WINDCREST®/McGRAW-HILL

THE STEPHEN COBB COMPLETE BOOK OF PC and LAN SECURITY

Stephen Cobb

The Stephen Cobb Complete Book of PC and LAN Security

Stephen Cobb

WINDCREST®

FIRST EDITION
FIRST PRINTING

Library of Congress Cataloging-in-Publication Data

Cobb, Stephen. 1952-
The Stephen Cobb complete book of PC and LAN security / by Stephen Cobb.
p. cm.
ISBN 0-8306-9280-0 ISBN 0-8306-3280-8 (pbk.)
1. Local area networks (Computer networks)—Security measures.
2. Computers—Access control. I. Title.
TK5105.7.C62 1990
005.8—dc20 89-70748
CIP

TAB Books offers software for sale. For information and a catalog, please contact TAB Software Department, Blue Ridge Summit, PA 17294-0850.

Acquisitions Editor: Ron Powers
Technical Editor: Sandra L. Johnson
Production: Katherine G. Brown
Series Design: Jaclyn J. Boone SCS

About This Book

Security can be defined as freedom from risk and danger. This book shows you how to make your work with personal computers relatively free from risk and danger. With the aid of this book, you can secure your personal computer equipment, and the data that it holds, from the following:

- Hackers and other interlopers.
- Viruses, worms, and logic bombs.
- Vandals and thieves.
- Competitors and industrial spies.
- Employees, both belligerent and careless.
- Power failures.
- Fires and other catastrophes.

WHAT THIS BOOK OFFERS

While the goal of *complete security* is probably unattainable, this book provides a complete treatment of security issues facing those who work with personal computers, from corporate management, to information technology managers and end users. Because increasing levels of security usually involve increasing costs, this book discusses how to weigh security benefits against security expenses. An increase in security levels can also mean a reduction in accessibility, so this book discusses security measures in light of user comfort levels and administrative feasibility.

Now that more and more offices are connecting their computer systems together, this book looks not only at the security aspects of stand-alone personal computers, but also at the problems facing local area networks, the systems of interconnected personal computers that are of growing importance in the data management strategies of companies, governments, and educational institutions.

If you do not use a personal computer but manage other people who do, you will also benefit from this book. You will gain insight into what your current exposure from personal computers is, and how to reduce it. For those of you who worry about losing data even though you do not understand how a database works, I have taken pains to discuss the problem of protecting data without excessive use of computerese (that strange mumbo-jumbo mumbled by guys with taped-together glasses and one too many pens in their plastic pen protectors). When a special term is used it is explained within the text. An effort has been made to avoid excessive use of acronyms, and those that are introduced are explained.

Of course, if you *do* know where your data is, if the possibility of other people

getting at the information you have stored on your personal computer does *not* bother you, if the sudden disappearance of your data in a disk crash would not hurt your business, then you might not need this book. However, if you harbor any doubts about the security of your data, or the equipment that stores it, then this book should help. After all, if you read it from cover to cover and find nothing new, then you will have satisfied yourself that now your data and equipment is about as secure as it can be.

WHAT THIS BOOK IS NOT

This book does not approach security from the mainframe perspective, treating personal computers as annoying interlopers into the previously safe world of terminals and central processing departments. The premise of the book is that personal computers are here to stay and, given a responsible approach by users and information system managers, they can be as secure as any other form of computing equipment.

You might be aware that there are numerous books on the theory and practice of data security as it applies to mainframe and minicomputers. However, most of these do not address in sufficient detail the special issues facing the user and manager of personal computers and personal computer networks. Indeed, some mainframe experts have used the security deficiencies of the personal computer in attempts to reverse the trend away from centralized control of computing resources.

You might also have found that very few books concentrate on the subject of security for personal computers and personal computer networks without veering off into extended discussions of specialized areas like viruses, mainframe connections, data communications, or the morality of hacking. There are several excellent books about viruses and how they work. Indeed, some of them are listed in the resource section of this text. However, such books will not give you the comprehensive approach to data security that you will find here. There are also texts on encryption algorithms, code-cracking, and the art of hacking. Again, these do not cover the broad subject of data protection as it relates to personal computer usage.

While I did seek the advice and input of other computer professionals when putting this book together, this text is not a collection of articles culled from trade journals. A consistent point of view can be found behind the analysis and comments presented here. While you might eventually decide that you do not agree with the perspective, it is presented in sufficient depth to allow you to develop your objections coherently and productively.

This book is not simply a catalog of security-related products. You will find an extensive product listing at the back of the book which should be helpful, but in the fast-moving field of computers, no book can be completely up-to-date. (A few years ago I wrote several computer books that recommended joining The Source, a very reputable on-line database owned and operated by the Reader's Digest group of companies. Today The Source is no more, and the books are outdated.)

