



PROTECT YOUR MACINTOSH

**FILE
ENCRYPTION**

**VIRUS
PROTECTION**

**BACKING UP
YOUR FILES**

**PHYSICAL
SECURITY**

**NETWORK
SECURITY**



Bruce Schneier



Protect Your Macintosh

by Bruce Schneier

005.8
S 359P



Peachpit Press

CUYAHOGA COMMUNITY COLLEGE
WESTERN CAMPUS LIBRARY

PROTECT YOUR MACINTOSH

Bruce Schneier

PEACHPIT PRESS, INC.

2414 Sixth St.
Berkeley, CA 94710
(510) 548-4393
(510) 548-5991(fax)

Copyright © 1994 by Bruce Schneier

Cover design: Visual Strategies (ViS)

Cover illustration: Gordon Studer

Interior design and illustration: Olav Martin Kvern

Production: Rhonda Boothe, John Carl, Neil S Kvern, and Tracy Tobin

DISTRIBUTION

Peachpit Press books are distributed to the US book trade by Publishers Group West, 4065 Hollis, PO Box 8843, Emeryville, CA 94609, phone (800) 788-3123 or (510) 658-3453, fax (510) 658-1834. Peachpit books are also available from wholesalers throughout the US including Baker & Taylor Books, Golden-Lee Book Distributors, and Ingram Book Company. Bookstores can also order using Wordstock or IBID (SAN 2028522). Resellers outside the book trade can contact Peachpit directly at (800) 980-8999.

NOTICE OF RIGHTS

All rights reserved. No part of this book may be reproduced or transmitted in any form by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher. For information on getting permission for reprints and excerpts, contact Trish Booth at Peachpit Press.

NOTICE OF LIABILITY

The information in this book is distributed on an "As Is" basis, without warranty. While every precaution has been taken in the preparation of the book, neither the author nor Peachpit Press, Inc., shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the instructions contained in this book or by the computer software and hardware products described in it.

ISBN # 1-56609-101-2

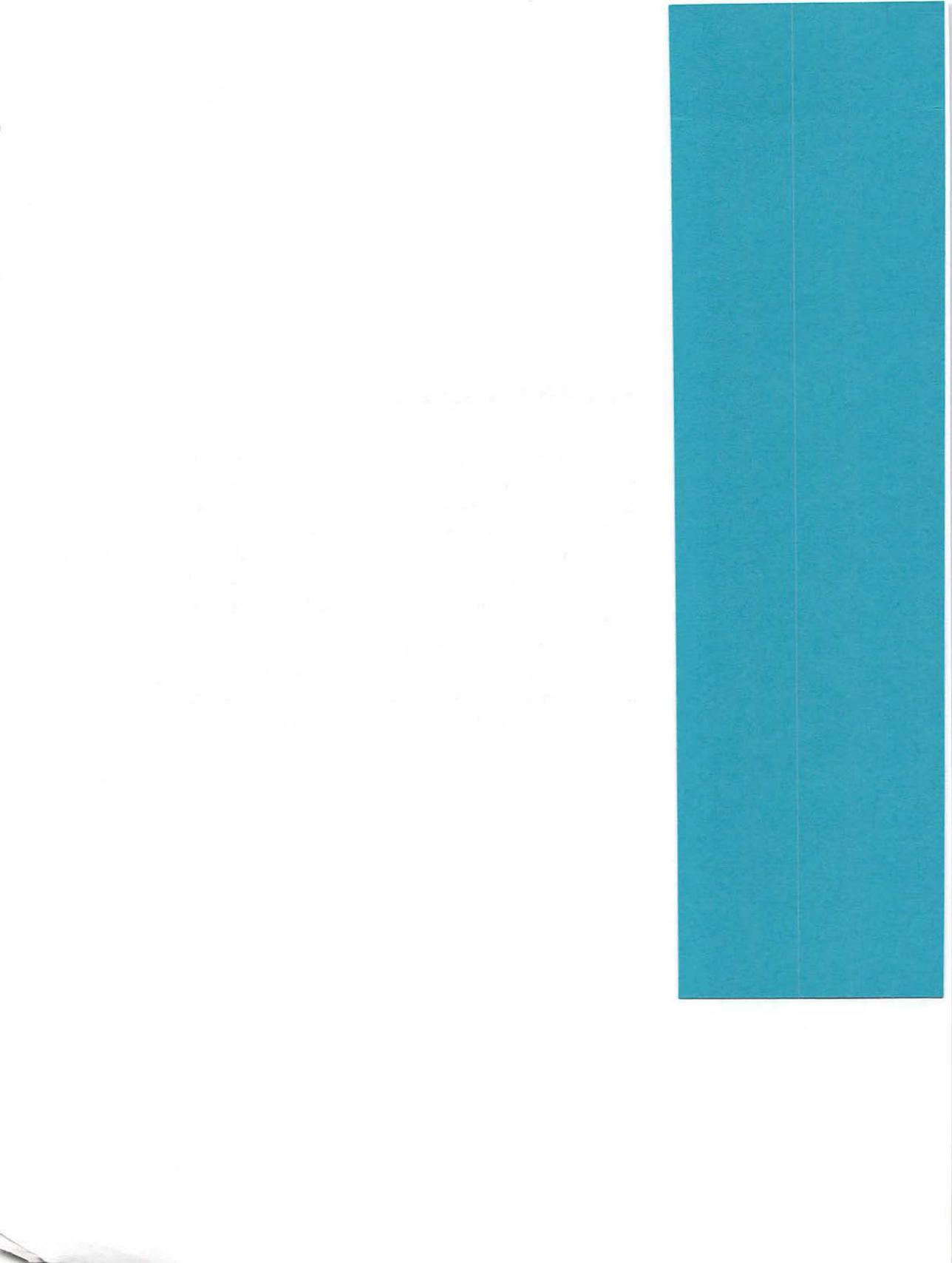
9 8 7 6 5 4 3 2 1

Printed and Bound in the USA

erica

Acknowledgments

Putting together a book like this is an arduous task, but fortunately I had help from many people. I would like to thank Mike Bentley, Ido Dubrawsky, Greg Edwards, Elliotte Rusty Harold, Tom Kan, Ben Liberman, Paul Robichaux, and Andrew Spring for reading and editing all or part of the manuscript; Karen Cooper for copyediting the entire manuscript, for finding and correcting problems with the book, and for everything else; Kristi Coale for stepping in and taking over the editing job; and everyone at Peachpit Press for shepherding the book into finished form. All remaining errors are my own, but without these people there would be far more than there are.





Foreword

Macintosh security has long been regarded as an oxymoron by mainframers. Even those who use DOS, Windows, or OS/2 (none of which have stellar security themselves), tend to shudder at the thought of sensitive data residing on a Mac. Positioning one of those “Apple things” as a critical node in a network is often viewed as an open invitation to all sorts of mischief.

Why all the fuss? For a number of reasons, not the least of which is that the Macintosh doesn’t have whole lot of embedded security. Part of what makes the Mac so much fun and so easy to use is that nothing gets in the way—well, almost nothing.

Aging mainframe bigots (and those of us who used to be) expect a certain level of security in the systems they use. They want to be prompted for an ID and password; to have access control over read, write, create, delete, and other such application functions; and to have group profiles, date/time access limitations, and encryption capabilities. These are not the things that Mac users have in mind when they say the Mac is “insanely great.”

Ease of use is not, and should not be viewed as, antithetical to security. It is one of the Mac’s defining features; but in the inevitable design conflicts that arise out of security considerations, something’s gotta give. The development team at Apple had it in mind

to build the computer that they wanted for themselves—intuitively easy to use, graphical, powerful, artful, and with a quirky personality. No one ever mentioned security.

The Macintosh was designed from its very inception as a personal computer intended to sit proudly on an individual's desktop, not a multi-user beast to live in some climate-controlled, access-restricted data center. If the Mac's a personal computer that only one person is going to use, then why do we need to worry about any of this access partitioning, log-on ID, password, encryption, and who knows what else?

Because nobody is perfect. We all make mistakes.

Security controls get a lot of press for their purported ability (and sometimes, glaring inability) to stop glamorous bandits. But the real money-saving effects of most security systems are that they reduce error rates, or losses from the errors that do happen. Granted, that is not nearly as exciting as thwarting techno-terrorists; however, it enables security drudges to justify to management our existence, the purchase of security equipment, and the implementation of seemingly cumbersome procedures.

Mistakes by authorized, well-meaning individuals constitute the greatest security-related losses. Perhaps the documentation was wrong, or the procedures were contradictory. Maybe the application design was faulty, or maybe the user actually was dumb. A single, small error may represent only a \$10 loss, but if that \$10 problem happens 10 times a workday, the annualized loss to the organization exceeds \$20,000. Eliminating even some of those mistakes, minimizing the extent of damage when the mistakes do occur, and ensuring the ability to recover quickly pays big-time dividends. The security controls for the Mac that Bruce Schneier describes help greatly in preventing, detecting and recovering from mistakes.

As Macs move in on the business computing landscape, the assumption that they are single-user machines becomes increasingly suspect. My old LC is single-user because everyone else thinks it's a decrepit relic from some bygone era. Upgrading to a Quadra 950 would make me a popular guy at the office, with new friends wanting to try out the gorilla Macintosh—whether I'm there or not. Macs are also appearing in ever-increasing numbers as workstation nodes on networks—not just AppleTalk networks, but NetWare, VINES, and other non-traditional places. Some of these network nodes are intended to be multi-user.

Without appropriate partitioning and access controls, anyone turning the machine on sees and can modify anything—e-mail

messages or project schedules. Combine this expansion of multi-user access with the propensity for mistakes—and the growing volume of sensitive and critical information residing on organizational Macs—and some frightening scenarios emerge. The bottom line is that it isn't wise to assume that a Mac is completely secure.

The primary reason for the knee-jerk negative reaction by security people when "Macintosh" and "security" are mentioned in the same sentence, is the attitude of Mac users. Mac users picture themselves as renegades, people who go against the establishment. This image carries over to corporations, which may not see a place for the Mac in their organization. Corporate bosses wouldn't put their "sensitive information" on a machine that is intended for individuals and has a definite individual personality. And who'd need to encrypt anything—the CIA?

Times have changed. The Mac is a corporate machine, a server, a network workstation, a repository of sensitive information. But the attitude of initial Mac users toward controls of any kind still abounds. And, not all of it is pirate swagger or a cavalier attitude. A substantial portion of Macintosh security problems stem from lack of awareness of the threats to their data, and of what they can do about them.

The Mac has been pretty fortunate with respect to viruses. When the Mac was being designed and built, malicious code (i.e., virus, worm, or Trojan horse) was unheard of—except for a very few mainframe shops, where the perpetrators were invariably programmers working at the installation. In the mid-to-late 1980s, Mac users saw SCORES, MacMag, nVIR, WDEF, and several other Macintosh viruses, with SCORES being the only really nasty one.

Now we find INIT-M and the other INITs, MDEF, CDEF, MBDF, and so forth. But now we have anti-virus software, and Bruce Schneier lists and reviews available products in this book.

The book is valuable for more reasons than the analysis of Mac viruses and associated software products. Bruce approaches Macintosh security from a global perspective, looking at more than just the specific hardware and software issues. Physical security, more important in these days of small, light, powerful machines, and dense, obscure storage media, gets covered—as do management controls, encryption, and personnel security. This book can definitely help protect the valuable information that users work with on the Mac, but effectiveness of any of the controls discussed depends primarily on one system element. Passwords don't keep bad guys out if they're obvious or given away. Virus

controls don't help if you don't use them. Backups don't run by themselves, especially if you disable them.

There's plenty of useful information in this book. Dig in and find it. Then use those wonderful Macintoshes. Have fun while you're being productive. Protect what needs to be protected. Make a dent in the universe.

John O'Leary
Director of Education
Computer Security Institute
Plano, Texas



Contents

CHAPTER 1	What Computer Security Is and Why It Counts	1
	Setting Security Goals	2
	Data Dangers	4
	Combating the Threats	5
	Assessing Your Data's Value and Security Risks	8
	Determining Your Risk	10
	Personal Computer Security Self-Audit Questionnaire	12
	Organization and Policy	12
	User Awareness and Training	12
	Physical and Environmental Protection	13
	Control of Storage Area	13
	Data and System Integrity	13
	System and Data Access Controls	14
	Contingency Planning	14
	Auditability	15
	Networks	15
	Miscellaneous Issues	15
	Macintosh Security from the Mainframe Perspective	16
	Keeping It All in Perspective	18
<hr/>		
PART 1	Protecting Your Data from Thieves, Spies, and the Competition	19
<hr/>		
CHAPTER 2	Protect Your Data with Access Control	21
	Macs and Data Security	22
	What is the "Orange Book"?	23

Access Control	24
Passwords	25
The Methods of Access Control	28
Hard Disk Security	28
Screen Locking	29
Finder Overlays	30
Folder Locking	30
Limiting Privileges	31
Audit Log	33
Physical Data Protection	33
Shopping for Access-Control Programs	34
Considering All the Factors	56
Chapter 2 Sources	58

CHAPTER 3 Encrypting Your Data 63

Choosing an Encryption Algorithm	65
The Development of DES	69
How Secure is DES?	71
Choosing Keys	73
Safeguarding your Keys	76
Encryption and Speed	77
Hardware DES Encryption	78
Features of Encryption Programs	79
Encryption and File Recovery	81
What to Encrypt	82
What to Buy to Encrypt Your Data	83
Chapter 3 Sources	91

CHAPTER 4 Why File Erasure is Important 93

What to Buy for File Erasure	94
Chapter 4 Sources	99

PART II Protect Your Data from Viruses 101

CHAPTER 5 What You Need to Know About Viruses 103

How Serious is the Virus Threat?	105
Detecting Viruses	106
Preventative vs Detective Anti-Virus Software	108
Networks and BBSs—Viral Hotbeds	110
Recovering from a Virus Infection	111

	Keeping a Level Head with Mac Viruses	112
	What to Buy to Prevent Viruses.....	113
	Chapter 5 Sources	120
<hr/>		
CHAPTER 6	Macintosh Viruses—a Rogue’s Gallery	121
	Encrypted and Polymorphic Viruses	137
<hr/>		
PART III	Back Up Your Files	141
<hr/>		
CHAPTER 7	The What, When, Where, and Why of Backups	143
	Being Smart About Backups	145
	Choosing a Backup Medium	147
	Backup Strategies	152
	Backup Data Integrity	155
	Keeping Your Backup Data Secure	155
	Care and Feeding of Your Backups.....	156
	Shopping for a Backup Program	158
	Chapter 7 Sources	177
<hr/>		
PART IV	Locks, Chains, and Bars	181
<hr/>		
CHAPTER 8	Secure the Computer on Your Desk.....	183
	Thieves Out and Equipment In	184
	Anti-Theft Locking Devices	185
	Screws, Adhesion, and Cables	186
	Setting the Alarms	189
	Plates and Entrapments	189
	Security On or Inside the Mac	191
	Keeping Your Laptop from Growing Legs	193
	What to Buy for Hardware Security	194
	Chapter 8 Sources	205
<hr/>		
CHAPTER 9	Computer Insurance	211
	What You Can Cover	212
	Questions to Ask About Computer Insurance.....	213
	What to Buy for Computer Insurance	215
	Safeware Insurance	215

ComputerInsurance Plus	216
Personal Computer Insurance	216
Powell-Walton-Milward Insurance	217
Chapter 9 Sources	219

PART V Keep Intruders Out of Your Network 221

CHAPTER 10 Network Security 223

A Sample Security Policy Plan	227
Network Vulnerabilities	228
Countermeasures	230
Management, Procedures, and Security	231
Controlling Zone and Device Access	233
Security with AppleShare	234
Remote Access Control and Security	236
AOCE Security	237
The Keys to the Network	239
Digital Signatures	239
Public-Key Cryptography	240
RSA	242
RC2 and RC4	242
International Data Encryption Algorithm (IDEA)	244
Kerberos	244
What to Buy for Network Security	245
Chapter 10 Sources	252

PART VI Additional Security Issues 255

CHAPTER 11 Power Into and Out of Your Macintosh..... 257

Surge Suppressors	260
Voltage Regulators and Line Conditioners	262
Chapter 11 Sources	268
Potential Security Problems.....	269

CHAPTER 12 Document Security 269

Printers	270
Elements of Personnel Security	273

CHAPTER 13	Personnel Security	273
	Once Clearance Is Granted	274
	Visitors	275
<hr/>		
CHAPTER 14	Software Integrity	277
	Programmers' Tricks.....	278
<hr/>		
CHAPTER 15	TEMPEST	281
<hr/>		
CHAPTER 16	Disaster Recovery	285
	Disaster Recovery Planning	286
	Developing a Disaster Recovery Plan	287
<hr/>		
CHAPTER 17	Computer Security Policy	291
	Informing and Motivating Employees	293
	Writing Your Company's Security Policy	293
	What to Cover	294
	Part I: Overview	294
	Part II: Risks.....	294
	Part III: Countermeasures.....	295
	A Network Security Proposal Outline.....	296
	Computer Security and the Law	297
	Computer Security and Liability	298
<hr/>		
	The Protect Your Macintosh Source Code Disk Set	301
<hr/>		
	Index	303



What Computer Security Is and Why It Counts

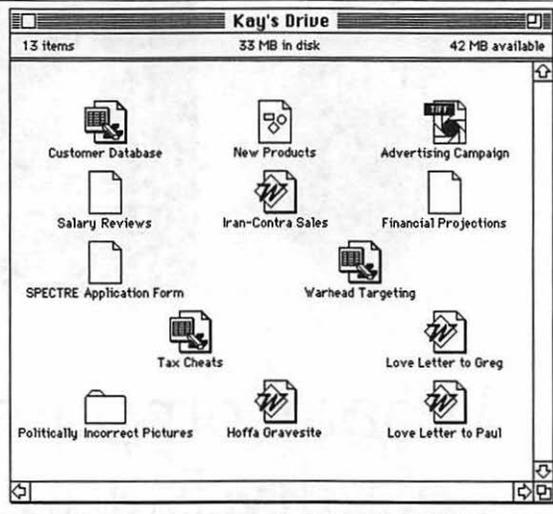
Computer security can simply be protecting your equipment and files from disgruntled employees, spies, and anything that goes bump in the night, but there is much more. Computer security helps ensure that your computers, networks, and peripherals work as expected all the time, and that your data is safe in the event of hard disk crash or a power failure resulting from an electrical storm. Computer security also makes sure no damage is done to your data, and that no one is able to read it unless you want them to.

Hardware is easy to protect: lock it in a room, chain it to a desk, or buy a spare. Information poses more of a problem. It can exist in more than one place; be transported halfway across the planet in seconds; and be stolen without your knowledge.

The fact that intruders will break into your computers and steal information, or that a computer virus will corrupt your data, may grab the headlines, but these are not the most common security threats. User and machine errors dwarf incidences of premeditated foul play. More people accidentally delete files than filch data. Hardware breaks down, and bit errors creep onto disks more often than viruses duplicate themselves in your files and applications.

Figure 1.1

Your secrets on
your desktop



Good security should guard against these infrequent incidences as well as the more likely human and machine error—the bottom line is to protect computers and the information stored on them.

The Six Enemies of Computer Security

Error. Human and computer failures lose data.

Ego. People break into computers because they're there.

Enmity. Animosity is a very powerful motivator.

Embezzlement. So is greed.

Extortion. A person who plants a virus in your Mac may then turn around and ask for millions of dollars to remove it for you.

Espionage. International and corporate competition bring prying eyes.

Setting Security Goals

Many people think of computer security in terms of keeping their data from the eyes of others—only those people authorized by the owner of the files should see this information. Certainly confidentiality is a big issue for safeguarding your files. However, it is

but one of the three aspects of computer security.

Accessibility is also important. If your security methods thwart the efforts of people authorized to get to the files, then the system is inefficient. These people should be able to get to their Macintoshes, network and servers, applications, and data.

Finally, data integrity is vital, though difficult to enforce because data moves around a lot. If it's changed on the server, it's not necessarily updated on individual machines. Data, correct or otherwise, must stay intact.

While all three of these aspects—confidentiality, accessibility, and integrity—should be the ultimate goal of a security scheme, not all of them are equally important in all cases. The relevance of each depends on the particular application. For example, a database of counterintelligence agents requires the utmost confidentiality; availability is of secondary concern. But emergency shutdown programs for a nuclear power plant must always be available; confidentiality is less important.

Moreover, there is nothing unique about these aspects: they apply just as easily to data in paper form. However, since computer data are more at risk than data in other forms, computer security measures have to be more stringent than other security schemes. At the very least, they must take into account the particular characteristics and vulnerabilities of electronic data.

The Nature of Information

Information is like gold to many organizations—but unlike this commodity, information can be:

- reproduced quickly and cheaply
- transported from one computer to another instantly
- sold with the seller also retaining the goods
- stored in a very compact form
- stolen without the owner losing it
- devalued when multiple copies of the same information are made
- valued higher as a whole collection than as component parts
- outdated quickly, which determines its value

Data Dangers

Electronic information is vulnerable to a number of threats (see “Nature of Information”), including intentional ones. These intentional attacks can result from your Mac’s setup—particularly if your office is easily broken into. Additionally, thieves can hack their way into a computer network and steal or corrupt data this way. Potential attackers may be those you know—a disgruntled employee or ex-employee, a contractor, consultant, or business competitor. They can steal data as well as put a virus on your computer.

While these attacks are the least common, they are the threats against which security packages protect. But your information faces other dangers that are not so easily combated.

For instance, enemies like business competitors or spies may prey on people—through blackmail, bribery, and other means—to coerce your users to give away passwords, leave doors unlocked, or simply look the other way while the theft occurs.

Accidents will, and often do, happen. Software can crash, and people can mistakenly erase entire hard drives when they really mean to delete only one file. It is the latter calamity that is your biggest worry. You can train users to follow certain procedures, but they can forget. In addition, someone who is preoccupied, or just plain tired, can do considerable damage to a Mac’s information. Safeguard your system by backing up the data regularly.

Nature can also warrant the need for regular backups through fires, electrical storms, and wild temperature fluctuations. If, for example, you keep all copies (electronic and otherwise) of your data in your office, and a fire destroys your office—your data will also be destroyed. While you cannot prevent such disasters, you can mitigate their effects: install a smoke detector and a sprinkler system, and store copies of your data offsite.

Computers can be susceptible to attack just because they are computers. Macs, and the equipment associated with them, have some built-in vulnerabilities that leave your information open to theft or corruption:

Hardware. The Macintosh is designed so that it is always possible to boot off a floppy disk, thus giving someone access to your hard disk, network, and ultimately your data. Certain modems might be susceptible to attack. Hardware failures can cause data loss as well as physical damage. It is possible for computer viruses to damage the hardware on some older Macintosh models. Lastly, computers and peripherals can be stolen.

Software. Many Macintosh security programs have major security holes that a clever attacker can exploit—such as the ability to boot the Mac off of a floppy. Software failures can lose data, or crash the entire system, or they can make the system more vulnerable to other kinds of attack. For example, the security program itself can bomb, or a backup program might not always work the way it is supposed to.

Media. Not only can magnetic media be stolen, but they can also be damaged by dust, accidental spills, and stray magnetic fields. Even after a disk is erased, a clever attacker can sometimes reconstruct the data. Print-outs are also susceptible to copying, destruction, or theft.

Communications. Many computer systems have been broken into via modem. An attacker might be content to tap into a network, and make copies of all messages passing through the network or all files on servers; or she might attempt to intercept and forge messages. Communications lines can also be severed, or otherwise damaged.

Emanation. All electronic equipment emits electromagnetic radiation, also known as TEMPEST (see Chapter 15). A sophisticated attacker can intercept this radiation, and use it to reconstruct the information being processed by your computer system.

Every computer system is vulnerable. The only way to eliminate all potential threats would be to lock your Mac in a steel vault, bury it in a secret location, and never write down or tell anyone where you hid it—and even then I'd have my doubts. A slightly less drastic situation would be to never turn the Mac on, because if it is in use, it is vulnerable to attack.

Of course, all of the above is extreme and wholly unrealistic—not to mention in violation of the goal of accessibility for a security system. You can enlist methods and products to reduce the risk of loss, destruction, and theft, or to minimize the damage to your information if these things do occur—but *there is no such thing as a completely secure computer system.*

Combating the Threats

So security is all about reducing risks and protecting your information. The steps you take to safeguard your data are called countermeasures, and they vary depending on how you want to define

your security—whether to physically keep someone out of an office or off a floor, or to deny people access to specific files.

The Goals of Countermeasures

A good countermeasure should do five things:

- prevent data corruption
- prevent data loss
- detect disasters and such, early enough to minimize data loss
- recover data in the event of a loss
- recover, via insurance, the costs involved in a loss

Certain countermeasures protect computer equipment from physical damage due to natural disasters or malicious intent. Such physical security can range from locks and keys to access-control key cards, and even biometric devices that use physical characteristics to identify authorized users.

Basic Types of Countermeasures

Direct: policies, standards, and procedures

Education: security awareness and training of users

Equipment: security hardware and software

Administration: management and training of security staff

Monitoring: creation and maintenance of audit logs

Follow-up: reporting of anomalies; frequent correction and updating of policies

Contingency: performance of periodic backups, data recovery

Other methods go to the actual computer level and help keep unwanted readers from seeing certain files. Through security software, you can grant users access to certain files by giving out software keys and/or passwords. Although backup programs will not stop a system failure from occurring or thwart a would-be thief, they are quite useful for preventing data loss in the event of hardware, software, or user error.

At the network level, you can use communications security packages to protect digital information while it is being transferred from one computer to another, whether over a Local Area Network (LAN), telephone lines, microwave link, radio, satellite, or any other means. These security countermeasures include encryption and authentication software.

Finally, throughout your company or department, you or your managers can set policies and procedures by which users may store or transport information and gain access to it. You may, for example, restrict employees at all levels of your organization from reading the e-mail of others. If you lay down these rules clearly, you can provide security by increasing employee awareness, and perhaps even prevent lawsuits in the event of a security problem.

At any level that you employ countermeasures, you should be sure that they have what I would consider the basic features. First, their operation should be consistent with the way people use the Mac. They must be simple, or people won't use them. They shouldn't depend on an attacker's lack of knowledge about the computer and/or security system.

Good security countermeasures must also be durable, efficient, and cost-effective, and they should be feasible for use within your organization. Finally, they should be as complete as possible, and should be adaptable as the prevailing threats change. For instance, anti-viral packages are frequently updated by the developer to reflect the discovery of a new virus.

At the very least, your countermeasures should prevent data corruption and loss. They should also determine when something goes wrong—early enough to prevent you from losing much data. Should you lose data, the countermeasures should recover it—and, via insurance, should recover any costs involved.

Evaluating Countermeasures

To be successful, a countermeasure should be:

- Reasonable
- Acceptable to your users
- Easy to set up and maintain
- Unobtrusive to the operation of other applications
- Effective against the most common threats

All countermeasures must be weighed against the potential attacks. As it is impossible to make a computer system completely invulnerable, it makes sense to implement the countermeasures that will do the most good. Protecting against low-risk, unlikely attacks, while ignoring the high-risk, more common ones, is not a good way to spend your security dollars. Countermeasures should protect against the most common attacks, and against those attacks that would do the most damage if successful. To do this, you first have to figure out which hardware and data are the most valuable, and what are the likely attacks. And then you must perform a risk analysis.

A formal risk analysis is a complicated undertaking. It involves interviews, studies, endless paperwork, and lots of money. A more ad hoc solution would be to decide how much time, effort, and money you want to expend protecting your data from these threats.

Assessing Your Data's Value and Security Risks

To determine how much effort should be applied to protect the data in a given computer, you first have to determine which data is most important, and then how much it's worth. One way to separate information that needs to be protected from information that doesn't, is to categorize it using one of the three aspects of computer security: confidentiality, availability and integrity.

"Confidentiality" is often the most important classification. The U.S. Department of Defense has official classifications of data including Unclassified, Confidential, and Top Secret. This rigid classification structure might be overkill for a small organization, but necessary for a larger one. For those with less formal needs, here is a sample of how you could classify your information:

Restricted. Data that are only meant for a small number of people within the organization, such as financial projections, product development plans, contract bids, marketing information, and negotiations.

Confidential. Data whose release might be detrimental to the profits of the company, including payroll information, customer lists, and sales and accounting information.

For Internal Use Only. Information that isn't meant for publication, but wouldn't undermine the profits of the company

if publicized—for example, employee-address and internal telephone lists, company policies, and organizational charts.

Unclassified. Everything else.

“Availability” indicates the effect caused by the loss of the data or computing facilities. Under this aspect, you could have classifications including:

Essential. No interruption of service is acceptable. Examples include the on-board computers of the Space Shuttle, air traffic control computers, and the safety computer functions of a nuclear power plant.

Desirable. Interruption of service should be avoided if possible. For example, airline reservation computers or ATMs.

Unimportant. Interruption of service would be inconvenient, but will not significantly affect operations. Most business and home computers fall into this category.

“Integrity” categorizes information according to how completely a system must keep the data intact. A sample classification might have:

High Integrity. No errors in data are allowed. For example, information about drug allergies in a person’s medical file, or the contents of someone’s police arrest record, would come under this heading.

Medium Integrity. There should be no errors that would seriously affect operations. Most computer information falls into this category.

Low integrity. Errors in data can be accepted. For example, a mailing list database.

Once you have determined the classifications of your computers, computer functions, and data, you can consider which threats are the most serious, which are worth protecting against, and how to go about doing it.

After sifting through your data to determine which categories are most valuable to you, you’re primed and ready to weigh the costs of acquiring, using, and maintaining a security product against the risk of doing without it. Remember, computer security is a trade-off.

Some people have the most minimal security. They lock their homes or office doors to make it harder for someone to steal their

machines, and leave it at that. Perhaps their data are not valuable enough to warrant more drastic measures.

Still, others need the best security they can get. They post armed guards around their facilities, deploy a backup computer system in a nuclear-hardened bunker somewhere, encrypt everything, and run a background check on everyone who sets foot near the place.

However, most people are somewhere in the middle. They have some sort of physical security—door locks, and maybe a chain securing the computer to the desk. They have an informal backup program, and occasionally scan their disks for viruses and hardware problems. Some might even install password protection on their machines.

Determining Your Risk

Any security program will do for some protection—but is it enough? The only way to answer this question is to perform a risk analysis. This need not be a complicated, formal document. It is simply a procedure used to estimate the probability of different attacks against a computer system, to estimate the potential losses, and to quantify the damage that may result if these attacks do occur. Risk analysis helps answer such questions as:

What would happen if your computers stopped working now, irrecoverably? Would it hurt? How much? Could your business continue?

What would happen if your competitor had a copy of everything on your file server? Would it hurt? How much? Could your business continue?

The ultimate goal of a risk analysis is to select cost-effective countermeasures that will reduce risks to an acceptable level—it cannot eliminate them. Only after determining exactly how valuable your information is, and how vulnerable your computers are to attack, can you determine how far you should go—in terms of people, equipment, and money—to protect them.

Risk analysis looks at the total value of your computers, the physical hardware as well as the information. Determining replacement costs for your hardware is easy. Ask your dealers or read the trade magazines. But to put a dollar value on your information, you have to answer these important questions:

How important or valuable is the information to you? There are many different types of information stored on computers: corporate records detailing financial information, and sales and marketing strategies; personnel records detailing salaries, health, and

employment history; classified national-defense information; personal letters; and perhaps your latest ventures into Sim City saved in a file. You have to identify all the different types of information stored on a computer, and estimate their value to you or your company. This is a very individual process. Information that has little or no value to one person or organization may have incalculable value to someone else.

How important or valuable is the information to others? The designs for next year's Acura car models are very valuable to the likes of General Motors. But the plot of your next novel probably won't fetch a dime on the black market—nor will the text of your love letters interest a thief (unless you are running for public office). If your information isn't valuable enough tempt a thief or competitor, it is probably not worth protecting.

Is the information replaceable? The latest company sales projections—recently downloaded from the company's corporate office, half a continent away—can be replaced easily; the only copy of a scientist's research data cannot. A digitized photograph can be rescanned; an original piece of computer artwork cannot. Think about the possibility of losing the information in a natural disaster: a fire, earthquake, or flood.

How vulnerable is the information? A computer near a window in a tornado is more vulnerable than a computer in an underground bunker. A computer attached to a network is more vulnerable than one that is not.

What is the cost of losing the information? Valuable time and money is lost, as people are reassigned to repair the security breach or reconstruct lost data.

What is the cost of compromising the information? If the information were a national-defense secret, the cost might be astronomical. If a file contained the identity of a secret agent, the cost might be the agent's life. Sensitive corporate information might cause the loss of employees, customers, or market share. Consider the costs of a hypothetical memo becoming public, one from the president of a tobacco company admitting the health risks of smoking—it could be in the billions of dollars. Other costs, such as lost prestige or public embarrassment, are harder to quantify. Still others, such as lawsuits, are painfully easy to attach a value to.

What is the cost of protecting the information? There's the initial cost of buying or producing the countermeasure. You may have installation costs, training costs, and maintenance costs. Finally, using this countermeasure may cause a loss in your users' productivity.

Personal Computer Security Self-Audit Questionnaire

This is a relatively simple self-audit of potential computer security risks. A version of this questionnaire was printed in the National Bureau of Standards Special Publication 500-120, "Security of Personal Computer Systems: A Management Guide." Even though the document was published in 1986, it still contains useful information.

The questions that follow are intentionally vague, since every computer system is different. The importance of different threats depends on many factors, as does the effectiveness of different countermeasures. The questionnaire is by no means exhaustive. Instead, it is intended as a starting point, to get you thinking about security.

Organization and Policy

Do you have organizational policies and procedures which address the handling of sensitive and proprietary information?

Are the procedures for protecting sensitive information on the Mac consistent with procedures for protecting sensitive information handled by other means within this organization?

Are policies regarding personal use of Macintoshes, software, and peripherals clearly stated?

User Awareness and Training

Are users provided with adequate training and awareness of the organization's information security policies, as well as each user's individual responsibilities?

In each of the areas discussed in this questionnaire, are users provided adequate training to perform required procedures, and use necessary equipment or systems?

Physical and Environmental Protection

Is computer equipment adequately protected from theft, damage, and unauthorized use?

Is the electrical power quality dependable? If not, are surge suppressors, uninterruptible power supplies, or other power quality enhancement equipment used?

Are temperature and relative humidity around the computer maintained within acceptable limits?

Is the computer adequately protected from airborne contaminants such as smoke and dust?

Control of Storage Area

Do you have labeling procedures for removable media that allow the organization to keep track of sensitive data?

Do you have adequate procedures to ensure the proper handling and storage of magnetic media and minimize physical or magnetic damage?

Do you have satisfactory disposal procedures such as paper shredding or disk degaussing for sensitive media?

Data and System Integrity

Are shared software or files protected from undetected or unauthorized modification?

Do you have adequate virus protection?

In situations where important decisions are based on data produced by the computer, do you have adequate procedures to validate that data?

Are users adequately trained in the software tools they are using?

Is custom software development for critical applications subjected to formal development controls?

System and Data Access Controls

If a system is intended for specific users, do you have adequate methods, physical or otherwise, to prevent unauthorized use?

If a system has multiple users, do you have adequate mechanisms to keep each user's work separate?

If access-control hardware or software is used:

Does the user interface prevent users from circumventing the control mechanisms?

Can you prevent users from running an unauthorized copy of the operating system?

If cryptography is used, do you have adequate key selection and management procedures?

Are users provided with utilities to overwrite sensitive hard disk drive files?

Contingency Planning

Do you have adequate procedures and equipment to handle emergency situations, such as fire, floods, or bomb threats?

Are routine backup procedures adequate for the confidentiality, availability, and integrity requirements of the data?

Are critical materials that are needed for backup operation, like data, software, hardware, and documentation, stored and available at an offsite or otherwise safe location?

Do you have formal plans for the backup operation of critical functions and for eventual recovery from emergency situations?

Is your organization's readiness to respond to emergency situations tested and reviewed periodically?

Auditability

If you need audit trails, is the user prevented from unauthorized modification or destruction of audit trail data?

Is the audit trail timely, or is it built after the fact?

Networks

Can you prevent users from storing sensitive host log-on information, such as the password, in the terminal emulation software? If not, are such computer systems provided with adequate controls to prevent unauthorized access?

If you require message security between computers, do you have adequate cryptographic or other communications security measures?

If a computer is accessible remotely, do you have adequate user identification and authentication mechanisms to prevent unauthorized access?

If the network supports dial-in capability, do you have adequate communications security measures to prevent unauthorized access?

Miscellaneous Issues

Do you have adequate monitoring, control, and accountability for computer equipment and software?

Do you have procedures to ensure compliance with software licensing agreements?

Is the software easy to use? Can users make mistakes that can lose or damage data?

Macintosh Security from the Mainframe Perspective

In the days of mainframes, computer security was easy—all computers were locked in the computer room and only trained professionals touched the machines. There were detailed procedures for access control, backups, and audits. Power was filtered into the room. There were special rules.

Macintoshes and their users are different, especially to a mainframe professional. In fact, to the mainframe professional who finds herself dealing with Macintoshes, the computer poses a number of security problems.

Macs are small and easy to steal. They're also attractive to a thief because they have a high resale value.

The Mac, in being user-friendly, is also abuser-friendly. It lacks built-in access-control features, so anyone who can turn on the machine has access to everything. Some people buy access-control programs, but they often don't use them properly. Additionally, Mac networks are easy to use. Adding a node is as simple as swapping a few plugs, and this can happen without your knowledge.

Mac users rarely do adequate backups. They back up at irregular intervals, and the backup disks are normally stored with the computer. These disks are usually poorly labeled, and they likely have never been tested.

Mac files are poorly classified. Data isn't categorized according to its sensitivity, but is instead labeled by color or by something like "cool" or "hot." Critical information sits on the hard drive right next to the day's "to do" list.

Portable Mac media are not stored properly. Floppy disks are frequently left lying around on desks, and they are often unlabeled or inadequately labeled.

Macs users aren't necessarily trained computer professionals. Just as anyone—experienced computer people and otherwise—can sit down in front of a Mac and do useful work, they can also sit down at a Mac and start deleting files. No one monitors what happens on all of these computers. No one can. If you thought it was difficult to implement a security policy within the Mac data processing department, just wait until you try to implement one company-wide.

Mac users don't ordinarily work with security constraints. Thus, they won't be very receptive to being told what they can and cannot do on a microcomputer. Additionally, if a user feels the security program on his Mac is getting in the way of his work, he will remove it. Unless you conduct a surprise audit of your machines, you will never know this.

Mac in-house documentation is informal. Commercial hardware and software comes with manuals, but these are ignored or sometimes lost by users. Custom software, like macros for databases and spreadsheets, poses a bigger problem because it is often written without any documentation. If the author leaves his job, a critical office function might depend on a piece of software that no one understands.

Macs are not locked up in a computer room. Thus, they are prone to physical damage that mainframes are not. For instance, it's easy to ban food and drink from the mainframe room, but it's next-to-impossible to stop people from eating and drinking at their desks.

Macs are susceptible to power fluctuations. So were mainframes, but at least you could protect a mainframe with a single large uninterruptable power supply (UPS). You'd have to buy a thousand surge suppressors and line filters to protect an entire Macintosh network.

Keeping It All in Perspective

While computer security is certainly important, it is also important to keep a sense of perspective. The typical Macintosh setup cannot, and indeed should not, be treated like a computer fortress. Determine the amount of protection to provide by assessing the value of your equipment and data and the likelihood of any threats. In some applications, this may dictate extraordinary countermeasures, but in most cases it won't.

Chapter 1 Summary

- Computer security protects your hardware, software, and information from environmental damage, user error, and malicious attacks, whether from inside or outside your organization.
- There are three aspects of computer security: confidentiality, availability, and integrity. Categorize your data by these criteria to determine its value.
- Threats to your system can be natural, accidental, or intentional.
- Any computer system has weaknesses. These include security holes in your software, vulnerability of your data storage media, and human error.
- Countermeasures to computer system threats and weaknesses can include physically securing the equipment, limiting access to equipment and data, making sure data is securely transferred in encrypted form, having company policies that increase employee awareness, and having adequate backup plans.
- The Personal Computer Security Self-Audit Questionnaire will help you analyze the risk to your system by examining your current security policy.



P A R T

Protecting Your Data from Thieves, Spies, and the Competition

One of the first security measures to consider is that which protects against intentional attacks on your data. Potential attackers include police and government intelligence services, disenchanted employees, snooping journalists, corporate competitors, vandals, and thieves. The possibilities are endless. If you have data that is valuable—to everyone or to just a few people—you should think about protecting it.

The countermeasures discussed here are designed primarily for deterrence and prevention. Detecting data theft is an admirable goal, but it doesn't do anything to recover the stolen data. Instead, you want to look into such deterrents as access controls, encryption schemes, and file erasure packages.



Protect Your Data with Access Control

Your Macintosh is sitting on a table at home, on your desk in your office, or in your briefcase. Anyone can walk up to it, turn it on, and do whatever he or she wants: copy or delete programs and files at will, read your personal mail, or peruse your business plans.

Even if unwelcome users aren't malicious, they can be irritating. Consider the tales of a Macintosh administrator at one university. Students using shared machines would pull such antics as turning the Trash Can icon into a black hole and the floppy disk icons into space ships, rigging the shut-down sound to play the Twilight Zone theme, and treating other users to a three-minute rendition of Dire Straits singing, "I want my MTV," at start-up. In addition to these novelties, the disks would become too full to create temporary files during printing, a different suite of fonts would be available every day, and new INITs would cause conflicts everywhere. Finally, applications would be accidentally thrown away or dropped inside nested folders where nobody could find them.

Access control attempts to prevent this kind of nonsense. It's a way of posting a guard at your Macintosh, someone to say "Hey, who are you? Let's see some identification." When the computer knows who you are, it can then limit what you can do. You may be restricted in the applications you can use or you may have

read-only access to certain files, preventing you from changing their content or deleting them all together.

Controlled-Access Data

- Memos and letters
- Sales figures and forecasts
- Marketing plans
- Personnel files
- Research plans and reports
- Reports about an organization's internal affairs
- Customer lists
- Advertising information
- Floor plans and cabling layouts

This type of protection isn't just for military computers in a super-secret sub-basement, it's also for average people. Businessmen with valuable customer lists, lawyers with confidential client relationships, people who don't want co-workers reading their personal mail, and parents who don't want their kids accidentally deleting important files all need this type of protection.

Macs and Data Security

The Macintosh is a friendly computer. It's easy to learn, easy to use, and at the same time it's not at all secure. Neither the Macintosh nor the Macintosh operating system were designed with access restriction in mind. There are lots of security products available for the Macintosh, but none come close to the level of security required by the Department of Defense (DoD) to secure classified information, though some situations need better security than the most basic defined in the Orange Book (see "What is the Orange Book").

Security on the Macintosh represents a trade-off. Every level of security you add to your computer reduces the ease-of-use that the Macintosh was originally intended to provide. Having to enter passwords to access your hard drive or to open particular folders makes it harder to work on your Mac. It's like living in a house with locks on every door and cabinet.

If you can get by with little security, there are a lot of options available for the Macintosh. Choosing among them depends on the nature of the data you need secured, whether one person or many people will need to use the Macintosh computer, and how intrusive you are willing to let the security software be.

What is the “Orange Book”?

The U.S. Department of Defense *Trusted Computer Systems Evaluation Criteria*, more commonly known as the “Orange Book,” sets standards by which to measure the relative security of computer systems.

It is an important reference in computer protection, mostly because the Orange Book was the first document to broadly characterize computer security levels.

However, it is not without shortcomings. Written in 1985, the Orange Book is outdated. It only considers security against espionage, not deliberate or accidental corruption of data, and it centers on government requirements. But it has relevance in business and research as well.

The Orange Book has four divisions of security criteria, from D at the low end to A1 at the highest level. Currently, the Macintosh is not rated under this system, but if it were, it wouldn't receive anything above the lowest level. Even AOCE (Apple's Open Collaboration Environment, see Chapter 10), with its built-in security, wouldn't rate above the D level.

Each division represents a major increase in the security of the system. The lowest criteria represents machines with no security mechanisms. Computer systems receive higher rankings for including some form of testing and documentation, and they are rated according to their relative impermeability as well as their ability to recover data.

Each criterion is based on four factors:

Security Countermeasures. The computer must prevent unauthorized access to and use of the system. These software security features include discretionary security controls allowing one user to specify which other users have access to his data, and labeling controls that label each item of information as to its security classification.

Accountability. For each user, the computer must check identity and access rights and authenticate this information. In addition, an audit trail must record every attempt to access, manipulate, and produce information.

Assurance. The computer must ensure that the software security measures have not been corrupted or bypassed. However, the Orange Book has no requirements for protection against data corruption.

Documentation. There are certain pieces of documentation relating to the system's security that must be prepared and maintained. These include security features' specifications, a trusted system manual, test documentation, and design documentation.

Access Control

If you want to prevent people from looking at your confidential computer data, your first line of defense is in keeping people from accessing that data. If they can't get to the data, they can't read it.

Access-control software encompasses many operations, but at the very least it should prevent access to a system by distinguishing between an authorized user and an unauthorized user, denying the latter access to the system.

It should also separate different data, distinguishing between the work of various users and giving privacy to each user's data. It should allow that data to be read and manipulated by others only with that user's permission.

Finally, access-control software should keep a comprehensive record of what has been happening on the system, including who has been using it, when, for how long, and what she did.

However, not all of these functions are required in every application. For instance, a single user protecting his machine from everyone else need only concern himself with the first function. A Macintosh used by a whole department, on the other hand, might be concerned with all three.

Some Macintosh access-control programs protect the hard drive or specific folders on the drive. Some of these programs allow different users access to separate areas of the hard drive, and enforce separation between those users. One user might have access to read files on the hard drive, and another might have access to both read and write files on the same hard drive, for instance. If your program has this sort of access control, it will prompt users for a user-ID and a password. This tells the program who they

are and, therefore, what kind of access to give them. Other programs also provide an audit log and a wealth of other features as described in the reviews.

It's important to remember that none of the access-control mechanisms mentioned in this book are foolproof. There are hackers who can get around them all. A savvy adversary will be able to read your data no matter which of these programs you choose. The break-in will be easy, too, because the thief is not going to be sweating over your machine, desperately trying to break in before the guard makes his next tour of the building. He's going to buy a copy of your security program and, in the comfort of his own hideout, figure out how to break the security scheme. Then he's going to write a program that will break it automatically, and put it on a disk. That's the disk he's going to use to break into your Macintosh, and it will take only seconds.

This is not to say that access-control programs are useless. There are lots of instances where you want a security program that protects against the masses: your children, the night cleaning staff, your co-workers.

Some of the access-control programs for the Macintosh are very good. They will protect your data against all but the best Macintosh hackers and those who can afford to hire them. The more secure solution, encryption, comes with a performance penalty that may be unacceptable in some circumstances. It all comes down to risk analysis: how much is the data on your Macintosh worth, how much effort would an adversary expend to get it, and what security measures are you willing to use to protect it?

Figure 2.1

Empower Access Control

Welcome to:
Empower® 14.0.8

Name:

Password:

Project:

Passwords

Access-control programs are built around the concept of a password, a secret term shared by you and the program. When you try to log on to the computer, it asks you for the password. If you know it, you type it in. The access-control program compares

what you typed in with the password it knows. If they match, you get in. If they don't, you don't.

Hints for Picking Passwords

- Don't pick passwords that are your name, or the name of anyone close to you.
- Don't pick passwords that are important dates, like your birthday.
- Don't pick passwords that are your Social Security number, license plate number, or any other number that can be traced to you.
- Don't pick passwords that are the street you live on, the model of car you drive, or any other word that can be traced to you.
- Don't pick passwords that are associated with the Macintosh, or with any computer program you use.
- Don't pick short passwords. Your password should be at least eight characters long—or longer if your password protection program permits it.
- Pick a mix of alphabetic characters, numeric characters, and punctuation marks. Vary capitalization. Never use an all-numeric password, like your Social Security or telephone number.
- Pick different passwords for different machines or different areas on the same machine. Do not use the same password more than once.

Should you forget your password, the access-control program won't let you in. Some programs have mechanisms for master passwords, which allow a back door if you forget your password. But they can be double-edged swords. In the hands of your network administrator, a master password can help you, but in the wrong hands, it can give someone easy access to your machine. So it is a *bad idea* to forget your password.

It is also a bad idea to choose a password that someone might easily guess. If someone intent on breaking into your computer tries to convince the access-control program that he is you, he's going to try some simple passwords. He'll try your name, your spouse's name, your pet's name, the word "password," and a

couple dozen other passwords. If your password is one of those, he'll get in.

You should follow certain guidelines for choosing a hard-to-guess password. Don't choose a short word. Don't choose a word that is related to you in any way. Choose a word that has upper and lower case characters, and has at least one non-alphanumeric character. How serious you get about this depends on the sensitivity of your data and the likelihood that someone is going to take the time to try and guess your password. The night cleaning staff might guess three passwords and give up, but your teenager will happily spend hours trying many possibilities.

If you write your password down on a piece of paper and leave it on your desk, a would-be spy is going to find it. So don't write your password down anywhere.

Don't tell your password to someone else. That's even worse than writing it down. Not only can this other person get into your computer, but also he might write it down or tell a third person. Before you know it, everyone could know your password.

Change your password regularly. No one is perfect. Sometimes you have to tell your password to a co-worker because you are sick or are away on a business trip and someone has to get into your computer. When you return, change your password immediately. Even if you have kept your password secret, change it after a few months.

Hints for Protecting Passwords

- Don't write your password down anywhere. If you *must* write your password down, don't identify it as your password.
- Don't ever tell anyone your password.
- Don't type your password when anyone is watching.
- Change your password regularly.
- When you change your password, pick a new password. Don't alternate between two passwords.
- If you accidentally divulge your password, change it immediately.

Remember, Macintosh password protection programs can be broken without figuring out the password. An adversary will only try a couple hundred trial passwords before it becomes more efficient to use other techniques.

The Methods of Access Control

Programs that restrict entry to the Mac or parts of it are hard to typify other than that they let users control access to their computers. Beyond this, however, the programs vary in how and to what degree they deny access—whether at the hard disk level or in the operating system.

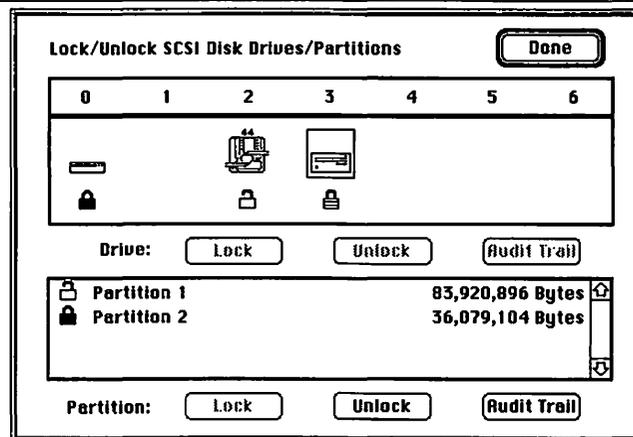
Additionally, whether a program locks a hard disk or a screen, it will vary in the way it does so. For instance, Berkeley Systems' After Dark screen saver has a screen-locking mechanism, as does Citadel, but Citadel allows for such background tasks as downloading e-mail while it guards access through the screen. After Dark does not. The lists of these kinds of differences are many.

Hard Disk Security

One of the simplest security measures is to password-protect your hard drive. If you want to access the hard drive, you have to type in a valid password. No password, and you can't use the drive.

Figure 2.2

Citadel Hard Drive Access Control



Many programs that provide this kind of security allow you to partition your drive into several sections, each with its own password. With this feature, you can set up a Mac so that several users each have a secure portion of the hard drive. Each user knows his own password, and can access his portion. No user knows the other passwords, so the other partitions remain secure.

This scheme is very useful in situations where several people share a single Macintosh. For example, if there are three people who use the same machine, you can partition the drive into four sections. Each of three sections could be password-protected for each of the three users, with the fourth partition accessible to everyone. Or perhaps you have a Mac at home and share it with everyone, but you want a small partition accessible only to you.

Some programs include the option of a master password, one that can open every partition. This can be useful for a system administrator to have, in case of an emergency or if someone forgets his password.

Screen Locking

Screen locking is the simplest means of access control, and the easiest to bypass. When you boot or reboot a Macintosh, you have to enter a password. Without the password, you can't do anything. Some security programs that provide screen locking will, after a specified period of inactivity, automatically lock the screen, showing a screen saver in place of your secrets.

Figure 2.3

DiskLock Screen Locker



The better programs will allow background tasks to run even if the screen is locked. This way, you can download files or mail from an on-line service while the screen locking program is active. Bear in mind, however, that this is one of the easiest security measures to bypass, and that screen-locking programs are no defense against data theft over a network.

Finder Overlays

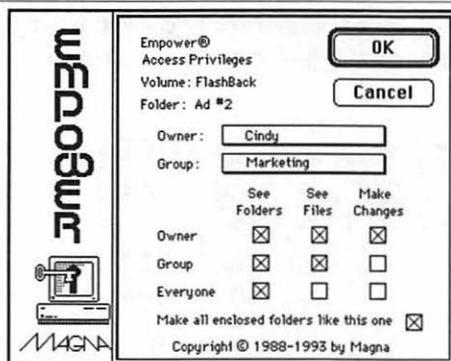
Finder Overlays replace the Finder at start-up with an alternate interface. In addition to simplifying the Mac interface, these products provide some security by allowing administrators to customize which files are displayed. These programs are primarily aimed at the educational market, and don't provide much in the way of real security.

Folder Locking

Finder Overlays restrict users' access to the Macintosh, but do not provide any security for those users. If several people use the same machine and store sensitive information there, locking individual folders and files provides more security.

Figure 2.4

Empower File
and Folder
Locking



There are different ways to lock folders. A folder can be locked so that only someone with the password can open the folder or add to the folder. A folder can serve as a drop folder—anyone can put things in the folder, but only someone with the password can take things out; or it can be a read-only folder—anyone can open and read files in the folder, but only someone with a pass-

word can change them. The file-sharing feature in AppleShare has some rudimentary folder-locking capabilities, but many commercial programs do much more, like encrypt folders. A determined adversary can defeat this security measure.

Proving Who You Are

Identification is the way you tell the computer who you are. Authentication is the way you prove to the computer that you are who you say you are. Authentication schemes look for:

Something You Know. A password is something both you and the computer know. Theoretically, if you know the password that belongs to the person authorized to use a certain Macintosh, then you must be that person. But problems with this arise, because you might tell your password to someone, or someone might guess it. Passwords are used by almost all of the access-control programs for the Mac.

Something You Carry. You may hold a token, or a key, a card, or a specially programmed floppy disk. If you have the token that belongs to the person authorized to use a certain Macintosh, then you must be that person. This also has problems. You might lose the token, have it stolen, or have it duplicated. Some authentication systems use the combination of a token and a password.

Something You Are. Biometrics is a means for identifying people by personal traits—fingerprints, palm prints, retina scans, and voice prints. The trick is to make these authentication systems sensitive enough to reject impostors but not so sensitive that they reject the authorized users. A user might have a bruise that obscures part of his thumbprint, for example. I haven't seen any Macintosh-specific security programs that use this method, but they're coming.

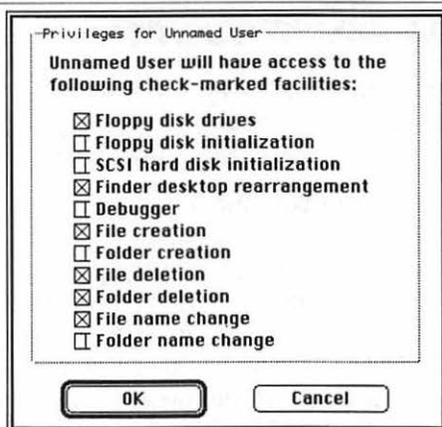
Limiting Privileges

Sometimes you want to let someone use your Macintosh, but at the same time want to limit what he can do. You want to keep a specific folder private. Perhaps you don't mind someone looking

at files, but you don't want the person changing anything. Or maybe you don't mind someone making changes, but you would mind someone making copies of your applications and taking the duplicates home with them.

Figure 2.5

ultraSecure
options screen



The most comprehensive Macintosh access-control programs can handle these sorts of things and more, including copy protection. This option prevents unauthorized copying of specific files or folders, and it can also prevent this from happening to specific applications.

In addition, programs might have deletion protection which prevents the deletion of specific files or folders. Similarly, modification protection guards against unauthorized changes to specific files or folders.

Two other options let the thief get away with your applications but foils their attempts to use them. A "poison pill" disables the duplicated application after a specified period of use. If you're concerned about software piracy, this is an option to use. Application restriction allows only password holders to launch certain applications.

Bear in mind, as you're using all these options, that many programs allow for guest log-ons, which allow people without valid passwords to log on to the computer and use unprotected programs and data.

One way to stop the unauthorized copying of files and applications is through floppy-drive disabling, an option available in programs like cypherPAD. It incapacitates the floppy drive, preventing both unauthorized copying and the introduction of computer viruses.

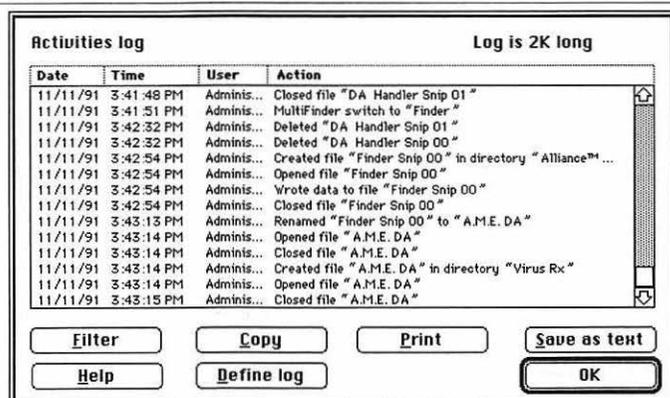
Audit Log

To keep track of who is using what on the system, many access-control programs keep an audit log. This file tracks who logs on, if there were any unsuccessful log-on attempts, and various other security-related events, including the times of the log-on attempts.

Some programs password-protect the audit log, so that no one can modify it. Other programs encrypt the audit log, for even more protection. But none of these products can provide you with an audit log that is intruder-proof. A sufficiently knowledgeable attacker can defeat the audit log, even if it has been encrypted. If you need an intruder-proof audit log, you will have to find specialized hardware and software because no commonly available Macintosh product will do.

Figure 2.6

A.M.E. audit log



Physical Data Protection

If a would-be data thief can't turn your computer on, he can't steal any data. Numerous products lock the computer's power switch; some computers even come with a key. Other products lock your computer's disk drive or SCSI port. Chapter 8, on physical security, discusses these locks in detail, but some software products come with hardware locks.

