  - referral deals, 331–332
  - syndication, 330–331
- Revenues/profits, from adware, 365–366
- Reverse spidering
  - click fraud attacks and response to, 177
  - overview of, 168–169
- RFID (Radio frequency ID), 89–99
  - applications, 90
  - attack types, 92–93
  - attacker model, 93–94
  - countermeasures, 97–99
  - growth in RFID industry, 91–92
  - identity theft, 95–96
  - overview of, 89–90
  - physical theft, 96–97
  - readers, 91
  - tags, 90
  - vandalism, 94–95
  - wearable computers, 520
- Rich site summary (RSS) feeds, 199
- Rights Object Acquisition Protocol (ROAP), 470
- RMT (real money trade), in online games, 280
- ROAP (Rights Object Acquisition Protocol), 470
- Robot delegates. *See* Zombies
- Robotic clicking, 339–342
  - custom bots and, 340
  - For-Sale clickbots, 341
  - forced browser clicks, 341–342
  - Malware-type clickbots, 341
  - overview of, 339–342
- robot.txt, 169
- Rock Phish kit, hacking toolkits, 357
- RockBox, 105
- ROI (return on investment)
  - ad revenue models and, 327
  - click fraud and, 352
  - click spam and, 333
- ROM (readonly memory)
  - embedded control systems and, 104
  - preventing ROM updates as rootkit prevention measure, 272
- Rootkits, 229–273
  - BIOS, 264–265
  - bot including rootkit capability, 207
  - defined, 229
  - detection, 272–273
  - detection avoidance strategies, 283
  - evolution of, 230–233
  - kernel-mode. *See* Kernel-mode rootkits
  - Linux. *See* Linux rootkits
  - overview of, 19, 229–230
  - PCI, 265–267
  - political uses of malicious code, 312
  - prevention, 271–272
  - user-mode. *See* User-mode rootkits
  - Virtual machine-based, 267–270
  - voice communication, intercepting for political advantage, 321
  - for web. *See* TGs (transaction generators)
- Router-to-router attacks, WiFi, 123–124
- Routers, wireless
  - attack vectors, 121–122
  - bricking, 109–110
  - computing capacity of wireless routers, 108
  - configuring and upgrading router firmware, 109
  - configuring home routers with CSRF, 163–164
  - countermeasures, 126–129
  - direct compromise and reselling, 125–126
  - epidemic spread and router density and, 151–153
  - human factors in UI design, 114–115
  - limiting administrative access, 111–112
  - malware epidemics. *See* WiFi malware epidemics, modeling
  - other security settings, 112–113
  - pharming attacks and, 161–162
  - preventing drive-by pharming attacks, 166–167
  - router-to-router attacks, 123–124

Routers, wireless (*contd.*)  
 security measures, 110  
 WAPJack attacks, 116–117  
 WAPKit attacks, 117–121  
 web scripting attacks, 124–125  
 wireless access and, 108  
 WLAN access and, 110–111  
 RSA SecurID, 155, 489  
 RSS (rich site summary) feeds, 199  
 Rule-based intrusion detection (RBID), 127–128  
 Rules, in game play, 278–280  
 Runtime kernel patching, Linux rootkits, 262–263  
 Runtime packers, botnets, 208  
 Rustock, spammer trojans, 377

## S

SAM (Secure Account Manager) file, usernames and passwords stored in, 85  
 Same-origin policy, botnets, 217  
 Scalability, botnet topology and, 190  
 Scams, book resources for, 402  
 Scancode, kernel-level keyloggers and, 10  
 Scheduler, Windows  
 hiding threads from, 254–255  
 thread-based scheduling, 253  
 SCM (service control manager)  
 loading kernel drivers without SCM, 258–260  
 unlinking service from, 254  
 Screenscrapers  
 installed by misleading applications, 284  
 keylogger implementation techniques, 8  
 overview of, 8–10  
 Script kiddies  
 RFID attacker model, 93–94  
 server-compromise attacks, 24  
 Scripts  
 malware attacks and, 179  
 MMOGs, 281–283  
 SDBot, 381  
 Sealing, protected storage, 463  
 Search engines, for finding web destinations, 326  
 Search node, OpenFT, 58  
 Second Life  
 bots in, 289  
 security measures, 287  
 Secure Account Manager (SAM) file, usernames and passwords stored in, 85  
 Secure boot, trusted computing, 463–464  
 Secure Sockets Layer. *See* SSL (Secure Sockets Layer)  
 SecureFlash, Intel, 264, 272  
 Security education, 397–412  
 cartoon-based case study, 408–412  
 difficulty of, 399–402  
 drawbacks of educational approaches, 405–407  
 existing approaches to, 402–404