For news of the latest security products, including reviews and benchmark tests, you can turn to the extensive array of computer magazines. There are also specialized newsletters on security issues, some of which are listed in the product directory. In

general, this text avoids detailed product descriptions, preferring to concentrate on the task of showing you how to determine what type of security products you need. When it is germane, you will find lists of features to look for in certain products and the factors that might affect their pricing. With the aid of this book, you will be able to evaluate which security products you need to purchase, but the emphasis throughout is on creating security through careful planning, simple precautions, and user-training rather than expensive equipment.

This book is not lavishly illustrated for several reasons. Many aspects of security do not lend themselves well to graphic expression. Lists and charts focus attention on specific points of information, but I have included few pictures of security devices. Glossy photos of security equipment tend to emphasize the value of equipment over less expensive strategies like the enforcement of well-designed security policies.

WHY THIS BOOK

This book is based on a commitment to making personal computers work for you, rather than against you. Without underestimating the problem, the general attitude is positive, showing you how to achieve workable solutions to your security problems as quickly and as cheaply as possible.

This book tries to avoid the scare tactics used by some companies that engage in the business of selling products that enhance data security. In some cases, such sales tactics are almost forgivable because they serve to heighten awareness of very real problems that were ignored by many personal computer users, sometimes with regrettable consequences. Yet the tendency to "cash in" on each new wave of concern on this subject has given rise to a plethora of products that are aggressively marketed as solutions rather than tools. These tools are useless unless applied within the type of security strategy that this book advocates.

You might be looking at this book as a text in an institution of higher education; however, the approach taken here is not academic. The canon and maxims put forward are based on "hands on" experience in the real world of personal computing. I have spent a lot of time in the offices of companies, institutions, and individuals who use personal computers, in order to learn what is feasible, what is realistic, when it comes to implementing security measures. When faced with more theoretical matters, like whether hacking is essentially a good activity or an evil one, the text is silent, preferring instead to help you assess your exposure to the adverse effects of hacking.

WHY THIS BOOK WAS WRITTEN

This book was written because many users and managers of personal computer technology are worried about risks and dangers. Obviously, some risks and dangers are very real, but some are imagined, the product of an over-sensational, under-informed media. Effective defense against some risks and dangers is difficult, but many can be thwarted by simple precautions. A very real concern is that the fears and worries of management and end-users will inhibit the spread of personal computing's

positive benefits. The mission of this book is to restore some of the sense of security, and spirit of optimism, that has marked previous stages in the growth of personal computing. If your comfort level with the systems you use or manage is increased by what you read here, then that mission is being accomplished.

A NOTE FROM THE AUTHOR

As someone who first encountered microcomputers as an empowering, even liberating tool, I am disturbed by the bouts of fear and dread that seems to grip the worldwide community of personal computer users with increasing frequency. My first efforts with a personal computer in 1980 allowed me to produce better-looking documents quicker. Almost by chance, I found that humble system to be capable of calculations that I had been trying for 12 months to get central data processing to bring on-line. I saw that by using a microcomputer an individual could carry out a wider range of tasks with faster and better results. As this fact sank home in corporations and institutions, the personal computer spread to the point where it is now a universal item of office equipment. These days few people would think about setting up any type of commercial enterprise without a personal computer on-hand. However, because so many tasks have been entrusted to personal computers, the weak points of these machines have become increasingly problematic. To the extent to which personal computers are subject to outside forces, they jeopardize the endeavors of the people who trust them in their work, their recreation, and their self-expression.

Over the past few years, I have written a number of books for personal computer users. All of these books draw on my experience as a trainer of personal computer users, and my work as an information technology consultant to businesses in both the United States and the United Kingdom. Most of these books are what the trade refers to as "software-specific," meaning that their purpose is to explicate one particular piece of commercial software, as in *The Stephen Cobb's User's Handbook to Excel for the IBM PC*. Writing such books allows me to convey what I have learned in the process of teaching the program to others, and pass along what students have revealed to me about the program's capabilities and shortcomings. However, my students have also taught me a lot about aspects of personal computing that are not "software-specific."

One of the recurrent subjects of discussions in the classrooms and offices where I have taught is the politics of personal computing. This might concern the question of who gets the new equipment and who chooses what software should be used, but often the real thrust of the discussion involves access to data. Strictly speaking, *data* is what is given, the given facts. However, a lot of information that we call data we obviously don't want to give away. In this book, I will use the term data to refer to information stored on a computer. Controlling access to that information is one of the central issues in computer security. You can see the issue is a question as simple as "How do I stop other people seeing my stuff?" The broader implications for company politics manifest themselves in questions such as "How do we access the main database on the company mainframe?"