Shopping for Access-Control Programs

Many security programs offer some form of access control. What you buy depends on your needs. If, for example, you have a number of users sharing a machine, then it would be prudent to look into packages that offer some form of file and/or folder locking—perhaps even those with partitions and passwords for each division.

At the very least, an access-control program will control access to disks, files, and folders. If it is really doing its job, such a program will also generate an audit log. Security is a trade-off in many ways, not the least of which is that your data are vulnerable to loss or damage when you install the program. As a general rule with security packages, make a backup of your data before installing the program.

Table 2.1: Access-Control Products

Product	List Price	Company	Consumer Phone Number	Main Function	Comments
Access Managed Environment (A.M.E.) 2.1.8	\$159.00	Casady & Greene, Inc.	(408) 484-9228	All-purpose security program	Strong network manager functions
At Ease 1.0	\$59.00	Apple Computer, Inc.	(408) 996-1010	Apple's software application designed to restrict unauthorized access	Finder overlay is easily bypassed
Bullet Proof 1.0	\$5.00	Spectra Micro Development	(602) 795-7288	Basic file and folder protection	Simple protection that is easily bypassed
Citadel with Shredder ¹	\$99.00	DataWatch Corp.	(919) 549-0711	All-purpose security program	Has strong DES encryption implementation
CPU 2.0.3	\$99.00	Connectix Corp.	(800) 950-5880	Simple password protection for PowerBooks	Is easily broken
cypherPAD 1.213	\$49.00	uzrEZ Software, Inc.	(714) 756-5140	Basic hard drive lock with audit log and floppy disable	Shuffling keypad helps protect password
DiskGuard 1.0	\$140.00	ASD Software, Inc.	(909) 624-2594	Network-oriented access control	Has master password option
DiskLock 2.12	\$189.00	Symantec Corp.	(800) 441-7234	All-purpose security program	Locks hard drives and partitions, encrypts in DES
DiskLock PB 1.0	\$59.00	Symantec Corp.	(800) 441-7234	DiskLock for PowerBooks	Locks PowerBook when in sleep mode
DiskMaker 1.6.5	\$99.00	Golden Triangle Computers	(800) 326-1858	Universal SCSI utility with hard drive protection	Has master password option

Product	List Price	Company	Consumer Phone Number	Main Function	Comments
Drive 7 3.0	\$89.95	Casa Blanca Works, Inc.	(415) 461-2429	Universal SCSI utility with hard drive protection	Has master password option
Empower I 4.1.1	\$169.00	Magna	(408) 282-0900	All-purpose security program	Administrator can set option to prevent use of simple passwords
Empower II 4.1.1	\$296.00	Magna	(408) 282-0900	More comprehensive than Empower I	Users can choose who can have access to particular files or folders
Empower Remote 4.1.1	\$396.00	Magna	(408) 282-0900	Comprehensive security controlled from remote machine	Good for network distribution and set up
FileGuard 2.7.8	\$249.00	ASD Software, Inc.	(909) 624-2594	All-purpose security designed to work with MaccessCard Reader	Offers copy protection; DES is bad
FolderBolt 1.02e	\$129.95	Kent*Marsh Ltd.	(800) 325-3587	Access control for folders	Flexible in locking options; administrator mode has master key
Folder Locker 1.2.8	\$30.00	Software Brewing Company	(415) 940-1946	Access control for folders	Allows for "drop" folders; System folder can also be protected
Hard Disk ToolKit 1.5	\$199.95	FWB, Inc.	(415) 474-8055	Disk driver software with security tools	Password protection at file, folder, partition, and drive level
Keylock Mac 4.0	\$89.00	Keylock, Inc.	(800) 366-2515	Hardware and software access control	Administrator can impose minimum password length
MaccessCard Reader 1.0	\$349.00	ASD Software, Inc.	(909) 624-2594	Hardware access card reader designed for use with FileGuard	Can be trained to recognize any identification card with magnetic strip
MacPassword 4.0 ²	\$35.00	Evergreen Software, Inc.	Write to company	Shareware access control for hard drives, folders, and files	Can enforce password rules to prevent use of old or easy words
Menu Master Mac 1.0	\$99.00	Electronic Learning Systems, Inc.	(800) 443-7971	Finder overlay	Easily bypassed
NightWatch II 2.5	\$159.95	Kent*Marsh Ltd.	(800) 325-3587	Hard drive security	Allows many users with different passwords on one Mac
Norton Utilities for the Macintosh (Norton Partition) 2.0	\$149.00	Symantec Corp.	(800) 441-7234	Disk partitioning utility	Users can password protect partitions, but security isn't too stringent
Passport 3.0	\$49.95	Praxitel, Inc.	(510) 846-9380	Simple password protection for hard drives	No Floppies option prevents the mounting of any floppy disk

Product	List Price	Company	Consumer Phone Number	Main Function	Comments
PassProof 1.02	\$99.95	Kensington Microware Ltd.	(800) 535-4242	All-purpose access control hardware and software	Locking devices prevent access to floppy drives and SCSI ports
Power Utilities 1.0.5	\$129.00	AlSoft	(800) 257-6381	Mac utility package with disk partition program	Password protection for partitions is easily bypassed
QuickLock 2.1	\$29.95	Kent*Marsh Ltd.	(800) 325-3587	Screen-locking utility	Not good security alone but it integrates well with NightWatch
SafeWord MultiSync cards ¹	\$34.00	Enigma Logic, Inc.	(510) 827-5707	Hand-held dynamic password generator	Designed for use with A.M.E.
SecureInit 2.5A	\$99.95	Direct Software Inc.	(619) 778-6555	Simple password-protection init	Easily bypassed when you boot Mac from a floppy
Silverlining 5.1	\$149.00	La Cie Ltd.	(503) 520-9000	Disk driver toolkit that has some security	Partitions can have passwords
ultraSECURE 3.0	\$239.00	uzrEZ Software, Inc.	(714) 756-5140	All-purpose access control	Has password parameters, network administration features, and DES encryption
ultraSHIELD 2.0	\$149.00	uzrEZ Software, Inc.	(714) 756-5140		More security than ultraSecure. Has DoD file erasure and anti-virus protection

¹ Programs are also a part of the SuperSet Utilities, \$149.00

² Evergreen's address: 15600 NE 8 St., Suite B1126; Bellevue, WA 98008

³ Cards range in price from \$34 and \$44

Access Managed Environment (A.M.E.) 2.1.8

A.M.E., from Casady & Greene, tries to be the most comprehensive security product available for the Macintosh. Among all its offerings, user management is A.M.E.'s greatest strength. You can create a hierarchy of users for multiple levels of access management. Global options let you prevent System folder changes, and lock out viruses or unauthorized applications. These levels are manipulated with a graphical editor that resembles an organizational chart.

The program allows a security administrator to tightly control access to a Macintosh and its data through the use of privileges which can apply to all users, to specific users, or to any and all files. Administrators can assign individual users six types of privileges, including the ability to copy files to the hard drive. A.M.E. is also the only program that restricts access to the serial and parallel ports.

Most access-control programs require users to place access-restricted files in protected folders. A.M.E. can prevent accessing, copying, or writing to a file regardless of its location. Files can be protected either with a password alone or with a password and a key disk. In the case of the latter, A.M.E. can work with dynamic password generators such as SafeWord MultiSync cards, which are reviewed on page 52. Users enter a number generated by A.M.E. into their token, which generates a response that the user enters back into A.M.E. If everything checks out, the user gets access.

Figure 2.7

A.M.E.

Date	Time	User	Action
11/11/91	3:41:48 PM	Admins...	Closed file "DA Handler Snip 01"
11/11/91	3:41:51 PM	Admins...	Multifinder switch to "Finder"
11/11/91	3:42:32 PM	Admins...	Deleted "DA Handler Snip 01"
11/11/91	3:42:32 PM	Admins...	Deleted "DA Handler Snip 00"
11/11/91	3:42:54 PM	Admins...	Created file "Finder Snip 00" in directory "Alliance™ ..."
11/11/91	3:42:54 PM	Admins...	Opened file "Finder Snip 00"
11/11/91	3:42:54 PM	Admins...	Wrote data to file "Finder Snip 00"
11/11/91	3:42:54 PM	Admins...	Closed file "Finder Snip 00"
11/11/91	3:43:13 PM	Admins...	Renamed "Finder Snip 00" to "A.M.E. DA"
11/11/91	3:43:14 PM	Admins...	Opened file "A.M.E. DA"
11/11/91	3:43:14 PM	Admins...	Closed file "A.M.E. DA"
11/11/91	3:43:14 PM	Admins...	Created file "A.M.E. DA" in directory "Virus Rx"
11/11/91	3:43:14 PM	Admins...	Opened file "A.M.E. DA"
11/11/91	3:43:15 PM	Admins...	Closed file "A.M.E. DA"

For all these virtues, however, A.M.E. is not without problems. First, the program is incompatible with some disk utilities, spoolers, and System extensions.

A.M.E.'s drive to be everything in a security program has its costs. A.M.E. has DES encryption, but because the program stores the key with the encrypted file, the implementation is insecure.

Finally, A.M.E.'s interface is complex and daunting. It requires a lot of work to set the program up, but you can't forget about it once you do. It offers a degree of security flexibility not found in other products, but spurious problems such as its failure during installation reported by various users make me leery of using this product.

At Ease

At Ease, from Apple Computer, is a System 7 extension from Apple Computer that ships with the Performa line, but it is available separately for other Macs. At Ease restricts access to the Mac by

replacing the Finder with a Finder Overlay, giving users a means of obscuring certain files. The program can prevent saving to the Mac's hard drive, forcing users to save files to floppies or to servers.

This is simple protection for simple applications, as starting the Mac from a floppy bypasses all security. Since it's widely distributed, almost everyone knows how to break At Ease, so don't depend on it as your sole means of security.

Bullet Proof 1.0

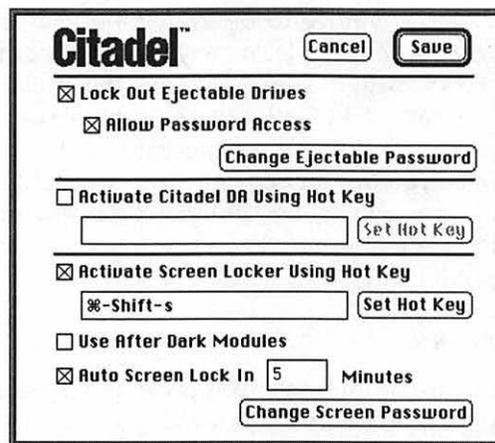
Bullet Proof, from Spectra Micro Development, is a simple application that can toggle on and off three attributes: locked, invisible, and protected. These attributes can apply to folders as well as files. Protected files and folders are visible and usable, but they cannot be moved, deleted or copied. A locked file or folder is visible but not usable. If this all seems simple and straightforward, it is. It is also easy to break, so I wouldn't recommend using it for any reason.

Citadel

Citadel, from Datawatch, is a complete security program, combining access control and encryption. You can encrypt files, lock up hard drive volumes, prevent people from accessing the floppy drive, erase files, and lock the screen. It even comes with a file erasure utility, Shredder (see Chapter 4), and both are also part of the SuperSet Utilities.

Figure 2.8

Citadel



Citadel lets you password-protect any SCSI volume, and any partition—passwords can be unique to each volume and partition. Additionally, you can also lock the floppy drive with a password so that, without the correct word, you can't copy files to or from your Mac.

The program gives you "vaults" to protect your files and folders, and each vault has its own password. Files can be moved into and out of unlocked vaults, and you can set the vaults to encrypt files using one of three algorithms: 1/4 DES, 1/2 DES, and full DES. DES is implemented in Cipher Block Chaining mode, an implementation that is more secure than the DES encryption in other products. For maximum security I recommend full DES, though the half-DES and quarter-DES options are sufficient to protect your data from most people.

Also included with Citadel is a screen and keyboard locker that locks either on command or after some specified period of inactivity. To reactivate the computer, you have to type in the password.

Because Citadel is designed for network use, it comes with an Administrator disk. This means *someone with this disk can open any drive locked with Citadel*, even if without the password.

This is an excellent security program because it provides good protection from screen locking all the way to encryption and file erasure. About the only drawback is that hard disk protection is pretty easy to break: Update the driver software and you can completely bypass volume protection. But with all it offers, including secure encryption, and its excellent price, I have to say I highly recommend this program.

CPU 2.0.3

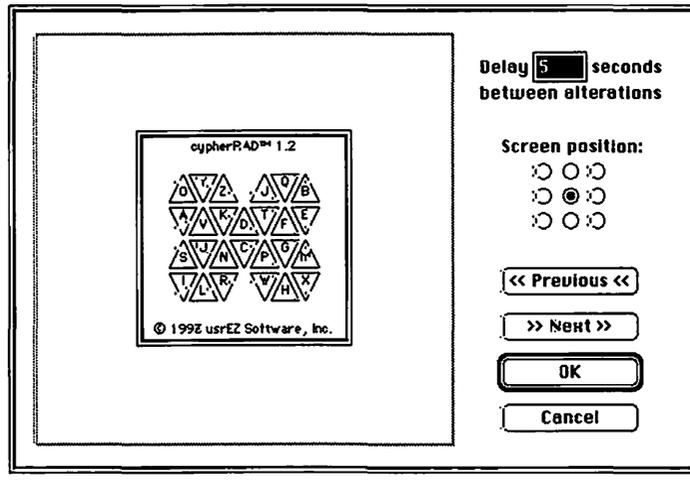
CPU, from Connectix, is a very simple password-protection utility designed for PowerBooks. It's easy to install, easy to use, and easy to break. Unless you are worried only about very naïve people, I'd recommend getting something stronger.

cypherPAD 1.213

What makes cypherPAD, from usrEZ Software, unique is a distinctive keypad scheme which constantly shuffles the letters around to prevent people from learning your password if they watch what you type.

Figure 2.9

cypherPAD



Otherwise, cypherPAD is a pretty basic package. It automatically locks your machine on shut-down or after a predetermined period of inactivity. You can also lock manually from the keyboard or with the mouse. It has a audit log and an internal virus checker, and prohibits booting from floppies.

Like all other programs in this chapter, cypherPAD can be bypassed. Still, its cool screen makes it worth using.

DiskGuard 1.0

Network administrators will like DiskGuard, from ASD Software, because of its remote installation that allows them to install, configure, and manage the program all from the confines of their own Mac desktops.

This software can password-protect one or several hard drives. Since DiskGuard is not an extension, the Control Panel can be removed after installation without affecting the protection.

DiskGuard offers three levels of access: network administrator, administrator, and user. Users occupy the lowest level of access with individual passwords while administrators have master passwords, which can give them access to some or all users. At the top of the hierarchy are network administrators who can define a single master password for the entire network.

An administrator can set additional features. For instance, she can configure passwords to be valid only during working hours and thus restrict hard drive usage to those times. She can set write-protection, which allows users to read from the hard drive

but not write to it. She might restrict file saves to an unprotected volume or to floppies. She can set a minimum length for passwords, and force a password to be changed.

DiskGuard has a keyboard and screen locker which works in much the same way as a screen saver does—they are enacted after a specified period of inactivity or when the mouse is placed in a pre-determined corner of the screen.

The program also generates a user log, which will track the use of a hard drive even if it is moved from one Macintosh to another.

DiskLock 2.12

DiskLock, from Symantec, locks up just about everything—any SCSI hard disk drive at the driver level, any and all partitions on your hard drive, and files and folders.

With files and folders, the software automatically asks you for the password when you double-click the file's icon. After you enter the password, the program launches the proper application and opens the unlocked file. When you shut down your Mac, DiskLock can relock all unlocked files and folders. Locked files cannot be thrown away, moved, written over, or renamed. Should you forget your password, DiskLock has a master password option that will allow you to get to your files.

DiskLock includes a password-protected screen locker, which can be set to secure your system after a certain period of inactivity. This screen lock lets you continue to run background jobs while it is active.

In addition, DiskLock keeps an audit log, recording each time a disk is locked and unlocked, and all unsuccessful log-on attempts. Another nicety is that the program checks itself for viruses and other forms of corruption each time it runs, and it includes on-line help, and a well-written manual.

DiskLock has three different levels of protection for files and folders beyond locking: FastLock, and two encryption schemes. FastLock, which is not an encryption scheme, uses patches in the file system to keep people out. Additionally, the program has DES encryption as well as a proprietary algorithm.

Although the program implements DES correctly, it stores the DES key with the encrypted file, so someone can decrypt your file without first knowing the key. This leaves the proprietary algorithm, which is unreliable. If you want the security of encryption, buy another product. If you don't need encryption, DiskLock is a good choice.

DiskLock PB 1.0

DiskLock PB, from Symantec, is a version of DiskLock for PowerBooks. It locks only hard drives, not files or folders. And besides locking at shut-down, it also locks when the PowerBook goes to sleep.

DiskMaker 1.6.5

DiskMaker, from Golden Triangle Computers, is a universal SCSI utility that contains some security features, including the ability to set passwords for individual partitions or entire drives. These password-protected volumes can mount at start-up or on demand. In the case of the start-up volume, you must enter the correct password to start the machine. Finally, DiskMaker has a master password option. This password protection can be overcome, but it can defeat the mildly curious.

Figure 2.10

DiskMaker



Drive 7 3.0

Drive 7, from Casa Blanca Works, is a universal SCSI utility with some security features. You can password-protect for individual partitions on a hard drive or entire drives, and these volumes can mount at start-up or on demand. If you password-protect the start-up volume, you have to enter the correct password to start the machine. Drive 7 also has a master password option.

Empower I 4.1.1

Empower I, from Magna, is part of a family of Macintosh access-control products which also includes Empower II and Empower

Remote. Of these, Empower I provides the lowest-level of security, but it is still a comprehensive product.

Users must register their ID and password with the program before they can use a Macintosh, and Empower I demands a password every time the machine is started, restarted, or after a screen lock-out. The program has an optional feature to prevent users from choosing simple passwords by requiring, for instance, a minimum length or non-alphabetic characters.

The screen-lock mechanism is activated by a manual command or after a pre-defined period of inactivity, and this lock allows background operations such as printing, electronic mail, and backups to operate normally.

An additional level of security comes from the program's floppy drive disable option which both prevents someone from starting up a Mac with a floppy System disk and controls the use of floppies after start-up. A comprehensive audit log records various events, including access attempts, user activities, administrator activities, security violations, and Macintosh events. The log can also monitor the start and stop times of various applications by project names, and Empower I lets you export and print the audit log.

All of Empower I's security measures can operate along a network, and the network manager can set all of the operations and options through the administrator mode. As the manager, she is the only one who can change security options and grant access privileges to new user-IDs. The network manager also has a special override and unlock capability to access protected volumes if users inadvertently lock themselves out.

Perhaps the best level of security in Empower I is encryption. The proprietary algorithm is not secure enough to bother with, but the DES option is good. However, to use DES you must turn off all the fail-safe options, otherwise, you are not getting the security of DES. Aside from DES encryption, all security features of this program can be bypassed.

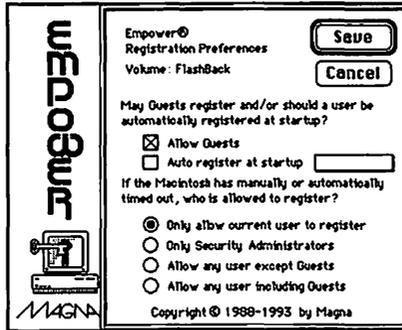
Empower II 4.1.1

Empower II, from Magna, has all the features of Empower I, with the addition of comprehensive access controls. You can customize security by choosing who, if anyone, may access specific folders and files. You can even allow guest users to register and give them access to unprotected data.

Folder-level access controls limit who can see and make changes to folders and files, including System and Application folders. Access privileges can be designated for "guests," "registered users," and "groups." You can control access to Desk Accessories or Apple menu items, and limit the launching of special applications such as powerful utility programs, on a per-user basis.

Figure 2.11

Empower II

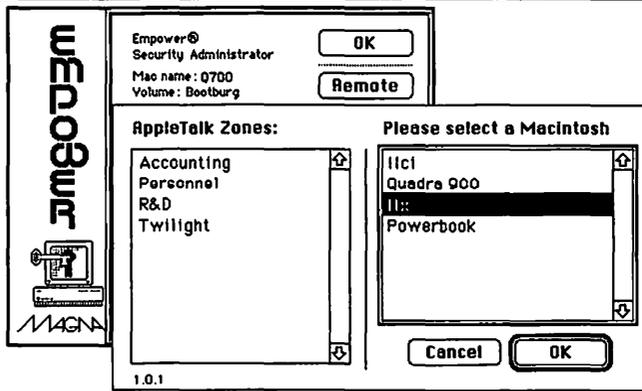


Empower Remote 4.1.1

As the name would suggest, Empower Remote, from Magna, is designed for use on a remote Macintosh, but this does not diminish its functions as it has all the features of Empower II. Remote can allow for control of an individual Mac or several Macs along a network. In this way, it is a great tool for a network administrator and her staff, as the system administrator under Empower Remote can be on any individual Macintosh. From her own Mac desktop, the administrator can manage every Macintosh on

Figure 2.12

Empower Remote



the network that is running Empower and perform such operations as verifying or changing security options, adding or removing users, and examining audit logs.

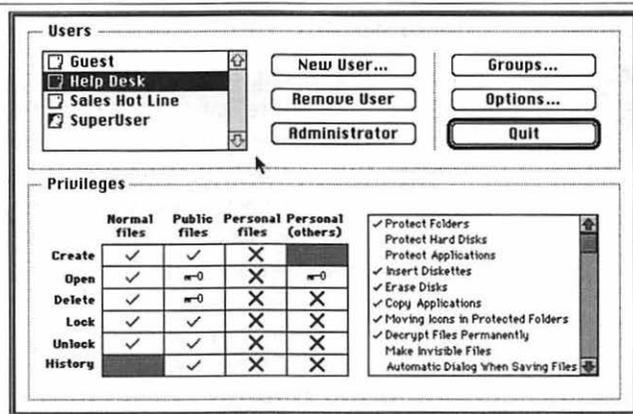
FileGuard 2.7.8

FileGuard, from ASD Software, is an access-control product that operates primarily in the background. Beyond password protecting folders, applications, files, and entire hard disk drives, FileGuard is designed to work with MaccessCard Reader, a physical security system (reviewed on page 48) that reads magnetic cards, not passwords, to authenticate users.

For networks, an administrator sets access privileges for each user, including the ability to create, open, delete, lock, or unlock files, as well as modify the Desktop and insert floppies. FileGuard can run a constant check on users: They can be required to re-enter their password at regular intervals if the administrator sets this option. FileGuard automatically locks the computer if no registered user is recognized.

Figure 2.13

FileGuard



The program prevents unauthorized access to, copying, and erasure of the hard disk drive. You can set access privileges to folders, including the System folder. Users can have access to certain folders, and folders can be write-protected or set up as drop folders. The program also lets you protect files. Upon saving a new document, FileGuard gives you the option to password-protect it. Opening password-protected documents adds just one more step to launching files, entering the password. As with many other programs, FileGuard has a master password option for emergencies.

As a protection against piracy, FileGuard offers both password and copy protection for all applications on your hard drive. Under password protection, the protected application retains this security on another drive even if FileGuard isn't installed there. However, if you choose copy protection, the protected application will run only on your hard drive. Additionally, you can protect applications with a time limit: A copy of an application will run for only a week, for example.

A screen-locking feature locks the screen with a screen saver until an authorized user needs to gain access. FileGuard also has an audit log that keeps a continuous activity record for all users including file creation, total use time, and attempts at unauthorized access. You can view the log, perform multiple searches, and export the user log data to a word processor or spreadsheet.

Although FileGuard has encryption, it is not DES encryption and is not secure, so don't use this feature. But then all of FileGuard's security measures can be bypassed by someone with enough expertise. Still, it provides good security against most adversaries.



FolderBolt 1.02e

Although FolderBolt, from Kent•Marsh, is designed to protect folders and not entire hard drives or individual files, it is amazingly flexible. You can specify three levels of folder protection: read-only folders to hold documents that can be read but not altered without a password; drop folders where anyone can deposit files, but only users with the password can read or delete them; and—most secure—password-protected folders where a password is required to do anything to files inside them.

Additionally, you can lock the System Folder, Control Panels, Extensions, the System 7 Trash, or the Chooser. You can specify several folders to be dealt with as a set, allowing you to handle them collectively at start-up or shut down by entering a single password. You can specify a minimum password length, how passwords are displayed when typed, whether they're case-sensitive, and whether they should be verified when first entered. And when you shut down, FolderBolt can automatically relock all folders.

Locking and unlocking folders is easy. You open the Control Panel, click on the Lock a Folder button, select a folder from a dialog box, choose the level of protection, and assign a password. To unlock your folders, you can use FolderBolt's control panel, or

you can unlock folders directly by just double-clicking on them and entering the password.

Should problems like lost passwords arise, FolderBolt's Administrator can save you. With this program, you can unlock any folder, set of folders, or every locked folder on the drive. A special password is required to run the Administrator, which is also needed to access the audit log. This file monitors successful and unsuccessful attempts to access any locked folder.

Folder Locker 1.2.8

With Folder Locker, from Software Brewing Company, you can password-protect folders, into which anyone can place files but from which only the password holders can delete or copy files. It also provides an option for locked folders without drop options. The System Folder can be protected by placing it inside a locked folder: This prevents user access while still allowing the System to function normally.

Hard Disk ToolKit 1.5

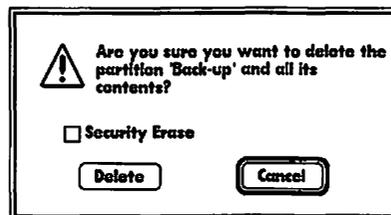
Although it's not primarily a security package, the Hard Disk ToolKit, from FWB, includes some security features. You can partition a large disk into several smaller volumes, each of which can be protected with a password. Once the partitions are created, users will be prompted for one or more passwords when starting up the Mac. A higher level of security is also afforded through write-protection of partitions as well as encryption. However, the encryption is not very good—an experienced cryptographer can break it easily.

The ToolKit includes HDT Util that offers file- and folder-level protection. Protected files, applications, and documents can be launched like regular files but not duplicated or moved. Protecting a folder protects every file in that folder.

None of what Hard Disk Toolkit offers is sophisticated protection, but it is the best security of all the SCSI utilities.

Figure 2.14

Hard Disk Toolkit



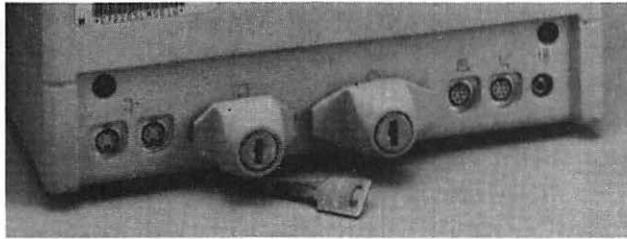
Keylock Mac 4.0

Keylock Mac, from Keylock, protects hardware and software. The software is based on MacPassword, a basic password-protection program with some useful options (discussed on page 49). It locks both individual files and folders, sets up guest access (locked files and folders become invisible), and sets up an audit log. Keylock's software also has an administrator option, allowing a network manager to bypass the user's password, and it has optional minimum requirements for password length.

For hardware, the package comes with physical locks that prevent access to the floppy drive, SCSI port, and serial port. These locks are decent—it took a locksmith a few minutes to pick them.

Figure 2.15

Keylock Mac

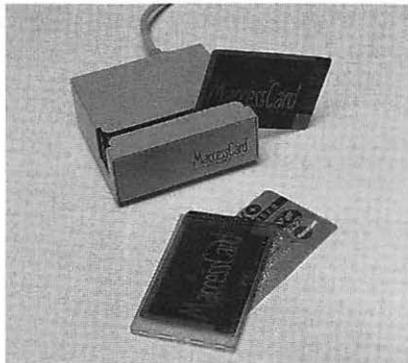


MaccessCard Reader

MaccessCard, from ASD Software, is a card reader designed to be used with FileGuard. Instead of logging on by entering a name and password from the keyboard, users log on in less than a second by sliding a magnetic card through the reader and, optionally, entering a password. The device connects to the Mac through the Apple Desktop Bus (ADB) port.

Figure 2.16

MaccessCard
Reader



You have the option of using the cards packaged with the reader or training the system to recognize any identification card bearing a magnetic strip including bank cards, credit cards, and company identification cards.

MaccessCard is a good protection measure for a lot of environments, though, as with any other product mentioned in this book, it can be bypassed by a clever adversary.

MacPassword 4.0

MacPassword, shareware from Evergreen Software, can lock hard drives as well as individual files and folders. People who don't know the password cannot access the machine, although there is an option for allowing guests to log on with minimum access privileges.

The password options can enforce a variety of parameters for creating, maintaining, and using passwords. For example, it can be set to prompt you to change your password after some interval. It also remembers old passwords and lets you know when you enter one that has already been used. An administrator override capability allows an administrator to access the secured matter if a user forgets his password.

MacPassword comes with a screen locker that allows all background tasks to run while it is active. The program has an encrypted audit log which can be printed, and it comes with a virus-protection option which loads virus detection software into memory during start-up. MacPassword also provides the software for the Keylock Mac access-control system discussed on page 48.

Like all other access-control programs without encryption, MacPassword can be broken. However, it offers a nice array of features at a very attractive shareware price. Please remember to pay the fee.

MacSecure

MacSecure was a Finder Overlay aimed primarily at the educational market. The product is no longer available, and Learning Performance Corp. is out of business.

Menu Master Mac

Like MacSecure, this is a Finder Overlay that restricts access to the Mac by selectively blocking access to the hard disk drive. But unlike MacSecure, Menu Master Mac is still supported by its developer, Electronic Learning Systems.

NightWatch II 2.5

NightWatch II, from Kent•Marsh, keeps unauthorized users from accessing the hard drive. It supports multiple passwords, so it allows many users to securely work on one Mac.

The program has three access-control options: password; key disk, which you insert to unlock the hard drive without a password; and token disk, which requires insertion of a key disk plus a correct user-ID and password.

System administrators using NightWatch II can designate which users can have access to which data: different people can have access to different areas of the drive. Moreover, you can specify which days of the week and what time of the day a particular person has access to the hard drive. An administrator disk lets a network manager—or anyone with the disk—override the security features in case someone has forgotten his password.

NightWatch II lets you configure the hard drive to lock on shutdown or at a predetermined time of the day, and it has an audit log that monitors all attempts to log on to the system. The program also has a screen locker which isn't trivial to bypass, and the hard drive lock is even more difficult to unravel. However, neither is infallible.

Norton Partition

Norton Partition, part of the Norton Utilities for Macintosh 2.0, from Symantec, allows you to create disk partitions, and to give each of those partitions a password. This isn't heavy-duty security, but it will work to keep out most unauthorized users.

Passport 3.0

Passport, from Praxitel, is a simple password-protection program. You enter a password at start-up to gain access to the Macintosh, and the program automatically locks the machine on shut-down.

There are no options to choose between files and folders, and there is no screen locker. Still, the program tracks the number of unauthorized attempts to access the system, and a "No Floppies" option will prevent a user from mounting any floppy in the floppy drive.

PassProof 1.02

PassProof, from Kensington Microware, is a comprehensive program that combines hardware and software protection. Its features work in the background and don't inhibit authorized use.

Hard disk access control is implemented by a password. Administrators can pick a master password, which serves as your key to unlock the entire system. You can then let other users on the Macintosh by assigning them individual passwords. With the master password, you can add and delete users at any time as well as make certain files invisible. A user log keeps a complete list of all attempts to access the computer, as well as other activities and their day, date, time, and user.

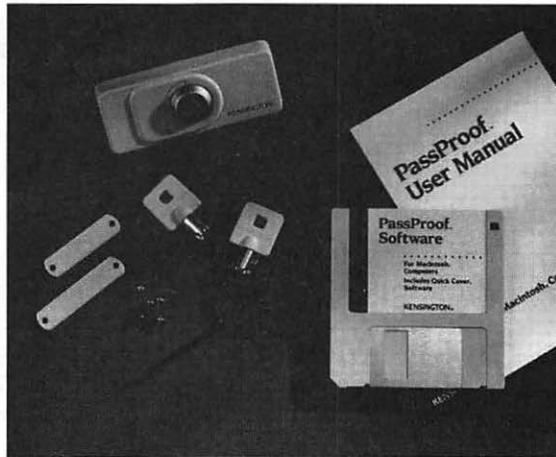
PassProof also includes a screen locker, which automatically blanks the screen when activated. Oddly, this locker includes an option to let users back into the Mac without a password, and that would mean the Mac isn't truly protected.

It's a good thing that PassProof includes hardware locks because all its software protections can be broken. A locking device using a round key physically prevents access to the hard disk drive. A good locksmith spent a few minutes before he was able to open them. In addition, metal security plates with tamper-proof screws block access to the floppy and SCSI ports.

PassProof has four different versions, each distinguished by the Macs on which it will work: One for the Mac SE, SE/30, and Mac II right-hand drive; one for the Mac IIci, IIcx, and Mac II, IIx, IIfx left-hand drive; another for the Mac Classic and the Performa 200; and finally one for the Mac IIsi.

Figure 2.17

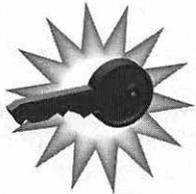
PassProof



Mac II owners with two drives should purchase PassProof for Mac SE and Mac II right-hand drive, and PassProof for Mac IIc computers and Mac II left-hand drive, as each drive requires a different hardware locking device. All other Mac owners with two drives should call Kensington for information on purchasing a second locking device.

Power Utilities 1.0.5

Power Utilities, from AIsoft, contains MultiDisk, a disk partitioner which assigns a unique password to each partition. This isn't exactly sophisticated protection, and it can be bypassed with ease. Still, it will protect your drive from the naïve but curious.



QuickLock 2.1

QuickLock, from Kent•Marsh, is a screen locker that password-protects your screen and network connections. You can activate QuickLock through a number of means, including using a command key, or by setting it to engage at a specific time during the day. QuickLock also has a screen saver to prevent phosphor burn-in, and background processes can continue even when the screen is locked.

In addition, QuickLock records all attempts to access the Mac. Password protection remains in effect even after power interruptions and system restarts, and this program allows users to leave messages on the screen and in the password dialog box.

This is not a program to be used as your sole means of security, since it is one of the easiest to break. Fortunately, QuickLock works smoothly in conjunction with NightWatch II. Using both programs together allows QuickLock to call the shut-down command at a specified time, and then hand off to NightWatch II for hard disk security. But then, NightWatch II has its own screen-locking mechanism.

SafeWord MultiSync card

The SafeWord MultiSync card, from Enigma Logic, is a hand-held, dynamic password generator that works with comprehensive programs like A.M.E. The user enters a number generated by A.M.E.'s software into the card, which then generates the dynamic password that they enter into the Macintosh. This is how the Mac verifies that you are the one with the card—the password is different

for each challenge. This system is more secure than simple passwords because an adversary must steal both the password and the MultiSync card.

The MultiSync card is packaged in a credit-card-sized plastic case that is about an eighth of an inch thick. It has a numeric keypad for entry of PINs and Challenges, and an eight digit LCD that displays passwords.

Figure 2.18

MultiSync Card



SecureInit 2.5A

This is a simple password-protection INIT that prompts a user for the password at start-up and which includes a screen locker. Despite these two levels of security, SecureInit, from Direct Software, is easy to get around: just boot from a floppy.

Silverlining 5.1

Silverlining, from La Cie, is a hard disk driver and utility package that includes a password feature. You can partition a large disk into several smaller volumes, each of which can be protected with different passwords. Since this program is primarily driver software, protection is secondary. Thus, the security isn't very sophisticated and can be disabled with a little work. Still, it's easy to use and will keep out the idly curious.

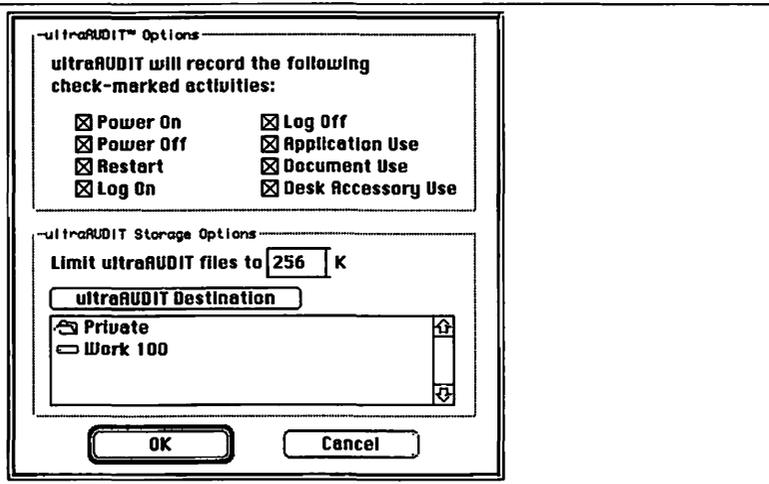
ultraSECURE 3.0

ultraSECURE, from usrEZ Software, is a complete access-control and encryption program that happens to be my favorite. It offers a wealth of features that will probably satisfy your every security need.

Because the program is built on the idea of a hierarchical user chart, assigned access privileges can mirror the security structure in your organization. So, at the top you might have the security administrator who has access to all the Macs in the whole organization, followed by a group of supervisors who would have access to those machines belonging to those who reported to them, and finally there would be those at the bottom of the hierarchy who have access only to their own machines. This rigid structure is powerful but limiting: users at the bottom level cannot have secure personal files. People above them in the hierarchy can always read their files.

Figure 2.19

ultraSECURE



The security administrator has a lot of flexibility in setting up privileges among users. He can restrict floppy-drive access, floppy initialization, SCSI initialization, file and folder creation, file and folder deletion, file and folder renaming, rearrangement of the Desktop, use of DAs, and use of the programmer's switch. These privileges can be changed for each level on the chart.

The administrator can also exercise various options for password usage, including setting a minimum password length and setting some form of system reaction to log-on failures. In addition, the administrator can add or delete users, or change the set of privileges that each level of users have.

The auditing capabilities of ultraSECURE include records of who has logged on and off the system and when, any unsuccessful log-on attempts, and what documents and applications were opened by which users. The audit log can be exported as a text file.

Part of what makes ultraSECURE so secure is its support of encryption. There's a proprietary algorithm called ultraCRYPT, DES, and double-DES. I cannot recommend ultraCRYPT or any other proprietary encryption method. You shouldn't bother with double-DES, either. Use DES: it's the standard and the very best encryption available now (see Chapter 3 for more on encryption).

But there's more to tight security than encryption. ultraSECURE not only lets you password- and copy-protect applications, but it also lets you give applications a "poison pill": an application can be copied to a floppy, but the copy will only work for a limited time before self-destructing. ultraSECURE also comes with a file erasure utility, and the most basic of virus prevention programs.

This is an excellent security program. It is complete, comprehensive, easy-to-use, and very effective. Its only drawback is the rigid hierarchical structure. If you can live with that, this program is an excellent choice.

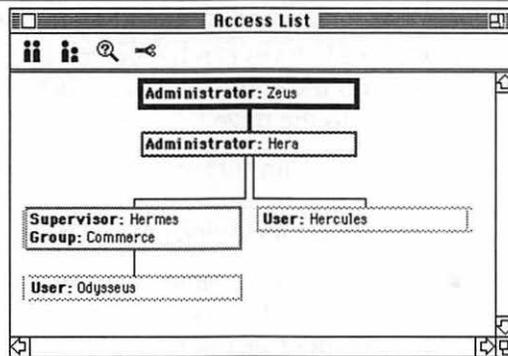
Aside from this DES encryption, all security features of ultraSECURE can be bypassed. But to the program's credit, bypassing them takes a whole lot of work and a whole lot of skill.

ultraSHIELD 2.0

ultraSHIELD, from usrEZ Software, is an easy-to-use and comprehensive security program for the Macintosh. It shipped too late to be reviewed for this book, but according to the product literature, it has password protection, user and guest privileges, activity logs, screen locking, anti-viral protection, folder- and file-locking, and DES encryption, and it can erase files to Department of Defense (DoD) specification.

Figure 2.20

ultraSHIELD



Considering All the Factors

Remember, no access-control program is foolproof. Someone can always write a program that can break in, even if you don't think your adversaries have the time or expertise to do it themselves. Sometimes, the authors of these security-breaking programs post them to BBSs, allowing anyone who wants a copy of the application to have it. If you are using the access-control program that was just broken, you've just lost any semblance of security you may have had.

For some of you, this scenario sounds too paranoid, but it is very plausible to others. If you can't afford to take the risk, then you have no choice but to look at encryption.

Chapter 2 Summary

- Access control keeps confidential files private, protects your system against intruders who could do mischief or worse, and keeps the work of different users on one computer separate.
- Security on the Macintosh is a trade-off between controlling access to the computer and the easy-to-use Macintosh interface.
- The first defense is to keep others from getting access to that data. Access-control software has three main functions: to prevent access, to provide separation, and to keep an audit log.
- Passwords must be protected and kept secret, must not be easy to guess, and must be changed regularly.
- Hard disk drives can be secured by using software that requires the correct password before allowing user access to the drive.
- Screen locking software requires a password to access the hard drive. Some of these programs also lock the screen after an interval of inactivity.
- Finder Overlays simplify the Mac interface, and can allow administrators to display only certain files. They provide poor security.

- Folder locking software allows only those with the password to open a folder, take files from a folder, or write to a folder.
- Privileges-limiting software has options that include: copy protection, deletion protection, modification protection, “poison pills,” application restriction, and floppy drive disabling, and allows guest log-ons.
- An audit log tracks who has been on a system and what they did, as well as any unsuccessful log-on attempts. Some software can encrypt the audit log.
- Some software comes with hardware locks.
- Some software is obsolete, unsupported, or so easily defeated as to be not recommended. These products include At Ease, Bullet Proof, MacSecure, SafeLock, and SecureInit.

Chapter 2 Sources

Access Managed Environment (A.M.E.) 2.1.8, \$159.00

Casady & Greene, Inc.
22734 Portola Drive
Salinas, CA 93908
(408) 484-9228
FAX: (408) 484-9218

At Ease, \$59

Apple Computer, Inc.
20525 Mariani Ave.
Cupertino, CA 95014
(408) 996-1010
FAX: (408) 996-0275

Bullet Proof 1.0, \$5

Spectra Micro Development
P.O. Box 41795
Tucson, AZ 85717
(602) 795-7288

Citadel with Shredder, \$99

SuperSet Utilities, \$149
Datawatch Corp.
Triangle Software Division
P.O. Box 13984
Research Triangle Park, NC 27709
(919) 549-0711
FAX: (919) 549-0065

CPU 2.0.3, \$99

Connectix Corp.
2600 Campus Drive
San Mateo, CA 94403
(415) 571-5100
(800) 950-5880
FAX: (415) 571-5195

cypherPAD 1.213 \$49

usrEZ Software
18881 Von Karman Ave, Suite 1270
Irvine, CA 92715
(714) 756-5140
FAX: (714) 756-8810

DiskGuard 1.0, \$140

ASD Software, Inc.
4650 Arrow Highway, Suite E-6
Montclair, CA 91763
(909) 624-2594
FAX: (909) 624-9574

DiskLock 2.12, \$189

Symantec Corp.
10210 Torre Ave.
Cupertino, CA 95014
(503) 334-6054
(800) 441-7234
FAX: (503) 334-7471

DiskLock PB 1.0, \$59

Symantec Corp.

DiskMaker 1.6.5, \$99

Golden Triangle Computers
10855 Sorrento Valley
San Diego, CA 92121
(619) 279-2100
(800) 326-1858
FAX: (619) 279-1069

Drive 7 3.0, \$89.95

Casa Blanca Works
148 Bon Air Center
Greenbrae, CA 94904
(415) 461-2227
FAX: (415) 461-2249

Empower I 4.1.1, \$169
Empower II 4.1.1, \$296
Empower Remote 4.1.1, \$396

Magna
1999 S. Bascom, Suite 810
Campbell, CA 95008
(408) 282-0900
FAX: (408) 879-7979

FileGuard 2.7.8, \$249
ASD Software, Inc.
4650 Arrow Highway, Suite E-6
Montclair, CA 91763
(909) 624-2594
FAX: (909) 624-9574

FolderBolt 1.02e, \$129.95
Kent•Marsh Ltd.
3260 Sul Ross
Houston, TX 77098
(713) 522-5625
(800) 325-3587
FAX: (713) 522-8965

Folder Locker 1.2.8, \$30
Software Brewing Company
270 Apricot Lane
Mountain View, CA 94040
(415) 940-1946

Hard Disk ToolKit 1.5, \$199.95
FWB, Inc.
2040 Polk St., Suite 215
San Francisco, CA 94109
(415) 474-8055
FAX: (415) 775-2125

Keylock Mac 4.0, \$89
Keylock, Inc.
8129 W. Highway 34
Loveland, CO 80537
(303) 667-4444
(800) 366-2515
FAX: (303) 663-7242 or 011-46-586-52016

MaccessCard Reader 1.0, \$349
ASD Software, Inc.

MacPassword 4.0, \$35 shareware
Evergreen Software, Inc.
15600 NE 8 St., Suite B1126
Bellevue, WA 98008

Menu Master Mac, \$99
Electronic Learning Systems, Inc.
4131 N.W. 28th Lane, Suite 3A
Gainesville, FL 32606
(904) 375-0558
(800) 443-7971
FAX: (904) 375-5679

NightWatch II 2.5, \$159.95
Kent•Marsh Ltd.

Norton Utilities for Macintosh 2.0, \$149
Symantec Corp.
10210 Torre Ave.
Cupertino, CA 95014
(503) 334-6054
(800) 441-7234
FAX: (503) 334-7471

Passport 3.0, \$49.95
Praxitel, Inc.
P.O. Box 452
Pleasanton, CA 94566
(510) 846-9380

PassProof 1.02, \$99.95
Kensington Microware Ltd.
2855 Campus Drive
San Mateo, CA 94403
(415) 572-2700
(800) 535-4242
FAX: (415) 572-9657

Power Utilities 1.0.5, \$129

AlSoft
22557 Aldine Westfield, Suite 122
Spring, TX 77373
(713) 353-4090
(800) 257-6381
FAX: (713) 353-9868

QuickLock 2.1, \$29.95

Kent•Marsh Ltd.

SafeWord MultiSync Cards, \$34-\$44

Enigma Logic, Inc.
2151 Salvio St. #301
Concord, CA 94520
(510) 827-5707
FAX: (10) 827-2593

SecureNit 2.5A, \$99.95

Direct Software, Inc.
100 S. Sunrise Way, Suite 407
Palm Springs, CA 92262
(619) 778-6555
FAX: (619) 778-6557

Silverlining 5.1, \$149

La Cie Ltd.
8700 S.W. Creekside Place
Beaverton, OR 97005
(503) 520-9000
FAX: (503) 520-9100

ultraSECURE 3.0, \$239

ultraSHIELD 2.0, \$149

usrEZ Software, Inc.
18881 Von Karman Ave, Suite 1270
Irvine, CA 92715
(714) 756-5140
FAX: (714) 756-8810



Encrypting Your Data

Access-control programs can be broken, some more easily than others. If you want the best Mac security available today, then encryption is your only option. Encryption is a mathematical operation that scrambles your data so that no one, except you or someone you designate, can read it. Even if an adversary breaks into your office, bypasses your computer's access-control features, and steals the entire hard drive, all he will be able to read is gibberish. He can disassemble your encryption software and spend millions of years trying to break the algorithm. Your files will remain secure.

Encryption Terminology

Plaintext: The message or file to be encrypted, an unencrypted file.

Ciphertext: The message or file after it has been encrypted, an encrypted file.

Encryption Algorithm: The mathematical operation used to turn plaintext into ciphertext.

Decryption Algorithm: The mathematical operation used to turn ciphertext back into plaintext.

Key: The secret piece of information needed to encrypt plaintext and then decrypt ciphertext. If the file is sent from one person to another, the key is a secret shared by the sender and the receiver.

Cryptography: The study of making encryption algorithms.

Cryptanalysis: The study of breaking encryption algorithms—turning ciphertext back into plaintext without the benefit of the key.

Cryptology: cryptography and cryptanalysis.

Secret-Key Algorithm: An encryption and decryption algorithm which uses the same key for both operations. Also known as a Private-Key Algorithm.

Public-Key Algorithm: An encryption and decryption algorithm which uses different keys for each operation.

Back Door: A secret attribute of an encryption algorithm that lets someone who knows it decrypt the ciphertext without the key. Also called a Trap Door.

At least, they will if you buy a good encryption product. There are two kinds of encryption you might buy: encryption that stops your kid brother from reading your files, and encryption that stops major governments from reading your files. Any algorithm that falls in the middle just takes time and money to break.

Think about your data. Would a disgruntled employee spend \$3000 worth of time to break into your database? Is it worth \$30,000 for someone to crack his ex-spouse's financial records in a nasty divorce case? Is it worth \$300,000 for a multinational corporation to get the marketing strategies of its major competitor? If someone could be willing to spend large amounts of money to steal your data, then you need good encryption.

Choosing an Encryption Algorithm

Encryption is based on the idea of an algorithm and a key. An encryption algorithm is a mathematical function that uses the key to scramble the message, called plaintext, into unreadable ciphertext. On the other end, the algorithm uses the key to unscramble a ciphertext message into plaintext. Someone with the ciphertext and the algorithm, but not the key, cannot read the message.

Passwords and Keys

Many security products use the words "password" and "key" interchangeably. They are different. A password is something you enter to gain access to the computer, or to a specific folder or partition or hard drive. A key is something you enter to decrypt a file or group of files. Even though the manuals for some security programs use the word "password" to mean "key," I will make the distinction in this book.

Some comprehensive security programs, which include password protection and encryption, use the password as the encryption key. This is not good security. The encryption key should be different than the password.

In any good encryption product, all the security is based on the secrecy of the key. There is no inherent security in keeping the algorithm secret. The algorithm should be public, so that other people can examine it and test its security. If any company refuses to reveal the mechanics of their encryption algorithm, claiming that it is proprietary, you should be suspicious of their products.

First off, there is no real secrecy in an algorithm that is secret. Anyone who wants the algorithm in order to break the encryption can easily get it. If someone wanted to know how a "proprietary" algorithm worked, it would take her only a few hours' work with a disassembler program.

In addition, algorithms that look secure are often not. The only way to ensure that an algorithm is secure is through peer review: publishing the algorithm and letting the world's best cryptographers examine it. Anyone who claims that his algorithm is secure without doing that is either a genius or a fool.

Types of Cryptographic Attacks

An attempt to break an algorithm is called an attack. There are three types of attacks:

Ciphertext-only: The cryptanalyst has in his hands the ciphertext of several files or messages that already have been encrypted with the same key and the same algorithm. His job is to recover the plaintext to as many files as possible or, better yet, deduce the key used to encrypt the files. This way, he can decrypt other files encrypted with the same key.

Known-plaintext: The cryptanalyst has both the ciphertext of several files and the plaintext of all or parts of those files. By comparing these files, he recovers the key used to encrypt them, so he can decrypt other files encrypted with the same key.

Chosen-plaintext: This is similar to a known-plaintext attack, except that the cryptanalyst can choose the plaintext files to be encrypted. For example, he can bribe someone to encrypt his own plaintext.

Known-plaintext attacks led to the breaking of the German Enigma machine during World War II. When trying to break a Japanese code during the same war, cryptanalysts fed remote Japanese posts false information in an attempt to get them to encrypt certain words.

On computers, many files have standard beginnings and endings that might be known to a cryptanalyst. "Dear Sir" might be a common beginning; a standard signature is just as vulnerable. Computer source code is full of known plaintexts: "#define," "struct," "else," and many others.

All of these attacks assume that the cryptanalyst has full access to the details of the algorithm. While this is not always true in military cryptanalysis, it is usually true with computer programs. It only takes a few hours to disassemble a proprietary encryption program and figure out the algorithm. A secure algorithm is secure even in the face of that.

Given the number of Macintosh encryption programs on the market, there are surprisingly few encryption algorithms to choose from. Most products offer DES and at least one proprietary algorithm.

You should stay away from the proprietary algorithms. Almost all of the proprietary algorithms used in Macintosh encryption products are some variant of the Simple XOR. To secure a file, XOR encrypts each byte of the plaintext with a byte of the key. To open the file, XOR decrypts each byte of the ciphertext with a byte of a key. It's lightning fast but appallingly easy to break—and it was, by the Union Army during the Civil War.

The companies that write encryption software rarely hire a cryptographer to do their cryptography work. Instead, they assign a staff programmer the task of writing an encryption algorithm. It is most likely that the programmer doesn't know any cryptography theory or theoretical mathematics, and he hasn't a clue how to proceed. His only guide is some peer review, but his peers are no more knowledgeable in the field than he is. The result is something that looks pretty good to a naïve observer, but something that can easily be broken by a trained cryptographer. So ignore all claims that it is "almost as secure as DES" because it isn't.

If you see an encryption product that advertises FEAL, Fast Encryption Algorithm, stay away from it. FEAL, developed at NTT Japan, is similar in design to DES. However, it has been broken. Two Israeli cryptographers, Eli Biham and Adi Shamir, developed something called differential cryptanalysis that can easily break FEAL. Although I have not seen it in any Macintosh encryption products, it has been used as a mainframe encryption algorithm. DES is far more secure than FEAL.

It's hard to trust anything in computer security, but if you have to trust something you might as well trust a lot of people who have been trained in cryptography.

Principles of Cryptography

The security of a cryptographic system should depend on the secrecy of the key and not the encryption algorithm. Anyone who refuses to make their algorithm public is only fooling himself as to its security. Steer clear of those algorithms.

The key must not be deducible from the ciphertext, from the ciphertext and the matching plaintext, or from the ciphertext of some plaintext that the analyst chooses. Assume that a cryptanalyst has a copy of both the plaintext and the ciphertext; if she still cannot deduce the key, then the algorithm is secure.

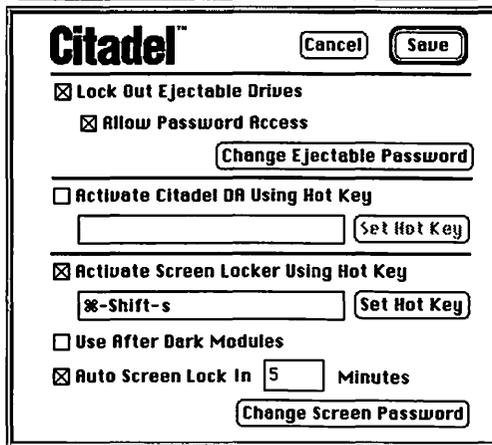
The upper limit on the amount of time required to break an algorithm is the time needed to try every possible key. If an algorithm uses a 32-bit key, then there are 2^{32} possible keys. If a cracking program can try a million different keys per second, that program will try every possible key in just over a minute. Clearly this level of security is unacceptable.

The Data Encryption Standard (DES) is a secret-key algorithm that has become an international standard. The algorithm was developed by IBM and the National Security Agency, and made public in 1975. Since then, countless cryptographers and mathematicians have analyzed it. Although DES is showing signs of age, it is still secure against all but the most powerful of adversaries. If you want to keep your Macintosh files secure, this is the algorithm you should use.

Many Macintosh products use DES encryption, and most implement it securely. The only way to break this encryption is to try every possible key in turn. Some security products implement DES, but allow for alternate ways to recover the key. Avoid these options.

Figure 3.1

Citadel DES Encryption

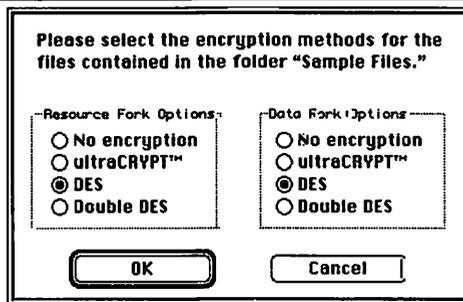


DES isn't the best algorithm. A DES-cracker can be built for about a million dollars. It tries every possible key in turn, and stops when it finds the correct one. No government or company has admitted to building this machine, but it probably exists in the basement of some military intelligence agency—possibly in the United States, the former Soviet Union, France, England, China, Israel, or Japan.

Currently, there is no public algorithm secure enough to replace DES. The military has several, but they are not forthcoming with their information. Candidates are out there, but none of them have been analyzed to the same extent that DES has. Most of these are protected by patents, making it illegal to use them without paying royalties to the patent owner. The U.S. government's Clipper chip with its Skipjack algorithm is thought to be more secure than DES, but the details of that algorithm are secret and it cannot be implemented in software. And even worse, Clipper's key management scheme is unacceptable to many users. For now, DES is the best alternative.

Figure 3.2

ultraSECURE Encryption



A DES variant that is known to be more secure is triple-DES. Using current technology, it would take a cracking machine 28 trillion years to try every possible triple-DES key—that's longer than the age of the universe. If you have data that must be secure against even the most powerful military intelligence agencies, use triple-DES and nothing less.

However, you should ignore something called double-DES. It takes twice as long to encrypt and decrypt, but it is no more secure than regular DES. Other DES variants to shy away from include half- and quarter-DES—they're not secure at all.

The Development of DES

The DES standard resulted from a program initiated in 1972 by NBS, the National Bureau of Standards (now NIST, the National Institute of Standards and Technology). This program called for the development of a single standard cryptographic algorithm to protect digital information—like computer and communications data—during both transmission and storage.

In 1973, the NBS got more specific and issued a public request for proposals for a standard cryptographic algorithm. Public response indicated that there was considerable interest in a cryptographic standard, but that there was little public expertise in the field. Some mathematicians sent in crude outlines of algorithms, but none of those came close to meeting the NBS requirements.

So, the NBS issued a second request in August 1974, which resulted in their receiving a promising candidate. It was an algorithm based on one developed by IBM during the early 1970s called LUCIFER.

The NBS requested the NSA's help in evaluating this algorithm's security, and to determine its suitability as a federal standard. Although IBM had already patented the algorithm, it was willing to make its intellectual property available to others for manufacturing, implementation, and use. The NBS worked out the terms of agreement with IBM and eventually received a non-exclusive, royalty-free license to make, use, and sell mechanisms that implemented the algorithm. Still, the algorithm was open to inspection, and the NBS invited feedback from agencies and the general public.

At first, many cryptographers were leery of the NSA's "invisible hand" in the development of the algorithm. They were afraid that the NSA had modified the algorithm and installed a back door. They complained about the inner workings of the algorithm and that the NSA reduced the key size from LUCIFER's original 112 bits to 56 bits.

Nevertheless, the Data Encryption Standard (DES) was adopted as a federal standard in 1976 and authorized for use on all unclassified government communications. It was later adopted as a standard by the American National Standards Institute (ANSI) and the International Standards Organization (ISO). ANSI and ISO call it DEA, for Data Encryption Algorithm, but it's the same algorithm.

