Internet Security: Hacking, Counterhacking, and Society

Kenneth Einar Himma
Seattle Pacific University

JONES AND BARTLETT PUBLISHERS
Sudbury, Massachusetts
BOSTON TORONTO LONDON SINGAPORE

World Headquarters
Jones and Bartlett
Publishers
40 Tall Pine Drive
Sudbury, MA 01776
978-443-5000
info@jbpub.com
www.jbpub.com

Jones and Bartlett
Publishers Canada
6339 Ormindale Way
Mississauga, Ontario
L5V 1J2
CANADA

Jones and Bartlett
Publishers International
Barb House, Barb Mews
London W6 7PA
UK

Jones and Bartlett's books and products are available through most bookstores and online booksellers. To contact Jones and Bartlett Publishers directly, call 800-832-0034, fax 978-443-8000, or visit our website www.jbpub.com.

Substantial discounts on bulk quantities of Jones and Bartlett's publications are available to corporations, professional associations, and other qualified organizations. For details and specific discount information, contact the special sales department at Jones and Bartlett via the above contact information or send an email to specialsales@jbpub.com.

Production Credits
Acquisitions Editor: Tim Anderson
Production Director: Amy Rose
Editorial Assistant: Laura Pagluica
Production Assistant: Jamie Chase
Manufacturing Buyer: Therese Connell
Marketing Manager: Andrea DeFronzo
Composition: Northeast Compositors, Inc.
Cover Design: Kristin E. Ohlin
Cover Image: © Vasil Vasilev / ShutterStock, Inc.
Cover Image: © Melissa King / ShutterStock, Inc.
Printing and Binding: Malloy, Inc.
Cover Printing: Lehigh Press

Library of Congress Cataloging-in-Publication Data
Internet security : hacking, counterhacking, and society / Kenneth
Einar Himma. – 1st ed.
p. cm.
Includes index.
ISBN-13: 978-0-7637-3536-4
ISBN-10: 0-7637-3536-1
1. Internet–Security measures. 2. Computer security–Moral and
ethical aspects. 3. Computer hackers. I. Himma, Kenneth Einar.
TK5105.875.I57I574 2006
005.8–dc22
2006014412

6048

Printed in the United States of America
10 09 08 07 06 10 9 8 7 6 5 4 3 2 1

Introduction

From North America to South America to Asia, computer-related misconduct is posing an ever-growing problem in the public and the private sectors for several reasons. First, nearly every nation, industrial and developing, is becoming increasingly reliant on new digital information technologies to perform legitimate commercial and governmental functions. While these new information technologies have impacted social well-being in a variety of beneficial ways, they have also exposed a number of important interests to possible intrusion or attack. For example, a reasonably sophisticated distributed denial of service attack can take a commercial Web site down for hours, potentially resulting in the loss of revenue, value to shareholders, and, ultimately, jobs that may be spread across the globe. The effects on the global economy are potentially significant.

Second, the frequency of digital attacks and intrusions directed at private commercial interests has been steadily increasing over the years as the number of people with the appropriate motivations and technical skills continues to grow. Compounding the problem is the increasing availability on the Web of easy-to-use hacker tools that can be used by comparatively unskilled users — so-called script kiddies — to stage malicious attacks and intrusions against private networks. These tools are available to anyone, anywhere in the world, who has access to the Internet.

Third, at this point in time, not a single nation has adequate law-enforcement resources to pursue investigations into the vast majority of computer intrusions involving that nation. But even in those occasions where a nation has sufficient resources to warrant intervention, the response is likely to come long after the damage is done. It is uncontroversial that law enforcement agencies have not been able to keep pace with the rapidly growing problems posed by digital attackers.

Hackers believe that, at the very least, non-malicious intrusions are morally permissible and have offered a number of arguments purporting to justify such intrusions. Some hackers believe, for example, these intrusions are justified by consequentialist considerations because they result in an increase in humanity's stock of knowledge about the relevant technologies. This, therefore, promotes the development of technologies that will ultimately help make the Internet more secure. Some hackers believe that any barriers to information are morally illegitimate and hence deserve no respect, including barriers that separate the information on an individual's computer from another individual's computer.

Recently, a number of writers have begun to suggest that attacks on government and corporate sites might be justified as a form of political activism. On this influential line of analysis, acts that are otherwise ethically impermissible or unlawful might be morally and legally acceptable if motivated by a political concern to protest unjust laws or institutions. Similarly, digital attacks that might otherwise be legally or morally objectionable are legally and morally permissible if they are politically-motivated acts of civil disobedience or "hacktivism."

