

COMPUTER SECURITY HANDBOOK

• SECOND EDITION •

RICHARD
H. BAKER

TP309
B168
Z.2

9161367

Computer Security Handbook

2nd Edition

Richard H. Baker



E9161367



TAB Professional and Reference Books

Division of TAB BOOKS

Blue Ridge Summit, PA

SECOND EDITION
FIRST PRINTING

© 1991 by **TAB Professional and Reference Books**, an imprint of TAB Books.
TAB Books is a division of McGraw-Hill, Inc.
The TAB Professional and Reference Books logo, consisting of the letters "TPR" within a large "T," is a registered trademark of TAB Books.

Printed in the United States of America. All rights reserved. The publisher takes no responsibility for the use of any of the materials or methods described in this book, nor for the products thereof.

Library of Congress Cataloging-in-Publication Data

Baker, Richard H.

Computer security handbook / by Richard H. Baker. — 2nd ed.

p. cm.

Includes index.

ISBN 0-8306-7592-2 ISBN 0-8306-3592-0 (pbk.)

1. Computer security. 2. Electronic data processing departments-
-Security measures. I. Title.

QA76.9.A25B35 1991

005.8—dc20

90-24383

CIP

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

Questions regarding the content of this book should be addressed to:

Reader Inquiry Branch

TAB Books

Blue Ridge Summit, PA 17294-0850

Vice President and Editorial Director: Larry Hager

Book Editor: Eileen P. Baylus

Production: Katherine G. Brown

Book Design: Jaclyn J. Boone

Computer Security Handbook

2nd Edition

Introduction

In 1983, a Milwaukee-based group of young computer hackers managed to find their way into the data banks of a hospital, a bank, the Los Alamos National Laboratory, and several other computers loaded with sensitive programs and data. Thanks to their efforts, the term *hacker*, previously applied to a rough-and-ready breed of computer enthusiasts, became synonymous with computer crime.

In 1988, a college student managed to invade a U.S. Defense Department communication network. A *worm* implanted in the system repeatedly multiplied itself and brought thousands of computers to a standstill.

Computer security experts pointed to these incidents to demonstrate that too few computer users were adequately concerned about the security of their systems.

In 1989, computer owners braced for the infectious outbreak of a “Columbus day” virus that was set to do its dirty work on a Friday the Thirteenth. It would attack the hard disks of unprotected personal computers, erasing crucial elements that could be restored only by a process that would erase everything else on the disk. This incident proved not to be as serious as was feared earlier, partly because many wary computer owners had sensibly backed up their files and had taken other steps to protect themselves.

Perhaps you can indeed learn from history—if the lesson is repeated often enough. Many computer security experts pointed to this incident to demonstrate that at least some computer users were adequately concerned about the security of their systems and had acted to protect themselves.

A succession of highly publicized security breaches has indeed made some managers more security conscious. The *Los Angeles Times* has gone so far as to proclaim that “the corporate war against computer crime has come out into the open.”

Still, the long-standing pattern of poor computer security prevails in many places. The computers in thousands of American businesses are highly vulnerable to the loss and corruption of their data. This risk is not to be taken lightly. In many companies, existing protection is far from adequate for several reasons:

- Security is inconvenient. Most techniques that deter illegitimate users are equally effective at hindering legitimate users.
- Companies want to be seen as secure. Many computer crimes have gone unreported because executives worry about what would happen to their company's image should they acknowledge that they were a victim. That attitude is diminishing, but it still prevails among the more fearful souls in many corporate headquarters.
- You cannot just throw technology at a security problem. Although this book will discuss the technical aspects of computer security, you must always be aware that security is primarily a human problem, not a technical one.
- The greatest threat to your computers and data comes from inside your company, not outside. The person most likely to invade your computer is not a gawky youngster in some other part of the country but an employee who is currently on your payroll.
- The next most likely threat is an employee who until recently was on your payroll. That means the best security techniques are not usually those that rely on technology, but those that concentrate on the human element.
- Awareness of the problem is not enough. As always, it is a necessary first step toward a solution, but it is not the final step.
- There are those who believe that there is no security problem. One expert has gone so far as to suggest it is all some kind of media plot, perpetuated by the computer trade press.