Today, DES has been implemented in both hardware and software, although only hardware implementations can be certified by the NIST as conforming to the standard.

Other restrictions are in place as well. The U.S. Department of State and the NSA strictly regulate export of DES products. Although DES products are widely available overseas, the government rarely approves export. Financial institutions and foreign subsidiaries of U.S. companies are the only exceptions.

How Secure is DES?

The security of DES has been disputed since the NSA modified IBM's original design of the algorithm. Some cryptographers accused the NSA of secretly adding a back door, allowing only the NSA to break it. Others accused them of deliberately shortening the key to make it easier to break. The government classified IBM's design notes and refused to give reasons for any of the changes it made. This added fuel to the debate.

Today's DES has a 56-bit key. Unfortunately, some encryption product manufacturers insist that DES has a 64-bit key, but they are wrong. The specification for DES adds eight bits of error-checking (called checksum) to the key. The key, with its eight extra bits, is 64 bits in total, but only 56 of those bits are used to encrypt data. This means there are 2^{56} , or 72,057,594,037,927,936, or about 72 quadrillion, different possible keys to choose from.

DES can be broken by trying all of the 2^{56} possible keys. This is a "brute force" attack. The cryptanalyst simply encrypts the plaintext block with each of the 2^{56} keys until he finds a result that matches the known ciphertext.

A hypothetical special-purpose DES-cracking machine, one that could test a million keys per second, could recover a key in 2285 years. However, a million such chips, working in parallel, could recover a key in only 20 hours. But how feasible is this?

Estimates on the cost of a brute-force machine capable of finding a DES key within a day were estimated at \$46 million just a few years ago—not astronomically expensive, but still beyond the reach of almost everybody. However, new research by Michael Wiener at Bell-Northern Research in Ottawa shows that this estimate is significantly high.

Wiener went through the entire design process for a brute-force DES cracker, designing the custom cracking chip down to the gate level, and sending it out for bids. He designed a controller board and had its cost estimated. He designed and priced peripheral hardware, power supplies, racks, and a complete mechanical housing and found that he could build a machine for \$1 million that could break DES in 3.5 hours. If someone was willing to wait a day and a half for a key, he could build the machine for only \$100,000.

These numbers are not guesses. Anyone could take Wiener's design and add another \$500,000 for development costs and have the machine built in about ten months. (Bell-Northern insists that it has no intention of doing so.) At this price, it is

almost certain that the better military intelligence organizations have DES crackers in their basements, even though none have admitted to having one. DES is secure against all but the most well-funded major governments including the United States, the former Soviet Union, China, Israel, Germany, Japan, and North and South Korea. These countries, major corporations and organized crime all have the budgets to build a brute-force DES-cracking machine.

Additionally, the cost for a brute-force attack will decrease over time. If your data must remain secure for years, then DES is not secure enough for you.

The last couple of years have seen new attacks against DES develop—differential cryptanalysis and linear cryptanalysis. Theoretically, these attacks are more efficient than brute force, but they require an enormous amount of ciphertext to work—about one hundred terabytes or more. Since it is not very likely that someone would have that much information to encrypt, these attacks are not very practical.

If you feel you need more than DES, the only option available for Macintosh users is a variant of DES called triple-DES. In triple-DES, you encrypt a single block of data three times with DES, each time with a different key. CryptoMactic is the only Mac program that does this automatically. With other programs, it is possible to do it manually. Simply encrypt a file once with DES and the first key, a second time with DES and the second key, and a third time with DES and the third key. To decrypt, reverse the process.

More Mac products will soon offer this option. Triple-DES is not crackable by the world's best intelligence agencies, and will probably remain secure for the foreseeable future. If you need security against the planet's best-funded and best-equipped adversaries, use triple-DES.

If there were any way to break triple-DES, I am confident that someone—perhaps a university—would have discovered it by now. The amount of time and effort spent cryptanalyzing DES over the past fifteen years has been enormous. I doubt that any other algorithm in history has received such intense scrutiny.

Triple-DES programs that cost hundreds of dollars—as well as those that are free—can withstand the room full of Cray computers in the NSA's basement. The computing power necessary to break a key doubles with every bit of that key. DES, with a 56-bit key, requires 2^{56} operations to break. Triple-DES, with a 112-bit key, requires 2^{112} operations to break. Computers just aren't that powerful.

Keep in mind, however, that nothing is truly infallible. I have seen implementations of DES that were implemented incorrectly, and implementations of DES that have included a back door. However, I have tried my best to test all of the DES software I reviewed. When I had reservations about the implementation and the security of the product, I have said so. No vendor let me look over the source code for their proprietary algorithms, but I have disassembled the different encryption routines. It is possible that some of the DES programs I claim to be secure may have an unnoticed back door, but I doubt it.

Choosing Keys

If the best way to break into your DES-encrypted files is to try every possible key, a smart cracking program will try all the easy keys first. With this in mind, it is very important to choose a random key and not a word, nor a word with a single digit or punctuation mark.

Even if you choose a random string of letters, numbers, and punctuation marks, you still have a potential problem. Most DES-encryption programs generate the key using the password as typed. This means that only certain keys, those that correspond to printable ASCII passwords, are used. This severely limits the number of possible keys to one tenth what it should be—and makes exhaustive key searching even more possible.

You want the computer to hash the password into the key. Camouflage and CryptoMactic are the only two Mac programs that do this now. If the computer allows you to type in an entire pass phrase—letters, numbers, punctuation, whatever—and then transform that into the DES key, then you can use all possible 2^{56} DES keys and make the algorithm as secure as it can be.

Choosing an encryption key is a much bigger deal than choosing a password. Remember, all password-protection programs can be broken without knowing the password. A good encryption program cannot. If your password is even the least bit obscure, an attacker will probably look for another way to break in. If your key is on the Ten-Million-Most-Commonly-Used-Keys list, then an attacker will be able to read your secret files a whole lot quicker than if it isn't. Choosing a key is serious business. Make the key something easy to remember, but don't make it something easy to guess. Your PC counterparts have help in this area

from Baseline Software which markets a program called Password Coach that checks for weak passwords. Perhaps this will be available for the Mac in the near future.

Hints for Picking Keys

- Don't pick keys that are words, English or foreign.
- Don't pick keys that are names, especially your own, that of a common fictional or mythological character, or that of a family member or pet.
- Don't pick short keys. Your key should be at least eight characters long—longer if your encryption program permits it.
- Pick a mix of alphabetic and numeric characters. Never use an all-numeric key, like your social security or telephone number.
- Pick different keys for different machines or different areas on the same machine. Do not use the same key more than once.
- The best keys mix upper and lower case letters, along with at least one number or punctuation character. There are ways to make these sorts of keys easy to remember, so you are not tempted to write them down:

Combine several short words with special characters. For example, Go2bed# or WANT!beer&\$.

Pick a nonsense word that is still pronounceable. For example, ticmar7 or glaw*wub.

Use an acronym from an easy-to-remember phrase. The phrase "Don't tell Mom I painted the cat" yields the password: DtMlptc.

Add a number or punctuation to the above for added security. For example, D!tMlptc.

Key Guessers

There are computer programs that attempt to guess your key by trying key after key, hoping that sooner or later they'll stumble upon yours. They might try every word in the dictionary and more. Below are the steps taken by a UNIX password guesser that managed to guess 25 percent of the passwords on the average multi-user computer. The same sort of attack could be mounted against your encryption key.

1. It tries the user's name, initials, account name, and other relevant personal information as a possible password—up to 130 different passwords based on this information. For example, on an account name **klone** with a user named "Daniel V. Klein," some of the passwords it might try include **klone**, **klone1**, **dvk**, **dklein**, or **DKlein leinad**.
2. It tries words from various databases, including lists of men's and women's names; places (including permutations so that "spain," "spanish," and "spaniard" are all considered); titles, characters, and locations from films and science-fiction stories; and Chinese syllables from the Pinyin romanization of Chinese, an international standard system of writing Chinese on an English keyboard. All told, more than 60,000 separate words are considered per user.
3. It tries various permutations on the words from step 2, including making the first letter upper case or a control character, making the entire word upper case, reversing the word with and without the aforementioned capitalization, and changing the letter 'o' to the digit '0'. These 14 to 17 additional tests add another 1,000,000 words to the list of possible passwords that are tested.
4. It tries various capitalization permutations on the words from step 2 that were not considered in step 3. This includes all single-, double-, and additional letter capitalization permutations; "michael" is also checked as "michael," or "miCHael," for example. The single-letter permutations add roughly another 400,000 words to be checked, while double-letter permutations add another 1,500,000 words. Tests of four-, five-, and six- letter permutations were deemed to be impracticable without much more computational horsepower to carry them out.

5. It tries foreign language words on foreign users. For this particular test, it tries Chinese language passwords on users with Chinese names using Pinyin romanization of Chinese syllables, combining syllables together into one-, two-, and three-syllable words. Since there are 298 Chinese syllables in the Pinyin system, there are 158,404 two-syllable words, and slightly more than 16,000,000 three-syllable words.
6. Finally, it tries word pairs. The magnitude of an exhaustive test of this nature is staggering. To simplify the test, it only uses real words of three or four characters in length. Even so, the number of word pairs is about 10,000,000. There was only time to complete about ten percent of this test.

The kind of computing power necessary for this kind of attack may seem excessive for some kinds of data, but it may be worth it for one multinational corporation to learn the password of a laptop computer stolen from the CEO of a rival multinational. One small company that sells large language databases lists the National Security Agency as one of its customers. You can be sure there are large mainframe computers in the basement of that agency doing this kind of thing all the time.

As computers get more powerful, those tests that were infeasible during the test described above might be perfectly reasonable five years from now. It's not that much harder to choose a good key—so play it safe and do so.

Safeguarding your Keys

All the security of DES rests in the secrecy of your key. It is as valuable as all of the data encrypted with it. All of the tips in Chapter 2 about safeguarding your password go double for your key. You should not write your key down. If you do write it down, you should store it in a secure place.

Also like passwords, keys should be changed periodically. There are good reasons for doing so. If a key is only used for a short time, then the window of opportunity in which it might be guessed will be smaller. Even if a key is compromised, then the damage will be somewhat limited, as fewer files could be decrypted with that key.

Unfortunately, things are not always that simple. If such a key is used to encrypt data being sent back and forth across a network, changing keys frequently will help protect your files. An attacker who collects a year's worth of network traffic encrypted with a single key is going to have an easier time than one who collects a year's worth of traffic encrypted with a different key each day.

If you are encrypting data on your hard disk drive, the picture is more complicated. It's bad security to encrypt two identical files twice, once with one key and once with another. This means that if you're encrypting your hard drive with a single key, do not decrypt your entire hard drive with that key and re-encrypt it with a new key. Assuming your attacker already has a copy of your hard drive (it may not be true, but it is a wise assumption), giving him the same hard drive encrypted with a new key will only make his job easier.

If your encryption program can encrypt individual files, the best solution is to use a different key for each file. Then, of course, the problem is to remember them all. Unless you have a photographic memory, you are going to have to make compromises.

Choose a solution that works best for your circumstances. Remember, though, that the more data you encrypt with a single key, the easier job a cryptanalyst has. Also, the more times you encrypt identical pieces of data with different keys, the easier job a cryptanalyst has.

Encryption and Speed

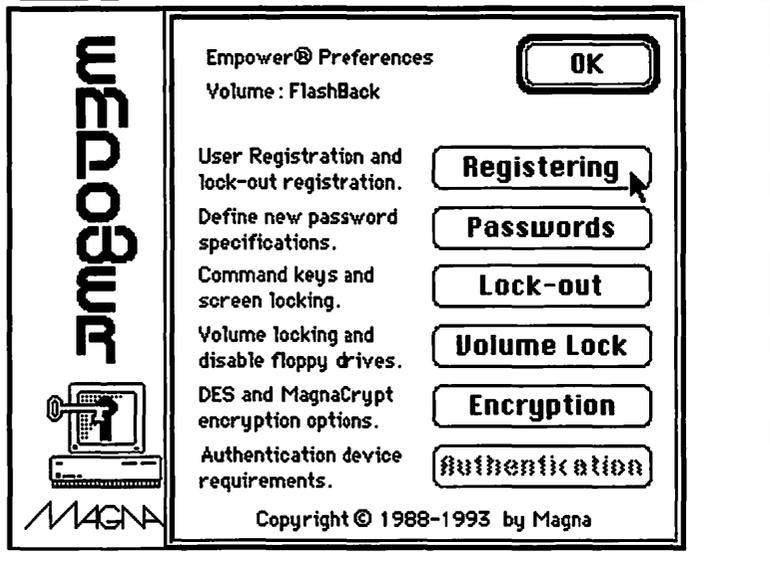
Good encryption is slow. Encrypting a one-megabyte file with DES can take three minutes on a Quadra 700. DES was designed to be implemented in hardware; software implementations are not very efficient. There's nothing you can do about this. If you need the security of DES, you have to pay the price in time. If you need the security of triple-DES, you have to pay an even bigger price.

There are those who say that encryption isn't worth the time and effort if it's slow. This goes back to risk analysis. How much is protecting the data worth? How much is the time needed to decrypt and re-encrypt your data whenever you need it worth? If the data is worth more than the time, encrypt it. If the time is worth more than the data, stick with password protection.

Simple XOR encryption is much faster than DES, but there is not much security in that algorithm. If you can't afford the performance degradation of DES encryption but need the security, you have to buy some dedicated hardware.

Figure 3.8

Empower Encryption



Hardware DES Encryption

There are DES chips that can operate much faster than your hard disk drive access controller. One of those chips sitting between your CPU and your hard drive can encrypt everything before it is written to disk, and decrypt it when it is read from disk.

Although specialized hardware is expensive—only one company makes a Macintosh encryption board—it results in much faster operation and better integration into your system. Hardware encryption is more secure than software encryption. While it is possible for someone to sneak in at night and modify your software encryption program, it is much more difficult to modify hardware.

Another hardware scheme is the Clipper chip. Clipper is an NSA-designed, tamper-resistant VLSI chip intended for the protection of voice and data over telephone lines. At this writing it is not in any computer security products, although it eventually may be.

The chip uses the Skipjack encryption algorithm, a secret encryption algorithm developed by the National Security Agency.

Whether the algorithm is secure is unknown—this depends on whether you trust the NSA or not. I suspect that the algorithm is secure, since a back door is built directly into Clipper.

Each Clipper chip has a special key that is not needed for messages. Instead, this special key is only used to encrypt a copy of each user's message key, and it is split and stored in two key escrow databases. Anyone knowing the both parts can decrypt wiretapped communications protected with this chip. Since the government knows both parts of the special key, it has the ability to conduct electronic surveillance. However, the government claims that it will use this ability only if and when it is authorized to do so by a court.

At this writing, much about the Clipper chip, including the actual key escrow mechanism, is undefined. What is defined follows:

The Clipper chip is designed for the AT&T commercial secure voice products. The functionality of the chip is specified by the NSA, the logic is designed by Mykotronx Inc., and the chip is fabricated by VLSI, though, at this writing there is talk of a second source for the chips.

Each chip is uniquely programmed before being sold to customers. The chip programming equipment writes the information into a special memory on the chip.

The chip automatically transmits information allowing someone with both halves of the special key to decrypt information encrypted with the chip.

There are enormous privacy issues associated with this scheme. Both the Computer Professionals for Social Responsibility and the Electronic Frontier Foundation are actively campaigning against any key escrow mechanism that gives the government the right to eavesdrop on citizens.

Whether or not Clipper will be accepted by the American public and eventually installed in commercial products is still unknown. I hope the whole concept will die a slow death, and that this information will be nothing more than an interesting footnote to history.

Features of Encryption Programs

Encryption can be done either at the file level or the drive level. At the file level, you have to take your confidential files and manually encrypt them. Then, if you want to use them again, you have to manually decrypt them.

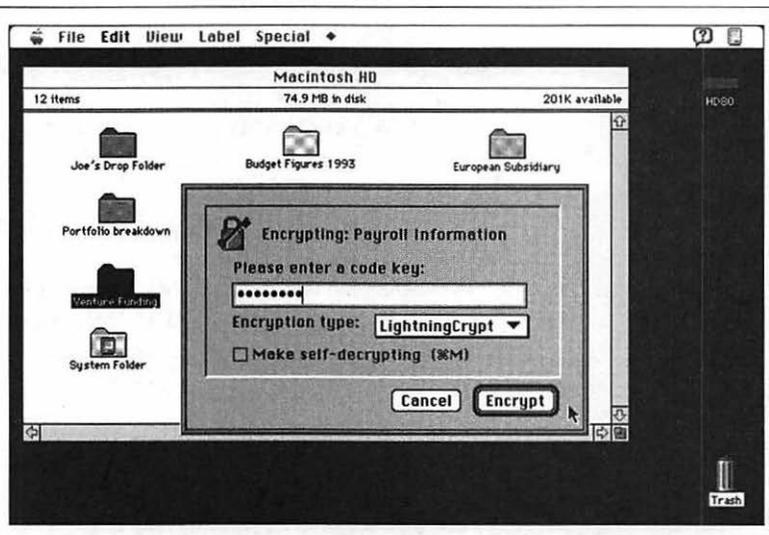
The best file encryption programs make the process as painless as possible. Under System 7, encrypting or decrypting a file should be as easy as dropping the file onto the encryption program's icon. A dialog box should then ask for the key, and the program should do its job. CryptoMactic makes it even easier: just highlight the icon and press Command-1.

One really nice feature, found in CryptoMactic and Camouflage, is the ability to create self-decrypting archives. This is an encrypted file with the decryption engine attached. To decrypt this file, simply double-click on the file's icon. Even if CryptoMactic or Camouflage is not installed on the machine, the file asks for the key and decrypts itself. This feature is perfect for sending encrypted files across a network. You don't have to worry about whether or not the recipient has a copy of CryptoMactic or Camouflage. All you have to worry about is whether or not he has a copy of the key.

No matter how easy file encryption is, it still has to be done manually. An easier alternative is to make the encryption and decryption programs part of the disk driver. Data would then be automatically encrypted when it is written to disk, and automatically decrypted when it is read from disk. Unfortunately, no software product does this kind of encryption.

Figure 3.4

CryptoMactic Encryption



Some programs have master password features. This allows an administrator to recover your files if you forget your password. While these features greatly reduce the chances of losing data if you forget your password, they also increase the chances that someone else can read your data even if he doesn't know your password. Stay away from these features. If your security needs aren't great enough to use real encryption, stick with password access-control.

With respect to products, you should know that cryptography is considered to be a munition by the U.S. government. This means it is covered under the same rules as a TOW missile or an F-16. Sell cryptography overseas without the proper export license, and you're an international arms trafficker. Unless you think time in a federal penitentiary would look good on your résumé, pay attention to the rules.

Two government agencies control export of encryption software. One is the Bureau of Export Administration (BXA), a part of the Department of Commerce, authorized by the Export Administration Regulations (EAR). Another is the Office of Defense Trade Controls (DTC), a part of the State Department, authorized by the Defense Trade Regulations. Generally, BXA has less stringent requirements, but DTC wants to see everything first and can refuse to transfer jurisdiction to BXA.

Any encryption product stronger than a certain level will not receive an export license. Although it has never been publicly stated, this means that anything the NSA can't break cannot be exported. DES cannot be exported. RC-2 and RC-4 with 40-bit keys can be exported. If a company advertises that their algorithm is exportable, you can rest assured that it isn't very good. Think of exportability as a negative endorsement: NSA's assurance that the program is breakable.

Encryption and File Recovery

Encrypted files are highly sensitive to disk errors. Because of the way the bits are scrambled during encryption, a single bit error in the ciphertext can result in the loss of many bytes of data after encryption. For this reason it is vital to keep backups of all encrypted files. These backups can also be encrypted. More details about backups can be found in Chapter 7.

There is no security without responsibility. The whole point of encryption is to make it impossible for someone without the key to decrypt your files. Assume you're using secure DES encryption. If you lose your key you will not be able to decrypt your files, and it won't matter how much you plead with tech support because they can't do anything for you. If you are going to encrypt your files, you must remember your key.

There are programs which advertise the ability to recover files without the key. These are precisely the encryption programs I recommend you avoid. If the manufacturer can recover your files without the key, so can someone else. There's little security in that.

What to Encrypt

In the end, you can't get any real security with software products. To see why, let's look at the problem from a paranoid point of view.

Let's say you have the best encryption product. It uses triple-DES or something even better that you *know* is unbreakable. It implements good key management. It erases plaintext files, as well as all those temporary files that might have been created during the encryption process. You use it religiously. Are you secure?

What if some adversary snuck in one night and replaced your encryption program with a Trojan horse, another program that looked like it encrypted your files with your secure algorithm, but instead used an algorithm with a back door? You wouldn't know the difference, but that agent would be able to read your files.

Remember, access-control programs won't help. They all can be bypassed by someone sufficiently skilled, and I assure you the adversary is this someone.

Let's say the encryption program has a checksum feature. If someone surreptitiously modifies it, then the checksum will be different and the foul play will be obvious. But the adversary is more clever than this. He modifies the checksum program as well, so it will report that nothing is wrong.

What if you carry your encryption program around with you on a floppy? Then the adversary can't get to it, you say. But he can introduce a program on your computer that waits until you put your floppy into the computer, and modifies it then. Or he can switch floppies on you when you are asleep.

You can play this game forever. The point is that unless the computer is locked away where the adversary cannot get to it, he will be able to rig the computer so that you think it is secure when it really isn't. There's nothing you can do about this. Unless your encryption is in hardware, where someone can't go in and modify it, you are at risk.

Now, let's step back to a less paranoid degree of concern. If the intelligence services of several major governments are after you, you have to worry about this sort of thing. You should be using hardware encryption. However, if your security needs are not that great, a software program will probably suffice.

What to Buy to Encrypt Your Data

Any self-respecting encryption package should include DES and triple-DES algorithms. It should not store the key anywhere with the encrypted files. Encryption requires a lot of responsibility of a user in maintaining a key because a good encryption program should not allow for file recovery if the key is lost. Finally, the program should accept passwords of any length and use a one-way hash function to transform the password into the key.

The following access-control products reviewed in Chapter 2 include encryption options: A.M.E., Citadel, DiskLock, Empower products, FileGuard, ultraSECURE, and ultraSHIELD.

Of these, Citadel is an excellent encryption product because it implements DES in Cipher Block Chaining mode. Additionally, ultraSECURE is a general access-control program that uses DES for file encryption. It has excellent key management.

Table 3.1: Encryption Programs

Product	List Price	Company	Phone	Main Function	Comments
Camouflage 1.62	\$149.00	usrEZ Software, Inc.	(714)756-5140	Dedicated data encryption package	Passwords can be up to 16,384 characters which gives a very secure key
CryptoMactic 1.0	\$99.00	Kent*Marsh Ltd.	(800)325-3587	Dedicated data encryption package	The best encryption package; offers DES Cipher Block Chaining and Triple-DES
Ft. Knox 1.0.5*	\$195.00	Transfinite Systems Co.	write to company	Basic security that includes encrypt	Also erases files to DoD standards
ISAC 4200	\$1,145.00	Isolation Systems	(416)231-1248	Hardware-based DES encryption	Complete security, screen and keyboard lock, is transparent; supports multiple passwords
Norton Utilities for the Macintosh (Norton Encrypt)	\$149.00	Symantec Corp.	(800)441-7234	Basic encryption	Does offer DES

* The company's address is: P.O. Box N; MIT Branch Post Office; Cambridge, MA 02139

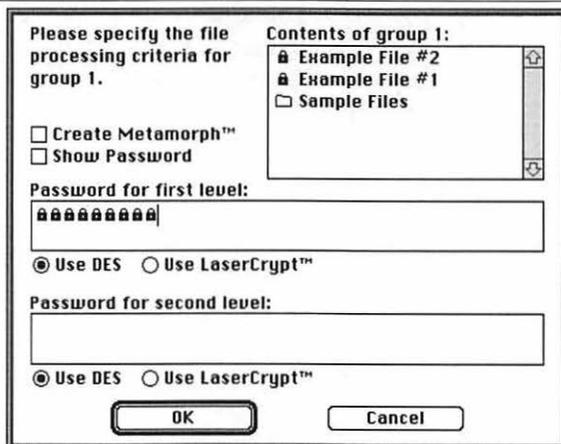
Camouflage 1.62

Camouflage, from usrEZ Software, is dedicated solely to the encryption of files, and it does this very well.

The program uses good key management. You are prompted for a password which is hashed to become the encryption key. You can enter a long password—up to 16,384 characters—and every character of that password will affect the key. The longer the password, the more secure your key is.

Figure 3.5

Camouflage



Camouflage has three encryption options: LaserCrypt, DES, and double-DES. LaserCrypt is a proprietary algorithm you'll want to avoid, and double-DES doesn't add any security. Stick with DES. The implementation here is about the fastest I've seen on the Mac.

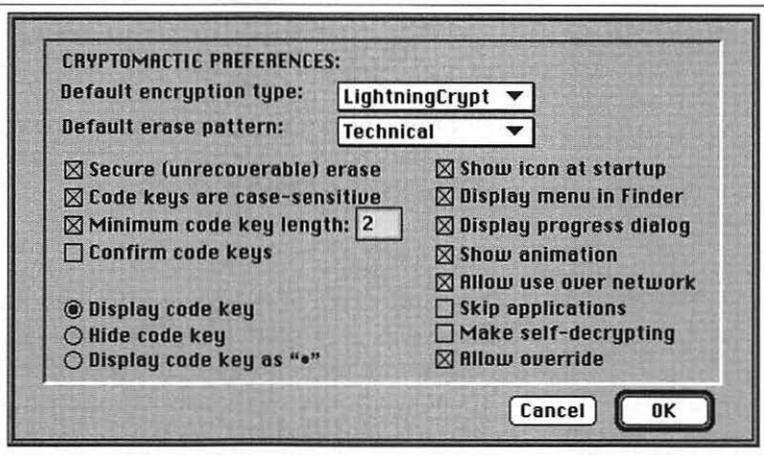
Camouflage can create self-decrypting archives. When you or the desired recipient double-click on these archives, you will be prompted for the key. You don't need the Camouflage program to decrypt these archives.

CryptoMactic 1.0

CryptoMactic, from Kent•Marsh, is the best encryption program you can buy for the Macintosh. With it, you can secure files so tightly that even the most advanced military intelligence organizations, with their multi-million dollar budgets and rooms full of Cray computers, can't read them. On top of all this, the program is easy to use.

Figure 3.6

CryptoMactic



To encrypt a file, just highlight a file on the Desktop and press Command-1. A dialog box will prompt you for the key, enter it and the program will encrypt the file. Decrypting is just as easy.

Like Camouflage, CryptoMactic can generate self-decrypting files. This feature is great for sending encrypted files across networks: You don't have to worry if the recipient has CryptoMactic. All you have to worry about it whether she knows the key.

Like many of the access-control programs, CryptoMactic has an Administrator Override option. This lets an administrator override the security in the event someone forgets his key. Remember, though, if you use this option your files are no more secure than they would be with an access-control program. If you want real security, you have to disable this option.

CryptoMactic comes with a variety of encryption algorithms: LightningCrypt, QuickCrypt, DES, DES Cipher Block Chaining, and triple-DES. Forget about LightningCrypt and QuickCrypt because they're not very secure. If you're going to use DES, use DES in Cipher Block Chaining mode. Triple-DES is the only option that is secure against *any* adversary, though it's slow—but that's the price you have to pay for ultimate security.

The program also comes with a utility that completely erases the unencrypted file after it is encrypted, either to DoD standards or better. This, too, is essential for real security.

CryptoMactic is the closest you'll probably ever see to military-grade encryption on the Macintosh. If you need that kind of security, this is the only program for you.

Ft. Knox 1.0.5

Ft. Knox, from Transfinite Systems, doesn't have a lot of features, but what it does it does well. It offers basic encryption, either with DES or its own OnesCrypt.

ISAC 4200

The ISAC 4200, from Isolation Systems, is an intelligent hardware-based DES encryption system for the Macintosh. It is also the only hardware-based option for the Mac. The package, which is made in Canada but can be legally imported into the United States, contains a NuBus card and System software.

The ISAC 4200 enforces automatic internal security procedures that are transparent to both the user and the Macintosh operating system. The board automatically encrypts and decrypts data as it is being written to and read from disks. All the user does is enter his DES key at the beginning, and everything else works behind the scenes.

Having everything automatically encrypted can cause problems, so ISAC recognizes and distinguishes between standard disks and disks that have been prepared to store encrypted data. All

reads and writes to a standard disk are unencrypted; all reads and writes to a prepared disk are automatically encrypted and decrypted, but appear the same as a normal unencrypted disk to Macintosh applications. The ISAC automatically recognizes which files are stored unencrypted and which are encrypted, and does all necessary decryptions without user intervention.

ISAC ensures privacy between multiple users by encrypting different people's files with different keys. Of course, a user can only decrypt files that have been encrypted with his key. This is also transparent to the user, since keys are handled automatically by the ISAC. Non-accessible files are hidden from view.

The ISAC supports screen and keyboard locking. There is a keyboard command that automatically locks the keyboard, and optionally the screen and keyboard. To unlock the screen and keyboard, the user must enter her key.

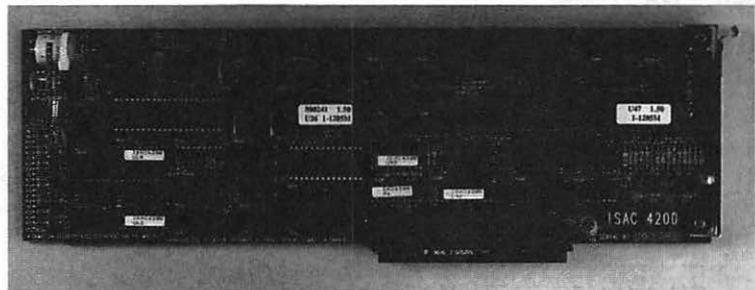
Communications can also be encrypted. The ISAC supports encrypted file transfer between computers. Key management can be either manual or automatic, though I recommend manual. All operations are transparent to the network.

Files are owned by the user who created them. The owner can assign to other users such privileges as the ability to read or write a file. Write permission includes permission to read and to execute. Copy protection can also prevent users from making unauthorized copies of software and files.

The key management is sophisticated. The system lets users generate their own keys, and can support requirements for minimum key length and forced expiration of the key. It can also prevent re-use of old keys.

Figure 3.7

ISAC 4200



The system also keeps an extensive audit log that tracks such things as successful and unsuccessful log-ons, file access, and resource use. This information can be printed out in a variety of report styles.

All of this security is controlled by a hierarchy of security officers: a Key Officer and a System Security Officer. These people set up the security, give different users access to the computer and different privileges, and can bail people out if they forget their keys. (This does not compromise security.) The system is complex enough to handle complicated access requirements for multiple users, but can easily be used by a single person to simply encrypt all the data on his or her hard drive.

MacSafe II 2.00

MacSafe was Kent•Marsh's old file encryption program. It allowed you to put files into "safes," which you could then encrypt. Although secure, the program has been replaced by CryptoMactic. Kent•Marsh no longer supports this product.

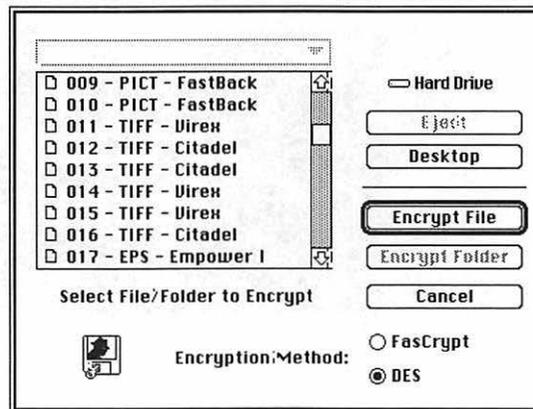
MacSafe's DES is correct, and it has an option for Cipher Block Chaining. Key management is basic: the password becomes the key.

Norton Encrypt

With Norton Encrypt, part of Norton Utilities for the Macintosh 2.0 from Symantec, you can encrypt and decrypt files in either Norton's own proprietary algorithm or DES. Under System 7, you can drag and drop files directly onto Encrypt to either encrypt or decrypt them.

Figure 3.8

Norton Encrypt



Chapter 3 Summary

- Encryption is a way to keep your data secure, even if an adversary gets around all your access-control methods. As long as the key to the encryption algorithm is secret, no one will be able to read your files.
- Encrypt your data using an algorithm that has been scrutinized and not broken by the world's cryptology community; such an algorithm is almost certainly more secure than using one that has not been analyzed. An algorithm that has not been studied could have back doors built in or could be easily breakable by a simpler method than trying every possible key.
- The DES algorithm, developed by IBM and the NSA, has become the international standard for data security. DES encryption can, in theory, be broken by anyone making the investment in a DES-cracking machine. No major government or multinational corporation has admitted to doing so.
- Triple-DES, encrypting the same text three times using a different key each time, is more secure than DES. It cannot be broken by any known technology. If your security needs are that high, using triple-DES is your only option.
- All the security in an encrypted file lies in the key, and not in the algorithm. To keep your files secure, you must choose a good key and keep that key a secret.
- Make your key easy to remember, but difficult to guess.
- Changing your key frequently means that anyone intercepting your files will have a smaller amount of encrypted text to work with in trying to deduce the key. This key management strategy works well for sending messages over electronic media.
- When encrypting files on your hard disk drive, the most secure strategy is to encrypt each file with a separate key. The problem then is remembering all those keys. Working with encrypted data can mean making compromises between security and key management.

- DES is a slow algorithm. Encrypting large amounts of data is a considerable investment in time. Weigh the risk you take in possibly compromising your data against the time needed to encrypt it.
- The faster encryption option, and the only truly secure option, is to use hardware DES encryption.
- As encrypted files are highly sensitive to bit errors, it's vital to make backups, which can also be encrypted, of all your files.

Chapter 3 Sources

Camouflage 1.62, \$149

usrEZ Software, Inc.
18881 Von Karman Ave., Suite 1270
Irvine, CA 92715
(714) 756-5140
FAX: (714) 756-8810

CryptoMactic 1.0, \$99

Kent•Marsh Ltd.
3260 Sul Ross
Houston, TX 77098
(713) 522-5625
(800) 325-3587
FAX: (713) 522-8965

Ft. Knox 1.0.5, \$195

Transfinite Systems Co., Inc.
P.O. Box N
MIT Branch Post Office
Cambridge, MA 02139

ISAC 4200, \$1145

Isolation Systems
26 Six Point Road
Etobicoke, Ontario, M8Z 2W9, Canada
(416) 231-1248
FAX: (416) 231-8561

MacSafe II 2.00

Kent•Marsh Ltd.
3260 Sul Ross
Houston, TX 77098
(713) 522-5625
(800) 325-3587
FAX: (713) 522-8965

Norton Utilities for Macintosh 2.0, \$149

Symantec Corp.

10210 Torre Ave.

Cupertino, CA 95014

(503) 334-6054

(800) 441-7234

FAX: (503) 334-7471



Why File Erasure is Important

When you delete a file, the Macintosh deletes only the file name from the directory; the actual bits of data remain on the hard disk drive until overwritten by another file. Many Macintosh utilities, like Norton Utilities and MacTools, can recover deleted files. To erase a file so that these software packages cannot read it, you have to physically write over all of the bits on the hard drive. To delete a file so that adversaries with electron-tunneling microscopes can't recover it, you have to do even more.

Many Macintosh utilities can erase files so that file-recovery utilities can't bring them back. If you are concerned about the security of your data, use one of them.

If you are concerned about an adversary with considerably more resources than a file undelete program, you have to do even more work to completely erase your files. The Department of Defense (DoD) recommends overwriting a deleted file not once, but three times: the first time with all 1s, the second time with all 0s, and the third time with a repeating 1-0 pattern. Any fewer overwrites and someone with special-purpose equipment can read the overwritten bits. Recent developments at NIST with electron-tunnelling microscopes suggest even *that* might not be enough.

Another budding concern is the virtual memory feature of System 7. Under virtual memory, a Macintosh can be reading and

writing memory to disk any time. Even if you don't save it, you never know when a sensitive document you are working on is shipped off to disk. The solution in this case is to find a utility that erases all free space on your hard disk drive and use it.

What to Buy for File Erasure

A decent file erasure program should be able to erase entire disks, specific files, and any free space on a disk. It should erase once, three times to meet DoD specifications, or as many times as the user specifies.

The following encryption products reviewed in Chapters 2 and 3 also include file erasure options: A.M.E., Camouflage, CryptoMactic, Citadel, ultraSECURE, and ultraSHIELD.

Of these, CryptoMactic and ultraSECURE have excellent file-erasure capabilities; they can erase files, disks, and all unused space on disks.

Table 4.1: File Erasure Products

Product	List Price	Company	Consumer Phone Number	Main Function	Comments
Citadel with Shredder	\$99.95	Datawatch Corp.	(919) 549-0711	All-purpose security	Companion package, Disk Cleaner, shreds all free space on a hard drive
Shredder 1.0.1	\$69.00	DLM Software	(619) 283-2343	Erasure program	Is two applications; Scrubber erases all unused areas of a volume.
TrashMaster 1.1	\$69.95	Utilitron	(800) 428-8766	Erasure and trash management	Incinerate function automatically erases files of defined types
TrashGuard 1.2	\$79.00	ASD Software, Inc.	(909) 624-2594	File erasure only	Intelligent Exceptions lets you erase certain files and delete others
Norton Utilities for the Macintosh	\$149.00	Symantec Corp.	(800) 441-7234	Basic erasure program	Creates special Trash dedicated to erasure, leaving
The Viper 1.0.2	\$49.95	Systematic Computer Services	(513) 275-2937	Disk drive erasure package	Can be configured to overwrite material six times
Ft. Knox 1.0.5 ²	\$195.00	Transfinite Systems Co. Write to company		Basic file erasure	Overwrites files in accordance with DoD regulations

¹Programs are also a part of the SuperSet Utilities, \$149.00

²The company's address is: P.O. Box N; MIT Branch Post Office; Cambridge, MA 02139

Citadel with Shredder

Shredder, from Datawatch, turns the Trash into a shredder, shredding all files you put into it. The program can shred in accordance with DoD specifications, and there are other options. It can be configured to ask for confirmation before shredding. Since you cannot recover a file after it is shredded, this is a good idea. It can shred files deleted from the Finder only, or extend this to temporary files created by applications, and all of this works in the background. A companion program, Disk Cleaner, shreds all free space on your drive.

Figure 4.1

Shredder
(Datawatch)



This is an excellent file shredder, part of a top-notch security program called Citadel. It also comes as a part of the SuperSet Utilities, also from Datawatch.

Shredder 1.0.1

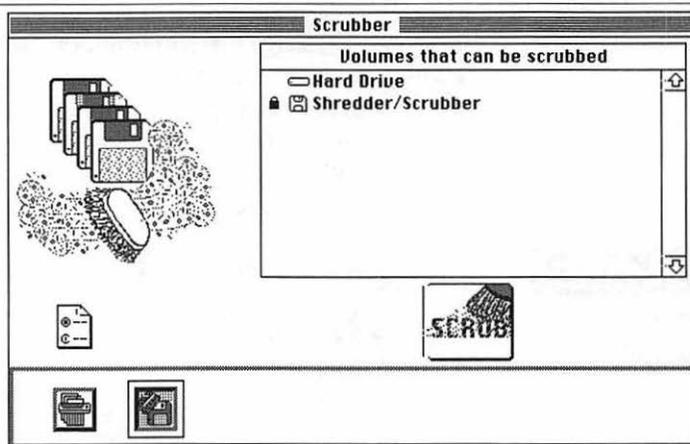
Shredder, from DLM Software, is actually two applications, Shredder and Scrubber. Shredder erases files by overwriting either once or the three times that meet DoD specifications. Scrubber does the same for all unused areas of a volume, with the same options. Scrubber can also delete the miniature backup that some applications tack onto the end of saved files.

You can use these programs in several ways. You can simply drag and drop file icons onto Shredder—or disk icons onto Scrubber—and use them as you would the Trash. Or you can set interval shredding or scrubbing to work in the background at a specific time.

Both Shredder and Scrubber are so easy to use, so complete, and work so smoothly, that I can't help recommending this program.

Figure 4.2

Shredder (DLM)



TrashMaster 1.1

TrashMaster, from Utilitron, is a control panel that lets you manage your trash to the finest detail by adding menu controls and filtering, to trash-emptying. In the realm of security, the program has a special Incinerate function. This function automatically erases files of defined types, like temporary and print-spool files, when they are deleted either by TrashMaster or by an application. TrashMaster can overwrite files either once, or three times to meet with DoD regulations. Unfortunately, this function is not that easy to find; you have to wade through a series of filters to get to the Incinerator's file-overwriting capabilities.

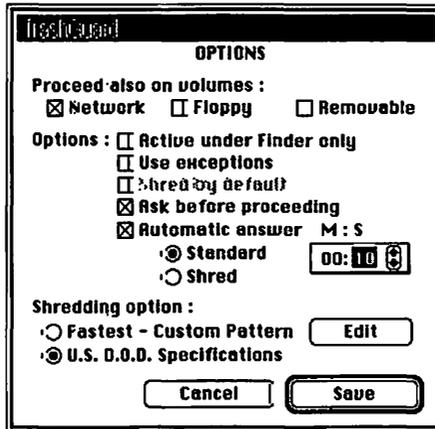
TrashGuard 1.2

TrashGuard, from ASD Software, is a file-deletion utility. It works in the background, shredding only those files placed in the Trash Can. It cannot erase entire disks, or all unused space on a disk, but what it does erase, it does in accordance with DoD specifications.

One nice feature of TrashGuard is something they call "Intelligent Exceptions." You can train TrashGuard to shred certain files and simply delete others. For example, you can set TrashGuard to shred all spreadsheet documents, and delete everything else normally.

Figure 4.3

TrashGuard



Norton Wipe Info

Norton Wipe Info is part of the Norton Utilities for the Macintosh 2.0, from Symantec, that erases files, entire disks, or all unused space on a disk. To erase a file, you have to enter Wipe Info and select the file from a menu. You can also create a special Trash Can, Wipe Info Trash, that erases all files dropped into it. Like other erasure packages, Wipe Info can erase files in accordance with DoD specifications.

The Viper 1.0.2

The Viper, from Systematic Computer Services, erases only entire disks. The user interface is mediocre, but the program does the job. The best feature of this program is that it can be configured to overwrite up to six times—twice the DoD recommendations.

Ft. Knox 1.0.5

Ft. Knox, from Transfinite Systems, contains a file-deletion utility that overwrites a file either once, or three times in accordance with DoD regulations.

Chapter 4 Summary

- On a Macintosh, a deleted file sits on the hard drive until that space is overwritten by another file. This is why file recovery programs can get back a file you have accidentally deleted.
- File-erasure programs ensure that no one, not even you, can read your deleted files. Some programs shred documents as they are put into the Trash. Others erase all free space on a disk once, others work to Department of Defense specifications and wipe the disk three times. Yet other programs can overwrite a disk six times. Utilities that wipe all the free space on your hard disk drive are essential to any good security program.

Chapter 4 Sources

Citadel with Shredder, \$99.95

SuperSet Utilities, \$149

Datawatch Corp.

Triangle Software Division

P.O. Box 13984

Research Triangle Park, NC 27709

(919) 549-0711

FAX: (919) 549-0065

Shredder 1.0.1, \$69

DLM Software

3525 Del Mar Heights Road, Suite 319

San Diego, CA 92130

(619) 283-2343

TrashMaster 1.1, \$69.95

Utilitron

P.O. Box 811

Allen, TX 75002

(214) 727-2329

(800) 428-8766

TrashGuard 1.2, \$79

ASD Software, Inc.

4650 Arrow Highway, Suite E-6

Montclair, CA 91763

(909) 624-2594

FAX: (909) 624-9574

Norton Utilities for Macintosh 2.0, \$149

Symantec Corp.

10210 Torre Ave.

Cupertino, CA 95014

(503) 334-6054

(800) 441-7234

FAX: (503) 334-7471

The Viper 1.0.2, \$49.95

Systematic Computer Services

3206 Harvard Blvd.

Dayton, OH 45406

(513) 275-2937

FAX: (513) 275-9476

Ft. Knox 1.0.5, \$195

Transfinite Systems Co., Inc.

P.O. Box N

MIT Branch Post Office

Cambridge, MA 02139



Protect Your Data from Viruses

Now that you have a grounding in security basics, we're going to look at computer viruses—what they are, how they work, and how to protect against them. Virus protection is like insurance. You'll probably never need it, but if you do you'll be really glad you have it.

Viruses fall in the gray area between active attacks and accidental attacks. Viruses are written on purpose, but they spread primarily by accident. While it is possible for a disgruntled individual to write a virus that specifically targets you or your company, it is far more likely that your Mac will catch a virus by accident—because either you or one of your co-workers did not take adequate precautions.

You can do two things to protect yourself against virus infection. The first is to not do things that needlessly increase your risk of exposure to computer viruses. This is often called practicing "safe computing." The second is to invest in a virus-protection program. This is not very difficult, since one of the best programs is free.

The best advice is to not spend more time worrying about this than necessary. Macintosh viruses exist, and they do spread. If you don't share files with others or download files from networks, your chance of contracting one is tiny. Even if you do share files, your chance is small. If you take some simple precautions the chance of a virus going undetected and doing damage is minute.



What You Need to Know About Viruses

Computer viruses are software programs, just like a word processor, spreadsheet, or utility program. Unlike those other programs, viruses run in secret. They hide inside other programs and run when those applications run, all without putting up dialog boxes or prompting users for input.

Technically, a virus modifies the behavior of another program to include an executable, and possibly altered, copy of itself. Note that this definition does not mention any malicious or destructive actions. In fact, many Macintosh viruses are benign: they spread from computer to computer without doing damage. Others don't overtly damage a program, but their mere existence may cause some system incompatibilities and lead to problems. Still, some viruses have explicit code to erase files and cause other mayhem.

Typically, the virus code executes when a user launches the program to which it is attached. The virus then attempts to "infect" other programs, thereby reproducing itself. A virus may start reproducing right away, or it may lay dormant until it is triggered by some event, Friday the 13th, for example. It then may do whatever damage the virus' author programmed it to do.

Field Guide to Malicious Software

A **virus** is a piece of computer code that copies itself into a larger program, thereby modifying that program. A virus is not an independent program: it must attach itself to another program to survive.

A **worm** is an independent program. It reproduces by copying itself in its entirety from one computer to another across a network. Like a virus, a worm can spread rapidly through a computer network, though a worm doesn't have to modify any other programs. Worms are more common in UNIX machines. Remember the famous 1988 Internet worm? No known worms have been written for the Macintosh.

A **Trojan horse** disguises itself as a legitimate program. Instead of being the useful utility or fun game you expect, these programs infect or damage your Macintosh. Trojan horses do not duplicate, but are a popular mechanism for disguising a virus. For example, the MBDF virus was installed by a Trojan horse, in a game named "Tetracycle" or "Tetris-rotating."

A relative of the Trojan horse, the **chameleon** acts like another familiar, trusted program. For example, it might act exactly like your encryption program, while at the same time recording passwords and keys in a secret file.

A **bomb**, also a type of Trojan horse, is used to release a virus, a worm, or some other type of system attack. It works by triggering some kind of action when a particular date, time, or condition occurs. Bombs come in two varieties. A **time bomb** goes off on a particular date or after some period of time has elapsed. For example, the INIT-M virus contains a time bomb that severely damages folders and files on any Friday the 13th. A **logic bomb** goes off when a particular event occurs. A developer might plant a logic bomb in one of his applications, set to go off if someone tries to make an illegal copy of the application, for instance. No known logic bombs exist in any commercially available Macintosh program.

Macintosh viruses reproduce themselves in several ways. Some duplicate when you open an infected file. Others infect the system first and infect other volumes when you access those.

Not all computer viruses cause damage; some are content merely to multiply. More malicious viruses can issue random sounds or display risqué screen messages. In extreme cases, viruses can destroy files or even hard disk drives.

Your Macintosh can acquire a virus anywhere it gets data. The most common source is from a floppy disk, including some shrink-wrapped software. You can also get a virus from a network or a BBS.

The analogy between biological viruses and computer viruses is pretty good. Both of them duplicate, and both of them require a host to survive. In both cases, the virus can severely damage the infected system. And with both kinds of viruses, it is sometimes possible to remove the infection without damaging the system, and it is sometimes possible to vaccinate the system to prevent it against future infection.

Even so, there are important differences between computer and biological viruses. Biological viruses are living organisms; computer viruses are not. Biological viruses usually occur naturally and are almost never created by people; computer viruses are all created by people. And more importantly, it is not possible to compare the enormous suffering caused by a biological virus such as HIV to the comparatively meaningless damage caused by computer viruses.

How Serious is the Virus Threat?

The likelihood that you'll encounter a virus depends on your computing activities. If your Mac is truly an island and you don't exchange files with anyone, then you have virtually no risk. On the other hand, if you exchange disks with another person, or files on network, you risk getting a virus. It's not a large risk, but it is a risk nonetheless.

Being a Mac user, your risk is lower than your PC counterparts. More viruses are written for PCs than are for Macs because a PC is easier to program. That PCs outnumber Macs in terms of users means the chances of a PC being in the hands of a potential virus writer are greater. Most Mac users never see a virus, though some major companies have seen their operations halted by Mac viruses. Despite the prevalence of anti-virus software, roughly two new Mac viruses are discovered each year. However, this pales in

comparison to the PC, which sees hundreds of new viruses each year.

The biggest risk you run is losing all your data—something that can be minimized by preventative measures like performing frequent backups and by installing anti-virus software. All Mac anti-virus software programs are easy to use, and they all protect against all known Macintosh viruses. Some of the best anti-virus programs are free. Given how easy it is to protect your data from viruses, there is no good reason not to use one of them.

How Viruses Can Get from One Computer to Another

- Downloaded files from bulletin boards
- Shared floppy disks
- Shrink-wrapped software
- Blank pre-formatted disks

Detecting Viruses

Identifying infections of known viruses is fairly easy. With the exception of polymorphic viruses, every virus has a distinct signature, strings of bytes that uniquely identify the viral code. Anti-virus software is programmed to recognize these signatures. If a virus does not contain a known signature, then the program will not detect it.

Common Symptoms of Virus Infection

Frequent system bombs: Not all system bombs are caused by viruses, but if your Macintosh begins to bomb on a regular basis, a virus may be the culprit.

Applications that do not work properly: Some viruses change the way an application works. It may hide a file, add or change a resource, bypass the resource manager for file system, or attempt to format a volume.

Disks or files that are damaged and cannot be accessed:

A virus may try to damage data files, the Desktop file, or the hard disk drive's directory. A file's checksum may change, too.

Printing does not work correctly: It can be significantly slower.

The System and applications malfunction: Pull-down menus are distorted, or windows will not open, close, or zoom correctly.

When the software discovers a known virus, a dialog box informs you of the infection and asks if you want the virus removed. Say yes. The program will then remove the virus and, to the best of its ability, restore your system to its pre-viral state.

In some cases, it is not possible to restore your system. In those cases the program will tell you, and you will have to reload applications from their original locked master disks.

Detecting unknown viruses is much harder. There is no identifying signature, so an anti-virus program has no concrete evidence telling it that a virus is present. It has to continuously monitor the system for suspicious activity which may or may not be linked to a virus. Some programs have the option of comparing the checksum of each file with a checksum it has stored away somewhere. A checksum is a numeric value derived from the individual bytes of a file. Changes in the checksum indicate that the file has been modified and may indicate virus infection.

The problem with detecting viruses using a checksum is that changes you deliberately make to files will also be reported as a possible virus infection. You then have to decide if there really is a problem, or if it's a false alarm. Most anti-virus programs that have a checksum option allow you to list files or file types that are often changed, telling the program not to view those changes as suspicious.

Still, this type of virus detection has several problems. First, there will be false alarms. Some applications do legitimate things that may be interpreted as an attempted viral infection, like installing fonts. False alarms are merely annoying to those users who understand them, but can cause unnecessary panic among naïve users. Additionally, there are ways to bypass any virus detection program. In the MS-DOS world, viruses have been written specifically to bypass virus detectors. Although no Macintosh viruses to date have this feature, it is just as possible.

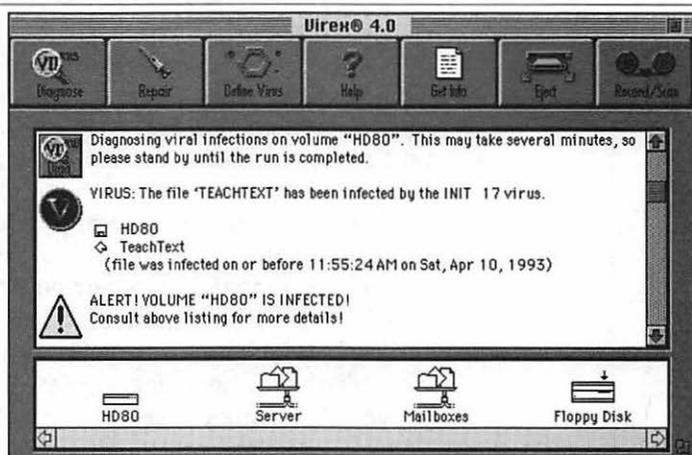
Advanced users may look to checksums. Because there are so many occasions during normal Macintosh operation when files change behind the scenes, I do not recommend using the anti-virus program's checksum operation all the time. Instead, use the checksum feature to take a snapshot of the system when you know it is free of viruses. Then, if you suspect a virus and regular scanning does not uncover one, use the checksum feature once again to see if there are any changes.

Preventative vs Detective Anti-Virus Software

Preventive anti-virus software that has INITs tries to catch viruses when they attempt to infect a system. Only this type of anti-virus software can prevent unknown viruses.

Figure 5.1

Virex INIT options



Detective anti-virus software doesn't work in the background. It is a separate application, and will only run when you tell it to. When you run the application, it can scan any mounted volume for known viruses.

Hints for Protecting Against Viruses

Macintosh viruses are a serious problem, but there is no need to panic over them. With current anti-virus software, it should only take a few minutes a week to effectively protect your Macintosh against known viruses. Most of these suggestions are from the on-line manual that comes with Disinfectant, a freeware anti-virus software package.

- If you do only one thing, use an anti-virus INIT. They only take a minute to install, and can save your Macintosh.
- Make backup copies of your applications' master disks and use the duplicates. Keep the master floppies locked at all times. It is impossible for a virus to infect files on a locked floppy.
- Don't install software from one computer directly onto another computer.
- Make periodic backups of your hard drive.
- Run your anti-virus software before each backup to ensure that your system has not been infected and to make certain the backups do not become infected. If a virus has infected any of the backed-up files, you won't solve anything by restoring from the backup.
- Before using new software, check for possible infections. This applies to all commercial software, and especially to shareware and freeware.
- Keep your anti-virus software up-to-date. Old versions of anti-virus software are often ineffective against new viruses. If you do not have a reliable information source to learn about new viruses, purchase a product that has an update service.

The benefit of this kind of anti-virus software is that it isn't always running in the background, slowing down the launching of applications and possibly giving off false alarms. The downside is that by the time a detective anti-virus program informs you of a virus infection, it is too late.

Some detective programs automatically scan floppies when you load them. This is an excellent feature; it is effective and only minimally increases the time required to mount a floppy disk. It should be implemented on every Macintosh.

Networks and BBSs—Viral Hotbeds

Any time you come in contact with another computer or a new piece of software, you run a risk of getting a virus. If you work on a network or access a bulletin board, the risk is even greater.

As a manager of a network or bulletin board, you have the big task of ensuring the risk to all users of getting and spreading viruses is low. You should take several precautions when managing such environments, the first of which is to install an anti-virus INIT on all your start-up disks. Once these are installed, your job is only beginning, however. You must check these disks frequently with anti-virus software to make sure they are uninfected. Additionally, you should make sure the anti-virus INITs are still installed and active.

Knowing about viruses is important. As a manager you should educate your users about viruses and how to protect against them. Make sure they all have copies of the anti-virus software so they can check their own disks.

Take great care with applications stored on an AppleShare server. Place them in write-protected folders, as viruses cannot infect applications if they are in folders which do not have the Make Changes privilege. If an application is in a writeable server folder, any infected Mac on the network which accesses the disk and uses the application might spread the infection to the application on the server. This then increases the likelihood that the virus will infect other Macs on the network which are not protected by an anti-virus INIT.

A further precaution is to check server disk drives frequently with anti-virus software to make certain they are uninfected. You should take the server off-line and restart it using a locked floppy disk. This is the only way to guarantee that your anti-virus software will be able to scan all the files on the server disk drive. Additionally, check all new software with anti-virus software before installing it on a server.

Back up your servers frequently, and when you do, run your anti-virus software before each backup.

You should never grant the Make Changes privilege on server root directories; otherwise, you run the risk of getting the WDEF virus, which can cause serious performance problems on an Apple-Share server. See page 126 for details about the WDEF virus.

In the event of an infection of a single Mac or the server, you should have at least three floppy disks to be able to remove viruses from any kind of Macintosh: an 800K System 6 disk containing System 6.0.7 and your anti-virus software, a copy of System 7.0 800K Disk Tools disk, and a copy of the System 7.0.1 1.4M Disk Tools disk. Keep all three disks locked at all times.

Finally, if you run a bulletin board, please carefully check all new software for viruses before distributing it. The same goes for those selling software, shareware and otherwise. Make sure you check them before sending the disks out to be duplicated.

Recovering from a Virus Infection

Most of the time, anti-virus software can remove a virus from your system and restore your files intact. Some viruses, however, make changes to your Macintosh files. An anti-virus program can remove the virus, but cannot undo the damage that the virus has already done. In those cases, the damaged files must be deleted and restored from backup copies.

So your Mac's been infected, and you've restored your hard drive. You think you have the virus licked, but you're forgetting something—prevention. If a new virus starts spreading and your anti-virus program doesn't know about it, you are at a disadvantage. Because new viruses are discovered all the time, you should make sure you have an up-to-date copy of your anti-virus software.

New versions of the major anti-virus software, including the public domain programs Disinfectant and GateKeeper, are released days—sometimes even hours—after a new virus is discovered. Major anti-virus vendors offer updates on their own BBSs as well as on the big electronic information services such CompuServe, Internet, GENie, and America Online. You can also subscribe to a service where the developer will send you an updated copy of its software every time a new virus appears.

Keeping a Level Head with Mac Viruses

The Macintosh virus threat is much less serious now than it was a few years ago, both in terms of the number of new viruses discovered and the number of reported incidents of infection. This is partly due to the widespread use of anti-virus software, but also to the difficulty in writing a Macintosh virus. Most Mac users will probably never see a virus, and if they do it will probably be a known virus. Use anti-virus software, but don't get paranoid over the problem.

Last-Ditch Macintosh Clean-Up Procedures

If you think you have been infected by a virus, and your anti-virus software can't find any known viruses on your system, don't lose hope. This procedure will recover as much as is practical after a virus attack has occurred.