In recent years, I have seen a steady increase in the number of questions that directly relate to matters of security for several reasons. Obviously, the extent to which organizations rely upon personal computers has increased dramatically. The media can now be relied upon to report large-scale security threats. The main reason for my getting more questions is the growing sophistication among users. They can see the broader implications of questions like "How do I stop other people from retrieving my budget worksheet?" and "What if my PC were stolen?" Personal computers have been out there long enough and in sufficient numbers for most users to know of at least one "disaster" in which a lack of security has negative consequences or an organization or individual.

Back when I sold personal computers in one of the more exotic parts of California, I met a client who, according to my manager, was engaged in the world's oldest profession. This explained her particular interest in the password protection systems used by the various database management programs she was considering for the tasks of bookkeeping and maintaining a client list. Subsequent raids by vice squads upon computerized houses of ill-repute have shown our client's concerns to be well-founded. An unprotected database of names and addresses from such an establishment has, on more than one occasion, provided a ready-made arrest list. The moral of the story is that, whatever endeavors we engage in, serious consideration of how to preserve and protect the growing quantity of data that we entrust to personal computers is part of the price we must pay for tremendous benefits of personal computers.

HOW THE BOOK IS ORGANIZED

The book is divided into several parts. In the first part, the overall problem of security is examined, focusing on the issues that are the proper subject of this book. Several inexpensive measures are discussed that allow you to immediately improve the safety of your data. Procedures that you can follow to perform your own security analysis are described.

In the second part, the hardware side of the problem is addressed. Ways of securing hardware from theft, vandalism, and unauthorized access are considered, along with the question of redundancy. The need for reliable power sources is examined, together with alternatives for backup power.

The software side of the problem is considered in the third part where file access, password protection, and encryption are discussed. This section also looks at the question of software piracy and the threat of viruses. Various methods of protection against viruses are examined.

The wider world of personal computing is the subject of the fourth part where the problems of security in local area networks are reviewed. This section also addresses the human factors in security, such as hackers and disgruntled employees.

In the last part, you will find the resource list, a collection of product descriptions and company names that might be of use as you implement a security plan for your system(s). This list is only intended as a starting place because this book needs to go beyond just being a list of security-oriented products that are available at a particular

point in time. Through reading this book, you will develop criteria for evaluating security issues, a methodology for assessing the security questions you are faced with and preparing an appropriate response. If this response requires purchasing equipment, then you will already be in a position to evaluate what is currently available and decide if it works for you.

Scattered throughout the books are tips, anecdotes, and other author's notes which should help enliven and enrich your reading on this rather dry subject. These notes are marked by the icon you see in the margin.

Contents

It is 10:00 P.M.
Do you know where your data is?

1
The Need for Security

THIS CHAPTER SEEKS to map out the subject matter of the book. Basic questions of security are reviewed as a preamble to the more specific threat/response suggestions that begin in Chapter 2. While you might already have a high level of security awareness and a strong urge to spring into action, begin with this chapter to help place your actions in a broader context, thus making them more effective in the long term.

GOOD NEWS AND BAD NEWS

On August 2, 1989, a United States federal grand jury indicted 24-year-old Robert Morris, Jr., charging him with one count of violating the Computer Security Act of 1987. The penalty for this crime is up to five years in prison and a fine of up to $250,000. What did young Morris do to get into this predicament? He wrote a software program and then, on November 2, 1988, placed it on a network of computers. The network, called Internet, is very large. The type of program Morris wrote, called a *worm*, is very clever. Within hours almost 6000 computers ground to a halt and were virtually unusable for several days until the worm was identified and destroyed.

Thanks to heavy media attention, this incident quickly became one of the most talked about cases of a computer virus attack (a *worm* is usually considered to be a type of virus). The Internet network is used by many colleges and universities and connects with several other networks, including Arpanet and Milnet, the latter being a Defense Department network. The virus attack and subsequent indictment of Morris hold both good and bad tidings for you, the personal computer user.

First, the good news for personal computers users: This attack did not directly affect personal computer users. The attack was on the operating software of the pow-

erful mainframe and minicomputers that provide computing power and data storage for users scattered over a wide area. These computers work on the Unix operating system. Although some personal computers can run Unix, the worm only attacked software that is used to log on to large systems and communicate between them.

There is more good news: The worm did not damage any important data files. Like many people who write this type of program, Morris seems to have had no desire to damage data, seeking instead to outsmart the operating software that runs the system. His intention might have been, and his effect definitely was, to show up weaknesses in the system. Furthermore, the culprit has been apprehended and prosecuted, a definite deterrent to others who might be contemplating similar attacks.