goals, 407–408  
 guiding principles, 397  
 role of, 398–399  
 Security exploitation  
 crimeware propagation and, 3  
 Internet worms and, 21–22  
 Security features, in Seven Pernicious Kingdoms  
 taxonomy, 43–44, 49  
 Security guidelines, for MMOGs, 286–287  
 Security measures, wireless routers, 110–113  
 Security model, for MMOGs, 285–286  
 Security patches, tips for beating thieves, 405. *See also* Patches  
 Security policies, countermeasures for RFID, 98  
 Security questions. *See* Life questions  
 Security software  
 botnets disabling, 207  
 improving state of the art in, 385  
 SEGV (segmentation fault), 479  
 Self-signed certificate, 79  
 Sensitive information  
 holding victim data hostage, 315  
 Spyblock for entering, 491–492  
 theft. *See* Theft of sensitive information  
 trojans for stealing, 372–373  
 Sensitivity, in malware filtering, 63  
 Server-compromise, distribution techniques, 24  
 Server-side vulnerabilities, port scanners and, 24  
 Servers, TCG specifications, 460  
 Service control manager (SCM). *See* SCM (service control manager)  
 Service hardening, HTTP and, 199  
 Service-oriented architecture (SOA), susceptibility to malicious code, 39  
 Service set identifiers (SSIDs). *See* SSIDs (service set identifiers)  
 Services, unlinking from SCM, 254  
 Session hijacking  
 man-in-the-middle attacks, 18  
 overview of, 11–12  
 Session identifiers, environment problems in J2EE, 52  
 Sessions, time and state problems, 49  
 Setting manipulation, input validation and representation problems, 47  
 Seven Pernicious Kingdoms (taxonomy of coding errors)  
 API abuse, 43, 48–49  
 code quality, 45, 50–51  
 encapsulation, 45, 51  
 environment, 45, 52  
 error handling, 44–45, 50  
 input validation and representation problems, 43, 46–48  
 more phyla needed, 52–53  
 overview of, 40–42