1. As soon as you notice virus symptoms, back up all *data* files.
2. Disconnect all peripherals and communications connections including modems, external disk drives, printers, and internal boards with a power source. If you have a Mac 128K, 512, 512E, or Plus, remove the battery and wait fifteen minutes to reset the PRAM.
3. Restore power to the machine, as well as any boards necessary for the Mac to function. If you have a Mac 128K, 512, 512E, or Plus, replace the battery. If you have any other Mac, reset the PRAM.
4. Reformat your hard-disk drive.
5. Restore the System files from a locked master copy.
6. Replace the remaining batteries, boards, and peripherals.
7. Restore programs from their original locked master copies.
8. Restore data from backups made in Step 1 and other current backups, but check these backups for viruses first.

If the symptoms of viral infection remain even after this procedure, there are two possibilities: One, the virus infected either one of your data files or one of your locked original master disks; or two, you have a hardware problem and not a virus infection. To

test if you still have a virus, repeat these steps, only this time you'll load applications and data files one at a time. If the problem occurs after a specific file is loaded, you know that is the one with the virus. If you can't isolate the virus to one file (or several files), you have a hardware problem.

Keep in mind that it is unlikely you will be hit with an unknown virus. Your chances are greater for getting one that is already known by the anti-virus software companies. If you keep your anti-virus software up to date, you will probably never have to deal with an unknown virus infection.

Table 5.1: Anti-Virus Programs

Product	List Price	Company	Consumer Phone Number	Main Function	Comments
MacTools (Central Point Anti-Virus) 3.0	\$149.99	Central Point Software	(503) 690-8090	Virus protection, detection, and removal	By watching for abnormal system behavior, the program detects unknown viruses
Disinfectant 3.2 ¹	Freeware	John Norstad	Write to developer	Virus protection, detection, and removal	The best anti-virus software available
GateKeeper 1.0 ²	Freeware	Chris Johnson	Write to developer	Unknown virus detector	Does not protect against WDEF or CDEF viruses
GateKeeper Aid 1.0 ²	Freeware	Chris Johnson	Write to developer	Virus protection and repair	Protects and repairs damage only from WDEF and CDEF viruses
Symantec Anti-Virus for the Macintosh (SAM) 3.5	\$99.00	Symantec Corp.	(800) 441-7234	Virus protection, detection and repair	Intercept init is key to detecting unknown viruses
Virex 5.0 ³	\$99.00	Datawatch Corp.	(919) 549-0711	Virus protection, detection and repair	Virus detection scanner is faster than either Central Point or SAM

¹ John Norstad, Academic Computing and Network Services; Northwestern University; 2129 North Campus Drive; Evanston, IL 60208

² Chris Johnson; available on the Internet

³ Program also comes with Superset Utilities, \$149.00

What to Buy to Prevent Viruses

A good anti-virus program should detect all known viruses and have some capacity to detect unknown viruses. The program should be able to scan any volume as well as compressed files, and should automatically scan removable disks when they are mounted.

AntiToxin

AntiToxin is an old anti-virus program for the Mac. It is no longer supported, and hence does not detect newer viruses. Do not use this product.

Central Point Anti-Virus

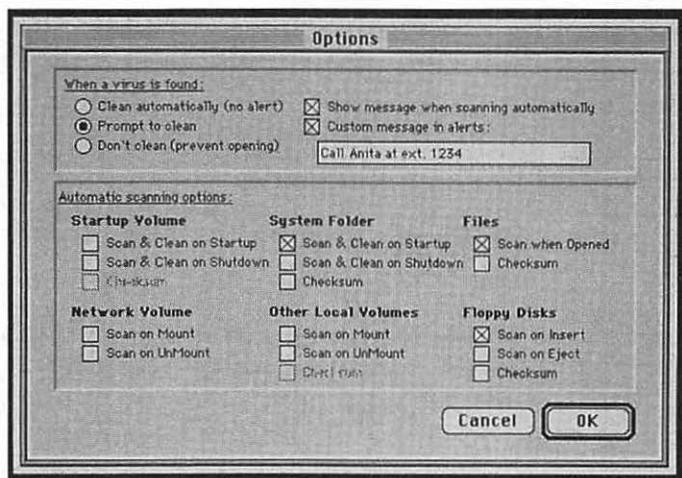
Central Point Anti-Virus is part of MacTools 3.0, from Central Point Software, a comprehensive utilities set that can back up disks, diagnose disk problems, recover deleted files, repair some damaged files, optimize drive performance, and more.

The Anti-Virus program checks for all known Macintosh viruses. It can scan drives automatically or manually, and other options include automatic scans of files on opening, floppies on insertion, and system folders on start-up. It can even scan files while they are still compressed with Stuffit.

When Anti-Virus finds a virus, it can automatically remove the virus, wait for a user prompt, or prevent the infected application from running. You can choose how you want the program to handle this situation.

Figure 5.2

Central Point Anti-Virus



Central Point has several alternatives for keeping Anti-Virus up to date. There is a 24-hour virus hotline for information on the latest viruses, (800) 976-6703. New virus signature files, necessary for detecting and removing viruses, are available on Central Point's BBS, through AppleLink and CompuServe, or you can buy

a disk subscription service and receive updates to the program through regular mail. Central Point can fax the virus signatures to you so you can enter them manually. Finally, the company can send you periodic mailings notifying you when new viruses are discovered if you are too isolated for any of these other options.

Anti-Virus also protects against unknown viruses by continuously watching for suspicious system behavior. To this end, the program can also create file checksums. You can modify what constitutes “suspicious behavior” and tell Anti-Virus to ignore actions by certain programs. If Anti-Virus detects a suspicious activity, it alerts you and you have the choice to halt the action or ignore the threat.



Disinfectant 3.2

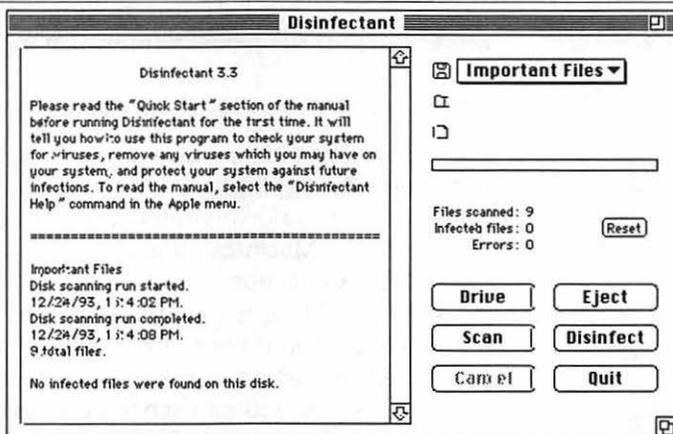
Disinfectant, freeware written by John Norstad, is an excellent virus detection, protection, and removal program. It is complete, easy to use, can detect and remove all known viruses, and best of all, it's free.

Disinfectant has a two-tiered means of doing its job: a main application that detects and removes viruses on request, and an INIT that watches in the background for viruses and provides a warning before the virus can do any harm.

Author John Norstad works with an international network to keep Disinfectant up to date. This group has improved it consistently since the first release, and within days of the discovery of a new virus they deliver a new version of Disinfectant that can identify and remove it.

Figure 5.3

Disinfectant



Another remarkable thing about this freeware package is its 60-page manual detailing everything you ever wanted to know about Disinfectant, including how to use it, what it does, how it does it, and details on the viruses it detects.

Disinfectant is readily available on most Macintosh BBSs, all major on-line services, from Macintosh user groups, and from a lot of Macintosh dealers. If you can get your hands on Disinfectant, there's no reason to spend money on anything else.

GateKeeper and GateKeeper Aid

GateKeeper, freeware written by Chris Johnson, is a control panel document INIT that protects against unknown viruses by monitoring and blocking suspicious activities that are characteristics of viruses.

Unlike the Disinfectant INIT, GateKeeper can sometimes detect new viruses. It's been effective enough at this that several viruses were first discovered by Macintosh users who had GateKeeper installed.

Because some legitimate programs do things that GateKeeper flags as suspicious, you have to configure GateKeeper for your system. This can be very confusing for novices, and may cause a lot of unnecessary panic from false alarms.

One drawback about GateKeeper is that it cannot protect against the WDEF or CDEF viruses, and this is where it gets some help from GateKeeper Aid. This INIT protects against WDEF and CDEF and repairs files infected with these viruses.

Rival

Rival is an anti-virus INIT. It is no longer supported, and does not protect against the newer viruses. Use something else.

Symantec AntiVirus for Macintosh (SAM) 3.5

SAM, from Symantec, has two parts: an application and a control panel. The application, SAM Virus Clinic, scans for and repairs files infected by known viruses. The control panel, SAM Intercept, monitors your Macintosh and alerts you to activities that may indicate a virus infection.

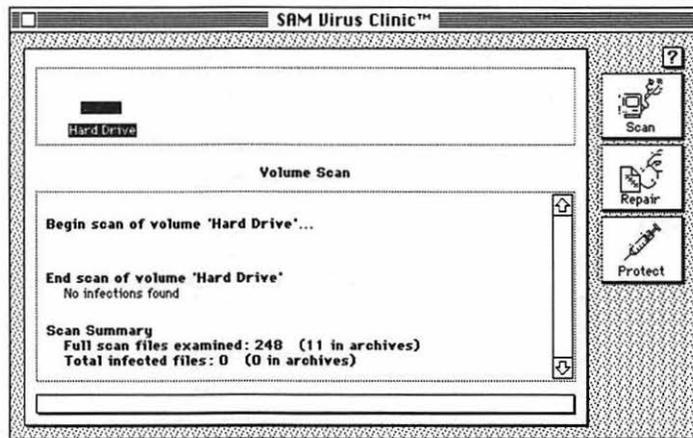
SAM Virus Clinic is easy to install and use. The Installer automatically scans your hard disk for viruses before it begins installation. After installation, you can scan drives for viruses with a few mouse clicks, or you can schedule virus scans to run at specific times on specific dates. Unfortunately, you must leave Virus Clinic

running for the automatic scanning feature to work. Virus Clinic can scan for viruses in StuffIt and CompactPro archives by temporarily decompressing them into RAM.

SAM Intercept sits in the background and watches your disks. Whenever you load a floppy or launch a file, SAM Intercept checks for viruses. A real nice feature of the Intercept is that it recognizes when you're running Apple's Installer, which is likely to do things that could be caused by a virus, and asks if you'd like it to cease virus checking until you've finished with the installation. Many programs that run Installer ask you to turn off your virus protection program during installation, which puts you at risk of forgetting to reactivate this later.

Figure 5.4

SAM



Virex 5.0

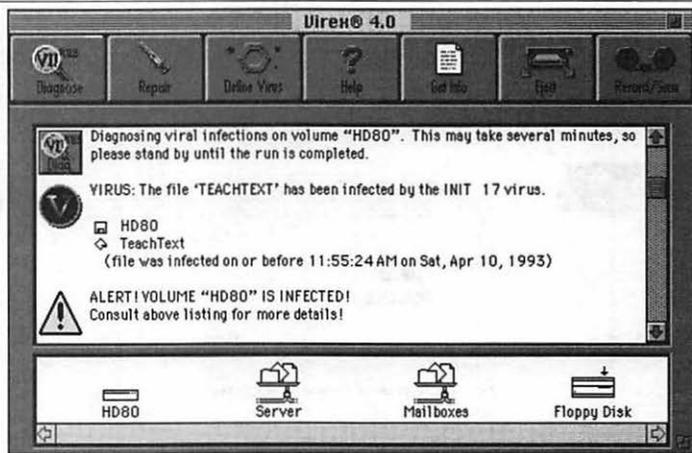
Virex, available alone or as part of the Superset Utilities from Datawatch, is comprehensive: It's a preventer, detector, and eradicator of all known viruses. The detector scans disks and volumes while the preventer continuously monitors the computer, looking for virus infections before they happen. If a virus has attacked your system, Virex will repairs the infected files. All of these operations are fast, thanks particularly to "SpeedScan" which flies through the scanning process at a much faster clip than either Symantec's or Central Point's virus detection scanner.

Virex can also scan for unknown viruses. In Expert Mode it lets you take checksums of files on your system that are susceptible to virus attack. Virex can then detect if a virus should change these files.

Using Virex is easy. With a single button, you can scan all hard drives for viruses. Another button repairs infected files, and yet another function lets you update Virex manually to diagnose newly discovered viruses. If you register your copy of Virex, you will receive information in the mail whenever a new Macintosh virus is discovered. This card will give the specific information necessary to update your copy of Virex.

Figure 5.5

Virex



You can configure Virex to automatically diagnose all files as soon as a program is launched, to automatically diagnose floppies as soon as they are inserted into the disk drive, or to diagnose applications only.

Virex is also completely compatible with Apple Installers, so you don't have to disable it whenever you install new software.

VirusBlockade and VirusDetective

VirusBlockade and VirusDetective are a control panel and a desk accessory, respectively. Both detect known viruses and are excellent shareware programs, but the authors will no longer support new users for the product. While they say they will still promulgate search strings for any new viruses that are discovered, they recommend that new users find an alternative anti-virus program.

Chapter 5 Summary

- A virus is a program that modifies another program to include an executable, and possibly altered, copy of itself. Viruses run in secret, often when the user launches the program the virus is attached to. Some are content merely to multiply, other viruses are malicious and try to damage your files or system.
- Anti-virus software is easy to come by and easy to use.
- Detective software finds known viruses by looking for the unique string of bytes that identifies that virus' code. The program can remove the virus and attempt to restore your system to its pre-viral state. This is a separate application that runs only when you tell it to. It looks for known virus signatures.
- Unknown viruses are harder to detect. In this case, preventative software looks for changes to a file's attributes such as length, checksum, file header, etc., since changes to files are one symptom of a virus infection. However, since files' attributes change all the time during normal Mac operation, running this type of software continuously will result in many false alarms. It also slows down your system.
- Once the virus has been found and removed, the anti-virus software will not be able to restore files that have been changed by the virus. In this case, replace your applications with copies from your locked master floppy disks. The damaged files must be deleted and replaced from backup copies.
- New versions of major anti-virus software are released within hours or days after a new virus is discovered. You can keep your anti-virus software up-to-date through one of the electronic information services, through the bulletin board service of the software company, or through a subscription service.

Chapter 5 Sources

MacTools 3.0, \$149
Central Point Software, Inc.
15220 N.W. Greenbrier Pkwy.
Beaverton, OR 97006
(503) 690-8090
FAX: (503) 690-8083

Disinfectant 3.2, freeware
John Norstad
Academic Computing and Network Services
Northwestern University
2129 North Campus Drive
Evanston, IL 60208

GateKeeper, freeware
Available on the Internet
Chris Johnson

Symantec AntiVirus for Macintosh (SAM) 3.5, \$99
Symantec Corp.
10210 Torre Ave.
Cupertino, CA 95014
(503) 334-6054
(800) 441-7234
FAX: (503) 334-7471

Virex 5.0, \$99
Superset Utilities, \$149
Datawatch Corp.
Triangle Software Division
P.O. Box 13984
Research Triangle Park, NC 27709
(919) 549-0711
FAX: (919) 549-0065



Macintosh Viruses— a Rogue's Gallery

This chapter describes all of the Macintosh viruses known as of this writing, including the two most common ones, nVIR and WDEF. By the time you read this, there will almost certainly be one or two more. Check the current manual of your favorite anti-virus software for updates.

The Scores Virus

Aliases: Eric, Vult, NASA, San Jose Flu

According to news reports, the Scores virus was written by a disgruntled programmer to attack two applications that were under development at his former company. Fortunately, neither of the applications was ever released to the general public.

Scores, first discovered in 1988, can be easy to detect. Open your System folder and check the icons for the Note Pad and Scrapbook files. They should have distinctive icons, under System 7, or look like little Macintoshes under System 6. If they instead look like blank sheets of paper with turned-down corners, your software may be infected by Scores.

However, it is possible to be infected by Scores and still have normal Note Pad and Scrapbook icons. You should run an anti-virus program to make certain your system is not infected, even if it shows no signs of infection.

Scores infects your System, Note Pad, and Scrapbook system files. It also creates two files in your System folder, named "Scores" and "Desktop," that are invisible in all cases except when you are using ResEdit or some other resource editor. Do not confuse Scores' invisible Desktop file with the Finder's invisible Desktop file; they have nothing to do with each other. The Finder's Desktop file lives at the root level on your disk, outside the System folder, while Scores' Desktop file lives inside the System folder. Also, Scores' Desktop file has an extra space character at the end of its name.

Scores does not infect or modify document files, only applications and system files. Two days after your system becomes infected, Scores begins to spread to each application you run—Finder and DA Handler can also be infected in this time. For technical reasons, some applications are immune to infection. The infection occurs between two and three minutes after you launch the application.

Scores does not intentionally do any damage other than spread itself and attack the two specific applications. It does occupy memory and disk space, however, and this by itself can cause problems. People have reported difficulties with printing and using MacDraw and Excel. Scores creates several errors which could cause system crashes or other unexplained behavior.

There is a serious conflict between Scores and Apple's System Software release 6.0.4—and later releases of System 6. In System 6.0.4, Apple began using some resources with the same type and ID as those used by Scores. When Scores infects the System file in these cases, it replaces Apple's versions of these resources with Score's own versions. When some anti-virus programs repair the System file, they delete the Scores viral resources, but do not restore the Apple versions. In this situation, most anti-virus software will display a special error message, telling you that the resulting file is damaged and should not be used. You should immediately delete the damaged System file, and replace it with a copy from original locked Apple release disks.

The nVIR Virus

Variants: AIDS, F***, Hpat, Jude, nFLU, MEV#, Modm, nCAM, nVIR-f, prod, zero

nVIR is simpler than Scores. It infects the System file, but not the Note Pad or Scrapbook files, and it does not create any invisible files. nVIR begins spreading to other applications immediately, without the two-day delay incorporated in Scores. Whenever a

new application is run, it immediately becomes infected, without the two- to three-minute delay. As with Scores, some applications are immune to infection, as are document files, though the Finder and DA Handler are usually infected.

According to news reports, the nVIR virus first appeared in Europe in 1987, and in the United States in early 1988. There are two basic strains, nVIR A and nVIR B, though other reports indicated an earlier and more malicious third version that destroyed files in the System folder. This third variant appears to be extinct.

nVIR A and nVIR B only duplicate themselves at first. When the System file is first infected, a counter is initialized to 1000. The counter is decremented by one, each time the system is started up, and it is decremented by two each time an infected application is run.

When the counter reaches zero, nVIR A will sometimes say "Don't panic" on Macs with MacinTalk, or beep on those without MacinTalk. When the counter of nVIR B reaches zero, it will sometimes beep, but it does not call MacinTalk.

As with Scores, nVIR occupies both memory and disk space, and this alone is enough to cause problems.

It is possible for nVIR A and nVIR B to mate and reproduce, resulting in new viruses combining parts of their parents. Anti-virus software will generally report that such offspring are infected by both nVIR A and nVIR B, and will properly repair them.

You must run a virus detection tool to identify an nVIR infection, because there is no way to tell that you have been infected just by looking at your system. One of the viral resources added to infected files by nVIR has the resource type "nVIR," which is how it got its name.

In addition to the two basic strains, nVIR B has many "clones," that are all identical to it with the exception of a few very minor technical differences. All anti-virus programs reviewed here recognize all of these clones, and treat them exactly the same as nVIR B.

The INIT 29 Virus

Variants: INIT 29 A, INIT 29 B

The INIT 29 virus is extremely virulent, and spreads very rapidly. Unlike Scores and nVIR, INIT 29 can infect applications even when they are not running. Also, it can and will infect almost any file, including applications, system files, and document files. However, the virus spreads only through system files and applications—infecting document files cannot spread INIT 29.

INIT 29 makes its presence known when you try to insert a locked floppy disk into an infected system, by giving the following alert:

The disk "xxxxx" needs minor repairs.
Do you want to repair it?

If you see this alert whenever you insert a locked floppy, your system is probably infected by INIT 29.

As with Scores and nVIR, INIT 29 does not intentionally do any damage other than spread itself. Nevertheless, because of bugs in the code, the virus can cause problems with printing, system crashes, and using MultiFinder under System 6, and incompatibilities with several start-up documents.

One of the viral resources added to infected files by INIT 29 has the resource type "INIT," and the resource ID 29. The virus was discovered in late 1988, but its origins are unknown.

The INIT 29 A virus also first appeared in late 1988. We do not know much about its origin. A second minor variant appeared in March 1994: INIT 29 B. There are no significant differences between these two strains.

The ANTI Virus

Variants: ANTI A, ANTI B, ANTI-0, ANDI-ANGE

ANTI infects only applications and other files which resemble applications—like the Finder—but not the System file or document files. It is possible for an application to become infected even if it is never run.

Due to a technical quirk, ANTI does not spread at all under System 7, nor under System 6 when MultiFinder is used. It only spreads when Finder is used under System 6.

An error in ANTI causes it to slightly damage applications in such a way that anti-virus programs cannot perfectly repair them. So, the repaired application doesn't usually resemble the uninfected original. However, the damage is very minor. If you do experience problems with an ANTI-infected application, after repairing it with an anti-virus program, you should delete this repaired copy and replace it with the uninfected original copy. Most anti-virus programs warn you of the possibility of permanent damage when the virus is discovered.

For the technically inclined, the error in ANTI is that it clears all the resource attributes of the CODE 1 resource. An anti-virus program has no way of knowing the values of the original attributes, so it leaves them cleared on the repaired application. As a

result of this error, the repaired application may use memory less efficiently than the original version, especially on old Macintoshes with the 64K ROMs.

As with the other viruses, ANTI does not intentionally do any damage other than spread itself. It is less contagious than the INIT 29 virus, but more contagious than the Scores and nVIR viruses. As with all viruses, however, it can still cause problems.

The virus is named for the string "ANTI" which appears within the virus' code. The ANTI virus has two major strains which were both first discovered in France—ANTI A, in February 1989, and ANTI B, in September 1990.

The A strain of the virus, which was written before the B strain, contains special code that neutralizes any copies of the B variant that it encounters. It is possible for an application to be infected by both the neutralized version of the B strain and by the A strain. Aside from this special code in the A strain, there are only minor technical differences between these two versions of the virus.

The MacMag Virus

Aliases: Aldus, Brandow, Drew, Peace

The MacMag virus appeared in December 1987. It was named after the Montreal offices of *MacMag* magazine, where it originated. Unlike the other viruses, MacMag does not infect applications, only System files. It originated as a HyperCard stack named "New Apple Products." The stack contained some poorly digitized pictures of the then-new Apple scanner. When the stack was run, the virus spread to the currently active System file. When other floppy disks containing System files were subsequently inserted in a floppy disk drive, the virus spread to the System files on the floppies.

Applications are not infected by MacMag. It spreads much slower than the other viruses, because people are less likely to share System files than they are to share applications. Even though the virus originated on a HyperCard stack, it does not spread to other stacks—only to System files.

MacMag was programmed to wait until March 2, 1988, the first anniversary of the introduction of the Mac II. The first time the system was started up on March 2, 1988, the virus displayed a message of "peace" on the screen and then deleted itself from the System file.

Since MacMag was programmed to self-destruct, it is unlikely that your software is infected with this virus. Nevertheless, anti-

virus programs recognize it and repair infected files, just in case you have some very old floppy disks that might still be infected.

Anti-virus programs repair both infected System files and infected copies of the original HyperCard stack. If you try to run the repaired stack, HyperCard will issue an error message.

There were two slightly different versions of MacMag. The differences were very minor, and both versions were programmed to behave identically. Anti-virus programs detect and repair System files infected with either version.

The WDEF Virus

Variants: WDEF A, WDEF B.

First discovered in 1989 in Belgium, and at Northwestern University, WDEF is a widespread virus that infects only the invisible Desktop files used by the Finder. With few exceptions, every Macintosh disk—hard drives and floppies—contains one of these files. WDEF does not infect applications, document files, or other system files. Unlike the other viruses, it is not spread through the sharing of applications, but rather through the sharing and distribution of disks—usually the floppy variety. And WDEF spreads only under System 6, as System 7 is completely immune to the WDEF virus.

WDEF spreads from disk to disk very rapidly, because the Desktop file opens immediately when a disk is mounted or inserted. If the Macintosh is already infected with the WDEF virus, disks are infected as soon as you insert or mount them. Similarly, if you insert an infected floppy disk in an uninfected Mac, the virus infects any mounted hard drive.

Although the virus does not intentionally damage machines, WDEF contains errors that can cause very serious problems with the operation of your Mac. For instance, newer Mac models, like the IIfx and later, that run System 6 can crash almost immediately after insertion of an infected floppy. The virus also causes other Macs to crash much more frequently than usual, and it can damage disks. The virus also wreaks havoc with the proper display of type styles—particularly with "outline."

You can remove a WDEF infection from a disk by rebuilding the Desktop. In fact, it is often easier to get rid of it this way than by using an anti-virus program.

Even though AppleShare servers do not use the normal Finder Desktop file, many servers have an unused copy of it. If the AppleShare administrator has granted the Make Changes privilege to the root directory on the server, then any infected user of the

server can infect the Desktop file on the server. If a server Desktop file becomes infected, performance on the network will be very severely degraded. For this reason, administrators should never grant the Make Changes privilege on server root directories. I also recommend deleting the Desktop file if it exists. Apparently, WDEF cannot spread from an AppleShare server to other Macs on the network.

WDEF can spread from a TOPS server to a TOPS client, if a published volume's Desktop file is infected and the client mounts the infected volume. It does not appear, however, that the virus can spread from a TOPS client to a TOPS server.

If you use ResEdit, VirusDetective, or some other tool to search for WDEF resources, do not be alarmed if you find them in files other than the Finder Desktop files. WDEF resources are a normal part of the Macintosh operating system. Any WDEF resource in a Finder Desktop file, however, is cause for concern.

When using an anti-virus program to repair WDEF infections under System 6, you must use Finder instead of MultiFinder. Under MultiFinder, the Desktop files are always "busy," and an anti-virus program is not able to repair them.

WDEF has two strains that are very similar, WDEF A and WDEF B. The only significant difference is that WDEF B beeps every time it infects a new Desktop file, whereas WDEF A does not. In addition to the two known strains of the WDEF virus, most anti-virus programs will also detect and repair other strains which may exist, but have not yet been reported.

The ZUC Virus

Variants: ZUC A, ZUC B, ZUC C

There are three known strains of the ZUC virus, all of which were discovered in Italy in 1990 and 1991. The virus is named after the reported discoverer of the first strain, Don Ernesto Zucchini.

ZUC only infects applications. It does not infect System files or document files. Applications do not have to be run to become infected.

ZUC A and B were timed to launch on March 2, 1990, or two weeks after an application was infected—whichever date was later. Before that date, they only spread from application to application.

Approximately 90 seconds after an infected application is run, the cursor begins to behave unusually whenever the mouse button is held down. The cursor moves diagonally across the screen, bouncing like a billiard ball and changing direction whenever it

reaches any of the four sides of the screen. The cursor stops moving when the mouse button is released. The behavior of the ZUC virus is similar to that of a desk accessory named "Bouncy." The virus and the desk accessory are different, and they should not be confused. The desk accessory does not spread and it is not a virus. ZUC does spread, and it is a virus.

ZUC C is very similar to ZUC A and B. The only significant difference is that ZUC C is timed to cause the same unusual cursor behavior only during the period between 13 and 26 days after an application becomes infected, but not earlier than August 13, 1990.

ZUC has two noticeable side effects. On some Macs, the A and B strains can cause the desktop pattern to change. All three strains can also sometimes cause long delays, and an unusually large amount of disk activity, when infected applications are opened.

ZUC can spread over a network from individual Macintoshes to servers, and from servers to individual Macintoshes. Except for the unusual cursor behavior, ZUC does not attempt to do any damage.

ZUC makes changes to a file, but it holds the modification date. Since the modification date doesn't change, you're left without a way of tracing the virus.

The MDEF Virus

Aliases: Garfield, Top Cat

Variants: MDEF A, MDEF B, MDEF C, MDEF D

There are four known strains of the MDEF virus, all of them discovered in Ithaca, New York. The MDEF A strain was discovered in May, 1990 and is also sometimes called the "Garfield" virus. The MDEF B strain was discovered in August 1990, and is also sometimes called the "Top Cat" virus. The C and D strains were discovered in October 1990, and January 1991, respectively.

Prompt action by computer security personnel, and investigators of the New York State Police resulted in identification of the author. The author, a juvenile, was released into the custody of his parents after consultation with the district attorney. The same person was responsible for writing the CDEF virus, described on page 130.

The A, B, and C strains of MDEF can infect applications, the System file and other system files, document files, and Finder Desktop files. Additionally, the Finder and DA Handler are also infected. The System file is infected as soon as an infected applica-

tion is run. Other applications become infected as soon as they are run on an infected system.

The D strain of MDEF only infects applications, not system files or document files. Applications can become infected even if they are never run. An application infected by MDEF D beeps every time it is run. Although it is believed that the D strain of MDEF was never released to the public, anti-virus programs recognize it anyway.

The MDEF viruses do not intentionally do any damage, yet they can be harmful. They do not display any messages or pictures. The MDEF B and C strains attempt to bypass some of the popular protection INITs. The MDEF C strain contains a serious error which can cause crashes and other problems.

The MDEF D virus can cause certain damage to applications that cannot be properly repaired by anti-virus programs. For example, the virus may distort an application's menus. In this situation, anti-virus programs can remove the virus from the application, but cannot restore the menus. To restore the menus, you should replace the damaged application with your known good copy from the locked master disk.

The MDEF viruses are named after the type of resource they use to infect files. MDEF resources are a normal part of the Macintosh system, so you should not be alarmed if you see them while using ResEdit or some other tool.

The MDEF, WDEF and CDEF viruses have similar names, but they are completely different and should not be confused with each other.

The Frankie Virus

The Frankie virus is quite rare, because it only affects some kinds of Macintosh emulators running on Atari computers. Frankie does not spread, or cause any damage, on any of the regular Apple Macintosh computers. Some reports say that it was targeted against pirated versions of the Aladdin emulator. It does not affect the Spectre emulator.

After a time delay, Frankie draws a bomb icon and the message "Frankie says: No more piracy!" at the top of the Atari screen, and then causes the Atari to crash.

Frankie infects only applications, not system files or document files. The Finder also usually becomes infected. Applications do not have to be run to become infected. For technical reasons, the virus spreads only under Finder, not MultiFinder.

The CDEF Virus

The CDEF virus was first discovered in Ithaca, New York, in August 1990, and was written by the same person who wrote the MDEF virus. See the description of the MDEF virus on page 128 for details. The CDEF virus is quite widespread.

CDEF is very similar to the WDEF virus, in that it infects only the invisible Desktop file used by the Finder and not applications, document files, or other System files. It spreads from disk to disk very rapidly. Fortunately, System 7 is completely immune to the CDEF virus.

CDEF infects the hidden Desktop file the Finder uses. When you insert a floppy disk, or mount a hard disk drive, the Desktop file is opened immediately, activating the virus. Once the Macintosh is infected with the CDEF virus, disks are infected as soon as you insert or mount them. Similarly, if you insert an infected floppy disk in the computer, the virus infects any mounted hard disk drive. It is not necessary to run an application for the virus to spread. Although the behavior of the CDEF virus is similar to that of the WDEF virus, it is not a simple clone of WDEF. CDEF is a completely different virus.

The virus does not intentionally do any damage. In some cases, the system beeps when a new Desktop file is infected, but this is by no means true in every instance. As with all viruses, however, the CDEF virus is still dangerous. There have been many reports of problems on CDEF-infected systems.

As with the WDEF virus, you can remove a CDEF infection from a disk by rebuilding the Desktop. Eradicating CDEF this way is often easier than using an anti-virus program.

The CDEF virus is named after the type of resource it uses to infect files. CDEF resources are a normal part of the Macintosh operating system, so you should not panic if you see them while using ResEdit or some other tool. Any CDEF resource in a Finder Desktop file, however, is cause for concern.

When using an anti-virus program to repair CDEF infections under System 6, you must use Finder and not MultiFinder. The Desktop files are always "busy" under MultiFinder, and the anti-virus program will not be able to repair them.

A new version of the CDEF virus was discovered in February 1993. There are only minor technical differences between the new version and the original virus. Anti-virus programs recognize both versions. In addition to the known strain of CDEF, most anti-virus programs will also detect and repair other strains which may exist but have not yet been reported.

The MBDF Virus

The MBDF virus was first discovered in Wales in February 1992. Several popular Internet archive sites contained some infected games for a short time, so a number of people around the world were affected. The games were named "10 Tile Puzzle" and "Obnoxious Tetris." A third game named "Tetricycle" or "Tetris-rotating" was a Trojan horse that also installed the virus.

The MBDF virus is non-malicious, but it can cause damage. It infects both applications and the System file. It can also infect the Finder and several other system files. The System file is infected as soon as an infected application is run. Other applications become infected as soon as they are run on an infected system.

The virus takes quite a long time to infect the System file in the initial attack. The delay is so long that people often think their Mac system is hung up, so they do a restart. Restarting the Mac while the virus is in the process of writing the System file very often results in a damaged System file, which cannot be repaired. The only solution in this situation is to reinstall a new System file from scratch.

There are reports that the MBDF virus causes problems with the "BeHierarchic" shareware program, and other reports of menu-related problems on infected systems.

Anti-virus programs detect MBDF in the infected files and in the Trojan horse. Repairing an infected file removes the virus and returns the file to the state it was in before being infected. Repairing the Trojan horse renders it ineffective and inoperable.

Two undergraduate students at Cornell University were apprehended shortly after the virus was discovered, and they pleaded guilty to charges of second-degree computer tampering for writing and spreading the MBDF virus. They were sentenced to community service and restitution of damages. A third student at Cornell also pleaded guilty to a charge related to helping to spread the virus, and was sentenced to community service.

The MBDF virus is named after the type of resource it uses to infect files. MBDF resources are a normal part of the Macintosh system, so you should not become alarmed if you see them while using ResEdit or some other tool.

The INIT 1984 Virus

INIT 1984 is a malicious virus, triggered to go off if an infected system is restarted on any Friday the 13th in 1991 or later years. Like INIT M, described later in this chapter, INIT 1984 damages a

large number of folders and files, changing file and folder names to random one-to-eight character strings; changing file creators and file types to random four character strings; and changing creation and modification dates to January 1, 1904. In addition, it changes the icons associated with the files, destroys the relationships between programs and their documents, and the virus can delete just less than two percent of files.

The virus, discovered in the Netherlands and in several locations in the USA in 1992, caused significant damage to the hard drives of several users on Friday, March 13 of that year. Because only a relatively small number of users reported damage, it is hoped that the virus is not widespread.

Unlike INIT M, this virus infects only INITs (also known as start-up documents or system extensions), and not the System file, Desktop files, Control Panel files, applications, or document files. Because INIT files are shared less frequently than are programs, the INIT 1984 virus does not spread as rapidly as most other viruses. The virus spreads only from INIT to INIT at start-up time.

The virus affects all types of Macintoshes. It spreads and causes damage, under both System 6 and System 7. On very old Macintoshes (the Mac 128K, 512K, and XL), the virus will cause a crash at startup.

If you have an INIT file that is infected by the INIT 1984 virus, most anti-virus INITs alert you to its presence during start-up. The virus is then neutralized, and does not spread or cause any damage—but the non-viral part of the infected INIT runs as usual.

The CODE 252 Virus

Discovered in California in April 1992, the CODE 252 virus is rigged to wreak its havoc if an infected application is launched—or an infected system is started up—between June 6 and December 31 (inclusive) of any year. When triggered, the virus displays the following message:

```
You have a virus.  
Ha Ha Ha Ha Ha Ha Ha  
Now erasing all disks...  
Ha Ha Ha Ha Ha Ha Ha  
P.S. Have a nice day  
Ha Ha Ha Ha Ha Ha Ha  
(Click to continue... )
```

Despite this message, no files or directories are deleted by the virus. However, a worried user might turn off or restart a Macintosh upon seeing this message, and this could corrupt the disk and lead to significant damage.

Between January 1 and June 5 (inclusive) of any year, Code 232 spreads from applications to System files, and then on to other application files. Under any system, the virus infects the System file, and it can and will trigger the display of the message.

Because of several errors in the virus, Code 232's infection depends on which version of the Mac operating system is in use:

Under System 6 without MultiFinder, it spreads to new applications, and sometimes to the Finder.

Under System 6 with MultiFinder, the virus infects the System files, but it does not spread to new applications.

Under System 7, the virus infects the System file, but it does not spread to new applications. Furthermore, other errors in the virus can cause crashes or damaged files.

The T4 Virus

Variants: T4-A, T4-B, T4-C, T4-beta

The T4 virus was discovered in several locations around the world in June 1992. The virus was included in versions 2.0 and 2.1 of the game GoMoku. Copies of this game were posted to the USENET newsgroup comp.binaries.mac and to a number of popular bulletin boards and anonymous ftp archive sites.

The game was distributed under a false developer name that was used in the posting and was embedded in the game's "About" box. The person named had absolutely nothing to do with the writing and distributing of the virus, so please don't use this person's name in reference to the virus. The actual author of the virus is unknown.

T4 spreads to other applications and to the Finder. It also attempts to alter the System file. When the virus infects an application, it damages it in such a way that the application cannot be repaired. When you use an anti-virus program to repair an infected application, the anti-virus program will remove the virus from the file, but will leave the file damaged. You should not attempt to use such a file. Instead, you should delete the application and replace it with a known good copy.

The change to the System file results in alterations to the start-up code under System 6 and 7, such that INIT files and system extensions will not load. Under System 7.0.1, the change may

render the system unbootable, or cause crashes in unpredictable circumstances. Anti-virus programs cannot repair this damage to the System file. If the virus damages your System file, you will have to reinstall it.

If your system suddenly stops loading INITs and system extensions for no good reason, that is a strong indication that you may have been attacked by the T4 virus.

The virus masquerades as "Disinfectant" in an attempt to bypass general-purpose, suspicious-activity monitors like Gatekeeper. If you see an alert from such an anti-virus tool telling you that "Disinfectant" is trying to make some change to a file, and if Disinfectant is not running, chances are T4 is attacking your system. The virus also may rename files "Disinfectant."

Once installed and active, the virus does not appear to perform any other overt damage, though it may display the following message:

Application is infected with the T4 virus.

There are four known strains of the T4 virus: T4-A (contained in GoMoku 2.0), T4-B (contained in GoMoku 2.1), T4-C (discovered in February, 1993), and a version which appears to have been used for testing—sometimes called T4-beta. The strains are very similar. The only significant difference is the trigger date. The trigger date for T4-A is August 15, 1992, while T4-B is set for June 26, 1992. The virus does not do anything before its trigger date. After the trigger date, the virus begins to spread to other files, and attempts to alter the System file. The T4-C virus has no trigger date; it begins spreading immediately.

The INIT 17 Virus

Discovered in New Brunswick, Canada, in April 1993, the INIT 17 virus infects the System file and applications. It does not infect document files.

The virus displays the message "From the depths of Cyberspace" the first time an infected Macintosh is restarted, after 6:06:06 A.M. on October 31, 1993. After this message has been displayed once, it is not displayed again.

The virus contains many errors that can cause crashes and other problems. In particular, it causes crashes on the Mac Plus, SE, and Classic—Macintoshes with the 68000 processor.

For technical reasons, the virus does not infect some applications, and on some systems it does not spread at all. It does, however, spread under both System 6 and System 7.

The INIT-M Virus

The INIT-M virus is a malicious virus that was discovered at Dartmouth College in April 1993. It is designed to go off on any Friday the 13th, at which time the virus severely damages a large number of folders and files. File names are changed to random eight-character strings; folder names are changed to random one-to eight-character strings; and file creators and types are changed to random four-character strings. It also changes the icons associated with the files and destroys the relationship between programs and their documents. Additionally, file creation and modification dates are changed to January 1, 1904, and in some cases, one file or folder on a disk may be renamed "Virus MindCrime." In some very rare circumstances, the virus may also delete a file or files, and it can sometimes cause problems with the proper display of windows.

The virus spreads, and attacks, only under System 7.0 or later. Anti-virus INITs, however, will detect an infected application under any system.

INIT M infects all kinds of files, including extensions, applications, preference files, and document files. The virus creates a file named "FSV Prefs" in the Preferences folder. If you use an anti-virus program to repair an infected system, it will delete this preferences file.

The damage caused by the INIT-M virus is very similar to that caused by the INIT 1984 virus. Despite this similarity, the two viruses are very different in other respects, and should not be confused.

The Dukakis Virus

The Dukakis virus was discovered in August 1988 on a Hypercard stack by the Compuserve and INFOMac on-line services. This virus was written in HyperTalk code, so it only infects other HyperCard stacks.

When activated, the virus displays this message:

Greetings from the HyperAvenger! I am the first HyperCard virus ever. I was created by a mischievous 14-year-old, and am completely harmless. Dukakis for president in '88. Peace on Earth and have a nice day.

The virus then duplicates itself to the user's Home stack, and to all other stacks on the system. Then it goes to sleep for three weeks before it activates again. The virus does no damage to the system.

The Mosaic and FontFinder Trojan Horses

These two Trojan horses were first detected in Edmonton, Alberta (Canada), in January 1990 where they were downloaded from a local Macintosh BBS. Mosaic and FontFinder are both malicious, and they deliberately destroy disks.

However, being Trojan horses and not viruses, they do not spread automatically from file to file, or from system to system. They can only be spread by users exchanging files, either by disk or via bulletin board.

The first strain was embedded in a program called Mosaic. When launched, it immediately destroys the directories of all available, physically unlocked, hard and floppy disks—including the volume on which it resides. Destroyed disks are renamed "Gotcha!", and the program mounts all unmounted, but available, SCSI hard disks to destroy their contents. The only disks that remain untouched are those that are physically locked.

The second strain was embedded in a program called FontFinder. This Trojan horse was a time bomb, with a trigger date of February 10, 1990. Prior to that, the program simply displayed a list of the fonts and point sizes in the System folder. On, or after, that trigger date, the Trojan behaved exactly like the first strain.

There is evidence that both of these Trojan horses are related, and that one is an "improved" version of the other. Neither version has ever been detected outside the Edmonton area, although there is some evidence that they were uploaded to a BBS in the Seattle area. No other versions of this Trojan horse have ever been reported.

The CODE 1 Virus

The CODE 1 Virus was discovered at several colleges and universities on the East Coast of the United States in November 1993. The virus infects both applications and the System file. It does not infect document files. It spreads under both System 6 and System 7.

The virus renames the system hard drive "Trent Saburo" whenever an infected Mac is restarted on any October 31. Although the virus does not contain any other intentionally destructive code, it can cause crashes and other problems.

The INIT 9403 Virus

Aliases: SysX

The INIT 9403 virus was discovered in Italy in March 1994. Unlike most of the other Macintosh viruses, INIT 9403 is very destructive. After a certain number of other files have been infected, the virus will erase disks connected to the system. It attempts to destroy disk information on all connected hard drives (greater than 16MB in size) and attempts to completely erase the boot volume.

The current strain of the INIT 9403 virus has been found only on Macs running the Italian version of the Macintosh system software. Even so, you should use anti-viral software that protects against this virus even if you do not run the Italian system.

The virus spreads under both System 6 and System 7. Once present, the virus alters the Finder file and may insert copies of itself in various compaction, compression, and archive programs. These infected files can then spread the virus to other Macintoshes.

Encrypted and Polymorphic Viruses

Two really nasty types of viruses currently exist only in the PC world, but could possibly find their way over to the Mac—encrypted and polymorphic viruses.

Encrypted viruses have their code encrypted, with a different encryption key for each copy of the same virus. This makes them harder to analyze, harder to fingerprint (the bits are different for each infection), and harder to find. These are particularly insidious when they infect a program. Most viruses of this type attach themselves to the end of a program, then remove a small piece from the beginning of the program, and insert code there that causes the virus code to run first. After the virus code runs, it executes the small piece of code it removed from the beginning of the program—and then your original program runs.

Now, when you run an infected program, you will only notice a slight hesitation at the beginning when the virus code runs, and then the infected program runs normally.

Encrypted viruses store this piece of the normal program within the virus code, and then encrypt the virus code. To patch an infected program, an anti-virus program must be able to decrypt the encrypted virus to find and replace the piece of miss-

ing code. Encrypted viruses can have different levels of encryption, with each level varying for each infection. Decrypting this much code is a very difficult process, so most anti-virus programs will not be able to remove them cleanly. You will have to replace infected applications to ensure that you have undamaged copies.

Polymorphic viruses take encryption to the extreme, in that they are self-mutating. Each time a polymorphic virus duplicates itself, it changes. In addition to encrypting the virus, the remaining part of the code that does the encryption (the only unencrypted part) is variable.

In programming, it doesn't matter in what order certain operations are performed. This means that very small chunks of code—pieces too small to use as signatures—can be rearranged in different orders each time the virus infects a new file. Thus, it is impossible to find a signature string for this type of virus, because no string is common to all instances. In some polymorphic viruses, there can be upwards of six billion different possible instances.

Currently, a polymorphic-virus engine exists in source code somewhere. The means for making such viruses exists. It's only a matter of time before either encrypted or polymorphic viruses appear on the Mac.

Chapter 6 Summary

- You can identify Scores infections by checking the Note Pad and Scrapbook icons in the System folder. If they look like pages with turned-down corners, you may have a Scores infection. Scores spreads to applications and system files, and its memory and space requirements can cause problems on your system.
- The nVIR virus infects the Finder and DA Handler, and some applications. The virus sometimes announces its presence with a message of "don't panic," or with a beep. The two strains, A and B, can mate and produce new viruses.
- INIT 29 (and two variations) can and will infect almost any file. If you insert a locked floppy into a drive infected by INIT 29, you will get an alert that the disk needs repairs. This alert is a good indication that you have an INIT 29 infection.

- The ANTI virus infects applications even if they have never run. These programs are very slightly damaged and cannot be repaired by anti-virus software.
- The MacMag virus originated as a HyperCard stack named "New Apple Products." The virus spread to the System file and subsequently to floppies that contained System files. The virus was programmed to self-destruct after displaying a message of peace on or after March 2, 1988.
- WDEF is the most widespread Macintosh virus. It infects the invisible Desktop files used by the Finder, and it spreads from disk to disk very rapidly. The easiest way to get rid of a WDEF infection is to rebuild the Desktop.
- ZUC causes your cursor to bounce around the screen like a billiard ball whenever the mouse button is held down. It can also cause your Desktop pattern to change.
- The MDEF virus has four variations. These can infect the System file, document files or applications. Versions B and C attempt to bypass some of protection INITs.
- The Frankie virus infects only Macintosh emulators running on Atari computers. It is quite rare.
- System 7 is immune to the CDEF virus but it spreads under System 6 by infecting the Desktop file that the Finder uses. Rebuild the Desktop to get rid of a CDEF infection.
- MBDF spread through some infected games named "10 Tile Puzzle," "Obnoxious Tetris," and a Trojan horse game named "Tetricycle" or "Tetris-rotating." The virus affects the System file and takes so long to do so that some people will restart their computer while the virus is working. This causes severe damage to the System file.
- The INIT 1984 virus is malicious virus that severely damages files and folders when the infected computer is restarted after October 31, 1991. INIT 1984 only infects start-up documents, but can affect all types of Macintoshes.

- CODE 252 is a malicious virus that gives the user a message that all his disks are being erased. This does not actually happen. But the virus contains enough errors that it can cause crashes and other problems on any system.
- The T4 virus spread in versions 2.0 and 2.1 of a game called GoMoku. The virus spreads to applications, and damages them so that they cannot be repaired. You'll have to reinstall such damaged programs.
- The INIT 17 virus displays the message "From the depths of Cyberspace" the first time an infected Mac is restarted after 6:06:06 on October 31, 1993. The virus infects both the System file and application files, but not document files. It can spread under both Systems 6 and 7.
- INIT-M is a malicious virus that severely damages files and folders. It may change file and folder names to random character strings, and change file creation dates to January 1, 1904. It only spreads, and attacks, under System 7.0 or later.
- The Dukakis virus infects only HyperCard stacks, and does not appear to do any serious damage.
- The Mosaic and FontFinder Trojan horses attempt to destroy disks. Mosaic destroys the directories of all unlocked hard and floppy disks. FontFinder was a program with a time bomb, triggered on February 10, 1990. It, too, destroys the directories on all unlocked disks.
- CODE 1 infects applications and the System file. It renames the system hard drive "Trent Saburo" whenever the Mac is restarted on October 31 of any year. The virus can cause crashes and other problems
- The INIT 9403 is a very destructive virus that has been found on Macintoshes running the Italian version of the Mac system software. It can destroy disk information, alter the Finder file, and spread to other connected hard drives.



P A R T



Back Up Your Files

A variety of factors can flush away your data, including user malice, user negligence, computer viruses, hardware and software failure, and environmental hazards. Whatever the cause, a current set of backups will prevent this loss from being a catastrophe. No matter how careful you are, sooner or later you are going to lose a file or a hard drive. Backups are more than your first line of defense: they will save you.



The What, When, Where, and Why of Backups

Perhaps the single most important security procedure you can put in place is a regular backup plan. Backups will not protect your data from loss or corruption, but they will make it possible for you to recover from such calamities. If a tornado relocates your computers halfway down the block, or a thief empties your offices one day, or if a virus lays waste to your hard drive—you are going to need current backups to recover.

There are two basic approaches to backups: full and incremental. These methods differ in ease of use, ease of restoration, and the time required to execute them. The best backup plan uses both.

Full backups are easy to understand—every file on the volume is backed up. You do not need to keep track of individual files, creation dates, or anything else. If the original volume is damaged, just use the backup copy.

However, full backups can be impractical for large-capacity hard drives. They take a long time, and may require an inordinate amount of backup media. In situations like this, incremental backups are more efficient.

In an incremental backup plan, only those files that have been modified since the last full, or incremental, backup are copied to the backup media. This requires that the backup program be smart enough to recognize which files need to be backed up.

And for a program to do an incremental backup, it must perform a full backup first.

Additionally, incremental backups have their drawbacks: finding the backup of a single file is more involved, since you have to locate the last incremental backup containing the affected file. Recovering from a major disk crash requires loading each successive incremental backup.

A reasonable compromise, that saves both time and backup media, might be to do a full backup over each weekend, and an incremental backup every weekday night. Some backup software combines the speed and efficiency of an incremental backup with the convenience of a full backup. These modify the last full backup, by backing up only the files that have changed since the backup was made.

Another decision you must make about your backup is whether you want it to be archiving or mirroring. In an archival backup, you back up your entire drive, or all the new files on your drive. If you have older versions of the same file on your backup drive, they remain there. This is useful if you occasionally need to use your backup disks to find old versions of changing files.

On the other hand, a mirroring backup only saves the most recent version of a file. If you are backing up your drive and your backup disks already contain older versions of the same files, the backup program deletes the old versions and replaces them with backups of the new versions. This saves disk space, but you can only restore a file to its most recent backed up version.

None of this should be confused with a practice called twinning. Twinning is the process of running two drives, a primary and a twin, with identical information on them. Sometimes this is called mirroring, and the second drive is called the mirror. When you save a file to the primary drive, the file is saved to the twin drive as well, and the same happens when a file is deleted. The point here is redundancy: if you have a hardware failure on the primary drive, the twin is ready to step in and take its place.

However, there is a caveat. This system—available in products like DiskTwin, ExpressMirror, and TwinIt—only protects you from data loss due to disk failure. You get no protection from accidental file erasure, viruses, or data theft. With twinning installed, anything you do on the primary drive is automatically done to the twin as well—for better or for worse. If you accidentally delete a file from the primary drive, the file is deleted from the twin as well. If a virus infects a file on the primary drive, the virus infects the file on the twin as well. Likewise, this procedure

offers no protection against power outages, software corruption, or any other type of data problems.

Twinning takes work, and there is a performance penalty if you use a software-only product. It takes longer to write to a drive, because the twinning software actually writes to two drives. Also, there's the additional cost of buying a second drive. But when your primary drive dies and the twin saves the day, this will seem like a small price to pay. DiskTwin is a hardware and software twinning product; there is no performance degradation with it.

Twinning is not a substitute for a regular backup program, but it does provide extra security for data that must continuously be available.

Being Smart About Backups

It is fairly common for a user to back up one part of a hard drive onto another part of the same hard drive—to a partition or dedicated folder. The theory here is that if files are accidentally deleted, another copy of the files is within easy reach.

Although this system works fine for very short-term backups, you are asking for trouble if you come to rely on it as your sole backup method. If the hard drive develops a fault, both the original and the backup will be lost. If the Macintosh catches a virus, both the original and the backup will be corrupted. If the Macintosh is stolen, both copies will be lost. This is why you always want a backup copy stored on another set of disks—preferably kept at an off-site location.

I heard the story of a graduate student who kept the draft of his thesis, as well as all his doctoral research, on his computer. Although he was diligent about keeping backups, the disks were kept near the computer. One night, a thief broke into his lab and stole his computer and all the peripherals scattered on the table around it—including his backup disks. He lost years of research.

Rules for Performing Backups

- Back up everything.
- Back up everything regularly.
- Keep a set of backups off site.

- Encrypt your backups if the data is sensitive.
- Lock your backups in a fireproof vault; don't leave them lying around.
- Label your backup disks, as to their contents and the date of the backup.
- Verify your backup disks to make sure the media isn't corrupt.
- Change the media periodically so it won't wear out.
- Test your backup program by performing a trial restoration of your computer system.
- Sanitize your backup disks before throwing them away.

If you keep your backups in a drawer next to the computer, your backups are susceptible to many of the same attacks your computer is. Triply-redundant, full backups of your data won't help you at all if everything is lost in a fire, or a disgruntled employee erases both the hard disk drive and the backup floppies. Backups in the drawer next to your Macintosh aren't enough.

It is vital to keep a current set of backups off site. Rent a safety deposit box at a local bank, store a set at home, or buy space on a computer network and keep your backup data there. If you're worried about security, encrypt your backup copies.

You should also label your backup media properly. Imagine that you have to restore your hard disk drive from your backups, for one reason or another. Where are the backups? They're in the fireproof vault over in the corner. Good. You open the lock, look inside, and see a pile of fifty disks. Which disks are the backups of which computer? Which is the most current backup? Some of the disks are unlabeled, others have labels so poorly written they might as well be encrypted. How are you ever going to restore the hard drive?

A lot of guesswork would be needed to sift through all those disks. There's nothing more infuriating than looking for a particular file in a pile of unlabeled media. When you need those backups, you are not going to have the time to figure out which disks are the right ones. You are going to want your backups quickly. Make sure they are easy to identify, by labeling them clearly and consistently.

Choosing a Backup Medium

You can back up your data on anything from floppy disks to digital tape. However, there are many issues to consider when selecting the media that is right for you. Let's say you have 1 Gbyte of data to back up. Are you going to select floppies? This would be a bad choice, mostly because you would need so many disks to complete the backup. You should assess the storage capacity you'll need, along with other factors like convenience, price of the drives, and price of the media, when deciding where your backed-up data will go.

Storage Capacities of Different Backup Media

Backup Media	Storage Capacity
Floppies	1.4 MB
Flopticals	21 MB
SyQuest	44 MB, 88 MB, and 105 MB
Bernoulli	90 MB and 150 MB
3.5-inch optical	128 MB and 256 MB
5.25-inch optical	650 MB, 1 GB, and 1.3 GB
Removable hard drives	up to 1.6 GB
Recordable CD	650 MB
Digital tape	2 to 9 GB

SyQuest is working on a removable cartridge that will hold 210 Mbytes of data, while other companies are working on high-end, 5.25-inch magneto-optical drives that can hold 2.6 Gbytes of data. Sony is working on a small, inexpensive, removable-storage device that will use a 2.5-inch cartridge capable of storing 140 Mbytes. Look for it in late 1994.

Of all the backup media available, floppies are an easy choice, because they are cheap and ubiquitous. They are also the best choice when you have a few small files, or less than 20 Mbytes of data, to store. They are, however, the most unreliable storage media. They are vulnerable to magnetic fields, and floppy drives are slow in reading and writing. Large backups will take a long time. If you have to use floppies for your primary backup media, you should make multiple copies of your most important data, and replace the floppies every two to three months.

Floppy Disk Safety Rules

- Store disks at moderate temperatures, between 60 and 110 degrees Fahrenheit.
- Keep paper clips and other metal fasteners away from disks.
- Keep magnets away from disks, and vice-versa.
- Don't eat, drink, or smoke near disks.
- Don't leave disks out on desks where coffee or other substances might be spilled on them.
- Don't try to clean a disk.
- Replace your disks every two to three months if you use them regularly—newer disks are less likely to fail.
- Protect the disks from the elements when transporting them.
- Never expose your disks to direct sunlight.
- Clearly label all disks.

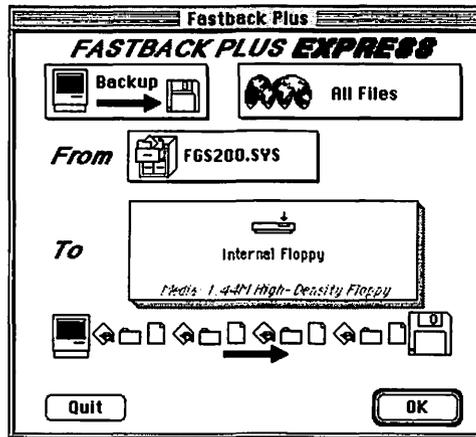
SyQuest and Bernoulli disks, however, are great media for short-term personal backups, because the cartridges are inexpensive but hold a reasonable amount of data. The drives for both are reasonably fast, and they're both reliable. Bernoulli is slightly more reliable than SyQuest because of the way the drive positions the disks. A Bernoulli drive allows air to pass between the disk surface and the drive's read/write heads, reducing the air pressure and causing the disks to almost come in contact with the heads. In the event of a crash, the disks fall away from the heads, reducing the chances of the disks incurring any damage.

Bernoulli cartridges are also less susceptible to dust than SyQuest. But SyQuest drives predominate, because many manufacturers produce compatible drives, while Bernoulli drives are made by only one company. SyQuest drives are thus less expensive, though the cartridges are pricey.

When you have a large backup, or when you want to back up and store files for a long time, you should use magneto-optical (MO) cartridges. These rugged cartridges are inexpensive—and, because data is stored optically, these disks are impervious to magnetic fields, and thus have longer shelf lives.

Figure 7.1

FastBack Plus
backing up to
disk



Magneto-optical technology derives its name from the way in which it writes data to disk. A laser beam and a magnet write, or erase, data on the plastic disk. The laser heats a spot on one side of the disk to about 300 degrees Fahrenheit. The magnet sits on the other side of the disk, and gives the heated area its polarity. These drives are expensive and slow, but those are the only drawbacks to this technology.

