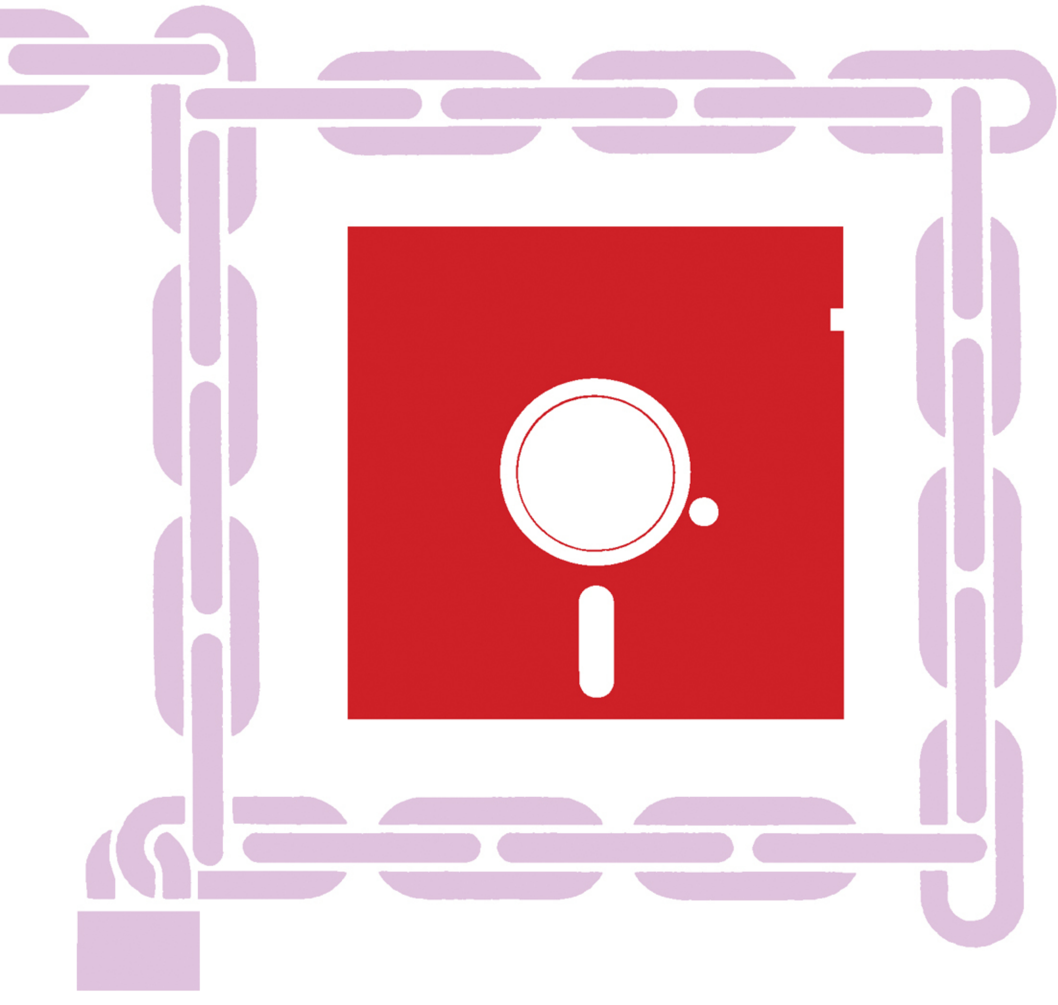
JOHN M. CARROLL

COMPUTER SECURITY

SECOND EDITION



Butterworths

COMPUTER SECURITY

This page intentionally left blank

COMPUTER SECURITY

Second Edition

JOHN M. CARROLL

Butterworths
Boston London Durban Singapore Sydney Toronto Wellington

All references in this book to personnel of male gender are used for convenience only and shall be regarded as including both males and females.

Library of Congress Cataloging-in-Publication Data

Carroll, John Millar.
Computer security.