In spite of all this, the *Los Angeles Times* cites several developments to support its optimistic statement:

- The fear of bad publicity is being supplanted by the fear of big losses.
- The federal government is promoting private-sector security to the point of requiring that defense contractors and regulated businesses increase their security over all sensitive information—both classified national defense information and sensitive nonclassified data.
- Although hackers get the publicity and insiders are the greatest danger, business has increasingly become aware of other threats as well. For example, industrial spying by computer has now been identified as a major threat.

The result has been an increased emphasis on computer security. It also means that security is increasingly the responsibility of all managers, not just

those who have direct charge of computer systems. As personal computers proliferate, so do the security risks, not only from the machines but from their operators.

This book is written for business managers at all levels who are responsible in any way for computer operations and who need the knowledge to meet that responsibility. In particular, it is written for those whose companies and departments make widespread use of personal computers, often hooked into networks and linked to corporate mainframes. You need not have a great deal of technical knowledge to be responsible for the security of a computer system. Happily, you need not have a great deal of technical knowledge, either, to discharge that responsibility.

ABOUT THIS BOOK

This book will discuss a wide range of security techniques, both technical and nontechnical. Much of it is derived from the experience and publications of the federal government, which became active in computer security long before the problem became a major concern for the private sector. You'll see techniques developed for federal installations that you can adopt or adapt to your situation.

You might notice that much of this federal material seems rather old by computer industry standards. Much of it predates even the advent of personal computers, and it is generally well known to computer security professionals. The information is still valid, however, and its age merely demonstrates how far the private sector has lagged behind federal efforts in this area. In addition, it is important that all managers become familiar with the basic techniques of computer security. The job can no longer be left to specialists alone.

Part I of this book will present an overview of the modern need for security, a framework for security management and planning, and a special discussion of two late-developing threats: computer viruses and radio wave interception.

Part II outlines a basic management approach, including ways to assess threats, identify computer criminals, and build the framework of a security policy.

Part III describes particular types of security, including passwords, physical access control, procedural safeguards, and technical measures.

Part IV tells how to apply these measures to specific security needs, including personal computers, networks, and disaster control. There also is a chapter on the legal requirements your security program should meet and another on security auditing.

Because this book is directed primarily at nontechnical managers, it will emphasize the information that is of greatest value to this group. Several chapters also include material that is more technically oriented. This material is presented at the end of the appropriate chapter, so you can read as far and in as much detail as your situation requires.

You also will find lists of security techniques you can apply to specific needs

and situations. A complete alphabetical listing of all these techniques is in appendix A. Appendix B discusses an analytical approach to security planning and implementation. A technical discussion of a high-security encryption system is included in appendix C.

Other Bestsellers of Related Interest

TROUBLESHOOTING AND REPAIRING THE NEW PERSONAL COMPUTERS—Art Margolis

This is a treasury of time- and money-saving tips and techniques that shows personal computer owners and service technicians how to troubleshoot and repair today's new 8- and 16-bit computers (including IBM PC/XT/AT and compatibles, the Macintosh, the Amiga, the Commodores, and other popular brands). Margolis examines the symptoms, describes the problem, and indicates which chips or circuits are most likely to be the source of the trouble. 416 pages, 351 illustrations. Book No. 2809, \$19.95 paperback, \$29.95 hardcover

DATA ACQUISITION AND CONTROL: Microcomputer Applications for Scientists and Engineers—Joseph J. Carr

A comprehensive overview of automated data systems for research and industrial applications. This book describes the professional applications of transducers and components and covers the spectrum of measurable input. The author describes in detail the peripheral components essential to data transference and signal processing including: op amps, electronic integrator and differentiator circuits, and more. 432 pages, 150 illustrations. Book No. 2956, \$34.95 hardcover only

CD-ROMs: Breakthrough in Information Storage—Frederick Holtz

This book provides a comprehensive overview of CD-ROM technology. CD-ROMs are a highly efficient multi-media storage device. Based on optical storage, as opposed to magnetic storage, CD-ROM applications include realistic simulations, publishing, education and training programs, video paint, animations, editing, special effects, home entertainment, graphic accompaniment to music, and more. 215 pages, 51 illustrations. Book No. 3026, \$14.95 paperback, \$22.95 hardcover

THE HANDBOOK OF MICROCOMPUTER INTERFACING—2nd Edition—Steve Leibson

"It contains a wealth of information needed by anyone working closely with microcomputers."