Network managers—and others who have enormous amounts of data to backup, and wish to have the back up executed in their absence—will find that digital tape is the best (and only) media to use. Digital tape systems are inexpensive—the tapes themselves cost \$15 each—and can store between 1 and 9 Gbytes of data. Tape drives are also convenient, as many manufacturers now offer models of their drives with a changer integrated into the drive. This mechanism allows the drive to load and unload multiple tapes, so it can operate unattended.

How to Compare 4mm DAT Drives

Macintosh compatibility. Make sure your tape drive has a SCSI port, and either comes with its own Macintosh backup software or is supported by your backup software.

Mechanism. Many manufacturers make DAT drives, but only a few make the actual mechanism. Some manufacturers, like Hewlett-Packard, Sony, and Conner Peripherals, have designed their drive mechanisms with computer operations in mind. Some older DAT drives were built around mechanisms based on modified audio DAT drives.

Standard. Most DAT drives built during the last few years conform to the Digital Data Storage (DDS) standard—developed by HP and Sony, and endorsed by ANSI and ISO—which specifies standards for drive length, data format, and compression. DDS drives use 60- and 90-meter tape, and put 2 Gbytes of uncompressed data on it at a transfer rate of 183 Kbytes per second. Newer drives conforming to the DDS-2 standard use 120-meter tape, and put 4 Gbytes of uncompressed data on it at a transfer rate of 366 Kbytes per second. DDS-2 drives are capable of reading and writing tapes in DDS format.

Capacity. Make sure you are comparing uncompressed capacities; some manufactures advertise compressed capacity. Although vendors claim compression ratios as high as 6.9-to-1, the actual amount of compression data-grade DAT tapes are available in lengths of 60 meters, 90 meters, and 120 meters. The length of the tape determines storage capacity.

Form Factor. The 3.5-inch form factor is more efficient, although some of the older 5.25-inch DAT drives are still available.

Buffer size. Data buffers hold data temporarily, if the drive processes data faster than the SCSI port can handle it, or the SCSI port feeds data faster than the drive can handle it. Data buffers can range from 512 Kbyte to 1 Mbyte.

Price. Some systems are cheaper than others.

Warranty. Warranties vary from none to three years, with one year being the most common. Check what the warranty covers, and what technical support you can expect.

Bundled Software. Most DAT drives are bundled with Retrospect or Retrospect Remote. Some are bundled with proprietary backup software.

You have a few choices to make in selecting the type of tape drive. Digital Audio Tape (DAT) drives are very popular because of their high storage capacity and low media costs. This is also the most reliable hardware you can buy. Based on the same design as DAT audio tapes, DAT mechanisms are helical scanning devices, where the spinning tape heads densely store data in

side-by-side diagonal tracks. Standard drives can store about 1.3 Gbytes of data on a tape, though some drives use automatic compression and can store up to 8 Gbyte of data.

The DC6000 mechanism is a more traditional backup tape technology, because it stores data linearly on each tape. As a result, data is stored less densely than on DAT drives, so capacities tend to be lower for similarly priced drives. DC6000 devices range in capacity from 60 MB to almost 1 GB.

A third type of tape drive is not yet available in the Macintosh market, but it is the de facto standard on VAX and Sun workstations for exchanging large amounts of data. 8mm Exabyte tape drives—DAT and DC6000 conform to a 4mm standard—are larger, hold more data, and have slightly better performance characteristics.

But, for all the choices and benefits of tape drives, they have two drawbacks. These tapes are not impermeable to magnetic fields, and you cannot mount them directly on the Desktop. Still, several backup packages support this media, including Central Point Backup, Fastback Plus, Norton Backup, NovaMac, Retrospect (and its remote version), and SafeGuard.

You should avoid making backups with three remaining types of media. Floptical disks, a hybrid of conventional floppy disk and optical technologies, are written on drives that use a laser to position the read/write heads on the disk (optical) and a conventional floppy read/write head to store and retrieve data. Because a laser is used to position the head, a floptical disk can store more data than a conventional floppy drive. But this isn't much of a plus for a backup media—it doesn't take much to outdo floppies in the storage capacity category. Like floppies, floptical disks are unreliable, the cartridges are vulnerable to magnetic fields, and the drives are slow. There is no ideal use for these disks as backup media.

Removable hard drives are definitely fast, but they're expensive and awkward, and heavy to carry. These are only good for locking data in a safe after hours.

Finally, recordable CD drives are a very reliable media—the disks are impervious to magnetic fields. They're also flexible, as any CD-ROM drive can read them. However, the recordable drives and the media are very expensive, and you can only write once to a single disk. These are not practical for regular backups, but for the long-term storage of large amounts of data-archiving, they're a good choice.

Backup Safety Rules

Floppy disks or tapes: Use only high-quality disks or tapes for your backups. If you have high-density floppy drives, use only high-density disks. You increase the reliability of the backup when you use high-quality media.

Hardware: Be sure that your hardware is fully operational. A backup program cannot operate effectively if the drive heads are worn, dirty, or out of alignment. Faulty disk controllers, and other circuitry, can cause information to be written incorrectly to a disk or tape.

Verification: Take advantage of your backup program's verification capabilities when backing up. Some verification routines also test the media before writing data, producing a more reliable backup.

Labeling: Clearly label all backup floppies and tapes.

Error Correction: Take advantage of any error-correction capabilities of your backup program. Error-correction code can actually correct, and compensate for, damage that occurs after the backup has been made.

Backup Strategies

Probably the most important consideration in developing a backup strategy for computers is deciding whether to use a distributed or a centralized one. If you, as a network manager, haven't thought about this before, you have a distributed strategy: all users are responsible for their own backups, and they all do them whenever they feel like it. The end result is that backups are done sporadically and haphazardly.

If you have a lot of autonomous or isolated users, a distributed approach might be the best choice. You keep the responsibility for backups in the hands of the individual users. Besides, users are often the first to appreciate the importance of the data they individually create, so they have a built-in incentive to back up that data. Another bonus is that you don't have to designate individuals with backup responsibility for others.

The key to success in implementing a distributed strategy is setting standards, and following a consistent program of user education and training. The biggest single disadvantage of a

distributed strategy is that individual users are notorious for not backing up their data. It is very difficult to enforce a minimum standard of backup by relying on user initiative. Also, when a large number of users require special hardware for backup, it can cost a small fortune.

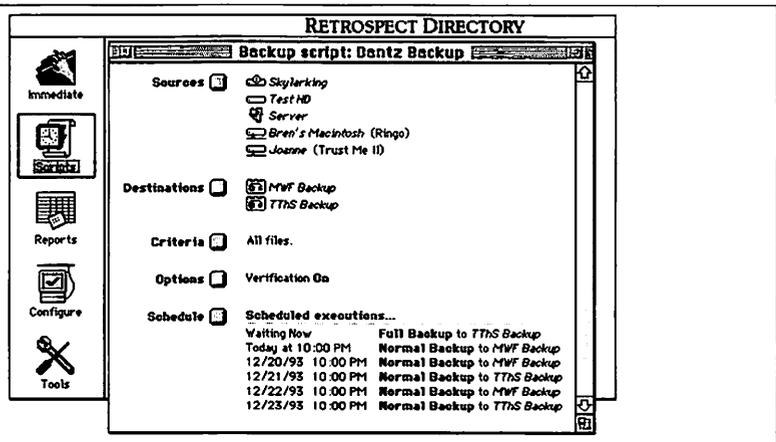
If all computers are networked, you can centralize the management of backups. There are two types of centralized strategy: server-only backups and comprehensive backups.

In many cases, the desire to centralize backup administration, and simplify the backup task for workgroups, has resulted in organizations deciding to back up servers only. Users are encouraged, or even required, to store important files on the server. Then, a network administrator sees that the server is backed up regularly. While this strategy centralizes the administration of backups on the network, it does not ensure that the data is protected. Also, server-only backup typically requires users to copy important data to the server, and as a result, they sometimes neglect their regular backups. However, this is a good first step toward a comprehensive backup strategy.

A comprehensive backup strategy encompasses the backup needs of both servers and desktop computers. It is more complete and more reliable, because the user is no longer responsible for any backup tasks. All of the data, on every desktop computer and server, is backed up. Typically, a backup application running on a central Macintosh, with a high-capacity removable tape drive, collects and manages all the data. While the central Macintosh can be an AppleShare server, with the backup application running in the background, it can just as easily be any other Macintosh on the network.

Figure 7.2

Retrospect backup strategies



Advantages of a Comprehensive Backup Strategy

- Simplicity and transparency for users.
- The lowest cost per user.
- Greater coordination and consistency of backups.
- Increased automation of the backup system.
- Greater security for backups.

Once you decide on a backup strategy, you need to devise a backup schedule.

In maintaining any backup schedule, you should always have a current copy of all hard-disk data files from which you can recover in the event of a hard-disk crash. One possible procedure creates three sets of backup disks, which you use in rotation. This is sometimes called the parent-grandparent backup scheme. Say you name your three sets: set A, set B, and set C. Here's the schedule you would follow:

Day 1: Make a full backup to set A.

Day 2: Make a full backup to set B.

Day 3: Make a full backup to set C.

On day 4, you would start the process over again by taking out set A and doing a full backup. Another method combines full and incremental backups, and happens over a three-week period. Full backups happen once a week, with incremental backups—named set 1, set 2, and set 3—performed every week-day. You would start by doing a full backup to set A, and then start the first week as follows:

Week 1

Mon: Incremental backup to set 1.

Tue: Incremental backup to set 2.

Wed: Incremental backup to set 3.

Thu: Incremental backup to set 4.

Fri: Full backup to set B.

Under this schedule, every Friday you would do a full backup, but to a different set—week 2, you'd use Set C, and week 3, you'd go back to set A. Using this system, you would always have at least two full backup sets—with partial backups at the

end of each day, to protect you if your computer fails in the middle of the week.

For greater security, you can keep still a third set of three disks or tapes, and use one set at the end of each month—rotating through the set every three months.

Once you devise a schedule, you may wish to automate the process by setting up an automatic backup. The repetitive nature of backups makes them perfectly suitable for automated operation. But to do this, you have to script and then schedule your backup. Scripting allows you to specify which operations should occur upon activation. Once you define a script, you don't have to make the same repetitive choices for every backup operation.

Backing up is most effective and unobtrusive if it is done when the Macintoshes and the network are relatively quiet. If your backup program allows you to schedule backups, all you have to do is to schedule when the backup should occur—at 3:00 a.m., for example—and the backup software will execute the script. If you are backing up to tape, or to a hard disk large enough to store all of your backup files, you don't even have to be around to change storage volume. With some backup software, you can configure the automatic backup to handle every Macintosh on your network.

Backup Data Integrity

Some backup programs check for write errors after the data is written to disk or tape. This is usually implemented as an option, and it increases the time it takes to make backups. If you have a backup program that automatically makes backups at night when no one is around, by all means engage this feature. If you have to sit around waiting while the program runs, use the feature if you can tolerate the wait. A backup without error checking is better than no backup at all, but error checking increases the reliability of the backup.

Other backup programs can be configured to check hard disk integrity before making the backup. Some even check for viruses.

Keeping Your Backup Data Secure

Generally, data compression doesn't speed up the time it takes to perform a backup of your hard drive. Only with very slow drives—floppies, or Apple Tape 405C—is a compressed backup faster. Otherwise, the time required to compress the data slows

down the entire backup operation. The resultant operation is much slower when backing up a single machine. On a network, where data transfer between computers is a bottleneck, compression can make a smaller difference.

The point of a compressed backup is that you can cram more information onto your backup media. Unlike the compression schemes used with images and video, there are data compression schemes that don't lose any information in the compression and expansion processes. After compression and expansion, the file is exactly the same as the original. Some backup programs have compression options built into them; they compress files when making backups, and expand them again during restoration. I recommend using compression, since it does not increase the danger of data loss, and it can double or triple the amount of data you can store on a single disk or tape.

Whether you compress or not, you should at least look into encrypting your backups—programs like FastBack Plus and Retrospect give you the option of encrypting your backup disks. But with respect to encryption, the same guidelines set down in Chapter 3 hold here: All programs that use a proprietary algorithm use one that can be easily broken.

If you want to securely encrypt your backups, either use the DES option in Fastback Plus or Retrospect, or use an encryption program on the data before you back it up. If the data on your hard disk are encrypted, then the backups will be encrypted. Even if the data on your hard drive is not encrypted, it might make sense to encrypt your backups. Maybe your hard drive is kept in your locked office, but your backup disks may be stored less securely.

Remember that the international version of any of these programs does not have a secure encryption algorithm. See Chapter 3 for details.

Care and Feeding of Your Backups

You have a schedule and a scheme for making your backups, and you make them. Will you need them? That depends on how careful you are, but things happen. You might accidentally delete a file or folder, in which case you will need to restore only those files from the backup disks. Also, you might completely trash a hard drive, in which case you will need to restore everything—perhaps even onto a different drive.

Even if you haven't needed to restore your data yet, you should work with your backups every so often, to keep them in shape. Backups are useless unless they work, and the only way you can determine if they will work is to test them regularly.

Rent a Macintosh identical to your own for a day. Take a set of backups, and try to restore your data on that new system. If you can do so, congratulate yourself for having an effective backup program. If you can't, imagine how you would feel if this weren't just a test. Figure out why your backup program didn't work. Are the backup disks or tapes bad? Is there a problem with the way you create the backups? Is there a problem with the backup software you are using? Find the problem, and fix it.

Another use for backups is long-term storage. In today's litigious society, you may someday need to prove that a certain piece of data existed on, or before, a certain date. If the data is computer data, long-term backup storage is essential.

These backup disks or tapes are a separate set from the ones you use for every day disk restoring. They are never erased, and are stored for years. Like all backups, they should be stored in a secure place, preferably somewhere that is locked and fireproof. Depending on the value of these archival backups, you may want to make two copies, and store them in separate locations.

Because these backups are made to prove the existence of data files, only data files need to be saved on these backups. You probably won't need to save a copy of your word processor or database program—but if these backups are going to be archived for a long time, consider the possibility that the program that created the files may not exist anymore.

These backup files can be compressed for more efficient storage. Remember to leave a copy of the data compression program—in uncompressed form—on each of the backup disks.

Backup disks and tapes can be used again and again. Eventually, however, there is a danger that the media will wear out and will no longer be reliable. Disks and tapes should be replaced regularly; check with your manufacturer for the recommended interval. If backup copies are also being saved for archival purposes, this outlet can be used to retire older disks. If not, replace your disks and tapes on a rigid schedule.

Before throwing away old backup media, they should be thoroughly erased, either with a file erasure program or with a degausser, to erase any valuable data. If you have very valuable data on the disks, consider buying a shredder. That's what the U.S. government does.

Maintaining Your 4mm DAT Tapes

In addition to all the measures you should take with backups on any media, DAT tapes and drives have a special set of concerns that need to be addressed:

- Make sure your backup program supports the tape drive. Most tape drives include a Macintosh backup program, but some don't.
- Use high-quality SCSI cables. Problems can arise from improper termination or bad cabling.
- Compare product specifications before buying, as some resellers cut corners to keep prices low. Some of the components that can adversely affect a drive include power supply, case, and cables.
- Allow tapes to equalize in temperature before using them in a different environment. If the tape, drive, and atmosphere are at different temperatures, the drive may wrap around the head and be damaged.
- Rotate backup tapes. Don't store everything on one tape or reuse a backup tape repeatedly.
- Test your tape backup equipment on non-critical jobs before relying on it for permanent backup.
- Use only high-quality, data-grade tapes, and not the inexpensive audio-quality digital tapes. Buy the tapes in batches, and test each batch before using it.
- Copy your backup application onto floppy disks, and store it with your backup tapes.
- Clean your DAT drive head at least once a month—unless your drive has a self-cleaning head—using an approved DDS cleaning tape.

Shopping for a Backup Program

The best backup programs should be able to back up disks automatically, and the user should be able to determine what she wants done, and when she wants it to happen.

Table 7.1: Backup Software

Product	List Price	Company	Consumer Phone Number	Main Function	Comments
MacTools/ (Central Point Backup) 3.0	\$149.00	Central Point Software, Inc.	(503) 690-8088	All-purpose backup package	Backs up to all media, including tape; verifies the reliability of data
DiskFit Direct 1.0	\$44.95	Dantz Development Corp.	(510) 253-3000	Basic backup for individual users	Does not compress files it backs up
DiskFit Pro 1.1	\$125.00	Dantz Development Corp.	(510) 253-3000	More comprehensive backup	Users can specify types of files for backup; auto- matic backups can run unattended
DiskTwin 2.0r7	\$999.00	Golden Triangle Computers, Inc.	(619) 587-0110	Hardware and software disk twinning	Automatic cut-over allows twin drive to auto- matically replace main drive in instance of failure
ExpressMirror 1.32	\$295.00	ATTO Technology, Inc.	(716) 688-4259	Disk twinning software	Speeds up seek and access times of drive
FastBack Plus 3.0	\$149.00	Symantec Corp.	(800) 441-7234	Single-user backup	Options for password protection, and/or encryption, of backups
FileDuo 1.0.4	\$149.00	ASD Software, Inc.	(909) 624-2594	Single-user backup	Easy to set up and use; automatic backups possible to all media except tape
Norton Utilities for the Macintosh (Backup)	\$149.00	Symantec Corp.	(800) 441-7234	Single-user backup	Good for making archive disks
NovaMac 2.31	\$149.00	Novastor Corp.	(818) 707-9900	All-purpose backup	Backs up to almost every tape drive on the market, and supports tape drive changers
Redux Deluxe 2.0	\$79.95	Inline Software, Inc.	(800) 453-7671	Single-user backup	Does automatic backups, although doesn't support tape drives
Retrospect 2.0	\$249.00	Dantz Development Corp.	(510) 253-3000	All-purpose backup	The best backup package; scripting language lets you set up many automated features
Retrospect Remote	\$449.00	Dantz Development Corp.	(510) 253-3000	Remote backups	Administrators can backup an entire AppleTalk network from their Mac; has DES encryption
SafeDeposit 1.2	\$129.00	Dayna Communications, Inc.	(801) 269-7200	All-purpose backup	Will cancel an automated back up if selected files exceed chosen volume's capacity
SafeDeposit Server 1.2	\$299.00	Dayna Communications, Inc.	(801) 269-7200	All-purpose server-level backup	Runs with AppleShare 2.0 or 3.0, or System 7's Personal File Sharing; same features/problems as SafeDeposit

Table 7.1: Backup Software (continued)

Product	List Price	Company	Consumer Phone Number	Main Function	Comments
SnapBack 1.0	\$129.00	Golden Triangle Computers, Inc.	(619) 587-0110	All-purpose backup for networks	After administrator set up, all functions can be run and monitored from a single window
SurfGuard 1.0	\$150.00	Surf City Software	(714) 289-8543	All-purpose backup for networks	Backs up across network zones and bridges; supports AppleTalk and EtherTalk
TwinIt 1.0f	\$199.00	Golden Triangle Computers, Inc.	(619) 587-0110	Disk twinning	User must manually unlock and mount twin drive when original disk drive fails

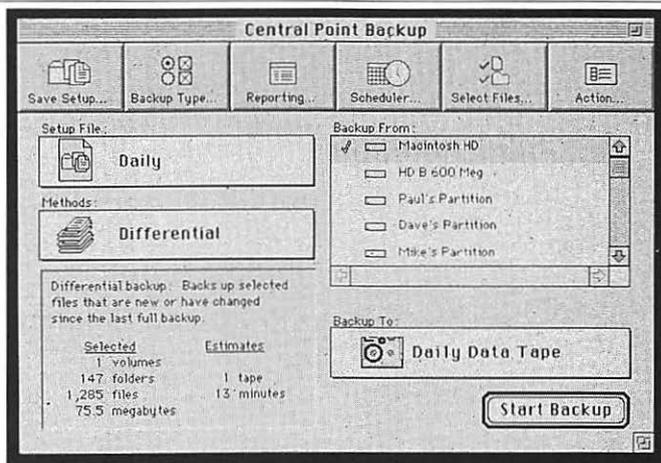
Central Point Backup

Central Point Backup, part of the Central Point's MacTools 3.0 package, is a comprehensive, well-written, and effective backup program. You can back up entire drives or selected files or folders. You can do a full backup, an incremental backup of everything that has changed since the previous backup, or an incremental backup of everything that has changed since the previous full backup.

You can back up to almost any device, including floppy disks, hard disk drives, SyQuest or Bernoulli cartridges, tape drives, or another volume across a network. You can select to have your backup run automatically at daily or weekly intervals, at start-up or shut-down, or after the system has been idle for a set amount of time.

Figure 7.3

Central Point Backup



The program allows you to name the backup file prior to running, and it appends the current data to the end of the user-supplied file name as a default. This is useful when backing up to a high-capacity disk, perhaps across a network. You can also select multiple drives as backup destinations, which useful if you have two floppy drives.

A set of backup options—too vast to list—gives you the ability to customize your backup procedure, and a reporting option lets you create a log of your backups.

This program gives you two options for verification: a complete bit-for-bit comparison of the backup and the original file, or a through-write verification during the backup. These options increase the time required to complete the backup, but for critical applications they may be worth the peace of mind.

Central Point Backup also includes options for anti-virus scanning before each file is backed up, data compression (which can reduce the size of your backups by as much as 55%), and password protection or encryption of backed up files. The available encryption algorithm, however, is not DES, and does not offer unbreakable data security.

Restoring data is easy. You can restore an entire disk, specific files, or all files missing from your hard drive. Easy-to-understand menus take you through all the options. Another nice feature is the ability to create not only special backup files, but Finder-readable backups that can be restored by any Macintosh—even one without a copy of Central Point Backup installed.

DiskFit Direct 1.0

DiskFit Direct, from Dantz Development, is for single users with simple backup needs. You can back up any disk onto as few removable disks—floppies, SyQuest or Bernoulli cartridges, or removable optical disks—as possible.

The user interface is clean and uncomplicated. The main window offers three options: initiate a full backup, initiate a partial backup, and restore from a backup. The program does not do automatic backups.

To initiate a full backup, you designate the data you want backed up—an entire drive, documents only, or the contents of a specific folder—and DiskFit Direct does it by erasing and filling floppies as needed, prompting you to change them on occasion. If a file is too large for a single floppy, DiskFit splits it into pieces on separate disks. DiskFit does not compress, nor encrypt, backup files.

Once you have a full set of backup disks, incremental backups are just as easy. DiskFit prompts you for the original set of backup disks, and backs up only the changed files. It also deletes files from the backup disks that have been deleted off the main disks, however it cannot be used for archival backups.

For each new set of backup disks it creates, DiskFit prepares a complete report, showing the date and time of the previous backup, the number of disks used, how much space was required for each file, and which files are on which particular disks. You can either store this file on disk, or print it out.

When you want, or need, to restore files, you tell DiskFit which disk or file you want, and the program goes about its work. If a file was split onto disks during the backup, DiskFit automatically rejoins it. Unfortunately, restoration is slow, since DiskFit does not compress files.

DiskFit Direct backs up files in standard Finder format, so you can access files on the backup disks from the Finder without having to launch DiskFit Direct.

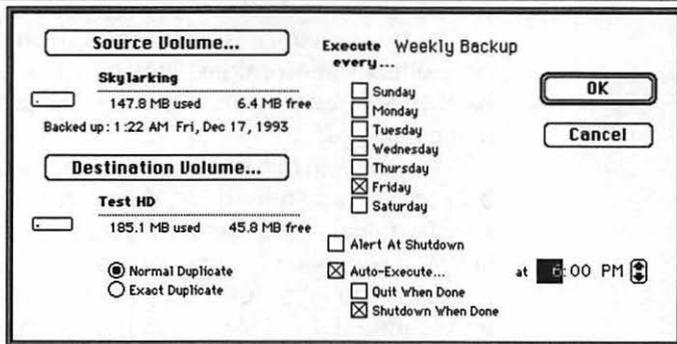
DiskFit Pro 1.1

DiskFit Pro, from Dantz Development, is similar to DiskFit Direct, but with more bells and whistles. You can back up any file, folder, or volume, with options that let you exclude particular files or folders; and you can even qualify what types of files you want to include.

The program can perform automatic backups, and it includes a control panel that can remind you when it is time to back up—though you can only specify the day of the week, and time, for a backup. It can do unattended backups and shut-downs, assuming your backup storage medium is large enough—you can back

Figure 7.4

DiskFit Pro
backup schedule



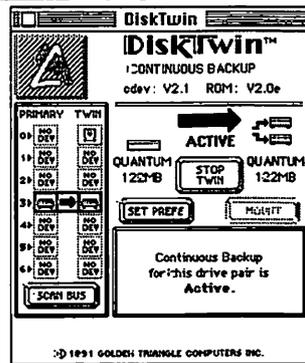
up to any medium except tape. The program also works on any kind of network and server setup, although this might be of little use without the ability to back up to tape.

DiskTwin 2.0r7

DiskTwin, from Golden Triangle Computers, is a hardware and software disk twinning product that provides continuous backup of any SCSI volume you can mount on your Desktop. Whenever the Macintosh writes to one drive, DiskTwin writes identical information to a second drive, constantly providing you with a current backup.

Figure 7.5

DiskTwin



DiskTwin consists of a Mac II, SE/30, or NuBus board; an application; an INIT; and a cdev. The hardware acts as a second SCSI port, to which one or more twin drives can be connected. After installing and connecting the hardware, the two drives must be synchronized: You must create an exact duplicate of the primary drive on the twin. Once the two drives are in sync, any changes that you make to the primary drive are instantly carried out on the twin drive.

DiskTwin has an option called automatic cut-over, which causes the twin to replace the primary drive the instant a failure occurs. This feature can be critical for users worried about downtime. Unfortunately, if the drive failure is accompanied by a system crash, this feature does not function, and you have to change drives manually.

DiskTwin works silently and unobtrusively in the background. You never even know it's working, until disaster strikes and you need it.

ExpressMirror 1.32

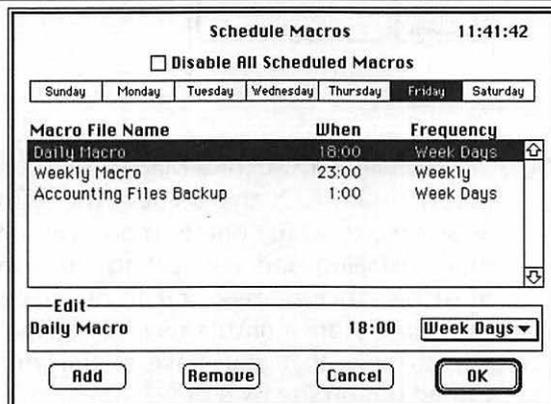
ExpressMirror, from ATTO Technology, is a full-featured, easy-to-use disk twinning package. You set up the two drives (or partitions), and the software does the rest. The package can mirror up to four drives.

The program can actually boost performance of a drive. Through a technique called "read costing," ExpressMirror determines which drive can most quickly retrieve the requested data. This determination is made on several factors, including the current position of the read/write head and the seek speed of each drive. Then, ExpressMirror gets the data from that disk. This technique can reduce overall seek times by as much as 50%, and reduce the performance degradation associated with a heavily fragmented disk.

If the primary drive fails, ExpressMirror will automatically retrieve the proper data from the twin. There is no manual switchover, and there is no downtime. The switch occurs in the background, without any interruption of the program. The software can be set up to alert the user about disk failures, using dialog boxes and audible signals.

Figure 7.6

FastBack Plus
automatic
backups



Fastback Plus 3.0

Fastback Plus, from Symantec, is a full-featured backup utility—designed for a single user—that performs full and incremental backups, either manually or automatically. The program can back up files to any disk or tape drive, and it lets you back up files on a network to a server.

FastBack Plus in its simplest mode, called Express, has almost everything the average user needs to do basic backups. A single

dialog box lets you specify backup criteria, including source drive, target drive, and whether to back up or restore. This interface lets you choose a full or incremental backup, lets you include or exclude application files, and lets you select specific files for backup. You can even print labels for backup floppies.

A Short Menus mode adds compression capabilities, and enables you to compare backed-up data with data existing on a hard drive.

The most advanced mode is called Full Menus, and it adds macro functions for unattended backups. There are also several filters that let you include or exclude files (data and applications) for backup. Other filtering criteria let you select files according to date, size, and file creator.

Fastback Plus does not back up files in a Finder-readable format, so you must launch the application and use its restore function to retrieve a file. This is not difficult, and there are several restore options. Advanced error correction features can recover data from damaged backup media.

There are other options. Fastback Plus can password-protect the backup copies, or encrypt them with DES. There is a write-verify option to ensure the accuracy of the backup disks.

A feature called Snapshot helps restore disks to a specific state. For example, let's say you do a full backup on Monday, and then delete several files on Tuesday. If you take a Snapshot of your disk on Tuesday (not another backup; this is a quick recording of your disk's directory) and your disk crashes on Wednesday, you can restore the disk to its Tuesday configuration by applying the Snapshot to the Monday backup.

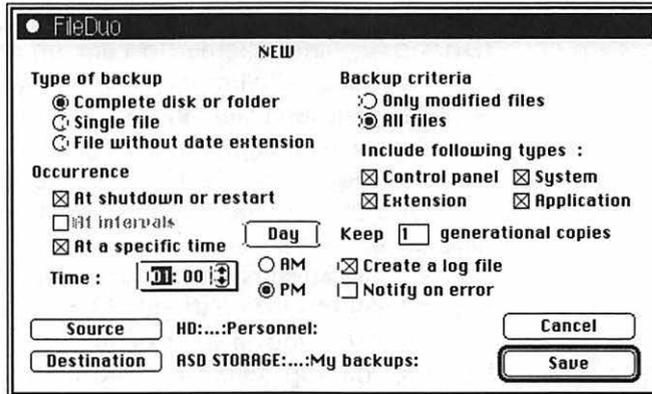
FileDuo 1.0.2

FileDuo, from ASD Software, is a simple backup utility that performs automatic backups to any mountable volume—although it cannot back up to tape. FileDuo is designed for individual users who don't have time to do backups. The utility works quickly in the background, without any user intervention except to change disks if needed.

The program is intuitive, and easy to use. Setting up an automatic backup takes just a minute or two, and there are no complicated macros or scripts required. Simply open the FileDuo control panel, click the Configure button, and set the various backup parameters. You can define your source and destination drives, set the time you want the backup to happen, and choose the files you want to include (all files, or only files modified since

Figure 7.7

FileDuo



the last backup). You can also opt for a backup log and error notification.

After that, everything is automatic. The program even backs up open files. The Backup List window lets you quickly add, duplicate, modify, or suppress a backup operation, and launch one at will. You can create generational copies—several versions of the same file that cover a period of time. This enables you to retrieve an older version of a document if you need to.

Should you lose an original file, and need to retrieve your last backup of it, the procedure is not complicated. The backup is an exact duplicate of the files on your drive. Just drag a file over to your hard-disk drive and you're done.

Norton Backup

Norton Backup comes with the Norton Utilities for the Macintosh 2.0, from Symantec. It can perform complete or incremental backups. It can also make partial backups of certain files, file types, or folders. You can only back up files modified since the previous backup. The program can back up to all media except tape.

Once you've specified the backup medium, and the files, folders, and volumes you want to back up, you can save all of those settings. If you need to perform regular, unattended backups, you can use Norton Backup's scheduling feature to set times for either incremental or full backups. The program can then either do the backup automatically, or send you a reminder message when the appropriate time comes.

The program comes with a nice selection of options, including compression and verification of the backup file.

Norton Backup never erases old files from a set of backup disks, so you end up using more and more disks if you continue to do incremental backups. On the bright side, this forces you to keep an archived copy of old versions of files.

Although Norton Backup works fine, I wouldn't recommend switching to it from another program. But if you own a copy of Norton Utilities, take a look at Norton Backup before spending money on a different backup program.

NovaMac 2.31

NovaMac, from Novastor, is a complete backup program. It works on single machines and networks alike. It does full and incremental backups, and it works with almost every tape drive on the market. Backups can be unattended—just tell NovaMac what you want backed up and when, and the program does the rest.

NovaMac lets you back up to tape, or to any Desktop-mountable drive. The program supports many advanced tape-handling features, such as tape-drive density select, support for stackers and changers, and tape-drive cascading.

NovaMac also provides a complete library of all tape transactions. Every backup, verify, and restore function is logged by NovaMac. This provides you with a complete audit trail, and the means to locate any version of any backed-up file. The program also has a utility that scans these libraries, and searches for any errors or files that you wish to store. This makes data management chores easy.

NovaMac has an easy-to-use interface that makes it simple for computer novices to handle backup chores. A scripting language lets you save any tape operation as a procedure to be run later.

Redux Deluxe 2.0

Redux Deluxe, from Inline Software, is simple and easy to use, making it the ideal backup program for individual users—though it also works well for network backups. Backing up your entire hard disk drive takes only three mouse clicks. Redux Deluxe will initialize the floppies if necessary, and back up the hard drive—prompting you to insert as many floppies as are required. Label the disks, store them in a safe place, and you're done.

You can set up a backup schedule that will back up your files automatically: daily, weekly, monthly, or upon shut-down. If you back up to large enough storage media—another drive, SyQuest drive, or a removable drive—the backup will be automatic. However, Redux Deluxe does not support backup to tape.

Figure 7.8

Redux Deluxe
restore options

What type of specialized Restore would you like?	
<input checked="" type="radio"/> Standard Restore	Restore all files that are checked.
<input type="radio"/> Restore Differences	Restore all files that have changed or are missing from the hard disk.
<input type="radio"/> Restore Newer	Replace old versions of files on the hard disk.
<input type="radio"/> Restore Missing Files	Restore all files that are not on the hard disk.
<input type="radio"/> Restore Newer and Missing	Replace old versions of files on the hard disk, and restore all files that are not on the hard disk.

You can set the backup to run in the middle of the night. Redux Deluxe can automatically back up a hard drive to a specific folder on your network. Otherwise, Redux Deluxe will prompt you to change disks as necessary.

Backups can be full or incremental. Redux Deluxe can back up only those files that have changed since the previous backup, but it can also back up individual folders, certain files, certain file types, or any combination thereof. There is a simple scripting language built into Redux Deluxe, allowing you to select what gets backed up and when. Once your script is set up, you can run it in three mouse clicks, or set it up to run automatically.

Redux Deluxe does archival backups as well. You can set the program to keep old versions of a file in your backup set, even if they've been changed or deleted from the original hard drive.

Restoring files or storage volumes is just as easy. An Info window gives information about when a file was last backed up, whether it's archived, and which disk it is on. You can restore files, folders, or selected archived items—to just about everything from a floppy disk to someone else's hard drive. Other options allow you to restore only those files missing on your hard drive.

Because it is a simple program, Redux Deluxe lacks some advanced features found in other programs. Although it will back up to other storage media along a network, Redux Deluxe is designed primarily to back up a hard disk drive to a single set of floppies. With a little more work, you can use it to implement the backup schedules described earlier in this chapter. Redux Deluxe does not have any compression capabilities—the backup is the same size as the original. Backing up a full hard disk drive

might require 100 floppies. This is where the scripting language comes in handy—most people with 100 Mbytes of data on their hard disk drive don't need to back *everything* up every night.

Redux Deluxe attempts to balance power with simplicity, and is an excellent choice for individual users who are concerned about losing data.



Retrospect 2.1

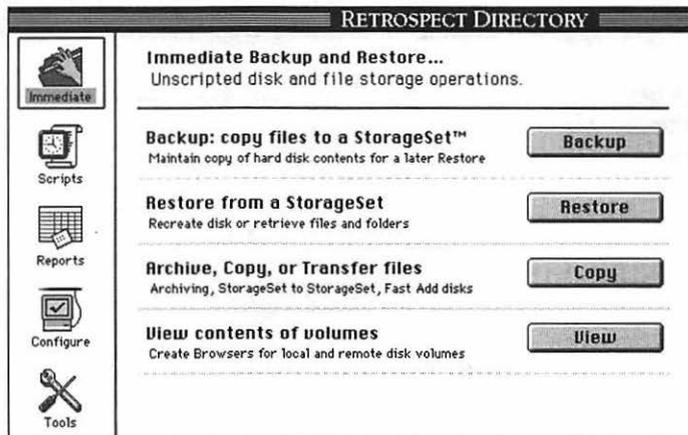
Retrospect, from Dantz Development, is the most popular backup program for the Macintosh, and it's also the best. It can do just about everything you want it to, from the simplest manual backups to the most complex, automated selective backup strategy.

You can do full or partial backups, and manual or automatic backups. You can compress your backups to save space, or encrypt them for added security. A complex scripting language allows you to set all this up in advance, and then let Retrospect do the backup automatically. And a wealth of scheduling options means that you can do backups at almost any interval and with almost any frequency.

Retrospect supports just about every possible backup device. Not only can you back up to floppies, hard drives, and removable disks, but also to most tape drives on the market—including DC2000, DC6000, TEAC, Exzbyte 8mm, and 4mm digital audio tape. Over the years, Retrospect has been the first backup program to support a new storage technology once it becomes widely available.

Figure 7.9

Retrospect



Restoring files is easy and straightforward. You can restore entire disks or just certain files. You can quickly search through multiple backups, looking for the exact file you want. If there's a restoration option you want, it's probably available.

The Snapshot feature restores disks to a specific state. See page 165 for an example of how this feature works.

There's a reporting feature to help you track the results of scheduled backups. The program maintains both a log and a report file, keeping track of all actions it performs. Data errors are highlighted with dots.

Although overkill for simple applications, Retrospect is the best backup program you can buy.

Retrospect Remote 2.1

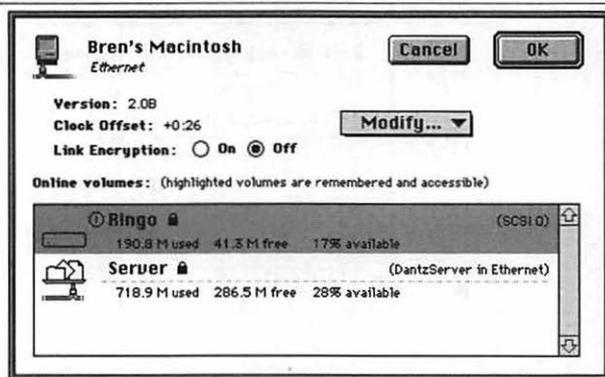
Retrospect Remote, also from Dantz Development, is an add-on to Retrospect that has remote backup capabilities, allowing you to back up Macs on an AppleTalk network. One Macintosh is the administrator, and is in charge of the whole backup process; the other machines are "remote."

From the administrator Macintosh, you can write a script to back up every hard drive on the network to a single tape drive, automatically, at a specified time interval. You have all the same options as in the single-user version of Retrospect, plus extras. You can skip over files that are identical on more than one Macintosh, saving both time and storage space. Additionally, you can configure the Control Panel to notify you after a successful backup, or to alert you if a specified amount of time has gone by without a backup.

If you're concerned about data security, you can encrypt the backup files, using DES, before they are transmitted across the

Figure 7.10

Retrospect
Remote



network. You can also password-protect remote nodes on your network, to prevent someone else with another copy of Retrospect Remote from accessing them over the network.

If you're a network administrator who wants to make sure that all Macs are backed up regularly and reliably, Retrospect Remote is an excellent choice.

SafeDeposit 1.2

SafeDeposit, from Dayna Communications, is a backup product that is intended to complement your normal backup strategy, by making copies of critical files in between normally scheduled backups.

The program will back up specified files to any mountable volume (disks, not tapes). You have to specify which files you want backed up, the backup schedule time, the destination volume, compression options, and whether you want a full or incremental backup.

SafeDeposit will not back up invisible files, empty folders, files in the Trash, or temporary files. Other than System files, SafeDeposit will not back up open files, unless you specify otherwise. This is an important option; you can configure SafeDeposit to back up open files, such as databases, throughout the day.

You can schedule backups regularly, at a specified time, on command, at shut-down, or upon disk insertion. If one backup isn't enough security for you, SafeDeposit will let you create multiple, synchronized backups of the same file.

But for all this flexibility, SafeDeposit has some costly drawbacks. It does not work in the background, so you have to sit and wait for SafeDeposit to finish its backup before you can use your machine. But don't stray too far from your machine while SafeDeposit does its work: SafeDeposit cannot split files between disks. So, if there isn't enough space on your backup disk to hold your files, the backup won't happen.

SafeDeposit can be used as a primary backup program, but it is better suited as a complement to a daily backup package. The program is suitable for cases in which your data is stored on a volatile medium, such as a RAM disk, or when you need constant backups of very critical items.

SafeDeposit Server 1.2

SafeDeposit Server, also from Dayna Communications, is a companion server product. It runs in conjunction with AppleShare 2.0 or 3.0, or System 7's Personal File Sharing, and backs up files while the server is running. Its features are identical to SafeDeposit.

SnapBack 1.0

SnapBack, from Golden Triangle Computers, is backup software for networks. Its main strength is its ease of use. Initial setup on a server, using the administrator software, takes only a few minutes. Afterwards, SnapBack has a one-window, easy-to-use interface. Just set it up and it works automatically.

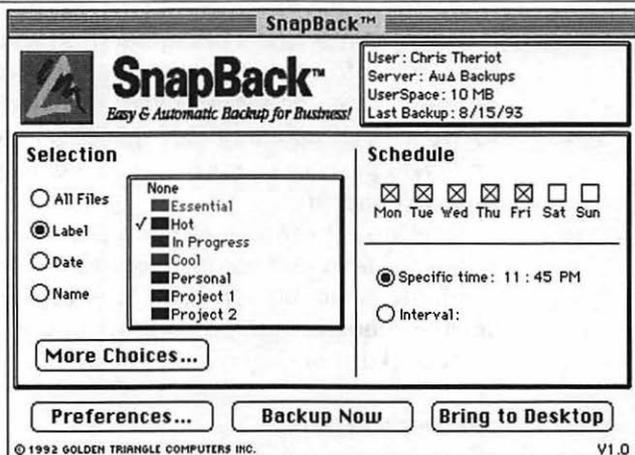
You can perform a full or partial backup, can back up only certain folders, or can back up files according to modification date. Even if you specify a full backup, SnapBack does not back up files that are unmodified since the previous backup. You can choose the time of day, and the days of the week, when you want the data to be backed up. Alternatively, you can specify a time interval between backups—anywhere from one minute to seventeen hours.

SnapBack backs up data to a networked hard drive, a removable drive, or an erasable optical drive that has been formatted and partitioned with the SnapBack server software into volumes—one for each SnapBack user. Since the network administrator fixes partition sizes on the server at setup, individual users are limited in the amount of data they can back up and store.

To retrieve files from the server, you simply click on the Bring to Desktop button, which mounts the backup partition just like an AppleShare volume. You can also copy, delete, and move files within folders in the backup.

Figure 7.11

SnapBack



SurfGuard

SurfGuard, from Surf City Software, is a full-featured backup program for the Macintosh, and can back up data to several destinations. The program supports a wide variety of tape drives: Quarter Inch Cartridge (QIC), Data Cassette, Digital Audio Tape (DAT), and 8mm Video Tape subsystems. SurfGuard can also back up to floppies, SyQuest drives, magneto-optical drives, and hard drives.

SurfGuard is easy to use, and flexible. A simple options screen lets you select which files to back up, what backup method to use (full or incremental), and when to schedule the backup. You can manually select which files to backup, or you can set your

Figure 7.12

SurfGuard

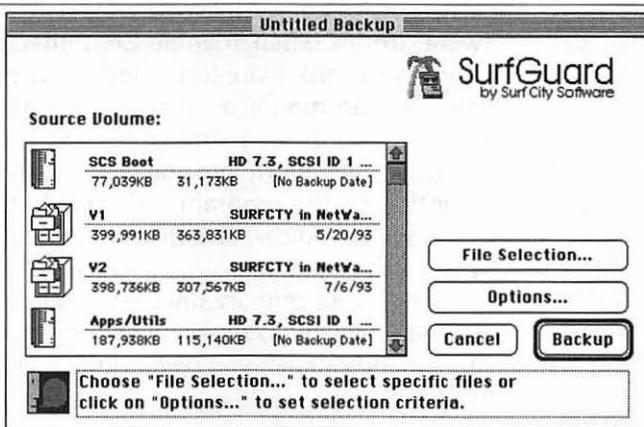
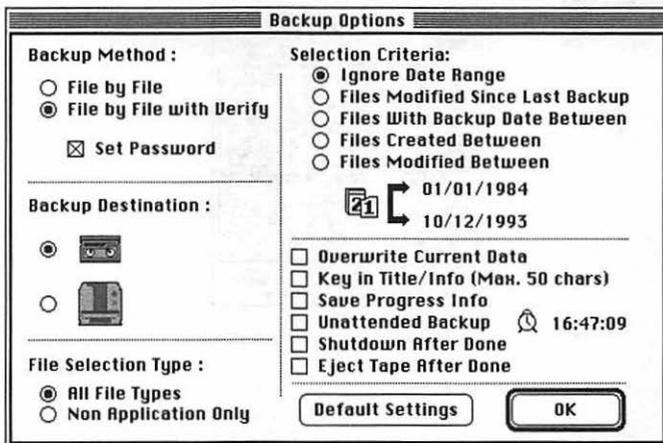


Figure 7.13

SurfGuard
backup options



criteria and have SurfGuard do it automatically. The program can compress or encrypt the backup files. A second-pass verify function ensures accuracy of the backup files.

Recovery is also easy. Uncompressed and unencrypted files can be restored by just mounting the backup volume. Backup log files help audit backups, and aid in drive restoration.

SurfGuard can back up and restore networked volumes. Network support includes handling of AppleShare volumes, Novell NetWare volumes, System 7 shared volumes, and any other Macintosh network system. SurfGuard will also back up across network zones and bridges, and the program supports AppleTalk and EtherTalk.

Twint 1.0f

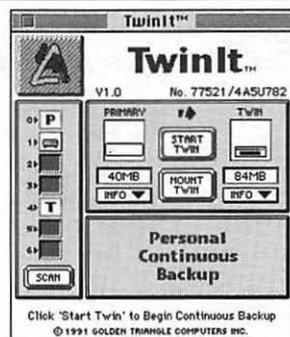
Twint, from Golden Triangle Computers, is a control panel that provides for disk twinning: continuous backup of any SCSI volume you can mount on the Desktop. Whenever the Macintosh writes to one drive, Twint writes identical information to a second drive, constantly providing you with a current backup.

Setting up the program is simple. Just drop the control panel in the System Folder, and designate the primary and twin drives. Synchronize the two drives, and you're ready to go.

Then, if your primary drive ever suffers a hardware failure such as a head crash, you can bring the twin into service. This process isn't automatic; you have to manually mount and unlock the twin.

Figure 7.14

Twint



Chapter 7 Summary

- Should disaster strike, backups are the only way you can recover your data. Backups are the most important part of a computer security plan.
- Full backups make a copy of every file on the volume. This can be impractical for very large amounts of data.
- Incremental backups begin with a full backup, then save updated versions of every file that has changed since the last backup.
- Archival backups save every old version of every file; mirroring backups erase old versions. The latter technique saves on the amount of backup media needed.
- A twinned drive will provide you with an up-to-the-minute backup version of your hard drive. Anything that is written to your hard drive is written to the twin; this technique is useful if you must have your data instantly available, in the event of a hardware problem on the primary drive.
- Your backups are just as vulnerable as the place where they are stored. Keep them where they won't be damaged, and keep them off site.
- If you don't label your backup disks clearly and consistently, you won't be able to find what you're looking for in an emergency.
- The types of disks that can be useful for backup include SyQuest or Bernoulli cartridges, which are good for medium-sized storage; and magneto-optical (MO) cartridges, which serve well for larger backups. Floppies are the cheapest alternative, and are useful for backing up smaller files.
- Digital Audio Tape (DAT) drives are a low-cost, high-capacity storage medium. Exabyte 8mm tape drives, not yet available for the Macintosh, are useful for exchanging large amounts of data across a network. DC6000 drives use a more traditional information storage pattern and as such cannot store data quite as densely as DAT or 8mm drives. Make sure your software and tape system can work together.

- Decide whether you want to use a distributed or centralized backup strategy. In the former, each user is responsible for his own backups. In a centralized backup strategy, an administrator is responsible for either backing up a server, or for backing up both the server and each node's hard drive.
- Some backup schedules make a full set of backups on a three-day rotation. Others use a three-week rotation, to make incremental backups throughout the week and a full backup on the weekends.
- Automatic backups are set up by scripting what the order of operations will be, and scheduling when they will occur.
- If your backup software allows you to check for write errors to the backed-up files, do so if you can accept the time penalty.
- Compression allows you to put more data on your backup media. In some instances, adding this operation to your backup scheme will also cost you a time penalty.
- Encrypting your backups can be an excellent security step, if the software you use supports DES encryption.
- In some cases, you might need to restore missing or corrupted files; in other cases, you might need to restore an entire hard disk drive. There are software programs that can handle either task.
- An important part of a backup strategy is making sure that you can actually restore your hard drive, using the backups you made. Run tests to see that your backups work as they should.
- Long-term storage backups are never erased, and are never replaced with newer versions. These archives are used to prove that certain data existed on a certain date.
- Replace your backup media on a regular and conservative schedule, as all types of backup media can wear out. Be sure your old backups are rendered unreadable if your data is at all sensitive.

Chapter 7 Sources

MacTools 3.0, \$149
Central Point Software, Inc.
15220 N.W. Greenbrier Pkwy.
Beaverton, OR 97006
(503) 690-8088
FAX: (503) 690-8083

DiskFit Direct 1.0, \$44.95
DiskFit Pro 1.1. \$125
Dantz Development Corp.
4 Orinda Way, Bulding C
Orinda, CA 94563
(510) 253-3000
FAX: (510) 253-9089

DiskTwin 2.0r7, \$999
Golden Triangle Computers, Inc.
11175 Flint Kote Ave.
San Diego, CA 92121
(619) 587-0110
FAX: (619) 587-0303

ExpressMirror 1.32, \$295
ATTO Technology, Inc.
Baird Research Park
1576 Sweet Home Rd.
Amherst, NY 14228
(716) 688-4259
FAX: (716) 636-3630

Fastback Plus 3.0, \$149
Symantec Corp.
10210 Torre Ave.
Cupertino, CA 95014
(503) 334-6054
(800) 441-7234
FAX: (503) 334-7471

FileDuo 1.0.4, \$149

ASD Software, Inc.
4650 Arrow Hwy. Suite E-6
Montclair, CA 91763
(909) 624-2594
FAX: (909) 624-9574

Norton Utilities for Macintosh 2.0, \$149

Symantec Corp.
10210 Torre Ave.
Cupertino, CA 95014
(503) 334-6054
(800) 441-7234
FAX: (503) 334-7471

NovaMac, \$149

Novastor Corp.
30961 Agoura Rd., Suite 109
Westlake Village, CA 91361
(818) 707-9900
FAX: (818) 707-9902

Redux Deluxe 2.0, \$79.95

Inline Software, Inc.
308 Main Street
Lakeville, CT 06039
(203) 435-4995
(800) 453-7671
FAX: (203) 435-1091

Retrospect 2.1, \$249

Retrospect Remote 2.1, \$449

Dantz Development Corp.
4 Orinda Way, Bulding C
Orinda, CA 94563
(510) 253-3000
FAX: (510) 253-9089

SafeDeposit 1.2, \$129
SafeDeposit Server 1.2, \$299
Dayna Communications, Inc.
Sorenson Research Park
849 W. Levoy Drive
Salt Lake City, UT 84123
(801) 269-7200
FAX: (801) 269-7363

SnapBack 1.0, \$129
Golden Triangle Computers, Inc.
11175 Flint Kote Ave.
San Diego, CA 92121
(619) 587-0110
FAX: (619) 587-0303

SurfGuard, \$150
Surf City Software
8144 E. Woodwind Ave.
Orange, CA 92669
(714) 289-8543
FAX: (714) 289-1002

TwinIt 1.0f, \$199
Golden Triangle Computers, Inc.
11175 Flint Kote Ave.
San Diego, CA 92121
(619) 587-0110
FAX: (619) 587-0303



Locks, Chains, and Bars

Compared to securing your data, safeguarding your computer and peripherals is easy. We know how to secure valuable objects: lock them in a room, chain them to the desk, put alarm systems on them.

In many circumstances, if your Macintosh is stolen, most other security concerns are moot. Data encryption will protect the confidentiality of data on a stolen machine, but there's no data availability or integrity on equipment that simply isn't there.

This part will look at physical security of both desktop Macintoshes and PowerBooks. There is a lot of good physical security out there; these chapters will help you figure out what will work for you.



Secure the Computer on Your Desk

Computers are easy prey for thieves: they're a cinch to steal, and easy to sell. Unless you have some sort of physical protection, you're taking a big risk that someday your equipment will disappear.

If your computer is at home, it is protected to the same degree as your other valuables. If someone breaks into your home, your computer will be stolen along with your television, stereo, and other expensive electronics. Assume that all computer disks lying around your computer will be stolen as well. If your only backups are in a pile next to your computer, you've got the potential for disaster.

On the other hand, if you are in charge of computer security for a small or large company, you have a lot more to worry about. More computers present a bigger target. Not only do you have to worry about thieves breaking in from the outside, you also have to worry about employee theft from within. The latter threat is more common and more serious.

A thief has opportunity on his side. You have to close all avenues to theft, and keep them closed at all times. If a thief finds just a single opportunity to steal a computer, it will be gone. He just has to get lucky once.

Thieves Out and Equipment In

The first level of physical security is also the most obvious—lock your doors. Many office doors don't have locks. In general, do not place computers in areas which have no physical access controls. This is only prudent, since the value of a typical Macintosh and any peripherals may well be over \$2000—probably more than all the other equipment in an office put together. Adding locks on the doors increases security, not only for computers but for everything else in the office. When you lock the door, you protect against theft, as you reduce the risk of unauthorized access.

A simple keypad-type combination lock on the door allows easy access to a computer room or office. This eliminates the need for issuing keys, keeping track of them, and dealing with lost keys. Also the manager also has the option of changing the combination, and this should happen at regular intervals. A manager might also want to do this when an employee with access to the combination leaves.

Intrusion protection guards all of your company's assets, not just the computer equipment. Alarms on doors and windows are a start, but there are other alarms you can install around your computers:

Photoelectric alarms, which include a transmitter that sends a infrared beam to a receiver, detects the movement of any object across its path. Mirrors can be used to bend the beam around corners, which increases the installation options.

Microwave alarms have a generator that sends microwaves bouncing off walls and objects in the protected area. A receiver diode in the unit scans these waves. Any changes in their frequency or occurrence indicates an intruder, and trips the alarm. Because it is difficult to contain microwaves in a given area, this type of alarm system is rarely used.

Passive infrared alarms measure the amount of heat in the protected area. Any radical change in the heat level, such as one generated by a warm-blooded thief entering the area, triggers the alarm.

Ultrasonic alarms have a generator that sends ultrasound energy bouncing off walls and objects in the protected area. Any change in the pattern of the sound waves indicates the presence of a new object or a noise, and trips the alarm. This type

of alarm is extremely sensitive—it can be triggered by a draft or a ringing telephone—so it is not often used.

Admittedly, these measures are more suited to securing a room with several Macintoshes, and are of limited use for securing the computer in everyone's individual office. Still, a well-placed intrusion alarm—in a central hallway or in a large office area—is a deterrent to a would-be thief.

In situations where it is not feasible to secure an entire area with locks and alarms, you can put your Macintosh and peripherals in a special workstation enclosure, and keep it closed and locked when the Mac is not in use. In addition to providing easy security for your equipment, the enclosure can protect other valuables such as printed documents and disks.

Anti-Theft Locking Devices

Keep in mind that physical security measures are deterrents. If your offices are harder to break into than the company down the street, a thief is more likely to go down the street. If your computers are hard to steal, a thief is more likely to leave empty-handed than to spend lots of time in your offices, possibly defeating your security measures but also possibly getting caught.

Anti-theft locking devices deter, but they are not foolproof. A thief with enough time and equipment will cut through the locks. However, such devices slow down the thief, and make the task of stealing the computer difficult. Any intelligent thief will leave the computer alone and search for easier pickings—there are a lot of them—while a stupid burglar will be forced to spend more time trying to steal the computer, and will most likely be caught.

Locking devices can take many forms, from anchor pads—metal plates that bolt each piece of computer equipment to each other, and to the desk—to restraining cables, which are metal cables that lock your computer equipment to the desk.

What to Look for in an Anti-Theft Locking Device

Ease of installation. If you can't install the device yourself, you will have to factor in the cost of having a contractor do it for you. If you *can* install the product yourself, do you need any special tools? Do you need any special training to use those tools? These will cost, too.

Time needed to install. This is not much of a factor if you are only securing one computer, but if you are responsible for physical security of a large number of Macintoshes, installation time can become an issue. Labor cost should be factored in to the overall cost of the security product.

What the device may do to the warranty. Make sure the installation of a device doesn't require you to drill into the Macintosh case, modify the chassis, or take some other action that will void your warranty. In addition, some security products don't allow for proper system ventilation and heat dissipation—make sure that your chosen device doesn't block more than a small percentage of the computer's ventilation holes.

Accessibility for service and relocation. The computer will have to unlock easily, when needed, for repair, reconfiguration of internal cards, and relocation. Some products can be removed just by unlocking a padlock; others may have many complicated steps that require special tools.

User-friendliness. The less obtrusive security is, the more likely it will be accepted. A security product shouldn't interfere with normal use of the Macintosh, by locking down the keyboard so that it cannot be moved to a more comfortable position, or by restricting the adjustability of the monitor.

Screws, Adhesion, and Cables

A number of manufacturers produce a low-cost theft-deterrent housing that mounts onto existing, external screws of the computer. A cable connects to this housing, and is then secured around an anchoring point, such as a desk leg or a pipe along

the wall. These kits come with a variety of standard-sized screws to fit most computer equipment in use today. The screws replace the screws that are already on the Mac. Most of the housings are cylindrical or hexagonal in shape, and made of metal, with a hole through which the vinyl-coated cable passes. You should check to make sure that shoulder spacers are provided; these take the pressure off the screws themselves, allowing the housing to turn freely without the screws unscrewing. Some kits supply plugs that fit on top of the screws, making them inaccessible with even the smallest of screwdrivers. Some kits also provide an adhesive plate.

Cable strength is an important consideration. You want a cable that cannot be easily cut with normal tools. Try to use a multi-stranded steel, aircraft-style cable.

These screw-on systems do not provide a high level of security. Cables can be cut, and the screws can be removed. Still, they prevent "grab and run" thefts, and deter casual crooks.

Another low-cost product is the adhesive plate, cable, and padlock kit. Typically, these kits include one to three adhesive plates, a vinyl-coated cable, and a lock. You mount one plate on the computer, another on the monitor, and a third to the underside of the desk (or wherever) to provide an anchoring point. The cable connects the plates together, and the lock secures everything in place. A few kits are designed specifically for laptops, with either a hinged or an angled adhesive plate, plus a cable, lock, and carrying pouch.