Bibliography: p.
Includes index.
1. Electronic data processing departments—Security measures. 2. Computers—Access control. 3. Computer crimes. I. Title.
HF5548.2.C29 1987 658.4'78 86-29901
ISBN 0-409-90032-X

Butterworth Publishers
80 Montvale Avenue
Stoneham, MA 02180

Printed in the United States of America

To Billie, who supported me . . . and Jude and Mike
who supported Billie

This page intentionally left blank

Contents

Acknowledgments

A lot of people talk about electronic data-processing security, but lamentably few do anything about it. I would like to recognize one group that is doing a lot about it. This group is the Protection of Property and Information Branch of the Royal Canadian Mounted Police, especially Superintendent Frank Fedor; inspectors Al Barkhouse and Jerry Bryan; civilian members Phil McLellan, Sandy Thom, and Grant McPhee; Major Tom Wiley; Staff Sergeants Doug Calverley, Ron Friesen, and Bill Innes; and Hugh Paterson of the Department of Communications. The branch is part of the Protective Policing Directorate under Assistant Commissioner Bert Giroux.

Since the first edition of *Computer Security* in 1977, we have lived in interesting times. That year I accepted a commission from the Department of Communications to tour the length of Canada and report on the national potential to carry out research into computer security. Among other things, this brought me into contact with the massive break-in (5,000 unauthorized entries) to the University of Alberta computer.

During 1982–1983, I worked as a computer scientist in the Information Technology Division of the Naval Research Laboratory where I had the pleasure of working with the amazingly prolific Carl E. Landwehr. I appreciated the close look at U.S. security practices but could not help but deplore the unquestioning trust Americans tended to place in people who had been put through the Department of Defense clearance procedure. I also tended to deplore the Mitre Corp.'s concept of "trusted" software, which can be vastly different from "trustworthy" software. One may reasonably question how much trust one can comfortably repose in the products of businessmen who ship their latest high-tech products to the Soviet Union while refusing to license pivotal patents to the Department of Defense.

While in Washington, I enjoyed filling in as a leave replacement for Lance J. Hoffman at the George Washington University by teaching his course on cryptography and data security. I was also able to work with Nander Brown of the Federal Home Loan Mortgage Company in developing a microcomputer-based risk analysis program. Nander now runs his own business selling this and other products.

I had many subsequent contacts with the U.S. security-intelligence-law enforcement communities. These included writing courses on data and information security and analytical accounting for Dave Harding at Ohio University and presenting seminars for Jacob Haber at the University of Delaware. In 1984, I reported on prospects for secure local area networks to the nascent Canadian Security and Intelligence Service.

Meanwhile, computer security gained increasing academic respectability at the University of Western Ontario and more power to do new work. We acquired a pair of CYBER computers, a VAX 8600 for departmental use, and my own fully configured and networked IBM-PC/AT. We became a major node in a national initiative in artificial intelligence attracting bright graduate students and professors. We also acquired a wide assortment of fifth-generation software, including, by reverse technology transfer, the fast MPROLOG language from Hungary.

I am pleased to be working with Helmut Juergensen, formerly of Darmstadt, who brought not only his own keen mathematical insight to the problems of security but also invaluable contacts with like-minded colleagues in Holland, Belgium, Sweden, and Germany. We are now regularly presenting at least one graduate course on cryptography and data security, as well as supervising masters' and, hopefully, doctoral research theses in this area.

As a result of all these augmentations, the university is now creating expert systems for security inspections, risk analyses, and threat monitoring; facile but still secure relational data bases; and easily followed audit trails. We are also designing stronger new cryptographic systems and enjoying some success in breaking older ones.

In addition to our own resources, we are able to call upon a vast network of friends like Jack Bologna of Computer Protection Systems in Plymouth, MI. They possess talents as diverse as fraud auditing, criminal law, undercover investigation, and hacking. All of the above-mentioned events and people have played a very important role in the revision of this book.

John M. Carroll

Introduction

The title of this book is a misnomer. There is no such thing as computer security. There are only various degrees of insecurity. Any person who can dial into your computer from a telephone; submit a deck of punched cards, a magnetic tape or cassette, a floppy disk, or disk pack at your service counter for processing; send you a message by electronic mail; or write a program that you subsequently run on one of your computers can do any or all of the following:

1. Copy all of your sensitive files.
2. Juggle your accounts to cause you financial loss.
3. Reprogram computers embedded in other equipment to manufacture defective products, wreck production equipment, kill or maim employees, or launch weapons at friends and allies.
4. Erase all your computer programs and data files.

