COMPUTERS UNDER ATTACK

INTRUDERS, WORMS, AND VIRUSES

Edited by

Peter J. Denning

Computers Under Attack

Intruders, Worms, and Viruses

EDITED BY

Peter J. Denning

Research Institute for Advanced Computer Science
NASA Ames Research Center

acm PRESS

ACM PRESS
New York, New York

ADDISON-WESLEY PUBLISHING COMPANY
Reading, Massachusetts ▪ Menlo Park, California ▪ New York
Don Mills, Ontario ▪ Wokingham, England ▪ Amsterdam
Bonn ▪ Sydney ▪ Singapore ▪ Tokyo ▪ Madrid ▪ San Juan

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 Addison-Wesley was aware of a trademark claim, the designations have been printed in initial caps or all caps.

Library of Congress Cataloging-in-Publication Data

Computers under attack : intruders, worms, and viruses / Peter J.
Denning, editor.
p. cm.
Includes bibliographical references.
ISBN 0-201-53067-8
1. Computers—Access control. 2. Computer viruses. I. Denning,
Peter J., 1942- .
QA76.9.A25C667 1990
006.8—dc20 89-18537
CIP

ABCDEFGHIJK—MA—943210

Preface

Network intruders—some would call themselves explorers or liberators—have found ways of using networks to dial into remote computers, browse through their contents, and work their way into other computers. They have become skilled at cracking the password protocols that guard computers and adept at tricking the operating systems into giving them superuser or system manager privileges. They have also created worm and virus programs that carry out these actions unattended and replicate themselves endlessly—electronic surrogates that can prowl the network independent of their creators. We can expect steady increases in acts of crime, espionage, vandalism, and even political terrorism by computer in the years ahead.

The growing world network shares many characteristics with biological organisms, especially an astronomical number of connections among a large number of simple components. The overall system can exhibit behaviors that cannot be seen in an analysis of its separate components. Like their biological counterparts, computer networks can suffer disorders from small organisms that create local malfunctions; in large numbers, these organisms can produce network-wide disorder. For this reason, the attacks against networks of computers have biological analogies, and two of them, worms and viruses, are designated by explicit biological terminology.

Newspapers tell tales of growing public concern about the integrity and privacy of information stored in computers. As electronic networking spreads around the globe, making possible new international interactions and breaching barriers of language and time, so rise the risks of damage to valuable information and the anxiety over attacks by intruders, worms, and viruses.

There also have been several recent books and numerous articles on this subject. The more I read, the more I have become convinced that I must listen to many people before I can understand the phenomenon of attacks on computers. The phenomenon arises in the context of a worldwide network of computers; no one single point of view will shape the outcome.

To help you listen to what many people have said, I have assembled this collection of about forty items. Each author speaks about the threats to our networks of computers, revealing the vulnerabilities inherent in a networked world through the stories of major incidents that attracted national attention in the media. They show how people have reacted and how we can strengthen our defenses. I have purposely sought material from many different perspectives, including those of hackers.

I have grouped the articles into six parts. The first describes the emergence of a worldwide network of computers, here called Worldnet, and the new practices that people have engaged in as a result. The Worldnet is an outgrowth of an invention conceived in 1965, a network of computers that came to be called the ARPANET. These authors discuss the history of the ARPANET, the emergence of the Worldnet, the large variety of networks that have come into existence, and the vulnerabilities of computers.

The second part describes the problem of electronic breakins. Since the mid 1970s, it has been possible for someone to log in to accounts on a chain of computers by using the remote login facility on each computer to access the next. Lengthy login paths are difficult to detect and trace. They are unlikely to be noticed by system operators through casual observation. The anonymity afforded by networks in this fashion has offered intruders a new kind of breakin. The intruder can copy, modify, steal, or destroy programs on those computers with little risk of detection. Logging in to many computers is relatively straightforward given the weakness of most password systems, weaknesses that lie not in the methods of enciphering passwords but in the practices of those who administer and use the computer systems. Even as the network has made possible the free exchange of information among colleagues and communities, it has opened a new threat to the information stored in their computers.

The third part of this book deals with the phenomenon of worms. In the early 1980s, John Shoch and Jon Hupp of the Xerox Palo Alto Research Laboratory experimented with a new kind of program, called a worm, that would "roam" a network looking for idle workstations that could be put to good use. In execution on a given workstation, a worm program would send probe messages to other workstations; on finding an idle workstation, it would send a copy of itself to that workstation. In their experiments Shoch and Hupp reported a possible misuse should the worms refuse to terminate themselves: They can take over the network and prevent users from gaining access. As it turns out, worms have developed along this unbenign line, gaining a reputation as troublemakers and resource preemptors rather than as aids to the efficient use of distributed resources. The Internet Worm incident of November 1988, which attracted front-page coverage in major international newspapers, clinched this interpretation of worms in the public mind. That incident occupies center stage in this part of the book.