Three factors determine the strength of the adhesive plates: the material the plate is made of, the adhesive used, and the surface area covered by the adhesive. Plates are made from plastic, aluminum, or steel. Plastics can often be removed by melting them with a cigarette lighter. Aluminum plates can be peeled away from the surface on which they are mounted. Steel plates are the strongest.

The adhesive should be a closed-cell industrial adhesive tape, 40 mils thick, manufactured specifically for use on plastic painted surfaces. The closed-cell property prevents chemicals from eroding the adhesion. Tape of this thickness allows the adhesive to conform to irregularities of the mounting surface, improving adhesion. The thick tape also allows the plate to be jarred without knocking it loose.

Tapes are rated at a tensile strength per square inch. The rating, multiplied by the surface area of the adhesive used, tells you how much pull it will take to remove the plate. For example, a plate with 16 square inches of surface area, covered with a tape

rated at 100 pounds per square inch, requires 1600 pounds of force to pull it off. This may be overkill, but you want to make sure that the plate cannot be removed by one person.

The plates need to be mounted properly. Follow the manufacturer's instructions. Surfaces need to be truly flat, and you have to clean them thoroughly. Once applied, it can take up to 72 hours for the adhesives to cure and bond completely, so don't try testing them before then. Some plates also come with holes and security screws, for added strength when used as an anchoring point.

The easiest-to-install products have the adhesive pre-applied to the plates. This simplifies the installation process, and saves curing time. It also increases the chances of performing the installation correctly and securely.

It is also important to look at the expansion possibilities of these products. Can you add to the kit, to easily secure peripherals? Can additional, or longer, cable be purchased? Are there specific plates for keyboard and printers?

Like the screw-on systems, this type of product does not provide a high level of security. It does deter opportunity crimes.

Figure 8.1

Kensington's
cable locking
system

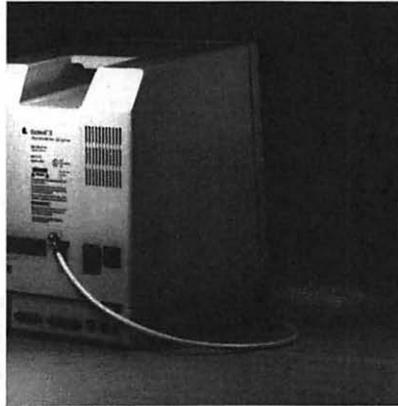


Apple has built-in security sockets on all of its Macintoshes and many of its peripherals, and a number of low-cost theft-deterrent kits are available that take advantage of these. Most provide between one and five security clips that slide into these sockets, and lock into place. A vinyl-coated cable is woven through the holes in the clips, and then anchored around a desk leg and secured

with a lock. Be sure that the clips are made of metal, so they will not snap off easily. You should also check cable strength, and the ability to expand the system at a later date. The security of these systems is no greater than those of either the adhesive plate or the screw-on systems discussed earlier.

Figure 8.2

PC Guardian
Anti-Theft Kit



Setting the Alarms

In addition to adhering your Mac to a desk, you can install a local alarm system. Most of these are battery-powered motion detectors that sound off when the system is moved. Other alarms adhere to the Mac, and plug into your AC outlet to monitor the current. If the current is interrupted, and the system moved, the alarm sounds. If the motion detector is removed from the computer without being deactivated with the key, the alarm also sounds.

Fiber-optic alarm systems are attached to the Mac, and are monitored by a security department or alarm monitoring service. These systems are sensitive, and can be set off by accidentally nudging the Mac. One thing about these alarms is that they will only be effective if someone is around to hear, and respond to, them before the alarms are smashed or punctured.

Plates and Entrapments

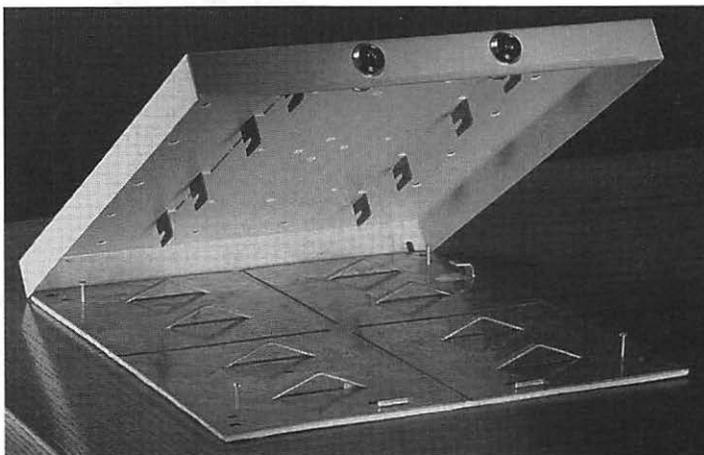
Security plates work on a variety of equipment to secure the computer to a given spot on the desk. These systems usually consist

of two metal plates that lock together. The bottom plate attaches to the desk, either with adhesive or bolts, and the top plate attaches to the computer with either adhesive or with epoxied adapter feet that receive a screw from the underside of the upper plate. The two plates lock together, and require a key to release them.

These security plates offer greater protection against theft than the products previously discussed. They are not usually designed for a particular Macintosh model, so you need to be sure that whatever plate system you buy will fit your equipment. If the plates attach with adhesive, you should review the type and strength, and be sure to follow the instructions for proper installation. Aside from the adhesive, the quality of the metal and the lock determine how secure this type of product is.

Figure 8.3

Qualtec security plate



Generally, security entrapments provide a higher level of security than plates alone, though most do use plates. But entrapments provide additional security by encasing the CPU box. Some products have metal belts that wrap around the CPU, and attach to the plates or metal brackets that sandwich the CPU. These products often fit a variety of systems, and have adjustable belts; make sure that this adjustability does not compromise the security of the system. Other products are CPU-specific, and have been designed to accommodate the box's ports, power switch, or ventilation holes. These products use metal box encasements, brackets, or rods that surround the CPU snugly, attaching to the plates.

Quality of construction is an important consideration with security entrapments. Aluminum is not as strong as steel. Cast metal may be brittle, and more likely to break when hammered. Sheet metal is unlikely to. Welded corners are difficult to pry open with tools. Products that use rods should closely conform to the CPU, to prevent a thief from using bolt cutters. The lock should also be of very high quality, and pick-resistant. This security product is designed to foil a very determined thief; don't overlook any details. The lock is often the weakest link of a security product.

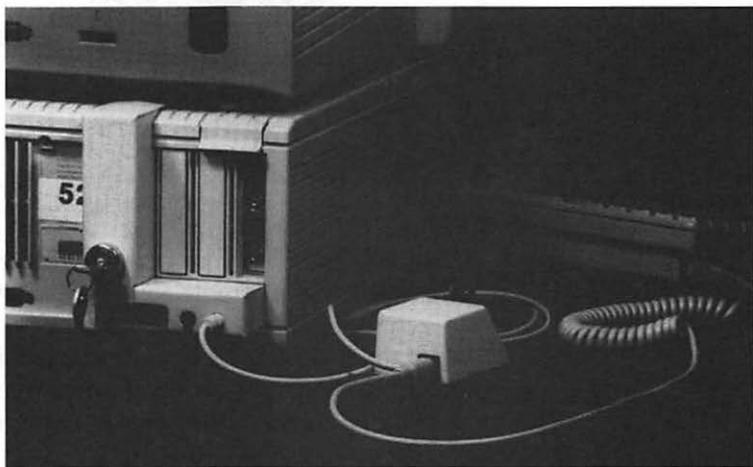
Installation tends to be more difficult with these high-end products, and some are more complicated than others. Check to see if you can do your own installation and removal without specialized tools, or if you will have to hire an installer.

Security On or Inside the Mac

Component scavenging is a more subtle form of theft, usually perpetrated by company employees rather than by outside thieves. Instead of stealing a computer, the thief steals system components: memory boards, graphics accelerators, internal hard drives. Sometimes thieves swap components, stealing a 300 Mbyte hard drive and leaving a 60 Mbyte in its place. It's easier to walk past a guard with a single board than with an entire computer, and if the thief is more than a little clever, the crime might not be noticed for a few days.

Figure 8.4

PC Guardian's
Keyboard and
Chassis Lock



The screw-on systems discussed above provide the lowest-cost solution to deterring component scavenging. Other products, of heavier construction, provide higher security. For example, in some units, a metal part mounts on two existing, external screw holes. A second metal part fits over the first, making the screw holes inaccessible. A padlock locks the second part to the first. If you have a lot of different computers sitting in a large open office, you should seriously consider these kinds of locks.

Not all security hardware is designed to keep your machine on your desk. Some thieves are looking to steal not the computer, but the data on the hard drive. Port locks prevent an unauthorized user from turning on the computer. These are locking devices that prevent access to the power switch, floppy drive, SCSI port, or keyboard port. While not designed to prevent theft, these locks prevent access to the Mac. If someone can't get to the floppy drive, he can't boot the machine from a floppy. If someone can't get to the SCSI port, he can't boot the machine off a portable hard drive he's carrying around just for the purpose. And if he can't even turn the Mac on, he can't do anything.

Figure 8.5

PC Guardian's
Floppy Drive
Lock



One way to make your computers less likely to be stolen is to make them less desirable for resale. Stamping your company's name in indelible ink on all computer parts is a good first step. One of the first things a thief does is to tear off the serial number plate attached to the back of your computer or peripheral, so it's a good idea to mark the serial number on your computer with

the same indelible ink. You can also buy a diamond-tip engraver, and engrave your company name and serial number directly on the piece of equipment. Make such marking visible and ugly; it makes the computer harder to fence.

You can get special serial number plates that are bonded with adhesives that cannot be removed. Another type of serial number plate, when removed, leaves the words "Stolen Property" indelibly stamped on the equipment's case. Of course a thief would be unlikely to know this, so its deterrent value is limited.

Keeping Your Laptop from Growing Legs

Laptop theft is a whole other matter, and it's serious business. Just before Operation Desert Storm began, a laptop belonging to a wing commander in Britain's Royal Air Force was stolen from his car in England. The computer contained highly classified plans for the Allied strike against Iraq. After a lengthy search, the laptop was returned by a fellow who insisted: "I'm a thief, not a bloody traitor."

Other thieves are not so benevolent. An article in *Computerworld* recently reported that a nationwide band of computer hitmen, with ties to organized crime, were being paid upwards of \$10,000 to steal portable computers from Fortune 1000 executives. Rival executives were believed to be behind the contracts. Their motive? They weren't after machines; it was data.

Most of the time, though, it's just the machines thieves are after. Laptop computers are a thief's dream: small, expensive, and easy to sell. Protecting your laptop from theft takes some work, but it's well worth the effort.

PowerBook Security Tips

- Don't leave your PowerBook unattended in a restaurant, at an office, on an airline seat, or anywhere else.
- Don't leave your PowerBook in your hotel room unless it is chained to the furniture.
- Write your company name and telephone on your PowerBook in indelible ink. This will make the computer harder to fence, and you may get your computer returned.

- Make copies of all important applications, programs, and utilities, in addition to any necessary data disks.
- Carry copies of all important applications programs and utilities in your luggage or some other carrying case and not with the computer.
- Use access-control software.
- If you will be working with confidential client data, encrypt that data.
- When working away from home or the office, use a communications program to daily transmit data-file backups to the Macintosh on your desk (or to your file server).
- After returning home, or to the office, and downloading confidential data to your primary machine, use a file erasure program to make sure the confidential data is completely removed from the PowerBook's hard drive. This is especially important if you share the computer with other users.

What to Buy for Hardware Security

Apple Security System

This cable-and-lock security system is designed specifically for Macintoshes. It contains everything necessary to secure a computer, monitor, keyboard, and two to five peripherals: security loops, an eight-foot galvanized-steel wire cable, tamper-resistant screws, a padlock, and two keys. The system uses the built-in security slots on Apple computers, and is very easy to install.

The LaserWriter security system contains everything necessary to secure any printer in the LaserWriter II family. LaserWriters do not have built-in Apple security slots, so the kit includes security brackets that attach to the printer. This kit includes security brackets, security bracket cover plates, screws, 8 feet of galvanized steel wire cable, a padlock, and two keys.

Aztec

Aztec Security Products sells security kits for various Macintosh models. They include clips that attach to the existing security

slots on most models, a vinyl-coated steel cable, and a lock to attach the whole thing to a desk leg. Aztec also sells individual components for other equipment: aluminum plates with a strong bonding adhesive, to anchor equipment without security slots, and other security products.

Cavalier

The Cavalier family of anti-theft products are low-profile security devices for all types of computers and peripherals. These products consist of two steel interlocking plates: a base plate that adheres to the desktop surface, and an insert plate that adheres to the equipment. The adhesive is 3M's 4950 adhesive, a powerful potion with 140 pounds of holding power per square inch. A lock and key holds the two plates together. Installation is easy; no special tools are required.

Cavalier locking systems are available in ten different sizes, from 6 inches by 8.5 inches up to 14 inches by 25 inches, and will secure anything from external hard drives to large printers. They come with a three-year anti-theft warranty.

Cavalier locking systems are also available in special kits for Mac computers. Kits include a "Top Shelf," which secures to the Cavalier base plate and houses the CPU, and adhesive adapter pads to secure the equipment to the insert plate. The Top Shelf also provides a platform for the monitor. A swivel plate, which secures the monitor to the top shelf while still allowing it to turn, is optional—as is a combination keyboard enclosure and keyboard slide assembly, which secure the keyboard.

Computer Owner Protection

Computer Owner Protection, or COP, doesn't prevent computer theft. It provides a way to identify your computer if it is stolen and then recovered by police. COP is identification code bearing software that makes computers permanently identifiable. It stamps a unique registration number on the computer's hard drive. If the machine is recovered by police, this number can be used to trace its owner.

Users must register their name, and software registration number, with the International Computer Recovery Center, an impressive-sounding organization that is actually run by the company that sells COP. In theory, the company is spreading the word about COP to police organizations, hotels, and rental car agencies. Still, this is no guarantee that recovered computers will be

returned to the owner. Whoever recovers the computer has to know enough to look for the COP registration number on the hard drive.

This doesn't impress me. It is far more likely that the police will look at the computer's case for obvious ownership markings, and—finding none—will auction the computer off with all the rest of the recovered stolen property.

LockingStation

LockingStation is a monitor stand with a locking drawer for a PowerBook. The drawer secures the PowerBook while it's attached to a full-size monitor and keyboard at the office—no cabling required. Strips of adhesive are included for securing the LockingStation to the desk. This is a good system.

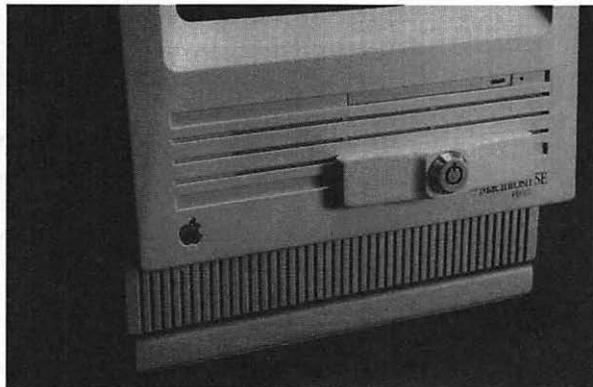
Secure-It anti-theft devices

Secure-It sells a variety of Macintosh locking products. The most comprehensive are its MacKablit security kits. The kits come with two brackets that fit into the equipment's security slots; with hex fasteners that attach using existing surface-mounted screws; with hinge fasteners that attach from the bottom, using existing surface-mounted screws; and with a ten-foot cable and lock. The cable threads through the fasteners, and then wraps around some immovable object. The cable is 3/16-inches in diameter, with a breaking strength of over 4000 pounds, and the whole thing is secured with either a key or a combination lock.

Secure-It also sells disk-drive locks for various Mac models, a heavy-duty locking pad that secures the computer to the desk-top, and a locking device that secures the keyboard.

Figure 8.6

Floppy drive lock



MacShackle

This device fits around the back of PowerBooks from the 140 through 180 series. A cable is placed against the PowerBook's pivoting feet, and secured with a padlock that attaches to the furniture.

MicroSaver Security System

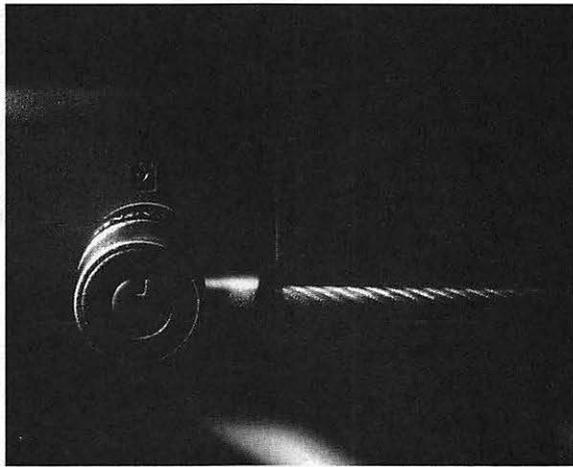
The MicroSaver Security System is a one-piece, cable-and-lock device that loops around your furniture, and locks cleanly into the small, standardized security slot on the back of most PowerBooks (160, 165c, 180, 180c, Mini-Dock docking station, and Duo Dock docking station). It works with some desktop Macs as well (Centris 610 and Quadra 800).

The cable is six feet of galvanized steel. The lock opens with a special round key, and can't be pried off the PowerBook without breaking the case and ruining the resale value of the machine. The whole contraption weighs only 5.5 ounces.

Because Kensington's MicroSave Security System uses a slot built right into your Mac, installation is easy. There are no adhesives, clips, or brackets to install—nothing that could damage your computer.

Figure 8.7

MicroSaver
Security System



PC Guardian Security Products

PC Guardian sells a whole line of physical security products for Macintosh computers. The PC Guardian Anti-Theft Kit includes a Perma-Plate that mounts onto the computer with a special adhesive, another plate that screws onto the desk with either the same

adhesive or with one-way screws, multi-strand steel aircraft-type cables, and a padlock.

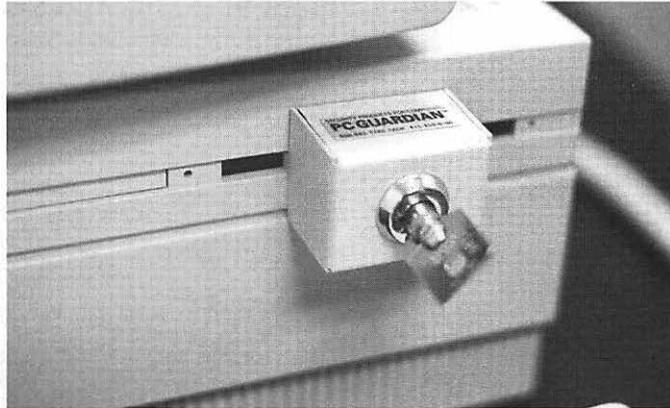
PC Guardian's Power Switch Locks control access to the Mac by securing the On/Off switch. The Mac can be locked and the key removed in either the On or Off position. A security cable can also be used for theft prevention.

Their Keyboard Locks control access to the Mac by locking and disabling the keyboard and mouse. The keyboard and mouse ports are protected, preventing someone from substituting an unsecured keyboard. The Mac can remain on, and continue processing data, while the keyboard and mouse are locked.

Floppy Drive Locks prevent access to the floppy drive. A disk can be locked in the drive, or the drive can be locked while empty. The drive remains operational even with the lock in place.

Figure 8.8

PC Guardian
Floppy Drive
Lock



Phazer/Net

Phazer/Net is a complete, fiber-optic-based, physical security system that protects equipment (computers, peripherals, and anything else) against unauthorized removal. The system uses a cable threaded through security fasteners attached to the equipment. However, unlike other systems, the cable isn't made of steel, and isn't hard to break. It's a fiber optic cable; if a computer is taken, alarms go off.

Specifically, the Phazer/Net security system generates a continuously monitored light-pulse signal. This signal is carried through a thin, lightweight, fiber-optic cable physically linked to

the equipment being protected. If the monitoring signal is interrupted—if the optical fiber is disconnected, cut, or broken—the system immediately alerts a guard, network administrator, or an alarm monitoring service.

The optical fiber circuit is attached by security fasteners, which cover existing equipment screws; by optical fiber Light Loops, which thread through ventilation slots; or by power/signal cable guards, for smaller devices. The Phazer Area Controller's intermittent light pulses monitor system integrity, and trigger a silent or audible alarm if interrupted. An alarm can also be passed on via hard-wire or telephone communications.

The cable is lightweight and unobtrusive, and snaps together for easy installation and relocation. Light-Pulse Amplifiers can extend the effective length of the fiber optic circuit, and therefore protect more equipment in a given area. Security fasteners, Light Loops, and Cable Guards install easily, and do not damage equipment or work surfaces.

An addition you might want is the Phazer Area Controller, which protects about 20 computers and peripherals. It transmits, and continuously monitors, light pulses through the fiber-optic circuit. It also has an optional 80 db alarm. There is also a Phazer/Net stand-alone, multi-zone control unit, that provides problem identification and location reporting. When a Phazer Area Controller detects a break in the circuit, it transmits an alert, indicating the location of the equipment, to the Phazer/Net. The Phazer/Net also has a 110 db audible alarm, a backup battery, and expansion capacity to protect about 100 workstations and peripherals.

This is a whole lot of money and technology to throw at the problem of computer theft, but it does work.

PowerBook Guardian

The PowerBook Guardian is a two-piece, physical security device. A permanent anchor plate screws onto the PowerBook (models 140, 145, 160 170, or 180) through an existing PowerBook screw hole. A cable attaches the plate (and by extension, the PowerBook) to the furniture. The package also comes with an optional lock for clamping the PowerBook display closed.

Figure 8.9

**PowerBook
Guardian**

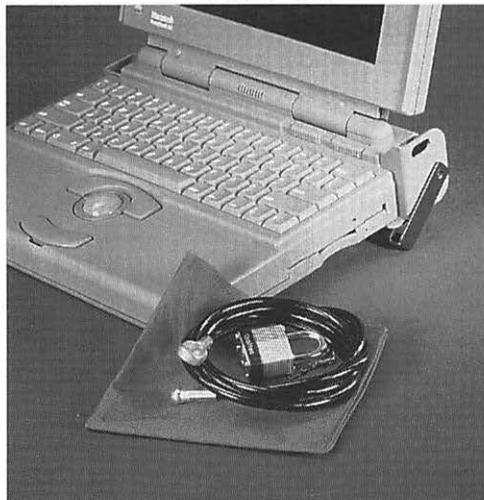


PowerBook Handle Security Kit

The Powerbook Handle Security Kit provides you with a lock and cable to secure your computer to the work area when it is not in use. When using your PowerBook, the kit converts to a handle that folds underneath the computer, holding it in the same ergonomically designed position as the elevation feet. When traveling, you can remove the lock and cable, and store them in the carrying pouch that is provided.

Figure 8.10

**PowerBook
Handle Security
Kit**



PowerLock Plus

PowerLock fits all PowerBooks. Its locking plate slips into the groove along the front of the case, and when the lock is in place, the PowerBook is clamped shut and can be secured by a cable. This device cannot be used to secure an open PowerBook.

Qualtec

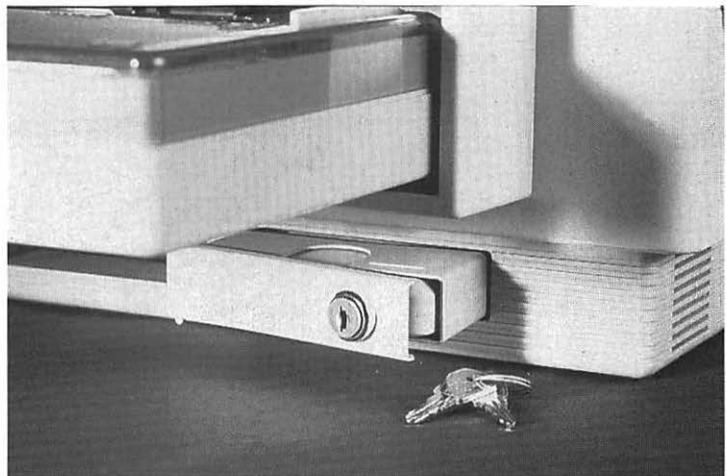
Qualtec makes a whole line of anti-theft products for Macintosh computers and peripherals. They also have a product line for other valuable electronic devices.

Qualtec's Macintosh Security Kits are designed to work with the full line of Macintosh computers and monitors. They consist of security clips that fit into the computer's security slot, cables, and a lock. Installation is simple. The system can also be easily expanded to include peripheral equipment—even equipment without security slots. Accessory products include adhesive plates, extra cable, and extra locks. The cables have a special fitting that allows the user to expand the system.

Qualtec's Heavy-Duty Anti-Theft product line secures your computer to the top or side of your desk. Simply mount the base plate on your desk with the fasteners provided, then attach your computer to the top steel plate with the 3/8-inch, case-hardened steel rods. Join the plates together, and lock the whole thing in place.

Figure 8.11

Qualtec
LaserSafe



Among other Qualtec products, LaserSafe prevents the removal of font cartridges from HP LaserJet printers. A Qualtec Floppy Disk Drive Lock prevents unauthorized access to the floppy drive. Cable Trap secures cable to your mouse or printer, so that it can't be removed without cutting the cable.

Qualtec products are not available directly from the manufacturer, but they can be purchased at many computer stores, and from several computer security companies.



S.T.O.P.

Security Tracking of Office Property (S.T.O.P.) is an anti-theft system based on the idea that a computer is less likely to be stolen if it can't be resold later. This system has several components.

The first is an identification plate, attached to each protected computer (or valuable peripheral) using a patented combination of adhesives, inks, and plastic foils. This ID plate has a bar-coded identification number, and an "800" telephone number. It requires over 1200 pounds of force to remove the plate.

If a thief removes the plate, there is a second line of defense. An indelible "Stolen Property" alert is automatically imprinted on the computer beneath the plate. This tattoo cannot be removed without seriously damaging the computer case.

The identification number, appearing on both the ID plate and the tattoo, is kept on file at S.T.O.P. headquarters, along with information about the machine's owner. If the owner reports the machine missing, the number is put on a list that is transmitted to law-enforcement authorities and major computer resellers.

Figure 8.12

S.T.O.P. Plate



The toll-free number, also on both the plate and the tattoo, is a direct line to S.T.O.P.'s offices. Potential buyers can call the number to verify that the seller is the legitimate owner.

Numerous users in Europe (the technology was first developed in France) and the United States attest to this program's success. Computer theft goes way down, and in some cases stolen machines are actually recovered.

Sentinel

The Sentinel is a system to secure PowerBooks and other notebook computers. It contains a floppy-drive lock that inserts into the drive slot and locks with a key. A vinyl-coated steel cable is fastened to the disk drive lock on one end, and to an immovable object on the other. This system prevents the disk drive from being used and also prevents the computer from being stolen. Although it is a pain to get the lock out of the drive, this system is pretty good.

Figure 8.13

Sentinel



SonicPRO Model AP128

This is an motion-activated, audible alarm that you secure to your PowerBook with high-bonding tape. You can set the alarm sensitivity, duration, and delay. The loud SonicPRO alarm also comes with a three-year, anti-theft insurance policy. You should note that your system is only secure with this if someone hears it. Otherwise, a thief will just break the device and take the PowerBook.

Chapter 8 Summary

- Put locks between your Macintosh and someone who might want to steal it.
- Several types of site alarms are available to help keep your Mac where it belongs. These include systems using photoelectric, microwave, passive-infrared, and ultrasonic technologies.
- Equipment enclosures secure entire workstations, including all hardware, disks, and paper files.
- Locking devices come in several forms, such as locking pads and restraining cables.
- Screw-on systems have inexpensive housings that mount on the existing, external screws on the Macintosh.
- Adhesive-plate-and-cable systems glue metal or plastic plates to the machine, and to the desk, cable them together, and lock the cable in place.
- Security clips use the built-in security socket in the Macintosh housing. The clips are put in place, and a cable is woven through the clips, securing the machine to a large object.
- Alarms for the Macintosh generally consist of battery-powered motion detectors.
- Security plates are bolted, or glued, to both desk and computer housing. A key lock keeps the two plates together. These offer a reasonable level of security.
- Security entrapments offer all the protection of a security-plate system, but are even more secure because they also encase the CPU in plates, belts, or brackets.
- Screw-on systems are useful in preventing component scavenging. Especially useful for those systems that deny access to the screw heads.
- Port locks prevent access to SCSI and keyboard ports, floppy drives, and even the power switch.
- Writing your company's name all over your computer equipment, in large, ugly letters, makes it far less likely that someone who wants to resell that equipment will steal it.

Chapter 8 Sources

Apple Security System, \$49.95
LaserWriter Security System, \$49.95
 Kensington Microware Ltd.
 2855 Campus Drive
 San Mateo, CA 94403
 (415) 572-2700
 (800) 535-4242
 FAX: (415) 572-9675

Mac Kit 1 (for Mac 512, Plus), \$20.45; Mac Kit 2 (for SE, Classic), \$20.45; Mac Kit 3 (for II, IIx, IIcx, IIci, IIcx, IIsi, Quadras), \$34.45; Mac Kit 4 (for LC series), \$27.45

Aztec Security Products
 21438 N. 7th Ave., Suite A
 Phoenix, AZ
 (602) 492-0111
 (800) 333-4002
 FAX: (602) 483-7996

Cavalier 10, 6.00" x 8.50", \$62.00; Cavalier 20, 9.50" x 11.00", \$78.00; Cavalier 64, 7.50 x 17.75", \$80.00; Cavalier 68, 11.25" x 15.62", \$87.00; Cavalier 70, 14.50" x 16.75", \$89.00; Cavalier 73, 15.00" x 20.75", \$96.00; Cavalier 75, 16.50" x 18.75", \$108.00; Cavalier 80, 16.75" x 22.50", \$113.00; Cavalier 85, 14.75" x 25.00", \$115.00; Cavalier 90, 16.80" x 25.625", \$123.00

CAV-MAC Kit (for Mac SE/Classic), \$76.00; CAV-MAC II/IIx/IIcx Kit, \$161.00; CAV-MAC IIci/cx/vx/Quadra 700 Kit, \$139.00; CAV-MAC IIsi Kit, \$139.00; CAV-MAC LC Kit, \$139.00; CAV-MAC Centris 610 Kit, \$156.00; CAV-Imagewriter Kit, \$99.00

MAC II FSS (Full system, includes Keyboard Enclosure, Keyboard Slide Assembly, Rear Cover, Top Shelf, and Monitor Swivel Plate), \$247.00

FMJ Security Systems, Inc.
741 East 223rd Street
Carson, CA 90745
(310) 549-3221
(800) 322-3365
FAX: (310) 549-2921

Computer Owner Protection, \$89
Computer Owner Protection - Laptop Version, \$49
IDX Technologies, Inc.
14 Research Way
Setauket, NY 11733
(516) 689-9886
FAX: (516) 689-1419

LockingStation, \$69.99
CMG Computer Products
P.O. Box 160310
Austin, TX 78716
(512) 329-8220
(800) 880-9980
FAX: (512) 329-5532

MacKablit MKC-120 (for 512 and Plus), \$39.95;
MacKablit MKC-130 (for SE, IIs LCs, Classics, Quadras),
\$39.95

Disk Drive Lock DLK-260 (for Plus, SE, Portable), \$24.95;
Disk Drive Lock DLK-261 (for IIs, Classics, Quadras),
\$24.95; **Disk Drive Lock DLK-262** (for LCs), \$24.95; **Disk
Drive Lock DLK-263** (for IIVx, IIVI, Performa 600), \$24.95;
Disk Drive Lock DLK-350 (for all 3 1/2" drives), \$24.95

Locking Pad CAV-21 (for SE), \$89.95

Keyboard Lock KB-LOK 7 (for SE, SE30), \$99.95;
Keyboard Lock KB-LOK 8 (for II, IIX, IIVx), \$99.95

Secure-It, Inc.
18 Maple Court
East Longmeadow, MA 01028
(413) 525-7039
(800) 451-7592
FAX: (413) 525-8807

MacShackle, \$44.95

Jeff Lastrofka
 P.O. Box 1031
 Agoura Hills, CA 91376
 (818) 597-1518
 FAX: (818) 597-1518 (same)

MicroSaver Security System, \$59.95

Kensington Microware Ltd.
 2855 Campus Drive
 San Mateo, CA 94403
 (415) 572-2700
 (800) 535-4242
 FAX: (415) 572-9675

Floppy Drive Lock, \$19.95

Universal Anti-Theft Kit—Adhesive (model UT36), \$39.95; Mac SE, Classic, Performa 600/700, II series, Quadra series, Centris 650 Universal Anti-Theft Kit (model 599), \$36.95; Mac LC series Anti-Theft Kit (model 575), \$46.95; Mac LC series Keyboard Lock (model 571), \$99.95; Mac II, IIx, IIfx Anti-Theft Kit and CPU Lock (model 535), \$94.95; Mac II, IIx, IIfx Anti-Theft Kit and Keyboard Lock (model 536+), \$139.95; Mac II, IIx, IIfx Keyboard Lock (model 531), \$99.95; Mac II, IIx, IIfx Keyboard Lock and Cable (model 531+), \$99.95; Mac II, IIx, IIfx CPU Locking Device (model 530), \$49.95; Mac IIcx, IIci, Quadra 700 Anti-Theft Kit and CPU Lock (model 545), \$94.95; Mac IIcx, IIci, Quadra 700 Anti-Theft Kit and Keyboard Lock (model 546+), \$139.95; Mac IIcx, IIci, Quadra 700 Keyboard Lock (model 541), \$99.95; Mac IIcx, IIci, Quadra 700 Keyboard Lock and Cable (model 541+), \$114.95; Mac IIcx, IIci, Quadra 700 CPU Lock (model 540), \$49.95; Mac IIsi Keyboard Lock (model 561), \$99.95; Mac IIvx, Centris 650 Anti-Theft Kit and CPU Lock (model 595), \$94.95; Mac IIvx, Centris 650 Anti-Theft Kit and Keyboard Lock (model 596+), \$94.95; Mac IIvx, Centris 650 Keyboard Lock (model 591), \$99.95; Mac IIvx, Centris 650 Keyboard Lock and Cable (model 591+), \$99.95; Mac IIvx, Centris 650 CPU Lock (model 590), \$49.95

PC Guardian Security Products
1133 E. Francisco Blvd. East, Suite D
San Rafael, CA 94901
(415) 459-0190
(800) 288-8126
FAX: (415) 459-1162

Phazer/Net 20, \$1000, to protect 20 workstations
Computer Security Products
One Computer Security Drive/Box 204
Northborough, MA 01532
(508) 393-7803
(800) 466-7636
FAX: (508) 393-2296

PowerBook Guardian (model 1010), \$79.95
PC Guardian Security Products
1133 E. Francisco Blvd., Suite D
San Rafael, CA 94901
(415) 459-0190
(800) 288-8126
FAX: (415) 459-1162

PowerBook Handle Security Kit
(for 140, 145, 160, 170, and 180), \$89.95
Qualtec Data Products, Inc.
47767 Warm Springs Blvd.
Fremont, CA 94539
(510) 490-8911
(800) 628-4413
FAX: (510) 490-8471

PowerLock Plus, \$49.99
CMG Computer Products
P.O. Box 160310
Austin, TX 78716
(512) 329-8220
(800) 880-9980
FAX: (512) 329-5532

Macintosh Security Kit Mac-Kit 1B (for Mac 512 and Plus), \$29.95; **Macintosh Security Kit Mac-Kit 2B** (for Mac SE and Mac Classic), \$29.95; **Macintosh Security Kit Mac-Kit 3B** (for II, IIx, IIfx, IIci, IIcx, IIsi, and Quadras), \$39.95; **Macintosh Security Kit Mac-Kit 4B** (for Mac LC Series), \$39.95; **Universal Macintosh Security Kit Mac-Kit 5B**, \$39.95

Security Clip Mac-Clip 1 (for Mac and Mac Plus), \$9.95; **Security Clip Mac-Clip 2** (For Mac II, SE, Classic, LC, and Quadra series), \$9.95

Apple Keyboard Security Loop KB-LOOP, \$2.95

Floppy Disk Drive Lock FILE-LOK II, \$19.95

LaserSafe LASER-LOK, \$29.95

Heavy-Duty Anti-Theft Product HD 20004 (for Mac II, IIfx, IIx), \$99.00; **Heavy-Duty Anti-Theft Product HD 20008** (for Mac IIci and IIcx), \$99.00; **Heavy-Duty Anti-Theft Product HD 2000-4** (for Mac SE series), \$99.00

Cable Trap (anti-theft device for mouse, keyboard, etc), \$24.95

Chassis Cover Lock MICRO-LOK 19 (for Mac SE series), \$69.95; **Chassis Cover Lock MICRO-LOK 20** (for Mac II IIx, IIfx), \$49.95

Keyboard Lock KB-LOK 7 (for Mac SE series), \$99.95; **Keyboard Lock KB-LOK 8** (for Mac II, IIx, IIfx), \$99.95; **Keyboard Lock KB-LOK 10** (for Mac IIsi), \$99.95; **Keyboard Lock KB-LOK 11** (for Mac IIci), \$99.95

Parallel, Serial & SCSI Port Security Plates, \$19.95

LaserJet Font Cartridge Lock, \$59.95

Qualtec Data Products, Inc.
47767 Warm Springs Blvd.
Fremont, CA 94539
(510) 490-8911
(800) 628-4413
FAX: (510) 490-8471

STOP Plates, \$8.75 to \$25 each, depending on quantity
Security Tracking of Office Property
56 Ocean Drive East
Stamford, CT 06902
(203) 359-9361
(800) 488-7867
FAX: (203) 359-4591

Sentinel, \$49.95
Secure-It, Inc.
18 Maple Court
East Longmeadow, MA 01028
(413) 525-7039
(800) 451-7592
FAX: (413) 525-8807

SonicPRO Model AP128, \$89.95
SonicPRO International, Inc.
5201 Great America Parkway
Santa Clara, CA 95054
(408) 982-2568
(800) 848-0300
FAX: (408) 982-2570



Computer Insurance

Insurance is the protection of last resort. While it can't recoup lost equipment or lost data, it can recoup your investment. Sometimes a good insurance policy means the difference between a large inconvenience and a business-debilitating theft.

Don't automatically assume that your computers are covered under your existing insurance policy. Some homeowner's or renter's policies cover home computers, at least partially. Some policies even protect business equipment you use at home, although the protection is usually limited to a couple of thousand dollars.

Read the fine print, though. Many homeowner, or even business, policies don't cover computer equipment—or cover it to only a small degree. Most insurance policies don't cover the full replacement value of computer equipment—only its depreciated value.

If you use your computer to run a business, you may need more extensive insurance coverage. You may need your insurance to cover the cost of renting a computer while you replace your system. You may need business-interruption insurance, to cover the cost of business lost due to the loss of your computer.

Some insurance policies explicitly cover computer equipment, but like other kinds of insurance policies, these vary widely. Often, what the policies do and do not cover seems somewhat arbitrary.

Some pay to replace computers damaged by fire or flood, but not by earthquake. Some pay only for losses at work and at home; some also pay for losses in transit. Some pay for loss of hardware; others pay for loss of hardware and software. Still more extensive policies pay for loss of data. Often, different policies from the same company cover different sorts of things. Pay attention to what the policy does, and does not, cover.

Prices also vary considerably. Annual premiums range between \$49, for \$2000 worth of coverage to \$400, for \$30,000 worth of coverage. Deductibles range from \$50 to \$200. Pay attention to these numbers, as well.

Don't pay for protection you don't need. Do take time to investigate different companies, and policies, before making a decision. Even if you decide to take the risk and not buy insurance, you want to be informed.

What You Can Cover

Although insurance companies can be arbitrary in what they'll cover, there are certain things they'll insure which are consistent with their coverage for homes. These include damage to, or breakdown of, computers and ancillary equipment as a result of the physical risks of fire, flood, and other disasters. This coverage can be equal to the replacement costs of the equipment, including such factors as clearing of the installation site and associated rebuilding costs.

Hints on Computer Insurance

- Buy reasonable protection for material assets and measurable risks.
- Include insurance as an element of your overall computer security policy, but not as the main feature.
- Base insurance purchases on accurate risk assessments as outlined in Chapter 1. Do not buy coverage you don't need.
- Obtain insurance from someone who is familiar with computer insurance, or from a company that specializes in computer insurance.

- Remember that no insurance can be comprehensive, and that you can never fully compensate for all losses incurred.
- Accidental failure or fluctuation of public electricity supplies is also covered.
- Deliberate acts, such as strikes, are excluded—except for those acts which disrupt the supply for reasons of equipment safety, or for the preservation of human life.

You can also buy insurance to cover:

- Failure of external communications links, such as land lines or satellite links, excluding deliberate acts.
- Loss of access to the computer following damage near the workplace.
- Loss of access to the computer as a result of any actions to safeguard lives by any public or police authority, such as the evacuation of an area during a bomb threat.
- The costs of reconstructing data after data loss or corruption.
- Fines, penalties and damages incurred as a result of the disaster.
- Loss, or accidental corruption, of software.
- The effects of fraudulent activity by staff.
- Costs of business interruption, such as overtime pay, cost of stand-by facilities, and hotel accommodations.

Questions to Ask About Computer Insurance

As with other types of insurance, you should do some homework before talking to a company. Other information will, or should, come out in an interview with the company. Write down a list of questions to take with you to the interview. That list should include the following questions:

- Are you covered against data loss if you or your employees fail to make backups, or if your backups turn out to be useless?

- Are specific disasters, such as floods, fires, or earthquakes, excluded?
- Are you covered against water damage from fire hoses or sprinkler systems?
- Are you covered for hardware or data loss due to negligence—either by you, your employees, or your visitors?
- Are you covered for loss of business, or the costs to replace the data, after a disaster?
- Are you covered for employing a disaster-recovery expert?
- Are you covered for the costs of putting disaster-recovery procedures in place?
- Must damaged equipment be shipped back to the manufacturer for repair, or will the policy allow it to be repaired on site? Who pays for the shipping?
- Will the policy pay for equipment rental while your own equipment is being repaired or replaced?
- Does the policy cover costs for investigating the cause of the disaster?
- Are you covered against the costs of removing debris from the disaster area, and doing general clean-up?
- Does the policy cover replacement costs for software, in the event that original master disks are stolen or destroyed?
- Do you have to wait for the insurance company to approve any repair costs, or can you go ahead immediately? Is there a dollar limit above which approval is required?
- Will the policy cover claims where no material damage has taken place? For example, what if a disaster prevents you from mailing out invoices? Will losses due to that disaster be covered?
- Does the policy cover losses due to computer viruses?
- Are there any criteria that you have to satisfy before being covered? You might have to install a sprinkler system or locks, for example.

What to Buy for Computer Insurance

Safeware Insurance

Safeware Insurance has a "Computerowners Policy," which is an insurance policy explicitly designed for microcomputers. The coverage is comprehensive, protecting you from loss or damage due to fire, theft, vandalism, water damage, lightning (including power surges, from any source), accidental breakage, and natural disasters (except for earthquake). Hardware and software is covered, and the policy even covers losses from a computer virus. It covers computers at home, in the office, or in transit (except if stolen from an unattended vehicle). The policy provides for replacement cost without regard to depreciation.

The company also has a special Gold Key Endorsement, which has additional coverage tailored to your business. Additional coverage can include:

- Computer rental, and other necessary expenses incurred to stay in business as a result of a covered loss.
- Other electronic equipment, including test equipment, copiers, phone systems, and typewriters.
- Extension of protection to newly acquired equipment.
- Reference materials, including textbooks, user guides, and instructional manuals.
- Loss from computer fraud, or from misuse of your computer by employees and others.

Safeware also has Fix:It insurance, which covers losses due to mechanical breakdowns, external damage, theft, and power surges. Software is also covered.

Safeware's International Property Policy covers loss or damage to computer equipment, as well as business and personal property, while you travel outside the United States and Canada. The coverage is comprehensive, protecting against fire, theft (except that from an unattended vehicle), vandalism, water damage, lightning (but not power surges or short circuits), accidental damage, and earthquake. This coverage is not only for your equipment, but also for the data-storage media and for programs on your computer.

ComputerInsurance Plus

The ComputerInsurance Agency specializes in insurance for computers. Its primary policy is called ComputerInsurance Plus; it protects computer hardware, peripherals, and software. This protection covers losses due to earthquakes, natural disasters, power surges, and covers equipment in transit. The policy's blanket-coverage provisions mean that no lists of equipment or serial numbers are needed to start coverage. This is especially convenient for computer owners who add components to their systems; the additional system hardware and software is automatically covered.

The company's Two-Way Coverage protects against the various natural disasters plus mechanical breakdown. This is repair insurance: you can take your equipment to any authorized repair facility, and be assured that the cost of repairs will be reimbursed, no matter what the cause. There are restrictions on this policy; don't think you can insure all your old clunky computer equipment.

The company's Insurance to Go is designed to serve the needs of traveling computer users. Many business insurance policies exclude coverage for equipment in transit. This policy covers earthquake, theft, power surges, fire, floods, and accidental damage. Also, it covers computers at home, in the office, and on the road. It pays replacement costs for equipment, with no depreciation.

Personal Computer Insurance

DATA Security Insurance has a comprehensive computer insurance policy for both home and business. It covers:

- All your equipment—all brands of computers and peripherals can be combined in a single policy.
- Loss or damage—from theft, fire, or vandalism—to your equipment, media (including floppy disks), programs (including custom programs), data stored on your system, and documentation.
- Repair or replacement, without deduction for depreciation.

- Damage from external electrical problems, such as power spikes, brownouts, or surges.
- Loss due to theft from an unattended automobile.
- Loss of data due to accidental erasure. Reimbursement is based on the actual costs incurred to reconstruct your data from source documents.
- Fraudulent use or misuse of your computer, by outside parties or employees.

The policy reimburses you for any extra expenses incurred while your computers are being replaced, or repaired, after a covered loss. This is comprehensive coverage, and the premiums are reasonable. Call DATA Security Insurance to get the fine print.

Powell-Walton-Milward Insurance

This company insures home offices, especially ones with a lot of computer equipment. It covers business liability, business interruption, and assets like inventory and business equipment.

Chapter 9 Summary

- Insurance, while it cannot get your lost computer or your lost data back, can recoup your investment. Double-check the insurance you carry now: are your computers and peripherals covered to the full extent of their value?
- Read the fine print of the policy, and ask a lot of questions. Prices, and the types of covered loss, vary wildly from insurance policy to insurance policy—even among those written by the same company.
- Safeware Insurance covers losses from all sorts of damage. Additionally, Safeware offers a mechanical breakdown policy, and a policy geared toward international travelers.
- ComputerInsurance Agency also offers several policies, including Insurance to Go, which covers traveling with a computer.

- DATA Security Insurance offers Personal Computer Insurance, a comprehensive policy that even covers fraudulent use of your computer.
- Powell-Walton-Milward specializes in insuring the home office.

Chapter 9 Sources

Computerowners Policy

Safeware Insurance
2929 North High Street
P.O. Box 02211
Columbus, OH 43202
(614) 262-0559
(800) 822-2345
FAX: (614) 262-1714

ComputerInsurance Plus

The ComputerInsurance Agency, Inc.
6150 Old Millersport Road NE
Pleasantville, OH 43148
(614) 263-5100
(800) 722-0385
FAX: (614) 263-5109

Personal Computer Insurance

DATA Security Insurance
4800 Riverbend Road
P.O. Box 9003
Boulder, CO 80301
(303) 442-0900
(800) 822-0901
FAX: (303) 443-4705

Powell-Walton-Milward Insurance

P.O. Box 2030
Lexington, KY 40594
(606) 254-8023
FAX: (606) 254-8020



P A R T

V

Keep Intruders Out of Your Network

Networks are designed to allow people to communicate via computers. AppleTalk, Apple's cabling that plugs into your Mac and hooks several Macs together, makes this simple. AppleShare, the Mac's networking software, makes it easy to share files among users. AppleTalk Remote Access software makes it easy for remote users to dial into the network.

The downside is that anyone connected to a network can read files. With the right software, anyone can read information being passed back and forth across an AppleTalk network—even if none of the information is addressed to him. Anyone can dial into the network and do such mischief from someplace else. Network connectivity is easy, but so is network spying.

Network security puts a damper on all this fun. Yes, you can connect to the network, but only if you are an authorized user. Yes, you can share files, but only with people authorized to see them. Yes, you can dial into the network, but only as an authorized remote user.



Network Security

When users talk about the security of a computer network, they often mean different things. Generally, people want their computer network to be as secure as whatever paper systems it might have replaced. When one user transmits information to another user across a network, these are the things they expect:

1. That the information is received at its intended destination, and nowhere else. This was easy in the world of physical paper. A piece of paper can be in only one place at any given instant. However, with computers, information can be in many places simultaneously—and the recipient has no way of knowing how many copies of a piece of data have been made.
2. That the information received is the same as it was at transmission—nothing has been added, deleted, or changed. Unauthorized modifications to a piece of paper can be easily detected, and forgery is an art unavailable to most people. Computers make it easy to change a piece of information without anyone ever detecting it.
3. That the sender can verify that the information was delivered only to the authorized recipient. Think of certified mail. Postal officers make sure you are who you say you

are, before giving you a piece of certified mail. But with computers, what is going to stop someone from pretending to be you, and reading all of your electronic mail?

4. That the recipient can verify that the communication's apparent sender is really the person who sent it. Paper signatures are not infallible, but they are fairly good. Longstanding legal precedents have developed regarding paper signatures. In the electronic world, how do you know where your data or electronic mail is coming from?
5. That while in transit, the information cannot be observed, tampered with, or extracted from the network by some unauthorized person or device. In the paper world, we put considerable trust in courier services and the Post Office. Even so, we use envelopes to prevent casual observers from snooping where they shouldn't. Computer networks don't have anything analogous to an envelope; anyone can look at everything.

Network managers, on the other hand, look at network security differently. They apply to their networks the three major goals of security: confidentiality, integrity, and continuity.

Confidentiality is the most obvious application of security. User expectations 1., 4., and 5. require it. Only authorized personnel should be able to access confidential information. Only authorized personnel—potentially a different set of authorized personnel—can modify or delete confidential information. For example, salary records should not be available to everyone in the company. Only the senior managers should be allowed to see who earns what—but they have no business changing people's salaries. The personnel office can change people's salaries, but they should be prohibited from seeing who earns what.

Trying to keep everything on the network confidential doesn't work. Confidentiality was difficult enough to achieve on an isolated Macintosh; it's almost impossible on a Macintosh network. Furthermore, imposing such restrictions needlessly is only going to create problems. It is also very difficult to legally prosecute someone who breaches confidentiality, unless you can show that there is a clear difference between confidential and public information.

Confidential information is defined as data that is critical to your business, that costs money to get, and that is not generally known. Examples include marketing strategies, trade secrets, re-

search and development information, financial information, personnel data, customer information, and information about the network itself.

Integrity means that nothing on the network can be tampered with—data is unchanged—and this is required for user expectations 2., 3., and 5. Integrity controls protect a network from both malicious and inadvertent tampering.

Network managers have an additional security requirement—continuity. Continuity means that the network stays available. It works when it is supposed to, and no one can disrupt critical applications on the network, either through malicious actions or carelessness. The need for continuity varies from network to network, function to function, day to day, and hour to hour. A network that controls a nuclear power station requires a greater degree of continuity than one that sends inter-office electronic mail. It might be especially important for a network to work problem-free during backups, or during a particularly busy time of the year. However, most enterprises have at least one critical application that requires a continuously available and accurately working network.

Integrity is vital throughout the network. If users cannot trust information on the network, then they will not use it. A lack of integrity in one area of the network can cause continuity, integrity, and confidentiality problems throughout the network.

AppleTalk Security Practices for Managers

- Allow only selected users to print to certain output devices, such as high-resolution imagesetters, slide makers, or printers in designated locations.
- Subdivide the AppleTalk network, so that one group's resources (like file servers and printers) cannot be used by another group.
- Allow only selected users to send faxes or electronic mail.
- Limit dial-in access to only selected callers.
- Control user privileges on shared workstations.
- Implement password protection on file servers and electronic mail accounts.

To meet these objectives—both user expectations and network manager security goals—you must implement security controls that prevent, detect, contain, and recover from security breaches. If an intruder just reads data files, the breach can compromise confidentiality. If the intruder changes data files, the breach can damage confidentiality and integrity. If the intruder damages or steals hardware and/or software, network continuity can be at risk.

Prevention mechanisms prevent someone from breaching the security of the network, either maliciously or accidentally. They are a network's first line of defense, and can include such things as dial-back modems, password tokens, or encryption on telephone connections. If you can stop security breaches with prevention mechanisms, you are ahead of the game.

Detection mechanisms sense any attempt to breach security. Besides the obvious benefit of warning that someone is trying to break into your network, detection mechanisms can also tell you that there was a successful attack against a computer on your network, and that the integrity of the data on that machine is in question. Mechanisms that fall into this category include audit logs, which keep records of network accesses, and checksum programs, which alert you if certain files have been modified.

Containment mechanisms, such as "firewalling"—requiring separate passwords for separate machines on the network—ensure that a successful attack against a single point of the network does not compromise the entire network. Finally, recovery mechanisms ensure that data integrity can be restored after a successful attack. These recovery methods can be as simple as a regular back-up schedule.

These security mechanisms may involve hardware controls, software controls, or procedures—and a good security strategy often requires a combination of the three. Before discussing some of these security controls, let us first look at the different vulnerabilities on a network.

To write a security policy, the first step is to find out what needs to be protected—what hardware and software is on the network? Don't just look at the present network configuration; look at future expansion plans as well. Then, look at what kind of data need to be protected. Determine its value to the company, and determine who is responsible for it.

After creating a map of the network, determine who needs access to which pieces of the network. This step will probably involve interviewing people. Your security policy must ensure that these people still have access to the parts of the network they

need to do their jobs. Only after all of this is completed, start looking at different countermeasures.

A Sample Security Policy Plan

I. Introduction

A. Mission Statement

II. Responsibilities

A. Management

B. Personnel

C. Corporate Security

D. Employee

III. Situational Analysis

A. Network Description

1. Hardware
2. Software
3. Expansion Plans
4. External Connections
5. Security Features

B. Resource Analysis

1. Value of Network Resources
2. Ownership of Network Resources
3. User Requirements for Access to Resources

C. Security Plan

1. Physical Security
2. Hardware Security
3. Personnel Security
4. Information Security
5. Software Security
6. Dial-In Security
7. Disaster Recovery/Contingency Planning

Related Documents:

Network Security Administration Manual
Users' Guide to Network Security

Network Vulnerabilities

With mainframes, security was a whole lot easier. The computer center protected the hardware, and there were all kinds of security programs to protect the software and data. Since a central CPU controlled everything, security was centered on that CPU.

In the world of Macintosh networks, security is considerably more complex. There is no central CPU to secure—instead, the Macs are on everyone's desks, and are distributed all over one or several buildings. The software on the different Macs comes from several different vendors—each of which may have their own security solution that doesn't interplay with the others. If the network has dial-in access, people can dial into the network from anywhere. Also, users with their individual Macs are capable of performing some subtle and powerful attacks against the network.

Threats to Communications and Networks

Passive attacks on a communications link involve listening, but not changing data:

Eavesdropping. Unauthorized capturing of signals, either by line tapping or by picking up the emanations (TEMPEST) broadcast from the electrical signals on the line.

Traffic Analysis. Analyzing who is sending messages to whom, can reveal much information—even if the messages are encrypted. The number, size, frequency, and times of messages can all be important information.

Active attacks involve taking steps to interfere with the data being transmitted. They are much harder to set up than merely listening:

Modification. Deliberately changing the message contents.

Re-routing. Diverting a message from the intended recipient to a third party. This kind of ploy could be used to collect valid passwords from unsuspecting users.

Addition of Fake Messages. Sending a bogus message to someone.

Re-play. Sending the same valid message again and again. In a financial network, replaying the message to credit \$1000 to a certain account could be very profitable.

Deletion. Wiping out a message so that it never reaches its intended destination.

Delay. Deliberately stalling the transmission of a message. If the message contained time-critical information, this could be disastrous.

Masquerade. Posing as an authorized user of the communications channel.

Man-in-the-Middle. Cutting the communications link between two computers, and conducting two conversations—one with each computer. The computers think they are talking with each other and that nothing is amiss.

Jamming. Entirely preventing communications from taking place.

Accidental attacks are not perpetrated by anyone, but they can be just as damaging as active attacks:

Message Loss. The message disappears during transmission.

Message Duplication. The message is accidentally copied, either once or many times.

Sequence Errors. The message is sent, but is jumbled in transmission.

Message Re-routing. The message is accidentally sent to the wrong destination.

Message Corruption. The message is garbled during transmission.

Where do you need security on a Macintosh network? The short answer is everywhere. Intruders can target the network from almost any point. They can break into an individual Mac, and

then into the network. They can listen in to the network communications links, and monitor traffic across it. They can break in through dial-in links. They can plant viruses that do their snooping for them. They can even steal a set of backup tapes.

After an intruder gains access to the network, he can do any number of things. He can copy and reveal sensitive data, or he can modify your data and programs. By simply forcing a denial of service, he can cause considerable damage. He can even destroy hardware.

File servers probably require more protection than workstations, especially if information about the users is stored on them. The applications server, which may be a different machine than the file server, requires special protection. This is a new piece of the security problem, made important by work-group computing applications like Apple's Open Collaboration Environment (AOCE).

Remote access by modem must be controlled. Potentially, modems are open doors to the network. More subtle vulnerabilities are bridges, routers, and gateways. Even if an intruder doesn't have modem access to a particular AppleTalk network, there may be a bridge to another AppleTalk network to which he does have access. Macs often share printers, and that is another potential security problem, since anyone can read the hard copy as it prints.

More subtle yet is the backbone itself: the wires of the network. Cheap packet sniffers are available for AppleTalk and other network protocols. They can read information as it flows back and forth along the network—no matter whom the packets are addressed to.

Countermeasures

Procedural countermeasures, hardware countermeasures, and software countermeasures are all designed to protect the various parts of a network. Strategically, each of these countermeasures does one of three things: protects the network links, protects the individual computers on the network, or protects the data on the computers. Network protection includes such things as power protection, physical locks, and secure dial-in modems. Computer protection includes user authentication, physical locks, and diskless workstations. Data protection includes data encryption, audit logs, and making regular backups. Many software programs provide comprehensive network security: they implement many

different types of hardware and software countermeasures at the same time.

Security countermeasures must be geared to a defined security threat. Assess your risks. It is not reasonable to spend more to protect information than that data is worth. Before implementing any security countermeasures, do a cost/benefit analysis, as outlined in Chapter 1. Costs include the initial design of the security plan, as well as the development, acquisition, implementation, and training costs. You should also factor in the annual recurring operations and maintenance costs, and the cost in time to everyone who has to work with these countermeasures. Any network has acceptable security risks. It is important that people understand the risks.