—BYTE Magazine

Offering practical insight and use-it-now information on every aspect of interfacing, Leibson covers hardware, software, and the history and theory of interfacing practices. You'll learn how to attach peripherals from any manufacturer—even homebuilt units—and use your computer to control everything from household appliances to radio equipment. 336 pages, 268 illustrations. Book No. 3101, \$19.95 paperback, \$29.95 hardcover

THE FROZEN KEYBOARD: Living with Bad Software—Boris Beizer

"... an entertaining, insightful, and wide-ranging computer volume for all collections."

—Booklist

Now you can learn to "live with" bad software, bad features, poor support, unreadable instruction manuals, and all the other ills that plague the personal computer user. Assuming a reluctant user's viewpoint, the author discusses bugs, user-friendly and other con games, menu-driven versus command-driven software, hostile software, and other key problems. 300 pages, 288 illustrations. Book No. 3146, \$17.95 paperback only

THE 8088 PROJECT BOOK—Robert Grossblatt

In his refreshingly humorous style, popular *Radio-Electronics*® columnist Robert Grossblatt leads you step-by-step through the design and construction of an 8088 controller and 17 hardware and software enhancements. When you have finished this book, you will have both a useful microprocessor-based controller and the knowledge and skills you need to build circuits around microprocessors in projects of your own design. 256 pages, 165 illustrations. Book No. 3171, \$19.95 paperback, \$27.95 hardcover

COMPUTER TOOLS, MODELS AND TECHNIQUES FOR PROJECT MANAGEMENT

—Dr. Adedeji B. Badiru and Dr. Gary E. Whitehouse

Badiru and Whitehouse provide you with practical, down-to-earth guidance on the use of project management tools, models, and techniques. You'll find this book filled with helpful tips and advice. You'll also discover ways to use your current computer hardware and software resources to more effectively enhance project management functions. 320 pages, 112 illustrations. Book No. 3200, \$32.95 hardcover only

HANDBOOK OF DATABASE MANAGEMENT AND DISTRIBUTED RELATIONAL DATABASES

—Dimitris N. Chorafas

This book provides database users and designers with the tools necessary to make informed decisions and to keep pace with the advancement of database technology. Now you can identify your needs, define the requirements, evaluate your priorities, choose supports, and determine solutions that are effective both in terms of cost and performance. 720 pages, illustrated. Book No. 3253, \$49.95 hardcover only

HANDBOOK OF MANAGEMENT: For Scientific and Technical Personnel—Dimitris N. Chorafas

Chorafas explains essential techniques in forecasting, planning, marketing, product development, finance, and office automation. Key areas covered include mathematical forecasting; long-term planning; developing new products; administering finances, budgets, and product pricing; controlling a marketing and sales network; and preparing for the challenges of the automated factory and advanced computer and network communications systems. 304 pages, 81 illustrations. Book No. 3263, \$42.95 hardcover only

MS-DOS® UTILITY PROGRAMS: Add-On Software Resources—Ronny Richardson

Combining the most useful features of a product catalog and magazine reviews, this book is the most comprehensive guide available for finding the utility programs you need to optimize your DOS-based computer system. Richardson candidly describes the capabilities and operation of virtually every DOS utility on the market. He clearly explains what each package does, who might benefit from the package, and what specific problems it can solve. 672 pages, illustrated. Book No. 3278, \$24.95 paperback, \$34.95 hardcover

Prices Subject to Change Without Notice.