- security features, 43–44, 49
- time and state, 44, 49–50
- Shadow walker technique, 255
- ShadowCrew, 356
- Shadowserver foundation, statistics regarding
  - botnets, 187
- Shoobox problem, two-factor authentication, 490
- Signature-based IDS, 127–128
- Signature generators, AGIS, 479, 481
- Signatures
  - automatic infection signature generation, 478, 481–482
  - detection of spyware infections and, 476
  - spyware scanners searching for, 475
  - viruses and, 473
- Signed applet case study, human-propagated crimeware, 77–82
- Simple Mail Transfer Protocol (SMTP), as vehicle for crimeware propagation, 3
- Single criteria filters, for individual networks
  - file name–based filters, 68–69
  - file size–based filters, 64–68
  - host IP–based filters, 69–71
  - overview of, 61–64
  - query string–based filters, 71–72
- Single criteria filters, used across networks, 72–73
- SIR (susceptible-infected-recovered) epidemic model, 140, 146–147
- Size metrics, bot networks, 186–188, 216
- Skimming, RFID attacks, 92
- Slanret incident, 231
- Slapper worm, 190
- slashdot, 520
- Small devices, 83–101
  - mobile devices, 99–102
  - RFID. *See* RFID (radio frequency ID)
  - USB drives. *See* USB flash drives
- Smart pricing for advertising, Google, 346
- Smokescreens, adware techniques for evading law enforcement, 364
- SMTP (Simple Mail Transfer Protocol), as vehicle for crimeware propagation, 3
- SOA (service-oriented architecture), susceptibility to malicious code, 39
- Social engineering, crimeware propagation and, 3
- Social networks, for bootstrap attacks, 520
- Software
  - burdens of surreptitious software, 417–418
  - difficulty in removal of surreptitious software, 417
  - improving state of the art in security software, 385
- Software-based security initiatives, approaches to improved security, 398
- Software features, bot networks
  - applications, 210–215
  - general software features, 205–206
  - overview of, 205–206
  - techniques for resilience, 207–210
- Software vendors
  - profit models, 390–391
  - spyware, 368–370
- Spam
  - botmasters use of, 379
  - botnets for relaying, 211
  - criminal applications of botnets, 382–383
  - filters, applied at chokepoints, 26
  - overview of, 332
  - pump-and-dump stock schemes and, 319
  - transmission, 33
- Spam, in advertising
  - click spam, 333–334
  - conversion spam, 334–335
  - impression spam, 332–333
  - types of, 332
- Spammer, trojan authors, 377–378
- SpamThru, 377
- Spear-phishing, 284
- Speculation, domain name abuse in politics and, 297–298
- Spidering, 169
- Spiders, click fraud attacks and response to, 177
- Spoof Email Tutorial, eBay, 403
- Spoofing attacks, client containment, 129
- Spyblock system, 491–492
- SpyShield, for containment, 478, 482–483
- Spyware
  - anti-spyware laws. *See* Anti-spyware laws
  - criminal applications of botnets, 383
  - for extracting sensitive data, 101
  - legitimate uses, 367
  - political uses, 313–314
  - software vendors, 368–370
  - trojans compared with, 367
- Spyware case study
  - AGIS for automatic infection signature generation, 478, 481–482
  - defense-in-depth, 476–478
  - overview of, 475–476
  - packet vaccine for automatic detection of exploit attempts, 477–480
  - SpyShield for containment, 478, 482–483
- Spyware/trojans, as business model, 367–378
  - downloader trojan authors, 376–377
  - espionage trojan authors, 370–372
  - information-stealing trojan authors, 372–374
  - overview of, 367–368
  - players in, 368
  - ransomware trojan authors, 374–376
  - spammer trojan authors, 377–378
  - Spyware software vendors, 368–370