Before implementing any security countermeasure, look at how it will integrate into the network. Is the countermeasure effective against the threat? Is the countermeasure reasonable protection against the threat? If it is unreasonable, not only will it be needlessly expensive, but users will not be happy about it. User acceptance is critical. Countermeasures are most likely to be accepted if they place minimal additional burden on user performance. They should also be easy to administer. Lastly, do not implement a security measure that is likely to become obsolete quickly, or one from a vendor who is likely to leave the business. Remember that 100 percent security is not the goal: The only way to achieve total security is to turn the computers off.

Management, Procedures, and Security

Controls imposed by management are the most effective of any countermeasure. These are not hardware additions or software solutions, but are procedural countermeasures—also known as security policies and practices. They can range from the simple “lock your door when you leave for the night,” to complex procedures for updating important databases.

In the end, any security countermeasure is only as effective as the efforts of those who must use it every day. Physical locks are useless if employees keep the doors propped open; no one will make regular backups unless management gives them the time and resources to do so. Unless all employees understand, and are behind, your security countermeasures, they won't work. And, unless corporate management supports your security program, the employees won't.

A written security policy is crucial. This is a document that lays out the overall security program for the network: what the threats are, what the solutions are, and who is responsible for what. Not only is this document essential for implementing any security countermeasures, but it would be required in court to prove a specific security violation. Chapter 17 describes in detail how to write a security policy.

After you write the security policy, and management approves it, two other documents follow: the Network Security Administration Manual, and the Users' Guide to Network Security. The first outlines how security is going to be administered on the network. This is important, because it details exactly what the administration responsibilities are. The second document is even more important: It explains to everyone on the network what security measures are going to be implemented, how they are going to affect the users, and what responsibilities the users will have for security. These documents will be specific to your network configuration.

Security-awareness programs are effective means of introducing the security policy to everyone in the company. Discuss the Users' Guide to Network Security; make sure everyone understands what is being done and why. Don't forget contractors and consultants, vendors, and customers; everyone outside the company dialing into the network should sign network access agreements.

Network administrators should look to implement these three, simple, policy measures to greatly increase the security of their networks:

Change passwords regularly. People must not write their passwords down, or reveal them to anyone. They also must not use obvious passwords. See Chapter 2 for more details.

Make regular backups. Everyone says this, but few people do it. Not only are regular backups important, but a copy must be stored offsite. Think about your entire office being burned to the ground. The backup sitting in the desk drawer next to the computer isn't going to help. The more important the data on the network, the more important the backup. There are many programs that can back up an entire network to tape, automatically.

Limit dial-in access. The easiest way for someone to penetrate your network is through the telephone lines. Limit the number of people who have access to the dial-in lines to an absolute minimum.

Four Possible Routes to Network Security

- Light Security is simply minimal password protection on logons. It's easy and unobtrusive, and users don't mind it. Unfortunately, it is not at all secure.
- Medium Security adds serious password protection, and audits activity on the network. This will deter the curious, it doesn't cost much to implement, and it is not difficult for employees to follow. It will not stop a serious adversary, however.
- Heavy Security adds encryption, dial-back modems, and portable identification tokens. This regimen is extremely difficult to break. Investing in security hardware is expensive, and you will have to train employees to follow the correct procedures.
- Absolute Security eliminates remote access, and strictly controls access to network terminals. While this is the best you can do, it is extremely difficult to use and to service.

Controlling Zone and Device Access

A simple and effective countermeasure on an AppleTalk network is to restrict access to certain areas of the network. The users who have authorized access to the area can use its resources—file servers, printers, modems, for example. Everyone else cannot.

If your security needs are great (perhaps foreign intelligence agents may try breaking into your network), the best way to restrict access to an area of the network is to physically disconnect it from the rest of the network. For most security needs, however, routers provide adequate security.

You can set up your network as a collection of zones connected by routers. To restrict access across these zone boundaries, the software provided with most routers has a filtering option. Filtering restricts what data packets are allowed across the router, and thereby limits the accessibility of resources in one zone from computers in another zone.

You should note that different router vendors implement filtering somewhat differently. Generally, they use one of three basic filtering methods: GetZoneList, NBP LkUp-Relay, or RTMP.

GetZoneList filters are designed to restrict a zone of users from accessing the rest of the network. For example, you may wish to set up a zone for "visitors," who do not have access to the confidential file servers—outside modem connections, among others. The router will not let any Macs inside this visitor zone see any services outside that zone. When a Mac from inside this zone sends a GetZoneList packet to the router, for display on a Chooser menu, the router returns a filtered zone list of only those services within the visitor zone. Services outside the zone do not appear on the various Chooser menus—users are not even aware that they exist. On the other side of the filter, the router will send a full zone list to any Mac that requests it. Users on the rest of the network will be able to access any services in the restricted zone.

NBP LkUp-Relay filters restrict the passage of NBP packets across the router. This is more flexible than GetZoneList filtering, because it allows for partial communication to a filtered area of the network. NBP filtering only restricts a particular device type: a printer, for example. You could set up a zone for graphic arts, with expensive color printers. An NBP filter between the graphic arts zone and the rest of the network could prevent users in other zones from using the graphic arts printers, while still allowing them access to file servers and other resources in that zone.

RTMP is a two-way access control filter. Users from one zone are restricted from accessing services in the second zone, and users from the second zone are restricted from accessing services in the first zone. RTMP filters are useful for dividing an AppleTalk network into several restricted areas. The filters look at individual data packets, and decide which to restrict and which to let through. This type of filtering is more complicated but more flexible. Check your router's software manual for details on how to set it up.

Security with AppleShare

The Macintosh operating system has a protocol called AppleShare, which allows for one computer on a network to use files or entire volumes on another machine. If you are on a network, and turn this option on, another Mac on the same network can put files on your hard disk and use your files. In networking circles, this is known as a peer-to-peer set up.

This makes it easier for two (or more) people to share files. No longer do you have to pass someone a disk when you want to

give them a data file. Unfortunately, File Sharing can be very generous. You can set your computer such that anyone on the network has complete access to your system. She can read all your mail, delete all your files, or do whatever mischief she likes. She doesn't even have to do mischief; she may delete your data accidentally.

AppleShare currently comes in three flavors: AppleShare 3.0, AppleShare 4.0, and AppleShare Pro. They differ in performance and platform. AppleShare 4.0 is designed to take advantage of 68040-based Macs, and AppleShare Pro utilizes the specialized hardware and operating environment of the Apple Workgroup Server 95. All three flavors have the same security features.

Table 10.1: AppleShare Supported Platforms

AppleShare 3.0	AppleShare 4.0	AppleShare Pro
Any Macintosh computer	Centris 610, Quadra 700, 800, or 950	Apple Workgroup Server 60 or 80 Apple Workgroup Server 95

AppleShare has three levels of access privileges: Owner, Group, and Everyone. These can be assigned to folders on shared volumes. A folder's owner can also assign a special set of other privileges to one other user, rather than to a group of users. These other privileges include full access, a drop folder with only write access, and no access.

Additionally, users can protect their data by preventing others from seeing files enclosed in folders, by preventing others from seeing folders enclosed in folders, by preventing others from writing to a folder, and by preventing others from writing to, or seeing, folders and files.

AppleShare 3.0 (and higher) uses a concept called "inherited privileges." When you create a new folder with AppleShare workstation software, it inherits the privileges of the folder within which it is created. When you create a folder and move it to another folder on the server, it adopts the privileges of that folder. Only if you deliberately change its privileges does it retain explicit privileges when you move it around.

AppleShare supports passwords for log-on. The software has options for minimum password length, password aging (to force users to change their passwords regularly), password history (to prevent users from using the same password over again immediately), and account disabling after a certain number of unsuccessful access attempts.

It also has mechanisms for temporary accounts and for guest logons (which can be turned off). Also, an administrator can force any user to immediately log off.

AppleShare Security Measures

- Minimum password length
- Password aging
- Password history to prevent immediate reuse
- User restriction from saving passwords in a file
- Account disabling after specified number of password failures
- Adjustable time limit for temporary accounts
- "Guest" access turned off by default
- Copy-protection setting for documents
- "Lock" setting for folders
- Inherited folder privileges
- Administrator log-off of any user

Remote Access Control and Security

The simplest, and least secure, way to protect incoming modem lines is to set up password security. Each user has a password, and he has to enter it correctly as part of the dial-in process. All remote-access hardware has password options that are easy to install and use.

Better security comes from a dial-back modem. With a dial-back modem, a user calls the device and types in his name. The modem breaks the connection, looks for the user's name in its database, and calls him back at the telephone number it has stored. This works great, but assumes that users always dial in from the same telephone number. Users who are constantly on the road, calling in from a variety of locations, won't be able to use this feature. There is also a way to defeat most dial-back modems, but it is so new that I am leery of describing it here.

Unlike the first version, AppleTalk Remote Access 2.0 consists of separate client and server applications. The ARA Multiport

Server software (which also includes the Apple Remote Access Personal Server software) combines the Remote Access Administrator with a number of additional security features.

Two new security features lock out unauthorized callers and place restrictions on unauthorized calls. Third-party developers can take advantage of a new modular design to implement additional security protocols, beyond the password and call-back measures in Version 1.0. Some of the security products announced include Kerberos, SecurID Cards, and SofKeyPlus (see reviews at end of chapter).

Using ARA 2.0, the administrator can also restrict specific users' access to only certain network zones. In Version 1.0, the only access options to give remote users are either to the ARA server, or to the entire network.

The Administrator application must always be running because it also functions as a server. A lock feature prevents unauthorized changes to the Administrator settings from the server keyboard.

The Administrator shares some of AppleShare's settings for password expiration, password length, and anti-infiltration measures. ARA 2.0 administrators can assign each user an individual connection time limit, and user accounts can be disabled after a specific number of incorrect password attempts. ARA 2.0 also supports an audit log to record calling and answering activities.

The Apple Remote Access Multiport Server uses Apple's License Manager. Each copy of the administrative software searches the network for other copies, and compares serial numbers. When duplicates are found, the applications begin sending messages to administrators urging them not to illegally copy software.

AOCE Security

Apple's Open Collaboration Environment (AOCE) has many built-in features, such as password authentication, encryption, and digital signatures. Software developers can take advantage of these authentication capabilities to improve the security of their applications. Such capabilities also simplify security administration: users need only one password to authenticate themselves to the system and gain full access to all of its services.

The AOCE catalog server acts as a trusted third party and grants authentication credentials. An application can use the Authentication Manager to handle the entire authentication process,

thereby validating the identity of various entities on the network—people, servers, and programs.

Future versions of AOCE will allow interoperability with other authentication systems running on other platforms, such as Unix's Kerberos.

The Authentication Manager helps establish encrypted AppleTalk data connections. This privacy capability prevents eavesdroppers from reading information that programs or users send through the network. The data is encrypted using the RC4 algorithm, licensed to Apple by RSA Data Security.

Note that none of this works unless companies program these capabilities into their applications. These are tools, just like QuickDraw. Hopefully, future AOCE applications will make use of encryption, digital signatures, and authentication.

The PowerTalk Key Chain, a part of AOCE, is a "single sign-on" system that enables users to access multiple services on a network, using just one access code. Services requiring passwords can incorporate something called "key chain access" within themselves, and then allow users to use the PowerTalk Key Chain to automatically provide access control. A user just has to provide a single access code, and PowerTalk Key Chain does the rest. It can unlock any network applications, such as electronic mail, scheduling programs, or file-server systems.

What is "Single Sign-On"?

Assume that your Macintosh is on a large network. Security is important, so everything is protected by a password. You need one password to start up your Mac, another to access your workgroup's file server, another to access the file server downstairs, and so on. Pretty soon, this is going to get unwieldy. You'll have to start writing your passwords down, or else you'll forget them.

Single sign-on makes this problem disappear. If your network has the single sign-on feature, you only have to enter your password once. Once you've done so, the network takes care of all your access privileges. If you're allowed to see the file server, you see it automatically. No other passwords are required.

Single sign-on is easy in a mainframe environment, but has long been a dream of distributed networks. AOCE's PowerTalk Key Chain is an implementation of single sign-on.

The Keys to the Network

Encryption and access-control have more relevance when you're a network manager contemplating a security system. In addition to the software products reviewed here, and in previous chapters, several technologies are currently in use across networks.

Digital Signatures

Handwritten signatures on documents have long been used as proof of authorship, or of agreement with the contents of the document. Generally, a signature on a document—and the act of signing the document—is compelling, because:

- **The signature cannot be forged by someone else.** The signature is proof that the signer deliberately signed his name to the document.
- **The signature is authentic.** The signature can convince the recipient of the document that the signer did indeed sign his name to the document.
- **The signature is not reusable.** The signature is written on the document, and cannot be moved to a different document. In other words, an unscrupulous person cannot move a signature on a document to a completely different document.
- **The signed document is unalterable.** After the document is signed, it cannot be altered. This is not really true, but if a typewritten and signed letter has substantive handwritten changes in the body, someone is going to get suspicious.
- **The signature cannot be repudiated.** The signature and the document are physical things. The signer cannot later claim that he didn't sign it.

Digital signatures are an attempt to create digital documents that can be mathematically and legally traced to their authors. A digital signature is a string of bits, attached to a digital document—a file, a piece of e-mail, etc. This string of bits is generated by the signer, based both on the document and on his secret password. Someone who receives the document can prove, both to himself and to a court, that the signer signed the document. If the document is altered, then the signer can prove, to himself

and to a court, that he did not sign the altered version of the document.

The mathematics behind this, is the mathematics of public-key cryptography. Public-key cryptosystems have two keys: a public key and a private key. You sign a document with your private key, and verify the signature with your public key. Only you can sign, but anyone can verify. The entire protocol—by which the receiver of a message is convinced of the identity of the sender, and of the integrity of the message—is called authentication.

Digital signatures satisfy our five security criteria outlined above. Whether digital signatures will stand up in court, in the same way as real signatures, is another matter. Preliminary legal research has shown that digital signatures would meet the requirements of a legally binding signature for most purposes, including those of commercial users as defined in the Uniform Commercial Code (UCC). A Government Accounting Office decision, made at the request of the National Institute of Standards and Technology, opines that digital signatures will meet the legal standards of handwritten signatures.

Even so, the validity of digital signatures has not been challenged in court, so their legal status is still largely undefined. In order for digital signatures to carry the same authority as handwritten signatures, they must first be used to sign a legally binding contract, and then be challenged in court by one party. The court would then consider the security of the signature scheme, and issue a ruling. As this happened repeatedly over time, a body of precedent rulings would emerge, regarding what digital signature methods, and what key sizes, are required for a digital signature to be legally binding.

Until then, if two organizations wish to use digital signatures for contracts (or purchase requests, or work orders, among other applications), it is recommended that they first sign a paper contract, in which they agree in the future to be bound by any documents digitally signed by them, with a given signature scheme and a given key size.

Public-Key Cryptography

Public-key cryptography was invented by Whitfield Diffie, Martin Hellman, and Ralph Merkle in 1976. Unlike secret-key algorithms like DES and IDEA, public-key algorithms use one key for encryption, and a different key for decryption. Furthermore, it is compu-

tationally impossible to derive one key from the other. Each user has a pair of keys: one public, and one private. The public key is stored in some public database somewhere.

People wonder which is better, the public or the private. Real-world applications of cryptography use both of them together.

The problem with public-key algorithms is that they are slow—much slower than secret-key algorithms. The benefit of public-key algorithms is that they can enable things that secret-key algorithms cannot: digital signatures and secure key exchange. You should understand that they are different, and as such, do different jobs. The best policy with cryptography is to use both together.

Let's look at an example of how these methods work. If Alice wanted to send a message to Bob, she would look up Bob's public key in the database. Then she would encrypt the message, using that key, and send it to Bob. Bob, upon receiving the message, would decrypt it using his private key. Only Bob knows his private key, so only he could decrypt the message. Bob's public key is public, so anyone can encrypt a message and send it to him.

Flip that around, and you have a "digital signature." If Bob encrypts a message using his private key, anyone can decrypt the message using Bob's public key. But since only Bob could have encrypted it (only he knows his private key), the encrypted message serves as Bob's digital signature.

There is a problem with key exchange, however. For Alice and Bob to talk securely using DES, they have to agree on a key. They can't send the key over the communications channel; that would be insecure. Either they must have met previously to agree on a key, or they must send a trusted courier to exchange keys. If Alice and Bob don't share a common key, they cannot communicate securely.

This is why public and private keys work. With public-key cryptography, Alice and Bob don't need to agree on a common key. Alice takes her message and encrypts it, using a secret-key algorithm and a random secret key. Then she encrypts the secret key itself, using Bob's public key, and sends both the encrypted message and the encrypted key to Bob. Bob decrypts the secret key with his private key, and then decrypts the message with the secret key. An adversary sitting between Alice and Bob only has an encrypted message and an encrypted key, which are not a lot to work with.

There are many different public-key algorithms. The most well-known algorithm, RSA, can be used for both encryption and

digital signatures. DSS, the U.S. government's Digital Signature Standard, can only be used for digital signatures.

RSA

RSA, invented in 1978 by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT, is a public-key cryptography algorithm that can be used for both encryption and authentication.

RSA gets its security from the difficulty of factoring large numbers. The larger the key, the harder it is to break under RSA. It makes no sense to ask about the security of RSA without talking about the length of the key. RSA with a 10-bit key can be broken in seconds. RSA with a 667-bit key cannot be broken in any human length of time.

The RSA algorithm is patented in the U.S. RSA Data Security, of Redwood City, California, was formed to develop, license, and market the RSA algorithm. Commercial use of the algorithm is licensed, although a reference implementation is available free to anyone who asks. To use the algorithm in commercial products, contact the company's licensing department.

Outside the U.S., anyone can use RSA. The best implementation of the algorithm is in a free program called Pretty Good Privacy (PGP). PGP is for electronic mail security, although it can also be used to encrypt documents on your hard drive. The program, including source code, is available on many computer bulletin boards. RSA Data Security views distribution and use of the program in the United States as infringements of its patent. There is a Macintosh version of the program.

RC2 and RC4

RC2 and RC4 are secret-key encryption algorithms, designed by Ron Rivest of MIT, who also helped design RSA. These are proprietary algorithms, and their details have not been published. Don't think, for a minute, that this helps security. These algorithms have already appeared in commercial products; I am sure they have been disassembled by someone. As far as I know, the algorithms have not been patented.

RC2 is a variable-key-size cipher, designed to be a replacement for DES. According to RSA, software implementations of RC2 are three times faster than DES. RC4 is also a variable-key-size cipher

that is, according to the company, ten times faster than DES. Both algorithms are quite compact, and their speed is independent of the key's size.

RSA Data Security claims that their algorithms are as secure as DES (with the same size key), but their refusal to make the algorithms public casts doubt on their claim. They are willing to provide details of these algorithms to scientists wishing to cryptanalyze it, and will allow them to publish any negative results. I don't know of anyone who has taken them up on their offer, since it amounts to doing their analysis work for them.

Ron Rivest is a respected and competent cryptographer, and RSA has hired a number of other cryptographers to examine these algorithms. I put a fair degree of trust in the algorithm, even though I would very much like to see their analysis for myself.

Assuming the algorithm is secure, and that brute force is the most efficient way to recover the key, then the security of either algorithm depends on the length of the key used. If a key longer than 56 bits is used, the algorithm is more secure than DES; if a key is shorter than 56 is used, the algorithm is less secure than DES.

A recent agreement between the Software Publishers Association (SPA) and the U.S. government gives RC2 and RC4 special export status. Products that implement one of these two algorithms have a much simpler export approval process, provided that the keys are no more than 40 bits in length. The maximum length was supposed to be revised upwards, but that has never happened.

Is a 40-bit key enough? There are a total of 2^{40} (10^{12}) possible keys. Assuming that exhaustive search is the most efficient method of cryptanalysis (a big assumption, considering that the algorithm has never been published), and assuming that a cryptanalyst can test one million keys per second, it will take him 12.7 days to find the correct key. One hundred machines working in parallel can produce the key in three hours.

RSA maintains that while encryption and decryption are quick, exhaustive key search is not. A significant amount of time is spent setting up the algorithm for encryption. While this time is negligible when encrypting and decrypting messages, it is not when trying every possible key.

The more cynical among us believe that the U.S. government would never allow export of any algorithm it couldn't, at least in theory, break. Another possible way to break RC2 and RC4 would be to create a magnetic tape, or CD, of a plaintext block encrypted with every possible key. To break a given message, just run the

tape, and compare the ciphertext blocks in the message with the ciphertext blocks on the tape. If you find a match, try the candidate key and see if the message makes any sense. If you choose a common plaintext block (like all zeros, or all ASCII characters for a space), this method should work. The storage requirement for a 64-bit plaintext block encrypted with all 10^{12} possible keys is eight terabytes—certainly possible.

International Data Encryption Algorithm (IDEA)

IDEA is an alternative to DES that was invented in 1991 by Xuejia Lai and James Massey at ETH Zurich. It has a 128-bit key, over twice the key length of DES. Breaking IDEA with a brute-force attack would require all the world's computing power, working for a time longer than the age of the universe.

IDEA is still a new algorithm, and there may very well be easier ways to break it. It will be several years before enough people feel enough confidence in IDEA for it to appear in commercial products. IDEA encryption is available for the Macintosh, but only as part of the PGP security program.

Kerberos

Kerberos is a secure authentication protocol that was developed at the Massachusetts Institute of Technology (MIT), and is now in the public domain and can be used by anybody.

Kerberos enables network users to securely identify themselves to network resources, such as databases, modems, and printers. To do this, users initiate an exchange of messages designed to send the resource proof of the user's identity. This proof takes the form of a "ticket," which identifies the user, and an "authenticator," which validates the ticket. A ticket is only valid for a given time; after that, the user needs a new ticket.

Users get their tickets through a trusted computer known as a Key Distribution Center (KDC). This computer—locked up somewhere, where no malicious user can get to it—shares a DES key with each user on the network. If a user wants to use a network application, he requests a ticket from the KDC. The KDC confirms the user's identity, and grants the ticket. The user then makes an authenticator, and then presents both the ticket and the authen-

icator to the resource. Finally, the resource examines both things and, assuming nothing is amiss, grants the user access.

Kerberos Version 4, the first public version, is widely used. Version 5, released in 1992, incorporates many improvements and enhancements, designed to make it useful in more network situations. Kerberos source code is available from MIT. One company—CyberSAFE of Redmond, Washington—supports commercial applications of Kerberos, on a variety of platforms including the Macintosh.

What to Buy for Network Security

Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP), from ViaCrypt, is an e-mail encryption program, and versions are available for UNIX, MS-DOS, Amiga, and Macintosh. PGP is designed to encrypt messages to send to other people, although it can also be used to encrypt files on your hard drive, in a pinch.

PGP uses the RSA public-key algorithm—with either a 512-bit, 1024-bit, or 1280-bit key—for key management, and digital signatures and the IDEA secret-key algorithm for encryption.

PGP-encrypted messages have layered security. The only thing a cryptanalyst can learn about a PGP-encrypted message is who the recipient is—assuming he knows the recipient's key ID. Only after the recipient decrypts the message, does he learn who signed the message—if it is signed. After verifying the signature, he decrypts the message and learns what it says.

The most interesting aspect of PGP is its distributed approach to key management. There are no key certification authorities. Every user generates, and distributes, his own public key. Users can sign each other's public keys, adding extra confidence to the key's validity. Someone who signs another's public key becomes an introducer for that person. When a user receives a new public key, he examines the list of introducers that have signed the key. If one of the introducers is someone he trusts, he then has reason to accept the new key as valid. This is all automatic. Tell PGP whom you trust, and how much—set your own paranoia level—and you're ready.

PGP uses RSA without paying any royalties to RSA Data Security, so if you use it in the United States, you risk a lawsuit from

RSA Data Security. If you are outside the United States, there is no problem. A company called ViaCrypt sells commercial, and fully licensed, versions of PGP for Unix, PC, and Macintosh computers.

RSA Data Security hasn't arrested or prosecuted any individual users of PGP. Certainly, large companies won't risk using it, and many people are afraid to put the source code on their bulletin boards. Even so, the Macintosh version is widely available on machines outside the U.S. If you have access to the Internet, it should be easy to find.

This is an excellent program, and easily the best thing available for e-mail security. If you don't mind violating the RSA patent, use the free version. If you do mind, buy the commercial version of the program from ViaCrypt.

Nok Nok 1.04

Nok Nok, from Trik, is a utility that enhances file-sharing security under System 7. The program is a control-panel device that alerts users when others log on to their networked System 7 Mac. It then tries to figure out the name and zone of the user—even when they use a Guest account. The program also keeps a log of all accesses by other users; this log can be printed.

Users have the option to disallow any connection. users can also limit connections to a pre-defined number of minutes, and log people off after that time.

There are two versions of the program. Nok Nok works with basic System 7 file sharing, and Nok Nok A/S 1.0 works with AppleShare servers (versions 3.0 and higher). Both are easy to use, and very helpful. If you want to know who is logging on to your computer and accessing your files, you need this program.

SecurID Card

The SecurID Card, from Security Dynamics, is a credit-card-sized smart card (and companion software) that displays a randomly generated access code that automatically changes every sixty seconds. Each user who is authorized to dial into the system carries his own card. Each card is keyed to an individual person, and each displays a different number. Meanwhile, the accompanying software on your Apple Remote Access MultiPort Server and Client mimics the cards.

To gain access to the network, a user simply enters his or her personal identification number (PIN), and the current access code displayed on his SecurID. On the host side, the software checks both the PIN and the access code. If everything is correct, the user is allowed access.

This combination of both a password and a token—something the user knows and something the user has—increases security significantly, without adding much complexity. Also, the host software keeps an audit log of all successful and unsuccessful access attempts.

This system is new for the Macintosh, but has been around for years on UNIX and PC systems. It's a good security mechanism. It's probably defeatable by major governments, but it is more than secure against anyone else.

SofKeyPlus for Macintosh

SofKeyPlus for Macintosh, from MicroFrame, is a user-authentication software package that resides on your Mac. It enables a remote user to conveniently access a network that is protected by MicroFrame's Network Security Systems, and is using Apple Remote Access Multiport Server and Client Software. To enter the network, the user dials in as she normally would. The security barrier attached to the Apple Remote Access Multiport Server intercepts the call, and requests the user's ID. Based on a valid ID, the user is instructed to activate SofKeyPlus for Macintosh, and enter his or her personal identification number (PIN). The SofKeyPlus software then automatically interacts with the security barrier, in a challenge-response security handshake, and generates the correct one-time dynamic password for the session. This is all transparent to the user, and takes only a few seconds.

SofKeyPlus for Macintosh offers the enhanced security of a DES-based random password generator, with minimal user involvement, and without the need to carry an extra piece of hardware. The fact that this program is in software doesn't necessarily mean that it is less secure than a hardware solution, and it probably offers more than enough security for most users.

This program should be available as you read this. The information above is directly from the company, as I didn't receive the product in time to test it.

OCSG/Kerberos Authentication Software 5.2

Kerberos, from OCSG, performs trusted "third-party" authentication for users and services on distributed networks. The Server component supports Kerberos version 5 administration, management, authentication, and ticket-granting functions. The Client component supports Kerberos version 4 or version 5 utilities (for processing Kerberos tickets and authenticators, and administration of the Kerberos database), and Kerberized network applications (such as telnet, ftp, rlogin, rcp, and rsh). The Client Development Toolkit component, based on DEC's GSSAPI, provides application developers with the Kerberos and encryption functions necessary to secure their own client/server applications.

The method Kerberos uses to secure an ARA connection includes the following:

- No password, encrypted or otherwise, is sent over the connection. (Phone lines are not a secure medium, so eavesdropping is a definite attack method.)
- The session key is not sent unencrypted over the network.
- The client must be able to access any compatible ARA server on a given network. "Compatible" here means: "uses the same authentication scheme as the client."
- The client must authenticate itself to the server.
- The server authenticates itself to the client. While maintaining the security of the network is the primary concern, it is also of interest to protect the client from Trojan-horse servers.
- A client can get a ticket-granting ticket, and use it repeatedly until it expires. This allows the client to dial different servers, or to use the same server multiple times, giving a password only once.
- The client verifies that the Ticket Granting Service (TGS) is legitimate.

To effectively use Kerberos in an organization, it must be implemented on every client workstation and server on the network that requires authentication services. The ARA concept, with the Kerberos extension, allows an additional component (dial-in network access) to be securely added to the enterprise-wide network.

OCSG also integrates other security mechanisms and technologies into Kerberos, to provide a robust network security system. These include token security cards, public-key encryption, and GUI-based security administration.

Kerberos is primarily a Unix security program, and OCSG supports Kerberos on Sun, HP, IBM, Sequent, Pyramid, and NCR. OCSG supports Kerberos client software on Macintosh, as well as on MS-DOS and Windows. The Toolkit is supported on all of the above platforms.

Software maintenance and telephone support are available for 15 percent of the software purchase price per annum. Consulting services, training, and network security tutorials are available.

Lookout! 1.0

Lookout!, from Trik, is a control-panel device that gives network administrators an easy way to check the security status of their AppleShare servers. For example, under System 7, if a user turns on the File Sharing option, anyone on the network has complete access to her system.

Lookout! helps pinpoint users who open their systems to the network, by showing three basic pieces of information about every machine on the network: whether a file server is an AppleShare or System 7 Fileshare server, whether Guest access is enabled, and—if the remote machine is running Nok Nok—who is the owner of the remote server. This information is displayed on the Chooser itself, modifying the AppleShare server names to include the status of these servers.

Armed with this information, network administrators can direct users to turn off Guest access, or simply warn them that their system is accessible by everyone. Lookout! is a nice utility that makes it easy to check every Mac on the network for Guest access.

Security Force

Security Force, from Globus Systems, is a physical-security program that prevents someone from stealing your computers, but it only works on an AppleTalk network. Macs monitor each other on the network, and sound an alarm if one is disconnected.

To install the software, users enter their name, computer configuration, serial number, and a password of up to 35 characters. After the Mac is restarted, it searches the network for another Mac running Security Force. This other Mac becomes its buddy.

If left unattended for a preset amount of time, the Macintosh goes into protection mode. It starts sending messages back and forth with its buddy Mac. If a protected machine disappears from the network (implying that someone is walking off with it), an alarm sounds on the buddy, and a report is transmitted to the specified network manager. Hopefully, this Mac network manager is in a guard room somewhere, or has a guard there. The program can keep track of SCSI devices attached to the Mac, but will not warn when these devices are disconnected.

It's easy to add new machines to the Security Force network, and move them around. They automatically find a new buddy when they move to a new floor, a new building, or even a new city. As long as it's still on the same AppleTalk network, Security Force continues to work.

Security Force remains active at all times, even when a user turns off his machine. When he selects Shut Down from the Finder, the Mac goes into protected sleep mode instead of turning off.

Security Force also provides a complete description of the hardware configuration of the stolen machine, including its memory size, peripherals, and serial numbers. Security Force protects against theft, or illegal swapping, of internal Macintosh components, such as boards, memory chips, and power supplies.

This is an amazingly clever concept, and a great idea for AppleTalk networks. The only problem I can think of is the false alarms generated during a local power outage.

Chapter 10 Summary

- All pieces of a network require protection from security breaches.
- Countermeasures must be reasonable responses to possible threats.
- A written security policy that has been approved and implemented by senior management is the best—and most effective—security countermeasure. Such a policy defines possible threats, their solutions, and employees' responsibilities.
- Three simple, easy-to-implement security measures are: change passwords regularly, make regular back ups, and limit dial-in access.

- Restricting areas of an AppleTalk network is a simple and effective way to control user access. Routers connect zones that you establish on the network. Implementing security measures here lets you restrict a zone of users from the rest of the network, restrict packets passing across the router, or divide the AppleTalk network into several restricted areas.
- If you run System 7, beware of the File Sharing option, as this allows anyone on the network to access all of your system.
- AppleShare software allows users to assign folders different levels of access security. It also supports password use and Guest accounts.
- The quick way to protect a network from breaches through the phone lines is with password security. Better security comes from dial-back modems.
- The security features built into AppleTalk Remote Access 2.0 can lock out unauthorized callers, and can restrict access to the network. Other manufacturers are developing additional security features that work in conjunction with ARA 2.0.
- Apple's Open Collaboration Environment (AOCE) has many built-in security features, such as password authentication, encryption, and digital signatures. PowerTalk Key Chain allows users to log on to several network services with a single password.

Chapter 10 Sources

Pretty Good Privacy (PGP)

ViaCrypt
2104 West Peoria Ave
Phoenix, AZ 85029
(602) 944-0773
FAX: (602) 943-2601

Nok Nok 1.04, \$49.95**Nok Nok A/S 1.0, \$295**

Trik, Inc.
400 West Cummings Park, Suite 2350
Woburn, MA 01801
(617) 933-8810
(800) 466-8745
FAX: (617) 933-8648

SecurID Card, starts at \$40

Security Dynamics, Inc.
One Alewife Center
Cambridge, MA 02140
(617) 547-7820
FAX: (617) 354-8836

SofKeyPlus for Macintosh, from \$.50 to \$5 per user

MicroFrame, Inc.
21 Meridian Road
Edison, NY 08820
(908) 494-4440
FAX: (908) 494-4570

Kerberos 5.2, \$95 per client

CyberSAFE
24244351 152nd Ave NE
Redmond, WA 98052
(206) 883-8721
FAX: (206) 883-6951

LookOut 1.0, \$49.95

Trik, Inc.

400 West Cummings Park, Suite 2350

Woburn, MA 01801

(617) 933-8810

(800) 466-8745

FAX: (617) 933-8648

Security Force, \$1895 for a 50-user license

Globus Systems, Inc.

1447 McAllister St.

San Francisco, CA 94115

(415) 292-6744

FAX: (415) 292-6531



P A R T

VI

Additional Security Issues

Macintosh security covers a lot of topics, some of which are difficult to classify under software, hardware, networks, or insurance. This part serves to collect together some of those areas that do not really fit anywhere.

The topics in this chapter are not limited to Macintosh computers. Power problems can affect computers of any type, printers, fax machines, and any other piece of electronic equipment. Personnel and document security must be addressed even if the organization doesn't use a single computer. Software integrity is important regardless of computer type.

These topics are discussed extensively in a variety of information security books, and are only touched upon in this book. Those wanting more information on any of these topics should look to other resources.



Power Into and Out of Your Macintosh

Your Macintosh is a sensitive device. It's filled with sophisticated electronic components that are extremely susceptible to minute changes in electrical power. Pollutants in the power lines that wouldn't bother a toaster could cause you to lose data or, in some circumstances, could destroy your hardware.

Power pollutants are extremely egalitarian; they can strike anyone, at any time. Some areas of the country are more susceptible to these problems. It depends on how your power company generates your power, whether your cables are above ground or buried, and a host of other things you can't control.

Possible Effects of AC Power Pollutants

- Wholesale data losses. If the system crashes, everything not saved to disk is lost.
- Input and output logic errors. These can affect the accuracy of disk read and write operations.
- Altered CPU performance. This could cause all kinds of errors, some of which may result in the loss of data.
- Loss of everything in RAM. Sometimes a jolt of power can zap everything in memory.

- A short circuit of the Macintosh's internal electronics. This will result not only in the loss of data, but in the loss of hardware as well.
- Electrical fires in the Macintosh. It's not common, but it has happened.
- The complete destruction of the computer hardware in a matter of seconds. I don't know of this ever happening to a Macintosh, but it has happened to other types of computers.

Generally speaking, there are four different types of electrical power disturbances that you have to worry about with respect to your Mac:

Power Line Noise is the most deadly, and the most common, electrical problem. Electrical currents flow as sinusoidal waves; line noise is disturbance in those waves. The noise can be spikes—sharp peaks of high voltage that flow down the power line—or transients, noise that rides in tandem with the voltage current and consists of high-amplitude pulse waves. Electrical power lines can generate line noise all by themselves. Current can get trapped within a power line, and build to volatile peaks within nanoseconds. Lightning is a source of electromagnetic noise. It can strike your building directly, or it can induce a surge of voltage into electric and communication lines from up to a mile away. It can strike the ground and charge underground power lines with enormous transients.

Radio Frequency Interference (RFI), or ambient noise passes through the air from one piece of equipment to another. Computers placed near refrigerators or air conditioners can experience data loss from ambient noise; so can computers placed too near electric typewriters and photocopiers. Computers near x-ray machines can have their magnetic media and EPROMs erased. Industrial machinery, when first powered on, generates a surge of power known as an inrush current—and this can cause problems for your computer.

Voltage Fluctuations are changes to the usual, even flow of electrical current. They are normal, and happen all over the country. Unfortunately, they not only wear down the performance of your computer, but in extreme cases they can short out its internal circuitry.

Power Failures not only erase everything in RAM, but deny you the use of your Macintosh until the power company gets around to restoring your power. In some situations, this is unacceptable.

The moral here is that you should never take your power lines for granted. They are unpredictable, working fine one day and faltering the next. The expense of replacing your Macintosh and peripherals is enough of a justification to install some of the cheaper protection devices discussed here. If your application is critical enough, you may want to invest in some of the more expensive power-disturbance protectors.

Major Causes of Blackouts

- High demand for commercial power at certain times of the day.
- Damage to electrical equipment, short circuits, and such.
- Faulty wiring within your building.
- Overloaded circuits in older buildings.
- Storms and lightning.

In protecting your Mac's power, it is easy to overlook some things. Make a check list for yourself—you'll be glad when you can safely boot up even after a huge electrical storm damages your power lines. Overlooking just the smallest detail can mean trouble for your Mac, and oversights are easy to make because there is so much to look after.

The obvious thing to look out for is your Macintosh itself. Surge suppression, voltage regulators, and line conditioners protect your Macintosh from damage. An uninterruptible power supply (UPS) ensures data integrity and allows you to work through power problems. In addition, you should protect long serial-cable runs. RS-232 serial cabling has no inherent power protection. If long runs are necessary, break them up with short-haul modems.

For network managers, the obvious things to protect are the servers. Even if your individual Macs don't warrant a UPS, your server might. Because servers are constantly writing to disk, the chances of a complete disk crash in the event of a power outage are greater.

Additionally, for a LAN or WAN to operate properly, equipment such as repeaters, gateways, connectors, hubs, and bridges must run smoothly through any problem. This is especially important if only part of your network is affected by the power problem.

On to smaller items, you'll want to protect your peripherals. Disk drives, modems, and printers should, at a minimum, be protected by a surge protector. Putting a printer on a UPS is overkill; print jobs can easily be rescheduled after the power is restored. Telephone lines represent a quick and easy route for surges to damage your equipment. Many surge suppressors come with telephone-line protection.

Finally, the best power-protection equipment in the world can't protect against problems that are endemic to your site. Make sure that your outlets are wired properly, and that your site has a proper ground.

Surge Suppressors

Surge suppressors are the cheapest form of power protection, and also the weakest. They offer some protection against high-voltage spikes and transients—softening their blow, but not completely sheltering your computer from damage.

Surge suppressors plug into your wall outlet, and have a series of outlets into which you can plug your computer, monitor, and any peripherals. Between the wall outlet and the terminal outlet you plug into, surge suppressors introduce components that clamp transients, dissipate spikes, and generally shelter the computer from line noise.

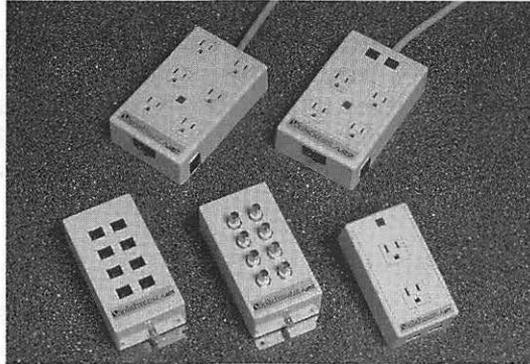
Technologies for surge suppressions vary, and different technologies offer different levels of effectiveness. Most surge suppressors are constructed of something called metal-oxide-varistors, or MOVs. They clamp larger transients and mid-range power glitches. A MOV-based surge protector offers some protection, but not much.

Better suppressors use silicon avalanche diodes (also called tranzorbs), in conjunction with MOVs. Tranzorbs are fast, and can recognize a high voltage spike within nanoseconds. Tranzorbs without MOVs are next to worthless, since tranzorbs only have a limited capacity to clamp or dissipate a spike.

The best suppressors use tranzorbs, MOVs, and a third technology called a spark gap, which is a gas discharge tube. Spark gaps shunt steep peaks of excess voltage to ground.

Figure 11.1

The best surge suppressors



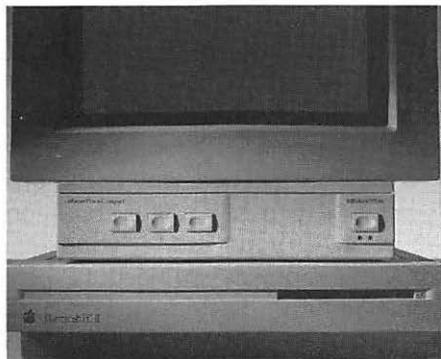
When buying a surge suppressor, you should look for several things to ensure that it is up to snuff for your computer. It should be U.L.-approved and carry a "U.L." seal, indicating that the device was tested by the Underwriter's Laboratory. It should have a clamping level between 50 to 100 joules. If it specifies a level below 50 joules, it will allow larger-voltage spikes through. You should see that it has a combination of MOVs, tranzorbs, and a gas discharge tube. Finally, it should have a label confirming that the product has met the IEEE 587 standard, which is the guide for "Surge Voltages in Low Voltage AC Power Circuits."

MasterPiece

The MasterPiece power control center, priced starting at \$99.95 from Kensington Microware, is a surge suppressor, an RFI/EMI (electromagnetic interference) noise filter, and an anti-static protector. It has a master switch, and individual switches for five separate outlets.

Figure 11.2

MasterPiece



The MasterPiece Plus includes all of the above, plus a modem/fax surge suppressor and a low-voltage indicator. The MasterPiece Plus Remote has all the functionality of the MasterPiece Plus, but in two pieces: a compact remote control unit that turns the computer on and off, and a floor outlet strip. The MasterPiece Compact includes all the features of the MasterPiece in a compact unit.

SurgeArrest

SurgeArrest is a family of high-quality surge suppressors from American Power Conversion. They have a multi-stage design—metal oxide varistors, capacitors, rod-core inductors, and a fast-acting fuse—to prevent power problems. The equipment is well-designed, well-made, and works. It even comes with an insurance policy against equipment damage due to electrical problems: from \$1,000 to \$25,000, depending on the surge suppressor.

One great feature is a wiring-fault indicator, which detects site wiring problems such as poor ground or reversed polarity. Another indicator warns you if SurgeArrest has sustained catastrophic surge damage. When such damage occurs, SurgeArrest disconnects itself, and your equipment, from the AC line.

There are five models, which differ in mounting style, protection rating, number of receptacles, and whether they include phone protection.

Voltage Regulators and Line Conditioners

A voltage regulator is a filter. It receives dirty current from the outlet, runs it through a multiple-stage filtration process, and finally sends it out to your computer as a clean and stable power wave. This filtration process eliminates ambient and power-line noise, detects and clips both spikes and transients, and regulates the output voltage.

Line conditioners are like voltage regulators, with one important extra feature. In addition to filtering transverse-mode noise, a line conditioner will deal with common-mode noise as well.

It is important to buy a line conditioner that can output the amount of power you need for your setup. Here's how to determine how much power you need: First, examine the back of your computer, monitor, disk drives, and other peripherals, and look for an amperage rating on the name plate—such as "3A." Add

all the amperages together, and multiply them by the voltage (120 volts in America, 220 in Europe) to get the number of volt-amperes required.

For example, if you only know the wattage of your equipment, you can convert from watts to volt-amperes by dividing by 0.7. So, a 200-watt CPU would rate about 285 volt-amperes.

Pad the result by at least 10%, and think about possible future expansion. Buy a line conditioner that is too powerful, rather than one that is too weak.

Figure 11.4

The best line conditioners



Line-R

Line-R, from American Power Conversion, is a microprocessor-controlled, tap-changing power conditioner. It automatically corrects brownouts by boosting low voltages, and corrects overvoltages by stepping down high voltages. It regulates power to levels that are safe for computer operation. This provides more protection than a surge suppressor.

There is a voltage meter on the front panel that displays relative input voltage level, and alerts you to high- or low-voltage conditions. It has an audible alarm for extreme conditions, and a surge-protection-integrity light to let you know the conditioner is working properly. The system also performs an automatic self-test each time you turn it on. A site wiring fault indicator spots poor ground connections and reversed polarity in the power line.

Line-R comes in two models: the 600 and the 1200. It also comes with a \$25,000 insurance policy against computer equipment damage when Line-R is installed.

Uninterruptible Power Supplies

An uninterruptible power supply (UPS) is the ultimate in power protection, performing the tasks of a surge suppressor, line conditioner, and backup battery in case of a power failure.

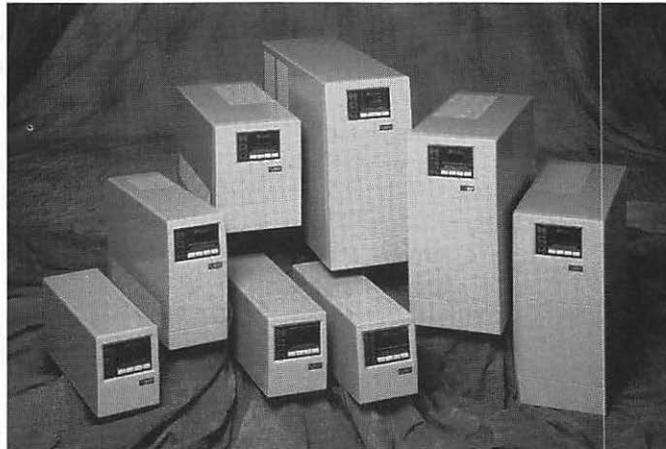
Uninterruptible power supplies come in three flavors: on-line, off-line (or standby), and line-interactive. Although vendors sometimes hype the relative merits of each, the differences are simple. They concern the speed with which a UPS switches to backup power, the "cleanness" of the power, and the way a UPS handles brownouts, or low-voltage situations.

A standby UPS passes commercial power to your computer while watching in the background, for power problems. Within milliseconds after detecting a power drop, it switches from external power to internal power. Then the battery supplies power until either it runs dry, or commercial power resumes. When power resumes, the UPS switches back to commercial power and recharges its batteries.

An on-line UPS is truly uninterruptible because it's always supplying power from its internal battery, which is continuously being recharged from the AC voltage. No switching is required, hence there is no switching time. Since the UPS always isolates the equipment from the power source, you get a smooth, clean, power wave.

Figure 11.5

ONEAC UPS



For Macintoshes, on-line UPS is overkill. Standby UPS switching times are short enough that you won't lose any data. Some mainframes might need an on-line UPS, but microcomputers don't.

A line-interactive UPS is a standby UPS, but with an output transformer that regulates the voltage level going out to your computer. This regulation is particularly useful in brownout situations, boosting power without tapping into the batteries. If you live in an area with frequent brownouts, then this is the best choice.

Larger-capacity UPS systems have larger batteries, and can power more equipment. To determine how much power you need, check the power requirements for all of your equipment (see the section on line conditioners). You also have to determine how long you want the batteries to last. Batteries that last for only a few minutes—enough for you to close all your files and save all your data—are cheaper than batteries that will allow you to run for hours without external power.

Power Backer Plus

Power Backer Plus UPS units, from Kensington Microware, are designed to provide standby power in the event of a power dip or complete power outage. When a power failure occurs, the Power Backer Plus starts supplying power to the system in less than one nanosecond. It also sounds an alarm to warn you of the failure, so you can save any work in progress, and safely shut down the system. In addition, Power Backer Plus clips surges and spikes at

Figure 11.6

Power Backer Plus



a safe level, and smoothes out line noise. Indicators on the front panel help you monitor the power flow to the computer and peripherals. There are different models available for different power ratings.

Power Security Tips

- Set up a dedicated power line for your computer.
- Put all of your computer components on this dedicated line.
- Ground your computer equipment.
- Keep other electrical equipment, like radios and air conditioners, away from your computer. Be sure to pay attention to equipment that might be near your computer, but separated by a wall. The wall offers minimal protection from RFI.
- Do not use your equipment in a lightning storm.
- Use shielded wires and cables, especially in a noisy environment such as a factory floor.
- Never turn your Macintosh off in the middle of a program; always use the Shut Down function from the Special Menu.

Chapter 11 Summary

- Minute changes in the power supply, or pollutants, can seriously damage your computer. There are four different types of power disturbances. Power line noise consists of spikes or transients in the power flow. Ambient noise, or RFI, comes through the air to your computer from other types of equipment. Voltage fluctuations are very common, and can wear down your computer's performance. Power failures erase everything in RAM, and shut your entire system down.
- Surge suppressors shelter your computer from spikes and transients. The best of these use metal-oxide-varistors to stop transients, silicon avalanche diodes (or tranzorbs) to level spikes, and spark gaps to ground excess voltage.
- Voltage regulators and line conditioners filter incoming power into a clean, reliable power wave. This process eliminates line noise, clips spikes and transients, and regulates output voltage. Consider your power needs when purchasing this type of equipment.
- There are three types of uninterruptible power supplies: standby, on-line, and line-interactive. The first type cuts in with battery-supplied power within milliseconds after a power loss. The second type also supplies battery power, but does so continuously. It recharges continuously from line power, and cuts in with no delay after loss of line power. The third type is a standby UPS that includes the ability to regulate outgoing voltage, and is most useful in areas with frequent brownouts.

Chapter 11 Sources

**MasterPiece, \$149.95; MasterPiece Plus, \$159.95;
MasterPiece Plus Remote, \$169.95; MasterPiece Com-
pact, \$99.95**

Kensington Microware Ltd.
2855 Campus Drive
San Mateo, CA 94403
(415) 572-2700
(800) 535-4242
FAX: (415) 572-9675

**SurgeArrest, \$29.95; SurgeArrest Plus, \$59.95;
SurgeArrest Plus (wallmount), \$39.95; SurgeArrest Plus
w/Tel, \$99.95; SurgeArrest Plus w/Tel (wallmount),
\$69.95**

**Line-R 600, \$179; Line-R 1200, \$269
Smart-UPS series, \$499 to \$1199; Back-UPS series, \$139
to \$799**

American Power Conversion
132 Fairgrounds Rd.
P.O. Box 278
West Kingston, RI 02892
(401) 789-5735
(800) 890-4APC
FAX: (401) 789-3180

PowerBacker Plus, \$349.95 to \$849.95
Kensington Microware Ltd.
2855 Campus Drive
San Mateo, CA 94403
(415) 572-2700
(800) 535-4242
FAX: (415) 572-9675



Document Security

If the data on your computer is valuable and worth securing, then so is the same data printed on paper. This book isn't about securing paper, but the topic should be mentioned in the context of computers.

Remember the different classifications of confidentiality we talked about in Chapter 1? They also hold true for documents. The U.S. military marks every page of every document with its classification. Not only does this alert everybody as to the proper procedures for handling the documents, but it puts the law on the military's side if someone deliberately circumvents security. Your employee has a plausible argument of ignorance if a document isn't clearly marked as confidential.

Potential Security Problems

Paper documents present a slightly different set of concerns with respect to their value, and to the ease with which someone can get to them.

Are documents worth much? Consider that documents are typically more valuable in the aggregate. One name from your company's client list isn't very valuable, but the entire client list is. That same client list, sorted in order of business volume, is even more

valuable. Keep in mind also that computer documents may need to be looked after more carefully than the apparent worth of their data may suggest.

Documents are also permanent. Unless you buy a shredder, throwing out your documents doesn't mean that no one will see them. Dumpster diving, the process of sifting through some-one's trash looking for interesting things, is not uncommon.

Finally, documents are easy to read. If an important document is lying on someone's desk, anyone walking by can read it. Maybe you're not worried about your co-workers, but clients and even competitors may be walking through your offices. Salespeople are often pros at reading documents upside down, and practice that skill whenever possible. Messy desks make for poor security practice.

Printers

Shared printers can be a security problem. The personnel manager could print a copy of everyone's salary at the shared printer down the hall, not knowing who may be standing nearby and be able to read the document.

There are two obvious solutions to this problem. One, buy multiple printers. Earmark one (or more than one) for sensitive documents, and don't put that printer out where anyone can pick up its printouts. On a Mac network, different zones can have different printers. One could be in the executive offices, and another for general use. The second solution, more suitable for smaller companies, is to do all sensitive printing when no one else is around.

Destruction of Computer Documents

- Documents should not be hoarded; they should be destroyed as soon as they are no longer needed.
- Valuable or sensitive outdated documents should be destroyed. Shredding and burning are the two most popular means of destruction.
- All waste should be considered as "classified" as the most valuable document within it. It is more economical to dispose of the whole pile securely, than to sift out the classified documents.

Chapter 12 Summary

- Information that is worth securing in its electronic form is equally worth securing on paper. Using military-type classifications on sensitive documents alerts employees to proper procedures for handling such documents.
- Printers are an obvious weak spot in document security. It may be appropriate to have several printers, and to segregate one for handling sensitive documents. It may be appropriate to print sensitive documents only when no one else is around.



Personnel Security

No security measure is worth anything if you can't trust the individuals involved. People can be careless and forgetful, they can ignore security because it is too much of a bother, or they can go out and sell your classified data to the competition.

Elements of Personnel Security

The big word for personnel security is screening. You have to determine whether you trust someone or not and to what degree. Agencies and corporations are implementing security clearances, a more stringent form of screening that goes beyond whether a manager trusts a prospective employee.

You need a system in order to screen, and you can start by identifying those jobs that require clearances. Not every job requires a clearance. Identifying those that do allows you to concentrate your resources on those jobs. Once this is done, then you can begin screening applicants for those jobs. It is best to do this before employment. The U.S. military does extensive background checks on some of its prospective employees. You may not get as detailed as the military, but you should check references and qualifications carefully.

Those people that pass screening should be awarded clearances. There may be different levels of clearances, or different clearances for different areas. So it's possible to award someone with a clearance that gives her access to some, but not all, of your company's operations.

With any clearance comes responsibilities, and the people should be made aware of those responsibilities, so you should plan a security training and awareness course. There should be an established computer-security training and awareness program to ensure that employees take their responsibilities seriously.

Not every system is perfect, however. You may grant clearance to someone who breaches security. In these instances, you should set up policies and procedures for terminating people in jobs that require clearances. Make sure the employee understands his responsibilities regarding sensitive information, which remains sensitive even after he's no longer on the payroll. After he leaves, you should make sure all passwords, keys, combinations, and such are changed.

Once Clearance Is Granted

Not everyone in an organization will have the same levels of security clearance. Even if someone is cleared to know something, it's generally a bad practice to tell him anything that doesn't directly affect his job. Thus, it is imperative that you classify information on a need-to-know basis. Information should be restricted to those people who need to know the information in order for them to do their job. A high position in the organizational chain doesn't imply a need to know. Sales people, no matter how senior, do not need access to research data. People who don't work with personnel data don't need access to personnel files. The more valuable the data, the more important this principle is.

However, it is not such a good idea to be so restrictive as to have only one person know certain information. Assign to more than one person responsibility for items that affect computer security. It is much harder for two people to make a joint mistake, or to both be bribed or coerced, than it is for one person.

Additionally, people in security-related positions, or people with responsibilities that present opportunities for dishonesty, should be rotated out of them occasionally. If there is a continuous problem, someone else might find it. U.S. banks require most employ-

ees to take their vacations in two-week chunks, so that any on-going embezzlement can be discovered.

Visitors

Keep a log of all visitors. This written record may be important to reconstruct events if a security breach is discovered. In larger organizations, visitor badges might be used, and employees might be required to escort visitors to certain locations. Remember, consultants and contractors are visitors, not employees of the company. Their loyalties often lie elsewhere.

Chapter 13 Summary

- The most carefully thought-out security plan is worthless if you can't trust the people involved.
- A written visitors' log can be important in reconstructing security breaches. Some companies also use badges and escorts to keep track of non-employees on their premises.



Software Integrity

If you are using software for a critical application, it may make sense to perform some kind of formal analysis of the software. Maybe an employee has planted rogue code in your personnel program, that will cause the program to crash if he is deleted from the payroll. Maybe there are serious errors that will cause the software to crash at the worst possible moment. Maybe one of the developers has planted a back door in your security program, which allows access only to him.

Integrity is really only relevant if you are doing custom software development for your organization. If you are using commercial software, you have to trust the software manufacturers. This is only some consolation; while it is very unlikely that there will be malicious code in an off-the-shelf application (at least I have never heard of any), it is probable that there will be some software bugs. And it is probable that, sooner or later, one of these bugs will cost you your data. Back up your data regularly to minimize this risk..

One way to minimize the risk of a single programmer writing potentially damaging code is to formalize the design and development process. Formal design documents, code walkthroughs (where at least two people examine every line of code), good source-code configuration-management software, and formal

testing plans and procedures, are all ways to ensure correct software. These methods are expensive and greatly increase the software-development cycle; but if you are worried about the threat, it is a small price to pay.

Documentation is critical to custom software development. It is often difficult and expensive to prepare adequate documentation, but in the long run, it will be more expensive to ignore documentation. The programmer or programmers you have writing your software will probably not want to take questions from users. Even if they do, they will not be around forever. Someone else might have to update the program, fix bugs, or train new users on the software. If you don't have good documentation, your investment in custom software will be wasted as soon as your programmers aren't around. The information has to be on paper, not only in their heads.

Programmers' Tricks

The dishonest programmer can deliberately place malicious code in programs he is writing. This is generally done as protection against dismissal or contractual problems. If the employer fires the programmer, the programmer is now in a position to blackmail the employer. Sometimes, the employer doesn't even know he is being blackmailed. Some of the surprises that could await an employer include:

A Logic Bomb. This is a piece of code designed to do damage, and is triggered by some event. For example, a programmer might put a piece of code in a program that will do serious damage if his name is ever deleted from the payroll.

A Back Door. This is a secret way to subvert security programs. For example, in an access-control program, a programmer could add code to allow a certain user ID and password the highest level of access. If the programmer ever loses his job, he could use this secret back door to gain access to the computer systems, and wreak whatever havoc he wishes.

A Delayed Bug. This bug is deliberately introduced into a program, and is designed to manifest itself a month or two after the program starts running. The scam here is that if problems appear in a program, the same programmer

hired to write the program will probably be hired to fix it. A dishonest programmer might be tempted to introduce time-delayed problems into his program as insurance for getting further work.

Remember, the vast majority of contract programmers are honest, and would never do such things. It's the few dishonest ones you have to worry about. Still, it is best to know the tricks before you are forced to deal with one of them.

Chapter 14 Summary

- Software used in any critical application is vulnerable to security breaches. Software developed by your company may require some kind of formal analysis to verify that no one has tried to exploit such vulnerabilities.
- One programmer might write damaging code. But formalizing the software design process, using two people to scrutinize the code, using good source code configuration management software, and employing formal testing are all good ways to keep it difficult for a programmer to write surprises into your programs.
- Carefully prepared documentation will allow other people than the programmer to understand how the program works. Those programmers will not be around forever, so get the information out of their heads and onto paper while you can.