Look for These and Other TAB Books at Your Local Bookstore

To Order Call Toll Free 1-800-822-8158

(in PA, AK, and Canada call 717-794-2191)

or write to TAB BOOKS, Blue Ridge Summit, PA 17294-0840.

Title	Product No.	Quantity	Price

☐ Check or money order made payable to TAB BOOKS

Charge my ☐ VISA ☐ MasterCard ☐ American Express

Acct. No. _____ Exp. _____

Signature: _____

Name: _____

Address: _____

City: _____

State: _____ Zip: _____

Subtotal \$ _____

Postage and Handling

(\$3.00 in U.S., \$5.00 outside U.S.) \$ _____

Add applicable state and local
sales tax \$ _____

TOTAL \$ _____

TAB BOOKS catalog free with purchase; otherwise send \$1.00 in check or money order and receive \$1.00 credit on your next purchase.

Orders outside U.S. must pay with international money order in U.S. dollars.

TAB Guarantee: If for any reason you are not satisfied with the book(s) you order, simply return it (them) within 15 days and receive a full refund.

BC

Contents

Introduction xvii

Part I

Computer security today

1 The scope of computer security	3
Security is a management responsibility	3
Many security threats	4
What managers are—and are not—doing	6
The annals of crime by computer	7
Watch out for ex-employees	8
Fund transfers	8
Getting along in age	9
Crime as a growth industry	9
Many ways to spread	9
How criminals use computers	10
Many criminal roles	10
Legal responses	11
Starting to worry	12
Laws aren't enough	12
A broader responsibility	13
Welcome to the information age	13
Coming together	14
National information systems	14
Problem areas	15
Information in conflict	16
Security has many faces	17
Secure data and equipment	17
Constitutional rights	18

Accuracy and reliability	18
Old trends—and new ones	19
When computers were big	19
Problems develop	19
Noticing the problem	20
Modern times	20
Why you need security	21
Collecting data	21
Organizing information	21
Computations	22
Communication	22
Innovation, security go together	22
The need for security	23

2 Viruses and electronic eavesdropping: the newest threats

25

The human factor	26
Repeat attack	26
A year later	26
Friday the Thirteenth, the sequel	27
More infections	27
How viruses spread	28
The danger of infection	29
Spreading around	29
Many types of infections	29
Friendly viruses?	30
Which system?	31
Where viruses attack	31
The life cycle of a virus	32
Gaining entry	33
Spreading the infection	33
Becoming active	34
Common types of viruses and their cures	34
Boot system viruses	34
System virus	35
Application infector	35
Infecting the Mac	35
Does immunization work?	36
Why so risky?	36
What to do	37
The best way to protect yourself	38
Recovering from an infection	39
Dealing with bad disks	39
Restoring the system	40
Find the source	40
The shopping mall spy	40

Over your shoulder 42
Equipped for espionage 42
What can you do? 42
Tempest in a CPU 43
Is the law on your side? 43

Part II

Managing the security program

3 Security is a “people problem” 47

Symptom of a larger problem 48
The problem with people 48
 Insiders take billions 49
 Crime of opportunity 50
Managing the “people problem” 50
 “Doomed to failure” 50
 Learn to manage change 51
 Set an example 51
 Maintain good human relations 52
 Keep the lines open 52
 Help wanted: criminal 53
 Start early 53
 On the job 53
 After the job is over 55
Security is a management responsibility 55
 New survey, same results 56
 Complacency doesn't help 56
 Bad press 56
 Not just a technical problem 57
 It can happen 57
Treat information as an asset 57
 To be feared? 58
 The nature of information 59
 The security challenge 59
 Protecting your information assets 59
 How much is it worth? 60
Selling security to management 61
 A sales campaign 62
 Analyzing the risk 63
 You do need support 63

4 Find your weak spots 65

Identifying the risks 65
 Government efforts 66
 List your security assets 66

Where to look for trouble	67
Uncommon threats	68
Zero-based analysis	69
Is all this necessary?	70
Method to the "madness"	71
Other factors	71
A baseline approach to planning	72
Three-level system	75
Selective controls	75
Special controls	75
No fixed list	76
Contradiction in terms?	76
Establishing your baselines	76
Add refinements	77
Who threatens your system?	79
One thing in common	79
Identifying the suspects	79
Attitude problems	82
Search for antagonism	83
Where are the weak spots?	85
Functional weaknesses	85
Physical locations	87
Preventing accidents	88
Coping with natural forces	88
In summary	89