- SQL injection
    - input validation and representation problems, 47
    - vulnerabilities, 23
  - SSDT (system service descriptor table) hooks
    - kernel-mode rootkits, 243–245
    - thread-based SSDT hooks, 246–247
  - SSIDs (service set identifiers)
    - weak security configuration and, 113
    - wireless access and, 110
  - SSL (Secure Sockets Layer)
    - client-side certificates as alternative to password authentication, 488
    - environment problems in J2EE, 52
    - man-in-the-middle attacks and, 18, 117–119
    - security education and, 401
    - TGs and, 156
  - Staged downloaders, for crimeware installation, 29
  - State and time, in Seven Pernicious Kingdoms
    - taxonomy, 44, 49–50
  - State laws, surreptitious code, 448–456
  - Statistical detection systems. *See* Anomaly detection systems
  - Stealthy attacks, active and passive, 179–180
  - Storage, protected storage in trusted computing, 462–463
  - Stored Communications Act (Title II), Electronic Communications Privacy Act, 431–432
  - String manipulation, API abuse problems, 49
  - String termination errors, input validation and representation problems, 47
  - Struts, input validation and representation problems, 47–48
  - stumbleupon, 520
  - Subvirt, 459
  - Sun Java, web browser vulnerabilities, 23
  - Super-botnet, 203
  - Surreptitious code, 413–456
    - anti-spyware laws, 425–430, 449–456
    - burdens created by, 417
    - CAN-SPAM Act, 434–435, 442
    - collecting/transmitting personal data, 416
    - Computer Fraud and Abuse Act, 418, 419–420, 443–444
    - Credit Card (or “Access Device”) Fraud Act, 445
    - difficulty in removal, 417
    - download, install, and operation of, 415
    - Electronic Communications Privacy Act, 430–433, 445–446
    - exploitation of intercepted information, 418
    - federal laws, 442–448
    - Federal Trade Commission Act, 420–423, 446–447
    - Federal Trademark Act of 1946 (Lanham Act), 435–436, 447
    - Gramm-Leach-Bliley Financial Services Modernization Act, 439, 447
    - Identity Theft and Assumption Deterrence Act, 436–439, 447–448
    - interfering with computer operation, 416–417
    - laws applicable to, 418
    - misrepresentation and impersonation strategies, 415–416
    - overview of, 413–415
    - state laws, 448–456
    - theft laws, 439–440, 456
    - trespass to chattels, 423–425, 456
    - Wire Fraud Statute, 448
  - Surveillance
    - email and instant messaging redirectors and, 10–11
    - spyware and, 367
  - Susceptible-infected-recovered (SIR) epidemic model, 140, 146–147
  - Susceptible, SIR epidemic model, 140
  - Symbrian
    - extensible platforms, 99
    - protection from untrusted applications, 101
  - SYN/ACK attacks, as example of API abuse, 43
  - Syndication, advertising deals, 330–331
  - SYSENTER hooks, 243
  - System call code patching, kernel-mode rootkits, 247
  - System call hooks, kernel-mode rootkits, 242–243
  - System data, information leaks as encapsulation problem, 51
  - System hooks, keylogger implementation techniques, 8–9
  - System reconfiguration attacks, 13–15
    - hostname lookup attacks, 13–15
    - information compromise and, 31
    - overview of, 13
    - proxy attacks, 15
  - System service descriptor table (SSDT) hooks. *See* SSDT (system service descriptor table)
  - System software, bots disabling, 207
  - SystemLoadAndCallImage, loading kernel drivers, 258
- ## T
- Tag cloning, RFID attacks, 92
  - Tag spoofing, RFID attacks, 93
  - Tags, RFID, 90
  - Task manager, thread-based scheduling, 253
  - Taxonomies
    - of coding errors. *See* Seven Pernicious Kingdoms (taxonomy of coding errors)
    - crimeware, 5–7
    - phylum and kingdoms in, 42
  - TCG (Trusted Computing Group)
    - attestation, 462
    - integrity measurement and storage, 461
    - protected storage, 462–463
    - secure boot, 464
    - specifications for trusted systems, 460