Not surprisingly, victims of such attacks disagree and have begun to respond to digital attacks with measures that have been characterized as "hacking back" or "active defense." These measures are distinguished from other kinds of private intrusion responses in that they are noncooperative and reasonably calculated to causally impact remote systems (i.e., those that belong to other persons or entities). While active defense measures are not necessarily "uncooperative," in the sense of being deliberately contrary to the wishes of other parties, they are undertaken unilaterally in situations where the interests of other parties are infringed and are thus reasonably characterized as non-cooperative in nature.

Active defense measures exhibit varying levels of force. Some of these responses are aggressive in the sense of being intended to inflict the same kind of harm on the attacker's machine or network as the attack intended to inflict on the victim's machine or network. Some active defense measures are, however, intended simply to gather intelligence about the attack and are significantly less aggressive in character. One increasingly common active defense measure involves an attempt to follow an attack path in reverse through intermediate networks and systems in order to identify the parties ultimately culpable for that attack. While there are more benign, cooperative tactics for tracing the path of an attack, these more invasive traceback technologies follow attack paths by entering into machines and networks involved in the attack.[1]

[1] Another related issue of theoretical interest arises in connection with the so-called Good Samaritan Worm—a worm that was designed to eliminate a security vulnerability to a more malicious worm and then was released onto the Internet where it was unwittingly downloaded by thousands of users.

Many individuals have come to believe that private persons and firms have a right to protect themselves against hacker attacks because (1) such attacks are, contrary to the arguments of hackers, unjustified and (2) law enforcement is currently unable to protect them. For example, Tim Mullen argues that the right to self-defense implies a right on the part of firms to adopt even aggressive active defense in response to a digital attack:

> *I propose that we have the right to defend our systems from attack. I am not talking about some vigilante strike upon script kiddies at the drop of a packet. I am not talking about a rampant anti-worm. I am talking about neutralizing an attacking machine in singularity when it is clearly and definitively infected with a worm that will continue to attack every box it can find until stopped.... The moment that I begin to incur costs, or the integrity of services that I pay for is reduced by any degree, is the moment that I have the right to do something about it.... It is simply self-defense.* (Security Focus, 2003)

Somewhat different issues arise in connection with the proliferation of a large number of "e-organisms," such as viruses and Internet worms. Whereas a person need not perform any affirmative acts to be victimized by a hacker attack, he or she must perform some sort of act, such as opening an email attachment, to be victimized by a virus or a worm. Some people have suggested that such acts amount to a form of "implied consent" that immunizes the writer of the virus or worm from moral and legal culpability. Further, some commentators argue that benevolent e-organisms, those designed to install a helpful fix or patch of some kind, are morally justified.

There are, of course, other important Internet security issues that arise directly from unwanted computer intrusions. These intrusions, for example, are becoming increasingly common in the growing world of on-line gaming, which poses a host of security risks—some more important and some less important. For example, a breach of security within an on-line gaming community might lead to something as serious as identity theft or it might, less seriously, lead to one person's hijacking another's resources to play a game under the latter's on-line name. Gamers, in every nation, are unfortunately vulnerable.

Still other important security problems are indirectly related to unwanted computer intrusions. For example, one concern pertains to the growing number of Web sites all over the world that are devoted to discussing code contrived to facilitate the commission of such intrusions. Indeed, some Web sites will publish code that can be used/abused to commit these very intrusions. One might legitimately ask whether the authors of such Web content should be criminally or civilly liable for the intrusions and associated harms that foreseeably result from them.

Other problems arise in connection with certain technologies that have been developed to protect persons from these various intrusions—technologies that raise a host of ethical questions themselves. There are many technologies, such as encryption and steganography, that enable a person to conceal the content of certain messages from potential hackers and crackers. These technologies, however, can also be used in ways that have social costs, raising the issue of whether, and to what extent, they may permissibly be used.

In any event, the problems associated with unwanted computer intrusions are of significant interest to ethicists and policymakers because they implicate a variety of morally significant considerations across the globe. Digital attacks, for example, not only affect the financial and privacy interests of victims, they can also affect other important interests. At best, a digital intrusion forces its immediate victim to shift resources from more productive uses to less productive security uses, costs that are passed on to consumers in the form of higher prices. At worst, a coordinated digital attack that takes key commercial firms offline for significant periods can result in millions of dollars in lost revenue and employment. These costs impact our collective material well-being in a variety of ethically significant ways. Unfortunately, such costs are likely to increase along with the frequency and severity of such incidents.

Not surprisingly, the various problems posed by unwanted computer intrusions are of growing concern to public officials and policymakers in every nation who are struggling to assess the costs, benefits, and legitimacy of coercive regulation. Public officials must attempt to weigh the risks and impacts of the various intrusions against the impacts of regulating such intrusions on morally legitimate speech, property, and privacy interests, along with the costs to taxpayers of ensuring efficacious regulation. As is evident by the controversial character of the various debates, there are no obvious answers to these problems.