5 Types of computer crime 91

Spies and snoops	91
Scavenging	91
Leakage	92
Piggybacking and impersonation	93
Wiretapping	94
Data manipulators	95
Data diddling	95
The salami technique	97
The superzap	99
Asynchronous attacks	100
Simulation and modeling	101
Retribution and damage	102
The trojan horse	102
Trap doors	103
Logic bombs	104

Part III

Basic security techniques

6	The perils of passwords	109
	What's wrong with passwords	110
	The not-so-secret password	110
	Wanting in	111
	Building a limited access route	112
	The basic schemes	112
	Secure the security measure	113
	Administering a password system	114
	How to create passwords	115
	Do it yourself	115
	Nothing's perfect	116
	The technology of passwords	117
	Effectiveness varies	117
	Generating passwords	118
	Limited lifetime	119
	Biodegradable passwords	120
	Another one-time system	120
	Physical characteristics	121
	Playing the odds	121
	Information content	121
	Handshaking schemes	122
7	Controlling physical access	123
	Kinds of computer security	124
	What the right protection can do	125
	New challenges for traditional methods	125
	What physical security can do . . .	126
	. . . And what it can't	126
	Recognize the limits	127
	Types of physical security	127
	Major security methods	128
	Maintaining degrees of access	128
	Two-class structure	129
	Several solutions	129
	The ultimate solution?	130
	Alternatives to the password	130
	Controlling site access	131
	Types of identification badges	131
	Advanced access controls	132

Biometric techniques	132
How they work	133
Less than perfect	134
Addressing site security	134
Site security checklist	134
Conditions to consider	135
The secure floor plan	135
Planning and evaluating physical security	136
Technical aspects of physical security	136
Badges and identification tokens	137
Time is important	137
Design objectives	137
Preparing badges	138
Resisting decoding and counterfeiting	138
Types of identification tokens	139
Verifying personal attributes	141
Problems of measurement	141
Two kinds of variation	141
Method of operation	142
Two classes of error	142
Using multiple attributes	144
Combining methods	145
Multiple trials	145
Allowing more than two trials	145
Examples of personal attributes	146
Fingerprints	146
Hand geometry	148
Signature dynamics	148
Speaker verification	149
Physical security techniques	150

8 Building secure procedures 153

The role of procedural security	153
What is it, anyway?	154
Do you worry enough?	154
Set your objectives	155
Establishing a need to know	156
Tailor your access controls	156
Promote use along with protection	157
Provide an integrated program	157
Put security where it's needed	157
The keys to secure procedures	158
Good procedures made better	159
A procedural security checklist	159
Controls built into the organization	160
Personnel controls	160

Programming controls	161
Operating controls	161
Staying in control	161
Good training is important	162
Procedures require people	162
What training should accomplish	162
Many ways to go	163
Use existing programs	163
Developing material	163
Subjects to cover	164
A choice of formats	164
Procedural backups for physical controls	164
Restricted file access	164
Control the controls	165
Control use of terminals	165
Log-on procedures	166
Other tactics	167
What a good program requires	167
Don't make assumptions	168
Strong points	168
Watch out	168
Procedural security techniques	168

9 Hardware and software security 171

No protection is automatic	171
Looking too good?	172
The growing role of technology	172
A matter of definition	173
Technical security goals	174
It's not always easy	174
Where to use technical security	175
Maintaining separation	175
Isolating users	176
Setting levels of sensitivity	176
Leaving an audit trail	177
Some typical applications	177
Backing up passwords	177
Restricting remote access	177
A security shopper's guide	178
Rating system established	179
The basic requirements	179
Systems classified for security	179
Security by default	180
A model for secure software	180
Top down, bottom up	181
The view from here	181