- Teardrop attacks, as example of API abuse, 43
- Technological controls, countermeasures
  - for RFID, 98
- Temporary files, time and state problems, 50
- Terrorware, future of crimeware, 515–517
- Texas Instruments Digital Signal Transponder (TI-DST), 97
- Text passwords, as authentication mechanism, 486–487
- TGs (transaction generators), 155–160
  - building, 156–157
  - cross-site forgery with, 156
  - information harvesting by bots, 223–224
  - mitigation techniques, 158–160
  - overview of, 12–13, 155–156
  - stealth of, 157–158
- Theft laws
  - state laws regarding surreptitious code, 456
  - surreptitious code, 439–440
- Theft of sensitive information
  - bots used for, 210
  - protecting sensitive information in online games, 286
  - stages of crimeware attacks and, 7
  - types of information at risk, 2
- Third-party applications, as targets of malware, 520–521
- Thread-based SSDT hooks, kernel-mode rootkits, 246–247
- Threads
  - creating remote thread in DLL injection, 234
  - kernel-mode rootkit for hiding threads from Scheduler, 254–255
- Threat model, 5–7
- Thresholds, in malware filtering, 63
- Throwing exceptions, error handling problems, 50
- TI-DST (Texas Instruments Digital Signal Transponder), 97
- Time and state, in Seven Pernicious Kingdoms
  - taxonomy, 44, 49–50
- TLB (translation look-aside buffer)
  - desynchronizing, 255
  - hiding code pages, 257
  - hiding data pages, 257–258
- TNC (Trusted Network Connect), 462
- Topology, botnets, 188–191
- TPM (Trusted Platform Module)
  - protected storage in trusted computing, 462–463
  - TCG specification for microcontroller design, 460
- Tracking attacks, RFID, 92
- Trademarks
  - Federal Trademark Act of 1946 (Lanham Act), 435–436
  - protecting registered domain names, 296–297
- Traffic, botnets for relaying, 211
- Trampoline, inline function patching (detours)
  - and, 238
- Transaction confirmation, TG mitigation techniques, 158
- Transaction generators. *See* TGs (transaction generators)
- Transaction pages, randomizing as TG mitigation technique, 158
- Translation look-aside buffer. *See* TLB (translation look-aside buffer)
- Trawler phishing
  - defined, 18
  - WAPKit attacks, 119
- Trespass to chattels tort
  - provisions of, 423–425
  - state laws regarding surreptitious code, 456
- Trinity of Trouble
  - complexity, 39
  - connectivity, 38–39
  - extensibility, 40
  - overview of, 37–38
- Trivial name-based obfuscation, botnets, 208
- Trojan authors
  - downloaders, 376–377
  - espionage program, 370–372
  - information-stealing programs, 372–374
  - ransomware programs, 374–376
  - spammer programs, 377–378
- Trojan.checkraise, 20, 517–518
- Trojan.Dowiex, 9
- Trojan.Gpcoder, 315, 375
- Trojan.Peacomm, 201–202
- Trojans
  - political uses of malicious code, 314–315
  - pricing and distribution of, 374
  - RedBrowser trojan, 100
  - spyware compared with, 367
  - web trojans, 12
- Trojan.Welomoch, 230
- Trust
  - boundary violations as encapsulation problem, 51
  - running malicious code in trusted process, 209
- Trusted computing, 457–472
  - attack anatomy and, 458–460
  - attestation, 462
  - case studies, 466
  - combating crimeware, 460
  - content protection, 469–472
  - credit card security, 467–468
  - hardware-enforced isolation, 464–465
  - integrity measurement and storage, 461–462
  - overview of, 457–458
  - as panacea, 465–466
  - protected storage, 462–463
  - secure boot, 463–464

Trusted Computing Group. *See* TCG (Trusted Computing Group)  
 Trusted Network Connect (TNC), 462  
 Trusted Platform Module (TPM). *See* TPM (Trusted Platform Module)  
 Trusted systems, specifications for, 460  
 Two-factor authentication, 488–490  
 Typo squatting  
   analysis conclusions, 300–301  
   analysis process, 299–300  
   domain name abuse in politics, 298–303  
   overview of, 298  
   redirection to web sites with different political viewpoint, 304–305

## U

U3-based malware, 86–87  
 UDRP (Uniform Domain Name Dispute Resolution Policy), 296  
 UI (user interface), human factors in UI design, 114–115  
 Ultrapeer mode, Gnutella protocol, 58  
 Uniform Domain Name Dispute Resolution Policy (UDRP), 296  
 UNIX utilities, rootkits, 229  
 Unknown malware  
   file name–based filters, 69  
   file size–based filters, 66  
 Unreal IRCd, 194  
 Updates, propagation by firmware, 103–104  
 URLs, malicious content embedded into, 23  
 USB devices, propagation techniques, 20  
 USB flash drives, malware propagation, 83–89  
   countermeasures, 89  
   DMA vulnerability, 87  
   example stealing Windows passwords, 85–86  
   gauging risk of, 88–89  
   overview of, 83–85  
   U3-based malware, 86–87  
 USB Hacksaw, 87  
 USB Switchblade, 86–87  
 User immersion, principles of educational approaches, 397, 411  
 User interface (UI), human factors in UI design, 114–115  
 User-mode rootkits, 233–240  
   DLL injection, 234  
   IAT hooks for modifying execution path, 236–238  
   inline function patching (detours), 238–240  
   overview of, 31, 233  
   remote code injection, 236  
   Windows hooks for loading, 235–236  
 User node, OpenFT, 58  
 Users, data leaks between (encapsulation problems), 51