The fourth part of this book deals with computer viruses. A computer virus is a program that examines the file system of a computer for executable programs that have not been "infected"; on finding one, it hides a copy of itself in that program. When that program is called into execution, the virus takes over, replicates itself further in the same manner, and may perform damage; the damage may be deferred for some time after the infection (Friday the thirteenth is a favorite). Virus programs have been a nagging problem for users of PCs (personal computers) because they are easily passed unwittingly by users who exchange programs via floppy disks. A disk can become infected by inserting it into a PC in which the virus has already infected the operating system. An infected disk can infect the next PC into which it is inserted. Thus virus programs have become an insidious method of attacking other computers. Because the virus can defer its attack for a long time after the infection, it can propagate widely before anyone detects it. The number of damaging virus incidents has become so large that there is a market for prophylactic software. You can now purchase virus eradictor programs that detect and erase viruses and check newly inserted floppy disks for signs of infection.

The fifth part of the book, which I have provocatively called "Countercultures," gives a glimpse of the worlds in which hackers live. Many of them advocate a philosophy that property rights are not absolute and that many security mechanisms foster the very attacks they are intended to prevent. Many revere the cyberpunk genre of science fiction. Many distrust accumulation of power by organizations that can build large, closed databases of records about individuals. These views, now in a minority, are nonetheless a significant part of the current reality.

The sixth and final part of the book deals with the social context in which people make ethical and moral interpretations and propose new laws. Many of these commentaries were inspired by the incidents discussed in the preceding parts. These commentaries reveal that people in business, science, and government who use computers attached to networks have a deep concern for the integrity and privacy of information entrusted to those computers.

How to Read This Book

We have been raised in a tradition enchanted with information. Without thinking, we see business transactions as exchanges of information, communication as the exchange of messages, books as containers of information, management as decision-making based on collected information, science and engineering as structured stores of information, research as the discovery of information, instruction as the transmission of information from the store of knowledge owned by the teacher into the student's mind. We get impatient if a speaker or author does not make the information accessible or understandable quickly.

In this tradition, we see reading as extraction of information from a book or article. We say an article is "lucid" when the exposition is clear and the information flows quickly and smoothly from the book to us. We say that the article is "opaque" when it impedes information flow. We might say that we "understood only 25% of the book," as if to say that the remaining 75% waits in its vessel for later drinking.

From that tradition, this book may appear as a collection of interesting items of information about intruders, worms, and viruses. I invite you to step outside the tradition.

Another interpretation of what lies before you is that the world is a large network of conversations, people talking with people every day, hour, and minute. What other people say in their conversations affects us by creating opportunities for us and by closing possibilities for us.

A portion of this network of conversations concerns computers and telecommunications, systems that support almost all other conversations, be they in global markets, business, organizations, news reporting, entertainment, banking, research, or development. A portion of that portion concerns the health of these systems and their protection against disruptions by external agents, for a disruption of these systems disrupts our ability to work and live together.

Suppose that there were a forum to which we invited speakers in the conversation about the health of our networks of computers. Are you a beginner in this subject? If you went and spent a few hours listening in this forum, you would emerge with a new ability to speak and ask questions of those already engaged in the subject. You would be prepared to engage in further learning. Are you already competent in this subject? For you, visiting this forum would be an opportunity to check your knowledge and discover whether there are new speakers you would like to meet. It would increase your capacity to speak and act competently in the future.

This is exactly what we have done for you here. We have created a forum of distinguished speakers. I invite you to come listen to their conversations as much or as little as suits you. At the start of each section I have included my own interpretations of what the speakers are talking about and what you might listen for when you visit with them.

This book is an investigation into the origins of these phenomena. It is your opportunity to become a listener, if not a speaker, in the ongoing conversation about attacks against our computers. As you read you will hear stories telling how people are reacting to these threats and what steps they are taking to protect themselves in the future. You will get glimpses of how the persons who designed these intrusions think and act. You will see a growing awareness of the need for cooperation.

Welcome to our forum!

Peter J. Denning
Portola Valley, CA
August, 1990

Acknowledgments

The idea for this book was born in a comment from David Gries of Cornell University, who said that ACM had lost an opportunity by not making the contents of its Internet Worm issue of the *Communications* (June 1989) available to the wider audience of people who would learn from it. To me, David's complaint was an invitation to undertake a project.

The selection of articles was made with generous advice from Peter Wegner (Editor-in-Chief of ACM Press Books), Peter Gordon (Publishing Partner at Addison-Wesley, ACM's partner in the ACM Press Books venture), Janet Benton (Associate Director of Publications at ACM), and Nhora Cortes-Comerer (Senior Editor for ACM Press Books). Nhora's creativity was special and her contribution exceptional: She made numerous suggestions for material that otherwise might have been overlooked, and she took the lead in negotiating with the many authors, editors, and publishers whose work appears here.