Finally, the event sparked further activity in the personal computer security market, with new and improved virus detection and prevention programs appearing all the time. Heightened awareness of the need for security makes it that much easier for those of us who endeavor to alert users to the risks, as well as the rewards, of personal computing.

The bad news is that the attack caused a lot of inconvenience to a lot of people and wasted much time and money. However honorable Morris's intentions, the effect of his actions was very negative. That other people might create chaos out of misdirected programming skills and innocent intentions is a strong likelihood. Unix is a mature and sophisticated software system, one that has been developed over a period of more than 15 years. Your personal computer probably runs on a much younger and less complex system, one that is undoubtedly easier to outsmart.

More and more personal computers are being connected on networks, increasing the chances of disruption from forces outside the user's control. While there are steps you can take to protect against viruses, the potential threats are probably increasing in number, rather than decreasing. In the rush to utilize the cheap and convenient power of the personal computer, many organizations have left the door open behind them, providing ample opportunities for interloping, theft, and fraud. Fortunately, it only takes common sense and diligence to close the door. Beyond that you can look at locks, alarms, and the finer points of personal computer security. But first, the subject itself must be defined.

PERSONAL COMPUTER SECURITY DEFINED

Personal computer security can be defined in several ways. In simple terms, personal computer security is about letting personal computers get on with what they do. A more academic definition might be "freedom to enjoy the benefits of personal computers without negative consequences." A more circumspect definition might be "freedom to use personal computers without fear of disruption or outside interference."

As you try to formulate a definition of personal computer security that is appropriate to your situation, you will see that it is a rather difficult subject to pin down. For example, we would all like the freedom from negative consequences suggested in the

first definition, but is this realistic? What about something like eyestrain, a negative consequence that many users experience but that is scarcely a question of security?

The last definition is less sweeping but says nothing of the personal computer's use. Concern for security suggests that there is something valuable that needs protecting. Yet how do you access the value of a personal computer? You might argue that the one which computes the fastest route for an ambulance rushing to an accident scene is in a different league from the one which attempts to predict the winner of the next election. This question of value can be addressed after taking a moment to make clear what exactly is meant by "personal computer."

Personal Computers Defined

As computer technology advances, the distinctions between different types of computers continue to get blurred. However, it is possible to roughly delineate three different categories of computer system.

Mainframe Computer. The mainframe computer is a large computer system, consisting of racks of centralized processing equipment supporting multiple users via separate *stations*, or terminals, as illustrated in Fig. 1-1.

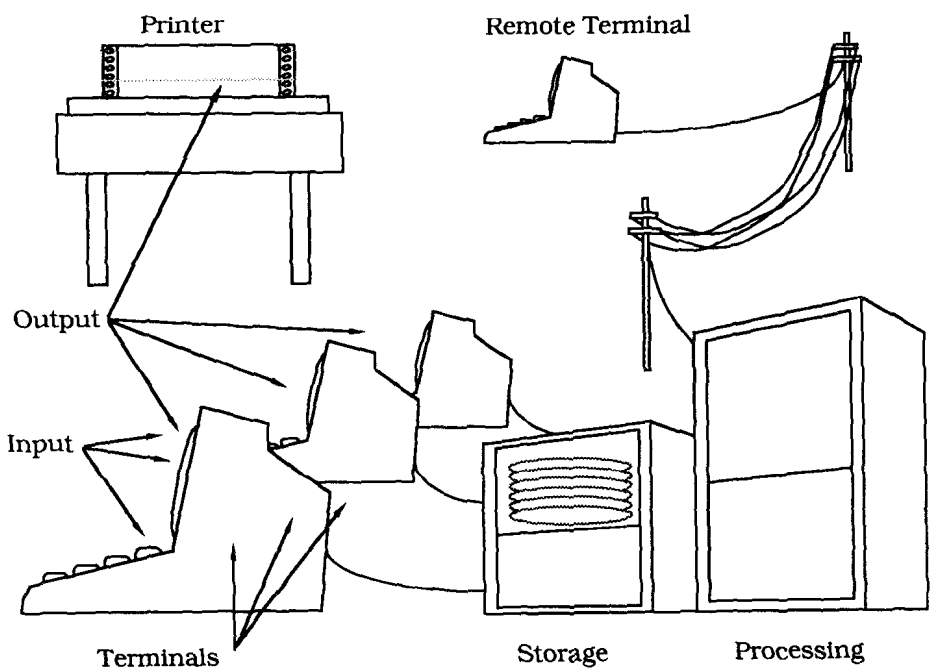

Fig. 1-1. The mainframe computer system.

This is the original architecture of computing, and it still exercises a powerful appeal. There are administrative benefits to the centralized control inherent in this