## V

Vaccine exploits, 478  
 Vaccines, 478  
 Value proposition, common problems in adware industry, 360  
 Vandalism, RFID-enabled, 94–95  
 Vandalware, 515–517  
 Variables, uninitialized variables as code quality problem, 51  
 Vehicles, future of crimeware and, 519–520  
 Vendors, software, 390–391  
 VFS (Virtual File System), 263–264  
 Video games, 276–278. *See also* Games; MMOGs (massively multiplayer online games)  
 Video, infection vectors, 77  
 Viral content, luring visitors to site for click fraud attack, 178–179  
 Viral marketing, 77–80  
 Viral videos, 77  
 Virtual File System (VFS), 263–264  
 Virtual machine-based rootkits. *See* VMBRs (virtual machine-based rootkits)  
 Virtual machine monitors (VMMs), hardware-enforced isolation and, 464  
 Virtual machines, as defense technique, 510–514  
   applications of, 513–514  
   data isolation and, 510  
   firewalls and, 513  
   physical machines compared with, 511  
   problems with multiple machines, 511–512  
 Virtual memory, kernel-mode rootkits for redirecting, 255–258  
 Virtual PC, 268  
 Virtual private networks (VPNs), security standards for network access, 110, 111  
 Virtual worlds, 275–292  
   cheating, 276–278  
   electronic fraud. *See* Electronic fraud  
   games and fraud, 276  
   MMOGs. *See* MMOGs (massively multiplayer online games)  
   overview of, 275–276  
 Viruses, signatures, 473  
 VMBRs (virtual machine-based rootkits), 267–270  
   hardware-assisted, 268–270  
   overview of, 267  
   software-based, 267–268  
   virtual machine detection in rootkit detection, 273  
   VMRUN/VMLAUNCH emulation, 270  
 VMMs (virtual machine monitors), hardware-enforced isolation and, 464  
 VMRUN/VMLAUNCH emulation, 270  
 VMware, 268

Voice communication, intercepting for political advantage, 320–322. *See also* Communication, bot networks

Voters

- deceiving via cognitive hacking, 316–318
- election fraud and, 294
- public voter information sources, 319–320

VPNs (virtual private networks), security standards for network access, 110, 111

VT-x (Vanderpool), Intel, 233

Vulnerability, cheating in games and, 277

## W

W32/RJump worm, 85

W32.Gaobot.gen!poly, 208

W32.Korgo.Q, 200

WAPFunnel, 116

WAPJack attacks

- attacking own computer as security measure, 126–127
- types of, 116–117

WAPKit attacks, 117–121

- attacking own computer as security measure, 126–127
- click fraud, 120–121
- man-in-the-middle attacks, 117–119
- overview of, 117
- race pharming, 119–120
- robot delegates (zombies), 121
- trawler phishing, 119

WAPs (wireless access points). *See also* WiFi

- case study, 107–108
- classes of, 108
- cloaking wireless networks, 110
- default settings, 115
- human factors in UI design, 114–115
- security warnings mandated for, 114
- as targets of malware, 107
- Warkitting attacks, 122–123
- weak security configuration as rule, 113–114

Wardriving, 161–162

Warez

- botnets harvesting, storing, and propagating, 213
- criminal applications of botnets, 382

Warkitting attacks

- drive-by pharming attacks and, 161–162
- WAPs and, 122–123

WDM (Windows Driver Model), layered model for drivers, 247–248

Weak security configuration, as rule for WAPs, 113–115

Wearable computers, future of crimeware, 519–520

Web 2.0 software, susceptibility to malicious code, 39

Web browsers, 155–182

- attacking third party applications, 521
- Botnet 2.0 (browser-based botnets), 216–217
- Browser helper objects, 8, 29
- click fraud using JavaScript. *See* Click fraud, using JavaScript
- drive-by pharming. *See* Drive-by pharming attacks
- forced browser clicks, 341–342
- same-origin policy and, 217
- session hijackers and, 11–12
- transaction generators. *See* TGs (Transaction generators)
- vulnerabilities of, 521–522
- web browsers exploits as distribution technique, 22–24