Furthermore, these things can be done not just to your computers but to any other computers with which they communicate. These adverse events can be arranged to happen at some future time when you will be most vulnerable, and they can continue to happen as long as you use computers.

These rogue programs can disguise or erase themselves, so you may never know you have been attacked. They need leave no evidence to incriminate their perpetrator or even suggest who he or she may be, or why an attack occurred.

If you are to function as a specialist in computer security, you have to know what you are up against. Accordingly, I will show you things the Pollyannas of the computer security industry say do not exist and that the Nervous Nellies say should never be discussed openly.

But for the greatest part of this book, I will be presenting the best ideas that high technology, classical security practice, and common sense have to offer to help you reduce your degree of insecurity to the lowest possible level.

This page intentionally left blank

PART I

The Threat to Computer Security

This page intentionally left blank

1

Essentials of Computer Security

A landscape painter begins with a rough background sketch that traces the bare outlines of his design. The cinematographer begins with a "long shot," a panoramic view that establishes the scene, before he moves in for a closer look.

In analyzing the security problems of a modern computer environment and seeking solutions to those threats, an overall view can be as useful as the painter's preliminary sketch or the cameraman's establishing shot. It can tell us in general where we are, what we are up against, and what resources are available to us for defense.

This introductory chapter presents such an overview of computer security—admittedly broad and sweeping—sketching the special problems and vulnerabilities, assessing the threats, enumerating the costs of losses, defining defense mechanisms.

While those who are new to computer technology will encounter unfamiliar terms, which will become completely understandable only as the text develops, these broad outlines should still be helpful, as a rough topographical map can be useful when entering strange terrain. Computer specialists, of course, will quickly find themselves on familiar ground.

UNIQUE EDP SECURITY PROBLEMS

The security problems associated with a computer environment include all those commonly associated with protecting property and information generally, as well as many problems peculiar to the electronic data processing (EDP) environment.

Several problems arise from the properties of EDP systems as a whole. The use of EDP can, for instance, reveal relationships among data that might forever remain obscure in a manual environment.

Classification is also affected by the nature of computer systems. The co-processing of two or more EDP documents can result in the production of documents or auxiliary items deserving of higher levels of security classification than those possessed by any of the input documents; and the aggregation of records in an EDP environment can often result in a file attracting a higher classification than that of any record in it.

The centralization inherent in computer systems also increases security concerns. The nature and cost of EDP systems tend to centralize corporate data processing, with the result that continuity of EDP service becomes essential to company operations.

There is also the problem of errors. Once an error is introduced into an EDP system, it is extremely difficult to extricate and tends to propagate rapidly through the entire system.

Personnel problems are common to all facilities, but a number of people problems seem peculiar to EDP. Effective supervision is often lacking because company management and security officers do not understand EDP sufficiently well to know what the employees are up to. And the actions of EDP employees, especially at remote terminals, are frequently anonymous, difficult to trace to a specific individual.

A high labor turnover rate is also common in computer facilities. All categories of EDP personnel seem to be plagued with this tendency. Related to this turnover is the fact that EDP personnel tend to demonstrate a higher loyalty to their profession and to each other than to their employers.

EDP media also have special characteristics that contribute to security concerns. Among these are:

- *Density.* The density of information in EDP media is much higher than the density of information in print media.
- *Obscurity.* The nature and contents of EDP documents and auxiliary items cannot be determined by visual inspection.
- *Accessibility.* Information stored in EDP systems is more accessible at remote terminals than is information stored in print-media files.
- *Forgery.* When information stored in EDP systems has been modified in an unauthorized manner, such modification cannot be detected.
- *Retentivity.* EDP media, after having been erased, may still retain images of data previously recorded on them.

Finally, in addition to the unique problems in computer security deriving from the systems as a whole, personnel, and EDP media, there are the special properties of the equipment itself. EDP equipment is fragile, and its behavior can be subtly modified by changes in its environment. Even more significant, there is the matter of machine intelligence to deal with. EDP equipment (hardware) and instruction sequences (software) together possess "intelligence" to such a degree that an EDP system can be subverted to assume the role of a hostile penetration agent.