John Markoff provided reprints of his articles from the *New York Times,* and Katie Hafner shared her first-hand knowledge of the hacker trials held in February 1990 in West Germany. Throughout the book, we have reprinted a series of Dick Tracy cartoons featuring a computer attacker who was (of course) foiled by Tracy. These cartoons reveal the extent to which the phenomenon of computer viruses has entered the public consciousness. We are grateful to the Tribune Media Services for granting us permission to use them.

Special personal thanks go to Dorothy Denning of Digital Equipment Corporation (and of the Denning family!) for many comments on drafts of my own articles, to Steve Mayer of *American Scientist* magazine for his editing of my manuscripts, and to Barry Leiner of the Research Institute for Advanced Computer Science for his advice on network technology.

My colleagues at the Research Institute for Advanced Computer Science, in the Universities Space Research Association, and NASA have been my constant supporters. Without their encouragement this book would not have been put together.

And finally I am deeply grateful to all the authors for their participation in this important undertaking. In the end, their words count, not mine.

P. J. D.

Introduction

It was early Friday, October 13, 1989, in Baltimore. My taxi driver and I got into a discussion of the misfortunes that might befall the world that day. I asked him if he'd seen the newspaper headlines about the computer viruses that might strike that day.

''Yeah, I've seen those headlines. What the heck is a computer virus anyway?'' he asked.

''It's a program that gets into your personal computer when you don't expect it, and then it does something nasty like wiping out your files,'' I responded.

''But how can a computer catch a virus? Does somebody sneeze on it?'' he asked, almost snickering.

''These aren't the usual viruses that you catch by contact with someone else,'' I said. ''They spread when you take a floppy disk from an infected computer and insert it into an uninfected one. They can also spread over the telephone network—computers dial each other up all the time these days, you know.''

''You mean those things aren't germs? They're created intentionally by people?'' he asked in a troubled tone.

''Exactly,'' I replied.

''Why would anyone do that?'' he exclaimed.

Why would anyone do that? This is one of the most important questions that we face as we enter the twenty-first century, a crowded world that will be linked tightly by networks of computers, a world that cannot work without the cooperation of many people. Our world already contains people who will steal information from computers attached to a network, people who will settle a grudge by attacking someone's computers, and an expanding culture of young people who see themselves explorers of vast electronic hinterlands that beckon to the adventurous.

Origins

Incidents of attacks against computers have been reported since the earliest days of electronic computing. Since those days, data security mechanisms have been an integral part of computer operating systems. Until the mid-1980s, however, most such attacks were the work of those who already had an account on a computer or knew someone who did. By that time, the cheap modem had transformed every personal computer into a potential terminal for any other computer with dial-in phone lines, and the rapidly widening Research Internet connected tens of thousands of computers by a high-speed data network. New opportunities for breakins became available to anonymous people in any part of the world. A few examples will illustrate the types of attacks.

In early September, 1986, an intruder broke into a large number of computer systems in the San Francisco area, including nine universities, sixteen Silicon Valley companies, nine sites on the government-operated computer network known as the Research Internet, and three government laboratories. The intruder left behind recompiled login programs to simplify his return. His goal was apparently to achieve a high score on the number of computers entered; no damage was done [1]. In the same year, another intruder surreptitiously broke into thirty supposedly well-secured computers in the Defense Department's MILNET and attempted breakin to several hundred others, apparently looking for militarily sensitive information that could be copied and sold. After nearly a year of detective work, Cliff Stoll of Lawrence Berkeley Laboratory amassed enough evidence to identify the West German perpetrator [2]. These are two of many examples of anonymous intrusions in computers connected by electronic networks around the world.

In December, 1987, an electronic Christmas message that originated in West Germany propagated into the BITNET network of IBM machines in the United States. The message contained a program that displayed an image of a Christmas tree and sent copies of itself to everyone in the mail distribution list of the user for whom it was running. This program, an example of a worm, rapidly clogged the network with a geometrically growing number of copies of itself. Finally, the network had to be shut down until all copies could be located and expurgated. In December, 1988, someone released another Christmas worm into NASA's Space Physics Analysis Network (SPAN), but alert system operators quickly detected and disabled it. Even so, it infected several hundred computers and sent unexecuted copies of itself to several thousand.

In November, 1988, Robert Morris, a graduate student at Cornell University, released a worm program into the Research Internet. Within five hours, this program replicated itself in approximately 3000 computers; network experts spent the next several days eradicating it. Although the worm damaged nothing, it produced a massive scare: The potential for loss of valuable information was enormous, and an actual loss would have been devastating to the many people who used those computers. In July, 1989, Morris was indicted under Federal computer crime law, charged with unauthorized entry to Federal interest computers that caused more than $1000 damage. His trial was held in January, 1990, and the jury found him guilty. He was given a suspended jail sentence, fined $10,000, and ordered to perform 400 hours of community service.