Web scripting attacks, WiFi firmware, 124–125

Web trojans, 12

WebAttacker, 357

Webroot, 475

WebWhacker, 398

WEP (wired equivalent privacy)

- Airsnort defeating, 122–123
- encryption options for wireless networking, 111
- epidemic spread and router density and, 151–153
- limitations of, 126, 134

wget, open-source utilities for building bots, 340

WhenU, trends in adware business, 366

WiFi. *See also* WAPs (wireless access points)

- computing capacity of wireless routers, 108
- countermeasures, 126–129
- limiting administrative access, 111–112
- other security settings, 112–113
- router-to-router attacks, 123–124
- routers. *See* Routers, wireless
- security measures, 110
- targets of malware, 103
- wireless access and, 108
- WLAN access and, 110–111

WiFi malware epidemics, modeling

- contagion network, 135–137
- epidemic model, 139–145
- epidemic spread, WEP and WPA deployment and router density, 151–153
- giant component, 137–139
- infecting router, 132–134
- methodology for, 131
- overview of, 130–131
- roadmap for case study, 132
- spread of synthetic epidemics, 145–151
- wireless security law in California, 153

WiFi protected access. *See* WPA (WiFi protected access)

WiGLE (Wireless Geographic Logging Engine), 135

Windows Driver Model (WDM), layered model for drivers, 247–248

Windows hooks, loading user-mode rootkits, 235–236

Windows Media Player, web browser vulnerabilities, 24

Windows Metafile flaw, trojans exploiting, 374

Windows Mobile

- extensible platforms, 99
- mobile devices, 101
- protection from untrusted applications, 101

Windows Object Manager, 258

Windows OSs

- example stealing Windows passwords, 85–86
- rootkit evolution and, 231–232
- rootkits. *See* User-mode rootkits

Windows Scheduler. *See* Scheduler, Windows

Windows Vista

- complexity as factor in malicious code, 39
- process-hardening technology, 199
- RSS feed manager, 199–200

Wire Fraud Statute, federal laws regarding surreptitious code, 448

Wired equivalent privacy. *See* WEP (wired equivalent privacy)

Wireless access points. *See* WAPs (wireless access points)

Wireless bridging, 116–117

Wireless devices, as targets of malware, 103

Wireless Geographic Logging Engine (WiGLE), 135

Wireless honeypots, as wireless countermeasure, 128–129

Wireless LANs (WLANs), 110–111

Wireless routers. *See* Routers, wireless

Wireless security law, in California, 153

Wiretap Act (Title I), Electronic Communications Privacy Act, 430–431

WLANs (wireless LANs), 110–111

World of Warcraft

- bots in, 289
- network architecture of, 281
- targets for malicious code, 39

World-player treatment, player treatment violations, 289

World Wide Web (WWW), commercialization of, 326

WPA (WiFi protected access)

- for encrypting wireless routers, 134
- encryption options for wireless networking, 111
- epidemic spread and router density and, 151–153
- protecting WiFi networks, 126

Write access, rootkit prevention and, 271

WRT54G router, Linux, 105, 113

WWW (World Wide Web), commercialization of, 326

## X

XCP (Extended Copy Protection), 230

XML-based command, botnets, 222

XML validation, input validation and representation problems, 48

## Y

YouTube, viral videos, 77

## Z

Zango, trends in adware business, 366

Zero days

- trojan authors exploiting zero-days flaws, 371
- web browsers exploits, 22

Zombies. *See also* Bot networks/Bots

- grids of infected computers, 378
- overview of, 184
- WAPKit attacks, 121

Zune

- malicious alteration of embedded control systems, 107
- vulnerabilities, 85