Vulnerabilities of Resource-Sharing Systems

The principal points of vulnerability in resource-sharing data systems are processors, storage devices, communications facilities, remote terminals, users, and systems personnel.

The hardware of the *central processor* is vulnerable to failure of protection circuits, confounding of bounds and relocation registers, and misuse of privileged instructions. The software of the central processor is vulnerable to bypassing of file protection and access control programs or falsification of user identification.

Storage devices are vulnerable to unauthorized copying of stored information and theft of removable EDP media and to hardware or software failure that could result in compromise.

Communications facilities can be compromised by undesired signal data emanations, cross-talk between secure and insecure circuits, and the insinuation of technical surveillance devices.

Users may misrepresent or forge their identification or authorization; may seek unauthorized access to sensitive material by browsing; and can use debugging procedures to circumvent security mechanisms.

Remote terminals can produce undesired signal data emanations; are vulnerable to technical surveillance devices; and produce a potentially compromising text in the form of hard copy or as remanent images on platens or ink ribbons.

Systems personnel have normal access to supervisor programs, accounting files, systems files, protective features, core dumps, and files stored on removable EDP media and if not loyal and reliable can become serious security risks.

These potential vulnerabilities are illustrated in figure 1-1.

Vulnerabilities of Microcomputers

Microcomputers are becoming increasingly common in homes and offices. Many are able to communicate with large mainframe computers. Microcomputers are able to identify neither themselves nor the people who use them. They store data on diskettes, some as small as three inches in diameter. Anybody who can physically approach a microcomputer can steal any of the data in it or even the machine itself. Moreover, that person can copy files residing in any mainframe computer with which the micro can communicate onto floppy diskettes and steal that information as well.

Probability of Attack

Attacks against a computer installation may be classified according to the quality assaulted, such as confidentiality, integrity, or availability; and by the material under siege, which may be data or property. Such actions may be launched by nonemployees or employees, or they may be accidental (acts of God). An attack by a person or group in turn may be unintended or malicious and in the latter case may be either surreptitious or overt.

The most probable kinds of attack can be collapsed into seven categories:

1. *Covert attacks by employees (subversion).* These can result in destruction of equipment or facilities, disclosure of classified programs and data, interrup-