For two months in the fall of 1987, a program called a virus quietly hid copies of itself in programs on personal computers at the Hebrew University. It was discovered and dismantled by a student, Yuval Rakavy, who noticed that certain library programs were growing longer for no apparent reason. He isolated the errant code and discovered that on certain Fridays the thirteenth a computer running it would slow down by 80%, and on Friday, May 13, 1988, it would erase all files. That date was the fortieth anniversary of the last day Palestine was recognized as a separate political entity. Rakavy designed another program that detected and erased all copies of the virus it could find. Even so, he could not be completely sure he had eradicated it. Computer viruses have become a widespread threat to users of personal computers. Many companies now market products that will detect and remove viruses. Many companies have adopted new operating procedures to prevent inadvertant viral contamination of their computers.

Since 1986, the media have run numerous stories about breakins, worms, and viruses. The number of incidents is on the rise. There is a growing concern among computer network managers, software dealers, and users of computers about these forms of electronic vandalism. The attacks have drawn everyone's attention to the general problem of computer security, which has fascinated researchers and developers since the early 1960s [3]. In his March, 1985, Computer Recreations column in *Scientific American,* A. K. Dewdney documented a whole menagerie of beastly threats to information stored in computer memories, especially those of personal computers (PCs), where an infected diskette can transmit a virus to the main memory of the computer, and thence to any other diskette or to hard disk [4]. Ken Thompson, a principal designer of UNIX, and Ian Witten have documented the threats to computers that have come to light in the 1980s [5, 6].

The concern over these forms of intrusion—breakins, worms, and viruses—arises from the possible damage to stored information on which our work depends and the ensuing disruption of our workplaces. We can expect steady increases in acts of crime, espionage, vandalism, and political terrorism by computer in the years ahead.

The distinction between a virus and a worm is a fine one. Both are forms of automated intrusion. Both propagate copies of themselves to other systems. Both are capable of damage and may delay inflicting it until long after the infection. The main difference is that a virus attempts to hide copies of itself inside other, legitimate programs, whereas a worm appears as a separate program—but worms can disguise themselves, as did the Internet worm of 1988. You may hear the terms used interchangeably in the trade and even in the professional press. No matter—they are virtually indistinguishable.

Security experts refer to the programs left behind by intruders, worms, and viruses as logic bombs and Trojan horses. A logic bomb is a program that damages or discloses files after an appointed interval or at an appointed time; it can evade detection by waiting to perform its deeds and many hours, weeks, or months after it has been implanted. Favorite dates include Fridays the thirteenth, April Fool's Day, and Halloween. A Trojan horse is a program that performs an apparently useful function but contains a hidden logic bomb. Its name recalls the legendary sneak attack by the Greek army at Troy.

The phenomenon of widespread electronic intrusion is very recent. It is made possible by the proliferation of personal computers and their connection to electronic networks. Although technically sophisticated, intrusions are always the acts of human beings. They occur against the background of a modern discourse that values individual rights more highly than community values and anonymity more than accountability. Intrusions can be controlled by a combination of technical safeguards—a sort of network immune system—and hygienic procedures for using computers. But they cannot be eliminated.

It would seem that some straightforward technological fixes would greatly reduce future threats. But technological fixes are not the final answer; they are valid only until someone launches a new kind of attack. Changes in the ways we use computers, however, will reduce our exposure to our own and others' frailties.

The authors remind us vividly that worms and viruses are mere programs. They are not capable of intelligent action, as envisaged by another taxi driver who spoke to me late that same Friday: "You know, everyone thinks we got off light on those computer viruses that were supposed to attack today. Everyone thinks it was a hoax. But the viruses outwitted them. They got into the stock market computers. That's what caused the crash today. I know!"

Where will the story go next? This book reveals only the opening moves in a new era of cat-and-mouse games to control computers and telecommunications. It is impossible to say now how the story will unfold in the years ahead.

References

1. B. Reid. Reflections on some recent widespread computer break-ins. *Commun. ACM 30,* 2 (February 1987), 103–105. (Reprinted in this volume.)
2. C. Stoll. *The Cuckoo's Egg.* Doubleday, 1989.
3. D.E. Denning. *Cryptography and Data Security.* Addison-Wesley, 1982.
4. A.K. Dewdney. A core war bestiary of viruses, worms, and other threats to computer memories. *Scientific American 252,* 5 (March 1985), 14–23.
5. K. Thompson. Reflections on trusting trust. *Commun. ACM 27,* 8 (August 1984), 172–180. (Reprinted in this volume.)
6. I.H. Witten. Computer (in) security: Infiltrating open systems. *Abacus 4,* 4 (Summer 1987), 7–25. (Reprinted in this volume.)

Contents