This book considers the ethical issues that arise in connection with unwanted computer intrusions. The collection begins with a chapter by Tom Forester and Perry Morrison, "Hacking and Viruses," that provides a general overview of some of the important issues regarding unwanted intrusions. In "The Conceptual and Moral Landscape of Computer Security," Herman Tavani articulates some general conceptual and ethical issues that must be addressed before proceeding to an evaluation of specific problems associated with unwanted computer intrusions.

Part Two is concerned with hacking, hacktivism, and counterhacking. The section begins with two chapters, Eugene Spafford's chapter "Are Computer Hacker Break-ins Ethical?" and Mark Manion and Abby Goodrum's chapter "Terrorism or Civil Disobedience: Toward a Hacktivist Ethic." The former chapter considers whether hacking motivated by curiosity and other benign purposes is morally permissible, while the latter considers whether politically-motivated hacking is morally permissible. It continues with two contributions by myself—one on whether hacktivism can be justified as a form of electronic civil disobedience and the other on whether it is permissible for victims of a digital attack to hack back at the perpetrators. This section ends with Dorothy Denning's chapter, "A View of Cyberterrorism 5 Years Later."

Part Three considers ethical issues that arise in connection with professionalism and design. Don Gotterbarn and David Tarnoff discuss certain ethical issues that arise in connection with computer professionalism in "Internet Development: Professionalism, Profits, Ethics, or Sleaze?" The chapter focuses primarily on the need to "professionalize" Internet development. Next is a chapter on informed consent and value sensitive design by Batya Friedman, Daniel Howe, and Edward Felten. Richard Epstein closes Part Three by exploring general issues of professionalism in development in "The Impact of Computer Security Concerns on Software Development." This chapter will be particularly valuable to software developers.

The book concludes with Part Four, which considers a number of miscellaneous problems associated with Internet security. The first chapter in this section is an in-depth discussion of steganography by Frances Grodzinsky, Keith Miller, and Marty Wolf, entitled "The Ethical Implications of the Messenger's Haircut: Steganography in the Digital Age." It continues with a chapter on the security issues associated with on-line gaming by Kai Kimppa, Andy Bissett, and N. Ben Fairweather, entitled, appropriately enough, "Security in On-line Games." Adam Moore's contribution discusses the relationship between putative justifications for hacking and intellectual property and privacy rights. Last, but not least, Maria Canellopoulou-Bottis discusses the issue of whether, and to what extent, software vulnerabilities may permissibly be exposed and publicized by third-parties in the chapter "Disclosing Software Vulnerabilities."

I am optimistic that the wide range and high quality of these chapters ensures that this book will be a valuable addition to the library of anyone who is concerned about the growing number of problems associated with unwanted computer intrusions.

Classroom Use

This volume can be used in a variety of classroom settings for a variety of courses at nearly every level. It is suitable as a principal text for courses concerned with security issues in computer science departments, information schools, philosophy departments, and even law schools. The interdisciplinary character of the volume, of course, mirrors the multidisciplinary interests of the authors. It is also suitable as a supplemental text for general courses in information ethics, which tend to gloss over security issues—despite their growing importance. Additionally, it can be used at both the beginning undergraduate and advanced graduate level; the theorizing, while always demanding and sophisticated, is uniformly clear and well-written. The diversity of uses to which this text can be put, I believe, makes it a valuable addition to academic and professional literature.

About the Author

Kenneth Einar Himma teaches philosophy at Seattle Pacific University. He formerly taught in the Philosophy Department, the Information School, and the Law School at the University of Washington. His specialties are legal philosophy and information ethics. He is the author of more than 100 scholarly articles, encyclopedia entries, book reviews, and op-ed newspaper pieces. He is on the editorial boards of *International Review of Information Ethics* and the forthcoming *INSEIT Journal*.

Acknowledgments

"Are Computer Break-ins Ethical?" originally appeared in the *Journal of Systems Science* (1992, Vol 17). "Hacking and Viruses" originally appeared in the book *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing, Second Edition* (MIT Press, 1994). "Terrorism or Civil Disobedience: Toward a Hacktivist Ethic" originally appeared in *Computers and Society* (2000, Vol 30). "Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design" originally appeared at the *Proceedings of the Thirty-Fifth Annual Hawai'i International Conference on System Sciences* (IEEE Computer Society: Los Alamitos, CA). I am grateful to the authors and to the publishers for allowing me to republish these essays here.

Table of Contents