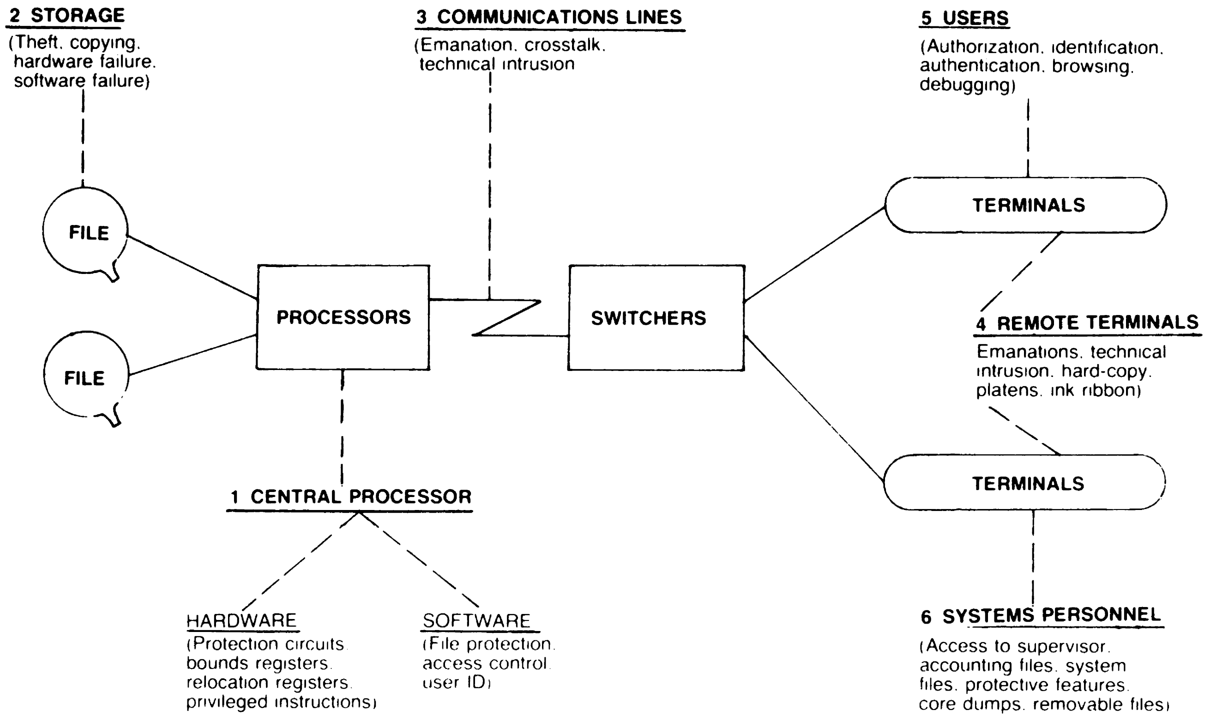

2 STORAGE
(Theft, copying, hardware failure, software failure)
3 COMMUNICATIONS LINES
(Emanation, crosstalk, technical intrusion
5 USERS
(Authorization, identification, authentication, browsing, debugging)
FILE
FILE
PROCESSORS
SWITCHERS
TERMINALS
4 REMOTE TERMINALS
Emanations, technical intrusion, hard-copy, platens, ink ribbon)
TERMINALS
1 CENTRAL PROCESSOR
HARDWARE
(Protection circuits bounds registers relocation registers privileged instructions)
SOFTWARE
(File protection access control user ID)
6 SYSTEMS PERSONNEL
(Access to supervisor, accounting files, system files, protective features, core dumps, removable files)

Figure 1-1 Vulnerabilities of resource-sharing systems. The principal points of vulnerability are (1) processors, (2) storage devices, (3) communications facilities, (4) remote terminals, (5) users, and (6) systems personnel.

tion of service, improper modification (corruption) of programs or data, including creation of negotiables, loss of programs or data, theft (removal) of property including supplies and negotiables, and misuse of resources (equipment, facilities, programs and data).

2. *Unintended actions by employees (negligence).* These can result in disclosure of classified information, corruption of programs or data, interruption of service, loss of programs or data, and destruction of equipment and facilities.
3. *Accidental occurrences.* These can result in interruption of service, corruption of programs or data, loss of programs or data, and destruction of equipment and facilities.
4. *Covert attacks by nonemployees* (stealth and deceit). These can result in disclosure of classified information, interruption of service, corruption of programs or data, destruction of equipment and facilities, and theft of property.
5. *Overt attacks by outsiders (force).* These can result in interruption of service and destruction of equipment and facilities.
6. *Overt attacks by employees.* These too can result in interruption of service and destruction of equipment and facilities.
7. *Unintended actions by outsiders (input error).* These can result in interruption of service and corruption of data.

While all of these threats are only too real (as we shall see in the next chapter), the overwhelming majority of loss-causing incidents affecting EDP centers are not criminal in nature and can usually be traced to the actions of careless or incompetent employees. In second place as a cause of loss are the defalcations of dishonest employees. Crimes perpetrated by outsiders, those possessing no lawful access to EDP resources, are, so far, a poor third.

Recently, however, a number of youthful computer enthusiasts have demonstrated their ability to penetrate resource-sharing computer systems using their home microcomputers and a device called a modem (modulator-demodulator) that connects the home computer to telephone lines. So far, their activities have been in the nature of pranks, but their actions demonstrate serious security weaknesses in the systems attacked.

EDP SECURITY IN A NUTSHELL

The protective features that computer security shares with other kinds of security consist of administrative and organizational measures, provisions to ensure the loyalty and reliability of personnel, and traditional physical and environmental safeguards.

The protective features peculiar to EDP security involve measures relating to hardware or EDP equipment, software or computer programs, and communications if a remote environment is under consideration. These three areas, as