TEMPEST

All electrical equipment, from toasters to computers, produces electromagnetic radiation. This radiation travels through the air as radio waves, or along wire and metal surfaces as electric currents. The laws of physics require this to happen; there is nothing you can do about it.

The problem arises when someone sets up a receiver to pick up this radiation. If the radiation is from a washing machine, this is no big deal. But if the radiation is from a video monitor connected to a computer, the receiver can pick up what is being displayed on the screen. Someone with the right equipment can “look over your shoulder” at your computer screen, through walls, at distances of up to 300 feet away.

The U.S. government code name for these kind of emanations is TEMPEST. It doesn’t stand for anything. This is serious spook stuff, and is something the government is very concerned about. There are massive government programs to make equipment TEMPEST-proof, so that the emanations out of the equipment are so faint as to be useless.

Should you care about TEMPEST? Unless you are working on classified military projects (in which case you already know the answer), the answer is probably no. It doesn’t take a lot of technical expertise to pick up and decipher TEMPEST emanations—someone could outfit a van to pick up the signals, and then park

the van outside your office. But it requires a lot of expense, in both equipment and personnel.

Still, this is not something to ignore. An adversary can collect your secret data without ever having to set foot onto your property. If you have information so valuable that it might be worth someone's time and effort to collect in this manner, consider protecting it.

Several companies make TEMPEST-proof Macintoshes. These are conventional Macintosh computers repackaged in special cases that reduce or eliminate emanations. They are very expensive, but if you are interested, check various government and military computer trade magazines.

Simple Precautions You Can Take Against TEMPEST Attacks

- Create a metal-free area around your computer and peripherals. Do not use metal desks, metal trash cans, or other metal objects. Locate computers away from heat pipes.
- Don't put telephones near your computer.
- Use power filters.
- Prevent unauthorized vehicles from parking near your building.
- Place computers near the center of your building, with as much concrete as possible between the computers and the outside.
- Use modern equipment; older computers tend to radiate more. Low-radiation video displays, which are marketed for health reasons, are also more secure.
- Swamp TEMPEST detectors with non-sensitive data. Locate computers processing non-sensitive data near windows, radiator pipes, and such. TEMPEST signals from sensitive computers will be swamped by signals from non-sensitive computers.

Chapter 15 Summary

TEMPEST is the U.S. government's code name for the electromagnetic radiation produced by all electrical equipment. Using specialized equipment, someone can read the data on your computer screen from 300 feet away—possibly further. However, unless your work produces extremely sensitive data, you probably need not worry about this security breach. Shielded Macs are available for those who need to worry about these emanations.



Disaster Recovery

Fire, floods, tornadoes, hurricanes, earthquakes—all of these can affect your computer and your data. The best way to protect your data is to back it up regularly, and to store a set of backups offsite. This way, whatever happens to your Macintosh, you can restore the data onto another Macintosh.

There is no such thing as total security. No matter how hard you try, or how much money you spend, there is a limit to how well you can defend your data. There is no risk that you can completely eliminate. This is where disaster recovery comes in.

To protect the hardware itself, look into insurance. It can be expensive, but a good insurance policy enables you to buy replacement computers immediately after a disaster, and to be up and running that much quicker.

Disaster recovery is about that period of time after the disaster, but before you buy all that replacement equipment. Disaster recovery is concerned with keeping the critical aspects of the business flowing in the event of a disaster. A complete disaster recovery plan addresses all aspects of a business, not just computers. This chapter, however, will just discuss computers.

Disaster Recovery Planning

Good planning is critical to your ability to recover from a disaster. The period after a fire has gutted your office building is no time to wonder where to get replacement computer equipment, or when was the last time the offsite backups were updated. Put your plan in place before disaster strikes.

Characteristics of a Successful Contingency Plan

Related to business requirements. Every disaster recovery plan is different. Make sure yours addresses your critical computing requirements. Remember that the purpose of a disaster recovery plan is to keep business operating as efficiently as possible in the event of a disaster.

Current and up-to-date. No organization is static. Any plan can quickly become out-of-date, so review and update the plan frequently.

Comprehensive and complete. A good plan must cover all aspects of disaster recovery. A poor plan can be worse than no plan at all, since it gives people a false sense of security.

Achievable, with existing resources, time, and people. It's easy to write a complicated and expensive plan. Unfortunately, the times a disaster recovery plan is needed are the times when simplicity and efficiency are required. If the plan is not workable, it is useless.

Adequately tested. The only way to prove whether the plan is achievable, comprehensive, and current, is to test it. Testing may be as simple as reviewing the plan's documentation, or as complex as simulating an actual disaster. Whatever the method, the plan must be regularly tested.

Fully documented. The plan must be formalized into a written document. Everything required to implement the plan must be spelled out. Do not assume that those who designed the plan will be around to implement it.

Explained to those who will participate in the plan's execution.

Developing a Disaster Recovery Plan

For small businesses, disaster recovery might not be much more than finding a company that can rent Macintoshes and peripherals on short notice.

Comprehensive disaster recovery plans will usually make use of stand-by computing facilities in the short run, pending replacement of original equipment. Many companies offer stand-by facilities. Some are complete facilities: portable computer rooms outfitted with hardware to carry on business. Others are fully equipped computer centers at distant sites, ready for occupancy if disaster strikes. Companies can also make arrangements with service bureaus to do their computing in the event of a disaster. Some companies might make private arrangements to help each other out in the event of a disaster.

Whether you rent, have a stand-by facility, or work without either of these situations, you do need to develop a recovery plan. The first step is to make a critical analysis of your organization's computing functions, and of the effects their loss would have on your overall business. There are different types of losses:

- Loss of sales
- Loss of revenue
- Reduced operating capacity
- Reduced decision-making and forecasting capability
- Legal implications
- Increased operating costs

Also, there are different time scales for these different losses—depending on the time required to recover to normal. For example:

Limited impact. Recovery within one working day. No significant damage incurred to the company's well-being.

Severe impact. Recovery within one week. Significant damage incurred.

Very severe impact. Recovery within one month, after the expenditure of considerable time, effort, and money. Major damage incurred.

Critical impact. Recovery unlikely. Fatal to the company.

After critical computing operations have been identified, start designing the recovery plan. The plan should focus on four stages of recovery:

Emergency response. This stage concerns itself with the protection of human life.

Immediate recovery. The purpose of this stage is to resume critical computing functions as soon as possible (within hours, minutes, or even seconds).

Longer-term recovery. Having survived the first few hours of a disaster, attention can be turned to those computing functions that are not as critical.

Replacement of computing facilities. As new computers and peripherals are bought and installed, procedures are required to return computing functions to normal. If this is not done smoothly, another disaster could occur.

Chapter 16 Summary

- The best way to protect your data is to make regular backups and store those backups offsite. With that precaution, and good insurance to replace hardware, you'll be back in business in no time after a major disaster .
- Disaster recovery is about keeping critical aspects of your business flowing after a disaster until a replacement system is up and running.
- A proper disaster recovery plan prepares for the problem before it happens—and, once disaster does strike, is ready to step into place. Know where that replacement computer equipment is coming from, before you need it. Know the backup schedule now.
- Equipment rental is probably all the disaster recovery a small business needs. Larger firms may require the use of portable or distant-site standby computer centers.

- To develop a disaster recovery plan, analyze your company's computer functions, consider how their loss might affect business, and look at how long it might take the company to recover from such loss. A disaster plan should have four stages: emergency response, immediate recovery, longer-term recovery, and replacement of computing facilities.



Computer Security Policy

If your organization is larger than a few people, you need a computer security policy. This policy needs to be formal, well-documented, and agreed-to by senior management, since no security solution will work without proper procedures. Management, supervision, and training are all critical to the success of any security countermeasure.

A Computer Security Policy

- It should be clear and concise. It should explain the aims of the policy and the means for accomplishing those aims. It should be well-documented, and issued by the highest levels of management.
- It should be written by those in charge of computer security. They have the most knowledge of the system, and they will eventually have to implement the policy.
- It should achieve a level of security at least equal to the security of similar information in non-computer form.
- It should be comprehensive, addressing all computer assets and operations.

- It should fit in with the organization's way of life. Otherwise, it will not be followed.
- It should be modifiable. No computer system is static; the document will have to change as new computers and peripherals are purchased, and as new uses are found for existing computers.
- It should be achievable. A policy filled with unachievable security objectives only makes itself useless. There should be financial means to achieve the security objectives.
- It should provide security training for everyone who is responsible for security.
- It should allow for worst-case scenarios where security fails, and contain contingency plans for dealing with those eventualities.

Any attempt to institute a computer security program—especially one that changes a longstanding organizational attitude—needs the involvement and cooperation of the highest level of management. If possible, seek out the approval and signature of the company president. Not only will this give the whole process an air of authority, but it also gives employees the feeling that everyone is going to comply with these procedures. If senior management does not believe in the rules, certainly no one else will.

How to Convince Senior Management

At some point, you are going to have to face senior management and present your security ideas to them. These are some of the key points to bear in mind when preparing and delivering your presentation:

- Explain why a formal security policy is required, as opposed to current measures like access-control or encryption software.
- Clearly explain the benefits of a new security policy.
- Show how low the costs are for implementation of such a policy, and how minimal its disruption will be to the organization.

- Explain that only essential measures will be taken.
- Show how senior managers will benefit.
- Back up the proposal with statistics. How frequent are virus attacks? How often do hard disks crash? How much time and money is lost dealing with these problems?
- Use true-life horror stories about companies that have suffered damages due to security-related problems. Show how your policy avoids those problems.
- Ensure that the presenters are technically qualified to answer questions.

Informing and Motivating Employees

Once you have the approval of senior management, make a formal announcement to all employees that security is going to become an important consideration, and that a security policy is being formulated. Invite people to air their feelings, and put your ideas and priorities on the table, where employees can add to them. The way to win people over is to tell them what is going on. Writing a security policy in secret, and then suddenly announcing it, only causes problems. Including people in the process makes them feel as though it is theirs, too.

Writing Your Company's Security Policy

This is where you take all the information about threats, vulnerabilities, and countermeasures, and decide how you are going to protect what. This is where you describe your risk analysis, and the security trade-offs you made. This is also where you document all security decisions.

The first step in writing a security policy is finding out what needs to be protected. What hardware and what software are you responsible for? Don't look only at your current setup: computer systems are always upgraded, and your policy needs to be flexible enough to cover future expansion as well. Then, look at what data needs to be protected. Determine its value to the company, and determine who is responsible for it.

If you are responsible for a network, make these same determinations. Map out the network, looking at which users need

access to what parts of it. This step involves interviewing people. Your security policy must ensure that these people still have access to the parts of the network they need to do their jobs. Again, letting people have some input to the policy makes them feel involved, not alienated.

After gathering all this preliminary information, start looking at different countermeasures.

What to Cover

There is no set format for a computer security policy; it will be unique and specific to your organization. This outline lists things that should be covered, in a general sense.

Part I: Overview

- Describe the computer system in detail: what it is, what its purpose is, why it is needed, and who uses it. For instance, discuss the physical location (or, more likely, locations) of the system, including peripherals and external network connections.
- Describe the different hardware and software vendors that are involved with the computer system. Describe any maintenance contracts, and any planned future enhancements.
- Specify the nature of the data that is stored and processed. Who has access to this data? What is its value?
- Identify who has responsibility for security. This could be a list of names or a list of job titles.
- Describe the administrative procedures for review and testing of the security policy, and the methods by which changes are made and approved. Someone should have responsibility for maintaining the security policy.

Part II: Risks

- Describe the results of a risk analysis: What risks to the computer system are important, and how important are

they? The dangers from various attacks should be explicitly defined. For deliberate attacks, describe the potential adversaries and their resources. Also detail accidental attacks, and outline contingency and disaster recovery strategies.

- Give a brief description of the strategy intended to protect against these risks. This is included so that the details of Part III can be read in the context of an overall plan.

Part III: Countermeasures

Physical Security. Give an overall description of the physical security of the system. Then discuss the following in detail:

The location of the computer equipment, and of the principal physical-security protections.

Arrangements for controlling entry into the building and specific rooms—including any plans for checking incoming and outgoing baggage.

Heating, air conditioning, and power protection.

Fire protection.

Document Security. Discuss any security measures surrounding computer documents. This may include handling, marking, accounting for, and destroying these documents.

Personnel Security. All aspects of personnel security relating to computer operations should be discussed—including the need-to-know principle, rotation of duties, sensitive duties and key posts, and procedures for terminating someone's employment.

Hardware Security. Discuss hardware security in detail, including maintenance procedures, fault tolerance, and any countermeasures to protect hardware from threats like tampering.

Software Security. Discuss the overall aims of software security, paying particular attention to such things as access control, data encryption, virus protection, backups, TEMPEST, and network security.

Disaster Recovery Plan. This plan should be a separate document, perhaps attached as an annex to the security plan.

Insurance. Discuss the general philosophy underlying decisions about which risks are being insured against, and which risks were deemed too insignificant to warrant insurance. Detail arrangements with insurance companies, and include copies of agreements and policies.

A Network Security Proposal Outline

The following is a written outline for a network security policy. Pick and choose pieces from the outline that match your company's unique security situation.

I. Introduction

- A. Mission Statement

II. Responsibilities

- A. Management
- B. Personnel
- C. Corporate Security
- D. Employee

III. Situational Analysis

- A. Network Description
 - 1. Hardware
 - 2. Software
 - 3. Expansion Plans
 - 4. External Connections
 - 5. Security Features
- B. Resource Analysis
 - 1. Value of Network Resources
 - 2. Ownership of Network Resources

3. User Requirements for Access to Resources

C. Security Plan

1. Physical Security
2. Hardware Security
3. Personnel Security
4. Information Security
5. Software Security
6. Dial-In Security
7. Disaster Recovery/Contingency Planning

In addition to a formal, written network security policy that outlines risks and security implementations, you'll also need these related documents: a network security administration manual, which explains the administration end of the policy (so that anyone serving as network administrator can understand the job); and a user's guide to network security, which lets the employees understand both the new system and their responsibilities under it.

Computer Security and the Law

You may want to include some of the following information in your presentation to management, in your discussions with employees, or in the security policy itself. In any event, this is a look at the legal position of computer security today.

The 1986 Computer Fraud and Abuse Act is a federal act that affects "federal-interest computers," or those computers used by the government or a regulated financial institution—including banks, savings institutions, and brokerage houses. According to the act, these activities are outlawed:

- Gaining unauthorized access, or exceeding authorized access, knowingly to obtain national-security information. This offense is illegal if the government has any reason to believe that information will be used to harm the United States, or to gain an advantage for a foreign nation.

- Intentionally gaining unauthorized access to, and obtaining, personal information contained in the records of a financial institution, credit card issuer, or consumer reporting agency.
- Intentionally gaining unauthorized access to a federally owned computer.
- Intentionally gaining unauthorized access to a federal-interest computer for fraudulent purposes. This section applies if the offender gains anything of value beyond use of the computer itself.
- Intentionally gaining access to a federal-interest computer and altering, destroying, or damaging information, when the act causes certain specified losses. Among these losses are the potential impairment of medical diagnosis or treatment.
- Knowingly, and with the intent to defraud, trafficking in any password used for computer access, where this act affects interstate commerce, and where the computer is issued by or for the federal government.

The act also specifies that the Secret Service has primary responsibility for enforcing this act.

Even with its broad definition of a federal computer, the 1986 act only applies to a very small percentage of the nation's computers. At least 45 states have passed their own laws on computer crime. Some states have passed variants of what is called the Computer Systems Protection Act; others have adapted their existing fraud and theft statutes to cover computer crime as well.

Computer Security and Liability

If an organization fails to institute appropriate computer security measures, it risks exposing not only the organization, but also its board of directors—individually and personally—to liability. The board of directors of a corporation has a responsibility to protect the corporation's assets. Failure to establish and maintain a reasonable security program is a breach of that responsibility. In the event of a data loss due to a security breach, the members of the board may be personally liable for the devaluation of the company's data assets. The corporation may also be liable to others, depending on the type of data that is disclosed or lost.

For example, if an organization maintains a database of information about individuals, and poor security procedures allow that database to be surreptitiously modified by intruders—and untrue information about an individual is subsequently released—then the organization could be held liable for having injured the individual.

The same thing could happen if an engineer relied on information in a database to build a critical aircraft part. If that information proved to be inaccurate, due to unauthorized modification of the data, the database company could be held liable for wrongful death if the plane crashed.

Organizations have been held liable for unauthorized copying of software, even if the copying was done by individuals acting on their own. The license agreement that comes with a piece of software is often between the organization and the software company.

Management is responsible for the security of data within its organization. If management does not act to establish and maintain adequate computer security procedures, then the organization could be liable for substantial damages.

Chapter 17 Summary

- Any security policy has a better chance of succeeding if the employees can see that senior management agrees with, and works within, that policy.
- Allowing employees to add their ideas to the new policy gives people a sense of ownership and contribution.
- A security policy measures threats, vulnerabilities and possible countermeasures against risk. A security policy documents all security decisions, based on those factors. Consider the hardware, software, and data you are responsible for now, and consider your company's likely expansion plans.
- A typical written policy might include an overview of the system, of the perceived risks to the system, and of the appropriate countermeasures to those risks.
- Network administrators also need to determine how the network is used, and by whom.

- A network security policy would also include details on the different people responsible for the network, as well as a network security administration manual, and a user's guide to network security.
- There are federal laws that cover illegal access to "federal-interest" computers. Such laws are enforced by the Secret Service. At least 45 states also have computer crime laws.
- If the security measures that are taken by a company fail, both the company and its board of directors can be held responsible for any loss of company assets.

The *Protect Your Macintosh Source Code* Disk Set

The *Protect Your Macintosh* source code two-disk set is loaded with scores of Macintosh security programs, including:

Auto Lock

Utility that terminates the Finder and locks a single application in the foreground.

Complete Delete

Secure erase program.

DES

DES encryption program

Elvis Decoder Ring

Simple encryption program.

Enigma

Partial DES encryption and secure file erasure.

FlameFile

Highly recommended file-erasure program that erases files, disks, or free space on drives in accordance with Department of Defense regulations.

Last Startup

Tells you the last time your computer was used.

Lee's Crypto

Encryption program using the Hill cipher.

Login

Multi-user password and log-keeping program.

MacEncrypt

A "drag and drop" encryption program that uses DES, has a nice interface, and is recommended.

Network Security Guard

AppleTalk utility that will scan multiple zones for servers, and report on the security of those servers.

Obliterate

File erasure program.

Password

Basic password protection program.

PowerLock

Password protection program with some nice features.

Privacy for Pals

Encryption program using unknown algorithm. Questionable security.

Rot13

Utility that converts the contents of the clipboard into its ROT-13 equivalent. Not useful for real security.

SecureInit

Comprehensive password protection utility.

Security

Encrypts using DES; makes files invisible on the desktop; and securely erases files.

SoftLock

Enables you to write-protect a disk using software alone.

StartupLog

Keeps a log of every time the Mac was started.

Stego

Utility that can hide a data file in the low-order bits of a PICT file. The PICT is not changed in appearance or size, so someone who doesn't know the data file is there, will not see it. Some-one with another copy of Stego can retrieve the data file.

Tonto

Utility that hides applications from the casual user.

And more!

The disk set also includes a file containing corrections for any mistakes found in the book, as well as updated information on topics covered in the text.

The disk set is available from the author, and will be continuously updated. The cost is \$35 for two high-density disks. Please send a check or money order to:

Bruce Schneier
Counterpane Systems
730 Fair Oaks Ave.
Oak Park, IL 60302

Please allow four weeks for delivery. Due to U.S. export restrictions on many of the encryption algorithms and techniques, it will only be mailed to addresses within the United States and Canada. My apologies to the readers of this book who reside in other countries.



Index

A

- Absolute Security,
 - defined, 233
- access control
 - audit logs, 33, 41, 43, 46, 48
 - data types, 22
 - device access, 233-234
 - dial-in access, 232
 - Finder Overlays, 30
 - key-chain, 238
 - limiting privileges, 31-32
 - methods of, 28-33
 - overview, 24-28
 - passwords, 25-28
 - protecting data
 - with, 21-62
 - remote, 236-237
 - screen locking, 29-30
 - security questionnaire, 14
 - software, 24-28, 34-57
 - zone access, 233-234
- accessibility, setting
 - security goals, 3
- Access Managed Environment (A.M.E.)
 - access-control software, 36-37
 - address, 58
 - SafeWord MultiSync
 - cards, 52-53
- accidental attacks
 - data dangers, 4
 - listed, 229
- accountability, security, 23
- active attacks, defined, 228
- adhesive plates, anti-theft locking devices, 187-188
- Adleman, Leonard, RSA public-key algorithm, 242
- AIDS virus, 122-123
- alarms
 - fiber-optic, 189, 198-199
 - infrared, 184
 - microwave, 184
 - motion-activated, 203
 - overview, 184-185
 - photoelectric, 184
 - setting, 189
 - ultrasonic, 184-185
- Aldus virus, 125-126
- algorithms
 - choosing encryption, 64-69
 - cryptographic attacks, 66
 - decryption, 64
 - encryption, 63
 - IDEA (International Data Encryption Algorithm), 244
 - LaserCrypt, 85
 - LUCIFER, 70
 - proprietary, 67, 242-244
 - publication of encryption, 67
 - public-key, 64, 240-242
 - RC4, 238, 242-244
 - secret-key, 64
 - Skipjack, 69, 78-79
- AlSoft
 - address, 61
 - Power Utilities access-control software, 52

A.M.E. (Access Managed Environment)
 access-control software, 36-37
 address, 58
 SafeWord MultiSync cards, 52-53

American Power Conversion
 address, 268
 Line-R power conditioners, 263-264
 SurgeArrest surge suppressors, 262

amperage, line conditioners, 262-263

ANDI-ANGE virus, 124-125

anti-static protectors,
 MasterPiece, 261-262

anti-theft considerations
See also security
 laptops, 193-194
 serial numbers, 192-193

Anti-Theft Kits
 address, 207-208
 PC Guardian, 189

anti-theft locking devices
 adhesive plates, 187-188
 overview, 185-193
 Qualtec Data Products, 201-202
 Secure-It, 196
 specifications, 186
 warranties, 186

anti-theft systems, Security Tracking of Office Property (STOP), 202-203

AntiToxin anti-virus software, 114

ANTI virus, 124-125

anti-virus software
 overview, 113-120
 preventative versus detective, 108-110

Apple Computer
 address, 58
 At Ease, 37-38

Apple Keyboard Security Loop
 KB-LOOP, 209

Apple Open Collaboration Environment (AOCE), 237-238

Apple Security System
 address, 205
 cable-locking systems, 194

AppleShare, network security, 234-236

AppleTalk
 remote access control, 236-237
 security practices, 225
 zone and device access, 233-234

application servers. *See* servers

ARA Multiport Server software,
 remote access control, 236-237

archival backups, Redux Deluxe, 168

archives
 backup considerations, 144
 self-decrypting, 80, 85

ASD Software
 address, 59
 DiskGuard, 40-41
 FileDuo backup software, 165-166
 FileGuard, 45-46
 MaccessCard Reader, 48-49
 TrashGuard, 96

Atari computers, Frankie virus, 129

At Ease
 access-control software, 37-38
 address, 58

attacks
 accidental, 229
 cryptographic, 66
 data dangers, 4
 passive and active, 228
 TEMPEST, 281-283

ATTO Technology
 address, 177
 ExpressMirror backup software, 164

auditability, security questionnaire, 15

audit logs
 access control, 33
 Access Managed Environment (A.M.E.), 36
 DiskLock, 41
 Empower I, 43
 FileGuard, 46
 ISAC 4200, 88
 Keylock Mac, 48
 network security, 226
 ultraSECURE, 54-55

Authentication Manager, Apple Open Collaboration Environment (AOCE), 237-238

authenticators, Kerberos authentication protocol, 244-245, 248

availability assessments, data, 9

Aztec Security Products
 address, 205
 hardware security, 194-195

B

back doors
 defined, 64
 malicious software, 278

backup programs
 choosing, 158-174
 countermeasures, 6
 data dangers, 4
 listed, 159-160

backups
 archival, 144, 168
 choosing mediums, 147-152
 data compression, 155-156, 157, 161
 data integrity, 155
 encrypting, 156, 161, 170-171
 encryption affects, 81
 full and incremental, 143-144
 maintenance, 156-158
 mirroring, 144
 network continuity, 225
 network countermeasures, 232
 overview, 143-178
 programs. *See* backup programs
 rules for performing, 145-146
 safety rules, 152
 scheduling, 154-155
 securing data, 155-156
 security vulnerability, 16
 strategies, 152-155
 twinning, 144-145
 virus protection, 109

BBSs, viruses, 110-111

beeping
 CDEF virus, 130
 MDEF virus, 129

BeHierarchic program, MBDF virus, 131

Bernoulli disks, 148

Biham, Eli, breaking of Fast Encryption ALgorithm (FEAL), 67

biological viruses, compared to computer viruses, 105

blackouts, causes of, 259

bombs, virus, 104

- bootup, floppy disk access
 danger, 4
 Brandow virus, 125-126
 bugs, delayed, 278-279
 Bullet Proof
 access-control software, 38
 address, 58
 Bureau of Export Administration,
 encryption export, 81
- C**
- cable-locking systems
 Apple Security System, 194
 Kensington Microware, 188
 MicroSaver Security System,
 197
 overview, 186-189
 PowerBook Handle Security
 Kit, 200
 Cable Trap
 address, 209
 Qualtec Data Products, 202
 Camouflage
 address, 91
 encryption features, 80
 encryption software, 84-85
 card readers
 FileGuard, 45
 MaccessCard Reader, 48-49
 cartridges
 See also tapes
 Bernoulli and SyQuest, 148
 magneto-optical, 148-149
 maintenance of, 157
 Casa Blanca Works
 address, 59
 Drive 7 access-control
 software, 42
 Casady & Greene
 address, 58
 A.M.E. (Access Managed
 Environment), 36-37
 Cavalier locking systems, 195,
 205
 CD drives, recordable, 151
 CDEF virus, 130
 centralized backup strategies,
 152-153
 Central Point Anti-Virus
 address, 120
 anti-virus software, 114-115
 Central Point Backup program,
 160-161
 chameleons, virus, 104
 Chassis Cover Lock MICRO-LOK,
 address, 209
- checksums
 network security, 226
 virus detection, 107, 108
 chosen-plaintext attacks, 66
 Cipher Block Chaining
 Citadel, 83
 MacSafe II, 88
 ciphertext, defined, 63
 ciphertext-only attacks, 66
 Citadel
 access-control software, 38-39
 address, 58
 Cipher Block Chaining
 Mode, 83
 Citadel with Shredder
 address, 99
 file erasure software, 95
 clean-up procedures, last-ditch
 virus, 112-113
 clearances, personnel security,
 273-275
 Clipper chip
 encryption, 69
 hardware DES encryption, 78-
 79
 CMG Computer Products, 206
 CODE 1 virus, 136
 CODE 252 virus, 132-133
 code disk, Protect Your
 Macintosh, 301
 communications
 See also modems
 encryption, 87
 security dangers, 5
 vulnerabilities, 228-229
 components, security
 considerations, 191-193
 comprehensive backup strategies,
 advantages of, 154
 compression, backup data, 155-
 156, 157, 161
 Computer Fraud and Abuse Act,
 297-298
 computer insurance, 211-219
 ComputerInsurance Plus
 address, 219
 computer insurance, 216
 Computer Owner Protection
 (COP)
 address, 206
 identification codes, 195-196
 Computerowners Policy
 address, 219
 computer insurance, 215
 Computer Professionals for
 Social Responsibility,
 Clipper chip, 79
- computer security. *See* security
 Computer Security Products,
 address, 208
 confidential data, defined, 8
 confidentiality
 assessments, 8-9
 network, 224-225
 security goals, 2-3
 Connectix
 address, 58
 CPU, 39
 containment mechanisms,
 network security, 226
 contingency plans
 disaster recovery, 286-288
 security questionnaire, 14-15
 continuity, network, 225-226
 control panels, Lookout!, 249
 COP (Computer Owner
 Protection)
 address, 206
 identification codes, 195-196
 copy protection
 access control, 32
 FileGuard, 46
 ISAC 4200, 87
 cost
 decryption, 64
 risk analysis, 11
 countermeasures
 evaluating, 7-8
 goals of, 6
 network security, 230-231
 security criteria, 23
 security policies, 295-296
 types of, 6
 CPU
 access-control software, 39
 address, 58
 CPU Locks, address, 207-208
 cryptoanalysis, defined, 64
 cryptographic attacks,
 types of, 66
 cryptography
 See also decryption;
 encryption
 defined, 64
 as munitions, 81
 principles of, 67-68
 public-key, 240-242
 public-key versus secret-key,
 241
 cryptology, defined, 64
 Cryptomactic
 address, 91
 encryption features, 80

cypherPAD
 access-control software, 39-40
 address, 59
 floppy drive disablement, 32

D

dangers to data, 4-5
 Dantz Development
 address, 177
 DiskFit Direct backup
 software, 161-162
 DiskFit Pro backup software,
 162-163
 Retrospect backup software,
 169-170
 Retrospect Remote backup
 software, 170-171

data

access controls, security
 questionnaire, 14
 assessing value and security
 risks, 8-10
 availability assessments, 9
 backing up. *See* backup
 programs; backups
 backup compression, 155-
 156, 157, 161
 combating dangers, 5-8
 confidentiality assessments, 8-
 9
 dangers to, 4-5
 encryption. *See* encryption
 filtering, 233-234
 integrity. *See* data integrity
 loss prevention, 6
 physical protection, 33
 port locks, 192
 protecting with access
 control, 21-62
 security overview, 1-18, 22-24

Data Encryption Standard. *See*
 DES (Data Encryption
 Standard)

data integrity
 assessments, 9
 backups, 155
 security questionnaire,
 13-14
 setting security goals, 3

DATA Security Insurance
 address, 219
 computer insurance,
 216-217

Datwatch
 address, 58, 99
 Citadel access-control
 software, 38-39

Citadel with Shredder, 95
 Virex anti-virus software, 117-
 118

DAT drives, 149-151
 DAT tapes, maintaining, 158
 Dayna Communications
 address, 178
 SafeDeposit backup software,
 171
 SafeDeposit Server backup
 software, 171-172

DC6000 mechanisms, backup
 tape, 151

DDS (Digital Data Storage)
 standard, discussed, 150

decryption
See also cryptology;
 encryption; self-decrypting
 archives
 algorithms, 64
 hardware, 86-88
 public-key cryptography,
 240-242

delay, network threats, 229
 delayed bugs, malicious software,
 278-279

deletion
 file erasure, 93-98
 network threats, 229

DES (Data Encryption Standard)
 Citadel access-control
 software, 39
 compared to RC2 & RC4,
 242-243
 described, 68
 development of, 69-70
 DiskLock access-control
 software, 41
 hardware, 78-79
 security of, 71-73
 triple-DES, 69, 72, 86

desirable availability,
 defined, 9
 destroying documents, 270
 detecting viruses, 106-110
 detection mechanisms, network
 security, 226
 dial-back modems, remote access
 control, 236
 dial-in access, limiting, 232

Diffie, Whitfield, public-key
 cryptography, 240-242

Digital Data Storage (DDS)
 standard, 150

digital signatures,
 network, 239-240
 digital tape, 149-151

Direct Software
 address, 62
 SecureInit access-control
 software, 53
 disaster recovery, overview, 285-
 289

Disinfectant
 address, 120
 anti-virus software, 115-116
 T4 virus, 134

Disk Drive Lock DLK-260,
 address, 206

DiskFit Direct
 address, 177
 backup software, 161-162

DiskFit Pro
 address, 177
 backup software, 162-163

DiskGuard
 access-control software, 40-41
 address, 59

DiskLock
 access-control software, 41
 address, 59

DiskLock PB
 access-control software, 42
 address, 59

DiskMaker, access-control
 software, 42

disk partitioners
 Power Utilities, 52
 Silverlining, 53

disks. *See* Bernoulli disks; floppy
 disks; hard drives; SyQuest
 disks

DiskTwin
 address, 177
 backup software, 163

distributed backup strategies,
 152-153

DLM Software
 address, 99
 Shredder, 95-96

documentation
 security, 24, 269-271
 security vulnerability, 17
 software integrity, 278

documents, destroying, 270

doors, locking, 184-185

Drew virus, 125-126

Drive 7
 access-control software, 42
 address, 59

Drive Lock DLK-260,
 address, 206

- drives
See also floppy drives;
 hard drives
 Bernoulli and SyQuest, 148
 floppy disablement, 32
 magneto-optical, 149
 protecting multiple, 52
 recordable CD, 151
 Dukakis virus, 135
- E**
 eavesdropping, network threats,
 228
 ego, as enemy of security, 2
 electrical storms, data dangers, 4
 electromagnetic surveillance,
 TEMPEST, 281-283
 Electronic Frontier Foundation,
 Clipper chip, 79
 electronic information. *See*
 information
 Electronic Learning Systems
 address, 61
 Menu Master Mac, 49-50
 electron-tunneling microscopes,
 file erasure, 93
 e-mail, PGP encryption,
 245-246
 emanation, security
 dangers, 5
 embezzlement, as enemy
 of security, 2
 employees
 data dangers, 4
 security policies, 293
 security precautions, 7
 Empower I
 access-control software, 42-43
 address, 60
 Empower II
 access-control software, 43-44
 address, 60
 Empower Remote
 access-control software, 44-45
 address, 60
 encrypted viruses, 137-138
 encryption
See also cryptography;
 decryption
 algorithms. *See* algorithms
 backups, 156, 161
 choosing what to secure, 82-
 83
 Citadel, 39
 Clipper chip, 69
 communications, 87
 DES. *See* DES (Data Encryption
 Standard)
 DiskLock, 41
 e-mail, 245-246
 Empower I, 43
 FastBack Plus backup software,
 165
 file recovery, 81-82
 hardware, 86-88
 keys, 73-76
 as munitions, 81
 overview, 63-92
 program features, 79-81
 public-key versus secret-key,
 241
 Retrospect Remote backup
 software, 170-171
 safeguarding keys, 76-77
 software, 83-88
 speed considerations,
 77-78
 terminology, 63-64
 time required to break, 68
 triple-DES, 69, 72, 86
 ultraSECURE, 53-55
 viruses, 137-138
 Enigma Logic
 address, 62
 SafeWord MultiSync cards, 52-
 53
 Enigma machine, known-
 plaintext attack, 66
 entrapments, security,
 190-191
 environmental protection,
 security questionnaire, 13
 erasure, file, 93-98
 Eric virus, 121-122
 error correction, backup safety
 rules, 152
 errors
 compared to premeditated
 foul play, 1-2
 as enemy of security, 2
 espionage, as enemy of security,
 2
 essential availability, defined, 9
 Evergreen Software
 address, 61
 MacPassword, 49
 Exabyte tape, backup medium,
 151
 exports, encryption, 81
 ExpressMirror
 address, 177
 backup software, 164
 extortion, as enemy of security, 2
- F**
 f*** virus, 122-123
 fake messages, network threats,
 229
 FastBack Plus
 address, 177
 backup encryption, 156
 backup software, 164-165
 Fast Encryption Algorithm (FEAL),
 breaking of, 67
 federal law, Computer Fraud and
 Abuse Act, 297-298
 fiber-optic alarms
 Phazer/Net, 198-199
 setting, 189
 field guide to malicious software,
 104
 file classification, security
 vulnerability, 16
 FileDuo
 address, 178
 backup software, 165-166
 file erasure
 importance of, 93-94
 software, 94-97
 FileGuard
 access-control software, 45-46
 address, 60
 file recovery, encryption
 and, 81-82
 files
 locking, 41, 49
 self-decrypting, 85
 sharing via AppleShare, 234-
 236
 file servers. *See* servers
 file transfers, encrypting, 87
 filtering data, zone access, 233-
 234
 filters, voltage regulators and line
 conditioners, 262-266
 Finder Overlays
 access control, 30
 At Ease access control,
 37-38
 MacSecure, 49
 Menu Master Mac, 49-50
 fires, data dangers, 4
 firewalling, containment
 mechanisms, 226
 Floppy Disk Drive Lock FILE-LOK
 II, address, 209
 floppy disks
 as backup medium,
 147-148
 backup safety rules, 152

floppy drive locks
 PC Guardian, 192, 198, 207-208
 Qualtec Data Products, 202
 Sentinel, 203
 floppy drives, disabling,
 32, 43
 FMJ Security Systems, address,
 206
 FolderBolt
 access-control software, 46-47
 address, 60
 Folder Locker
 access-control software, 47
 address, 60
 folder locking
 access control, 30-31
 DiskLock, 41
 FolderBolt, 46-47
 MacPassword, 49
 FontFinder Trojan horse, 136
 Frankie virus, 129
 FSV Prefs file, INIT-M virus, 135
 Ft. Knox
 address, 91
 encryption software, 86
 file erasure software, 97
 full backups, 143
 FWB, Inc.
 address, 60
 Hard Disk ToolKit access-
 control software, 47

G

Garfield virus, 128-129
 GateKeeper
 anti-virus software, 116
 source location, 120
 T4 virus, 134
 GetZoneList filtering,
 zone and device access, 233-
 234
 Globus Systems
 address, 253
 Security Force network
 security, 249-250
 Golden Triangle Computers
 address, 177
 DiskMaker access-control
 software, 42
 DiskTwin backup
 software, 163
 SnapBack backup
 software, 172
 TwinIt backup software, 174
 GoMoku game, T4 virus,
 133-134

guessing programs, key,
 75-76
 guest log-ons, access
 control, 32

H

Hard Disk ToolKit
 access-control software, 47
 address, 60
 hard drives
 access control, 24-25,
 28-29
 encrypting data, 77
 MacPassword, 49
 partitioning, 29, 52, 53
 PassProof, 51-52
 passwords, 28, 29
 hardware
See also physical data
 protection
 backup safety rules, 152
 DES encryption, 78-79
 floppy disk access
 danger, 4
 ISAC 4200 encryption,
 86-88
 Keylock Mac, 48
 PassProof, 51-52
 physical security, 181-204
 security products, 194-210
 Heavy-Duty Anti-Theft products
 address, 209
 Qualtec Data Products, 201-
 202

heavy security, defined, 233
 Hellman, Martin, public-key
 cryptography, 240-242
 hierarchical access-control
 software, ultraSECURE,
 53-55
 high integrity assessment,
 defined, 9
 Hpat virus, 122-123
 HyperCard stacks
 Dukakis virus, 135
 MacMag virus, 125-126

I

IBM, LUCIFER algorithm and DES
 development, 70
 IDEA (International Data
 Encryption Algorithm), 244
 identification
See also passwords
 access control, 31
 plates, 202

Security Tracking of Office
 Property (STOP),
 202-203
 identification codes, COP
 (Computer Owner
 Protection), 195-196
 IDX Technologies,
 address, 206
 incremental backups, 143
 indelible ink, security measure,
 192, 193
 infections
 recovering from, 111
 symptoms of virus,
 106-107
 virus, 105-106
 virus listing, 121-140
 information
 assessing value and security
 risks, 8-10
 availability assessments, 9
 combating dangers, 5-8
 confidentiality
 assessments, 8-9
 data dangers, 4-5
 encryption. *See* encryption
 filtering, 233-234
 integrity assessments, 9
 nature of, 3
 protecting with access
 control, 21-62
 security overview, 1-18, 22-24
 infrared alarms, passive, 184
 inherited privileges, AppleShare,
 235
 INIT 17 virus, 134
 INIT 29 virus, 123-124
 INIT 1984 virus, 131-132
 INIT 9403 virus, 137
 INIT-M virus, 135
 INITs
 anti-virus, 109, 110, 115
 SecureInit, 53
 Inline Software
 address, 178
 Redux Deluxe backup
 software, 167-169
 insurance
 computer, 211-219
 ComputerInsurance
 Plus, 216
 Computerowners
 Policy, 215
 coverage considerations,
 212-213
 DATA Security Insurance,
 216-217
 disaster recovery, 285

- Powell-Walton-Milward Insurance, 217
Safeware, 215
- integrity
assessments, 9
backup data, 155
data, 3
network, 225
security questionnaire, 13-14
software, 277-279
- International Data Encryption Algorithm (IDEA), 244
- ISAC 4200
address, 91
encryption software, 86-88
- Isolation Systems
address, 91
ISAC 4200 encryption software, 86-88
- J**
- jamming, network threats, 229
- Johnson, Chris, GateKeeper anti-virus software, 116
- Jude virus, 122-123
- K**
- KDC (Key Distribution Center), Kerberos authentication protocol, 244-245
- Kensington Microware
address, 61
cable-locking systems, 188
MasterPiece surge suppressors, 261-262
MicroSaver Security System, 197
PassProof access-control software, 51-52
Power Backer Plus UPS unit, 265-266
- Kent-Marsh
address, 60
CryptMactic encryption software, 85-86
FolderBolt access-control software, 46-47
MacSafe II encryption software, 88
NightWatch II access-control software, 50
QuickLock access-control software, 52
- Kerberos Authentication Software
address, 252
network security, 248-249
secure authentication protocol, 244-245
- Keyboard and Chassis Lock, PC Guardian, 191
- keyboard locking, DiskGuard, 41
- Keyboard Lock KB-LOK, 206, 209
- Keyboard Locks
address, 207-208
PC Guardian, 198
- key chain access, PowerTalk Key Chain, 238
- Key Distribution Center (KDC), Kerberos authentication protocol, 244-245
- Keylock Mac
access-control software, 48
address, 60
- key management, PGP (Pretty Good Privacy), 245
- keys
choosing, 73-76
compared to passwords, 65
defined, 64
guessing programs, 75-76
management, 245
passwords and, 73
safeguarding, 76-77
secrecy of, 67
- known-plaintext attacks, 66
- L**
- labeling, backup safety rules, 152
- La Cie
address, 62
Silverlining access-control software, 53
- Lai, Xuejia, IDEA (International Data Encryption Algorithm), 244
- laptops, anti-theft considerations, 193-194
- LaserCrypt algorithm, Camouflage, 85
- LaserJet Font Cartridge Lock, address, 209
- LaserSafe, printer security, 202
- LaserSafe LASER-LOK, address, 209
- LaserWriter Security System
address, 205
printer security, 194
- last-ditch clean-up procedures, viruses, 112-113
- Lastrofka, Jeff, MacShackle, 197, 207
- law, security, 297-298
- liability, security and, 298-299
- light security, defined, 233
- limiting privileges, access control, 31-32
- line conditioners, overview, 262-266
- line-interactive UPS, 265
- line noise, computer problems, 258
- Line-R
address, 268
power conditioners, 263-264
- lock-and-cable systems. *See* cable-locking systems
- locking
doors, 184-185
files, 41, 49
folders. *See* folder locking
keyboards, 41, 87
screens. *See* screen locking
- locking devices
anti-theft, 185-193
Secure-It, 196
- Locking Pad CAV-21, address, 206
- LockingStation
address, 206
PowerBook, 196
- locks
overview, 181-204
port, 192
- logic bombs
malicious software, 278
viruses, 104
- logs, audit. *See* audit logs
- Lookout!
address, 253
network security, 249
- low integrity assessment, defined, 9
- LUCIFER algorithm, DES development, 70

M

MaccessCard Reader
 access-control software, 48-49
 address, 61
 FileGuard, 45

Macintosh Security Kits
 address, 209
 Qualtec Data Products, 201-202

MacKablIt security kits
 address, 206
 Secure-It, 196

Mac Kits, Aztec Security Products,
 205

MacMag virus, 125-126

MacPassword
 access-control software, 49
 address, 61

MacSafe II
 address, 91
 encryption software, 88

MacSecure, Finder Overlay, 49

MacShackle
 address, 207
 PowerBook cable and padlock, 197

MacTools
 address, 120
 Central Point Anti-Virus, 114-115

Magna
 address, 60
 Empower I access-control software, 42-43
 Empower II access-control software, 43-44
 Empower Remote, 44-45

magnetic card readers
 FileGuard, 45
 MaccessCard Reader, 48-49

magneto-optical cartridges, 148-149

mainframe perspective, Macintosh security from, 16-17

maintenance, backup, 156-158

malicious software
See also viruses
 field guide, 104
 INIT 1984 virus, 131-132
 INIT 9403 virus, 137
 INIT-M virus, 135
 Mosaic Trojan horse, 136
 software integrity, 277-279

management
 network security, 231-232
 security policies, 292-293

man-in-the-middle, network threats, 229

masquerades, network threats, 229

Massey, James, IDEA (International Data Encryption Algorithm), 244

MasterPiece
 address, 268
 surge suppressor, 261-262

MBDF virus, 131

MDEF virus, 128-129

media
 backup, 147-152
 integrity assessment, 9
 security dangers, 5

medium security, defined, 233

memory, virtual, 93-94

Menu Master Mac
 address, 61
 Finder Overlay, 49-50

Merkle, Ralph, public-key cryptography, 240-242

messages, network threats, 229

Metal-Oxide-Varistors (MOVs), surge suppressors, 260-261

MEV# virus, 122-123

MicroFrame
 address, 252
 SofKeyPlus network security, 247

MicroSaver Security System
 address, 207
 cable-and-lock devices, 197

microscopes, electron-tunneling, 93

microwave alarms, 184

mirroring
 backup considerations, 144
 DiskTwin, 163
 ExpressMirror, 164
 TwinIt backup software, 174

modems
See also communications
 dial-back, 236
 security dangers, 5

modifications, active attack network threats, 228

Modm virus, 122-123

Mosaic Trojan horse, 136

motion-activated alarms, SonicPRO Model AP128, 203

MOVs (Metal-Oxide-Varistors), surge suppressors, 260-261

multiple drives, protecting, 52

MultiSync cards, access control, 52-53

munitions, cryptography as, 81

Mykotronx, Inc., Clipper chip, 79

N

NASA virus, 121-122

National Institute of Standards and Technology, DES development, 69-70

NBP LkUp-Relay filtering, zone and device access, 233-234

nCAM virus, 122-123

networks
See also servers
 AppleShare, 234-236
 backup strategies, 152-155
 confidentiality, 224-225
 containment mechanisms, 226
 continuity, 225-226
 detection mechanisms, 226
 digital signatures, 239-240
 digital tape backup, 149-151
 DiskGuard access-control software, 40-41
 integrity, 225
 Phazer Area Controller, 199
 prevention mechanisms, 226
 Retrospect Remote backup software, 170-171
 SafeDeposit Server backup software, 171-172
 security, 221-253
 security countermeasures, 230-231
 security products, 245-253
 security proposal outline, 296-297
 security questionnaire, 15
 SnapBack backup software, 172
 viruses, 110-111
 vulnerabilities, 228-230

Network Security Administration Manual, security policies, 232

nFLU virus, 122-123

NightWatch II
 access-control software, 50
 address, 61
 QuickLock, 52

- noise
 - filters, 261-262
 - power line, 258
 - Nok Nok
 - address, 252
 - network security, 246
 - Norstad, John
 - address, 120
 - Disinfectant anti-virus software, 115-116
 - Norton Backup, backup software, 166-167
 - Norton Encrypt
 - address, 92
 - encryption software, 88
 - Norton Partition, access-control software, 50
 - Norton Wipe Info
 - address, 99
 - file erasure software, 97
 - NovaMac
 - address, 178
 - backup software, 167
 - Novastor
 - address, 178
 - NovaMac backup software, 167
 - nVIR virus, 122-123
- O**
- Obnoxious Tetris game, MBDF virus, 131
 - OCSG, Kerberos Authentication Software, 248-249
 - Office of Defense Trade Controls, encryption export, 81
 - on-line UPS, 264
 - CyberSAFE
 - address, 252
 - Kerberos authentication protocol, 245
 - Orange Book, Trusted Computer Systems Evaluation Criteria, 23
 - organizational policies
 - network countermeasures, 232
 - security questionnaire, 12
- P**
- padlocks, anti-theft locking devices, 187
 - Parallel Security Plates, 209
 - partitioning hard drives, 29, 47, 52, 53
 - passive
 - attacks, 228
 - infrared alarms, 184
 - Passport
 - access-control software, 50
 - address, 61
 - PassProof
 - access-control software, 51-52
 - address, 61
 - passwords
 - See also identification
 - compared to keys, 65
 - hard drives, 28, 29
 - keys and, 73
 - overview, 25-28
 - picking, 26
 - protecting, 27
 - remote access control, 236
 - PC Guardian
 - address, 208
 - Anti-Theft Kits, 189
 - Chassis Locks, 191
 - Floppy Drive Locks, 192, 198
 - Keyboard Locks, 191, 198
 - physical security products, 197-198
 - Power Switch Locks, 198
 - PCs, Mac virus comparison, 105-106
 - Peace virus, 125-126
 - Personal Computer Insurance
 - address, 219
 - DATA Security Insurance, 216-217
 - personnel security
 - elements of, 273-274
 - overview, 273-275
 - screening, 273-274
 - PGP (Pretty Good Privacy)
 - address, 252
 - RSA public-key cryptography, 242, 245-246
 - Phazer Area Controller, network security, 199
 - Phazer/Net
 - address, 208
 - fiber-optic physical security systems, 198-199
 - photoelectric alarms, 184
 - physical and environmental protection, security questionnaire, 13
 - physical damage, security vulnerability, 17
 - physical data protection
 - See also hardware
 - access control, 33
 - Keylock Mac, 48
 - MaccessCard Reader, 48-49
 - MacPassword, 49
 - overview, 181-204
 - PassProof, 51-52
 - PC Guardian, 197-198
 - PowerBook Guardian, 199-200
 - SafeWord MultiSync cards, 52-53
 - plaintext, defined, 63
 - planning for disaster recovery, 286-288
 - plates
 - adhesive, 187-188
 - identification, 202
 - security, 189-191
 - poison pills, access control, 32
 - policies, security, 226-227, 232, 291-300
 - pollutants, power, 257-260
 - polymorphic viruses, 137-138
 - port locks, data security, 192
 - Powell-Walton-Milward Insurance
 - address, 219
 - computer insurance, 217
 - power
 - failures, 258
 - fluctuations, 17
 - line noise, 258
 - pollutants, 257-259
 - protection. See power protection
 - Power Backer Plus
 - address, 268
 - UPS unit, 265-266
 - PowerBook Guardian
 - address, 208
 - physical security devices, 199-200
 - PowerBook Handle Security Kit
 - address, 208
 - lock-and-cable devices, 200
 - PowerBooks
 - DiskLock PB, 42
 - LockingStation, 196
 - MacShackle, 197
 - PowerLock Plus, 201
 - security tips, 193-194
 - Sentinel security, 203
 - PowerLock Plus
 - address, 208
 - PowerBook locks, 201
 - power protection
 - security tips, 266
 - surge suppressors, 260-262
 - Uninterruptible Power Supplies (UPS), 264-265

power protection (continued)
 voltage regulators and line conditioners, 262-264

Power Switch Locks, PC Guardian, 198

PowerTalk Key Chain, Apple Open Collaboration Environment, 238

Power Utilities
 access-control software, 52
 address, 61

Praxitel
 address, 61
 Passport access-control software, 50

Preferences folder, INIT-M virus, 135

Pretty Good Privacy (PGP)
 address, 252
 RSA public-key cryptography, 242, 245-246

prevention
 anti-virus software, 108-110
 network security mechanisms, 226
 recovering from infections, 111

printer security
 documents, 270
 LaserSafe, 202
 LaserWriter Security System, 194

private-key algorithms, defined, 64

privileges
 inherited, 235
 limiting, 31-32

procedures, network security, 231-232

prod virus, 122-123

programs. *See* software

proprietary algorithms
 caveat, 67
 RC2 & RC4 secret-key cryptography, 242-244

Protect Your Macintosh source code disk, 301

protocols, Kerberos, 244-245

public-key
 algorithms, 64, 241, 242
 cryptography, 240-242

Q

Qualtec Data Products
 address, 208
 anti-theft products, 201-202
 Cable Trap, 202
 Floppy Disk Drive Lock, 202
 Heavy-Duty Anti-Theft products, 201-202
 LaserSafe, 202
 Macintosh Security Kits, 201-202
 security plates, 190

questionnaire, self-audit security, 12-16

QuickLock
 access-control software, 52
 address, 62

R

radiation emanation, security dangers, 5

radio frequency interference (RFI), computer problems, 258

RC2 & RC4
 compared to DES (Data Encryption Standard), 242-243
 secret-key cryptography, 242-244

RC4 algorithm, Authentication Manager, 238

read costing, ExpressMirror, 164

recordable CD drives, 151

Redux Deluxe
 address, 178
 backup software, 167-169

regulators, voltage, 262-266

remote access control, AppleTalk, 236-237

remote computers
 Empower Remote, 44-45
 Retrospect Remote, 170-171

replaceability, risk analysis, 11

re-plays, network threats, 229

re-routing, network threats, 229

restricted data, defined, 8

Retrospect
 address, 178
 backup encryption, 156
 backup software, 169-170

Retrospect Remote
 address, 178
 backup software, 170-171

RFI (Radio Frequency Interference), computer problems, 258

risk analysis
 overview, 10-16
 security countermeasures, 8
 security policies, 294-295

Rival anti-virus software, 116

Rivest, Ron
 RC2 & RC4 secret-key cryptography, 242-244
 RSA public-key algorithm, 242

rogue's gallery, viruses, 121-140

routers, zone access, 233-234

RSA public-key cryptography algorithm, 241, 242
 PGP (Pretty Good Privacy), 242, 245-246

RTMP filtering, zone and device access, 233-234

S

SafeDeposit
 address, 178
 backup software, 171

SafeDeposit Server
 address, 178
 backup software, 171-172

safeguarding keys, 76-77

safety rules, backup, 152

Safeware insurance
 address, 219
 computer insurance, 215

SafeWord MultiSync cards
 access control, 52-53
 address, 62

SAM (Symantec AntiVirus for Macintosh)
 address, 120
 described, 116-117

San Jose Flu virus, 121-122

schedules, backup, 154-155

Scores virus, 121-122

screening, personnel security, 273-274

screen locking
 access control, 29-30
 DiskGuard, 41
 Empower I, 43
 FileGuard, 46
 ISAC 4200, 87
 PassProof, 51
 QuickLock, 52
 SecureInit, 53

- screws, anti-theft locking devices, 186-187
- Scrubber, file erasure software, 95-96
- SCSI Security Plates, 209
- secret-key algorithms, defined, 64
- secret-key cryptography
 - compared to public-key, 241
 - RC2 & RC4, 242-244
- SecureInit
 - access-control software, 53
 - address, 62
- Secure-It
 - address, 206
 - anti-theft devices, 196
- SecurID Card
 - address, 252
 - network security, 246-247
- security
 - See also* anti-theft considerations
 - accountability, 23
 - AppleShare, 234-236
 - AppleTalk, 225
 - assurance, 24
 - backup data, 155-156
 - component considerations, 191-193
 - computer insurance, 211-219
 - countermeasures, 23
 - degrees of, 233
 - DES (Data Encryption Standard), 71-73
 - disaster recovery, 285-289
 - document, 269-271
 - documentation, 24
 - door locks, 184-185
 - hardware products, 194-210
 - indelible ink, 192, 193
 - Kerberos authentication protocol, 244-245
 - legal aspects, 297-298
 - liability, 298-299
 - mainframe perspective, 16-17
 - network, 221-253
 - network countermeasures, 230-231
 - network products, 245-253
 - Network Security Administration Manual, 232
 - overview, 1-18, 22-24
 - personnel, 273-275
 - policies. *See* security policies
 - PowerBooks, 193-194
 - power protection, 257-268
 - remote access control, 236-237
 - self-audit questionnaire, 12-16
 - setting goals, 2-3
 - six enemies of, 2
 - Users' Guide to Network Security, 232
- Security Clip Mac-Clip, 209
- Security Dynamics
 - address, 252
 - SecurID Card, 246-247
- Security Force
 - address, 253
 - network security, 249-250
- security plates
 - overview, 189-191
 - Qualtec Data Products, 190
- security policies
 - creating, 226-227, 232, 291-300
 - management, 292-293
 - network, 296-297
- Security Tracking of Office Property (STOP)
 - address, 210
 - anti-theft systems, 202-203
- self-audit questionnaire, security, 12-16
- self-decrypting archives
 - See also* decryption
 - Camouflage, 85
 - CryptMactic, 85
 - encryption features, 80
- Sentinel
 - address, 210
 - PowerBook security, 203
- sequence errors, network threats, 229
- serial numbers, anti-theft considerations, 192-193
- Serial Security Plates, 209
- servers
 - See also* networks
 - Apple Open Collaboration Environment (AOCE), 237-238
 - ARA Multiport Server software, 236-237
 - protection requirements, 230
 - SafeDeposit Server backup software, 171-172
 - SnapBack backup software, 172
 - UPS (Uninterruptible Power Supplies), 259
- Shamir, Adi
 - breaking of Fast Encryption Algorithm (FEAL), 67
 - RSA public-key algorithm, 242
- Shredder
 - address, 99
 - file erasure software, 95-96
- Shredder with Citadel
 - address, 99
 - file erasure software, 95
- signatures
 - digital, 239-240
 - polymorphic-virus, 138
 - virus, 106
- Silverlining
 - access-control software, 53
 - address, 62
- single sign-on systems, PowerTalk Key Chain, 238
- Skipjack algorithm
 - encryption, 69
 - hardware DES encryption, 78-79
- smallness, security vulnerability, 16
- SnapBack
 - address, 179
 - backup software, 172
- Snapshot
 - FastBack Plus backup software, 165
 - Retrospect, 169-170
- SofKeyPlus
 - address, 252
 - network security, 247
- software
 - access-control, 24-28, 34-57, 58-62
 - anti-viral, 113-120
 - encryption, 83-88, 91-92
 - encryption features, 79-81
 - field guide to malicious, 104
 - file erasure, 94-97
 - integrity, 277-279
 - key guessers, 75-76
 - malicious. *See* malicious software
 - preventative versus detective anti-virus, 108-110
 - security dangers, 4
- Software Brewing Company
 - address, 60
 - Folder Locker access-control software, 47
- SonicPRO Model AP128
 - address, 210
 - motion-activated alarms, 203
- source code disk, Protect Your Macintosh, 301
- spark gaps, surge suppressors, 260

Spectra Micro Development
 address, 58
 Bullet Proof, 38
 speed considerations, encryption,
 77-78
 standby UPS, 264
 STOP (Security Tracking of Office
 Property)
 address, 210
 anti-theft systems, 202-203
 storage
 security questionnaire, 13
 security vulnerability, 17
 storms, data dangers, 4
 SuperSet Utilities
 address, 99
 Virex, 117-118
 suppressors, surge, 260-262
 Surf City Software
 address, 179
 SurfGuard backup software,
 173-174
 SurfGuard
 address, 179
 backup software, 173-174
 SurgeArrest
 address, 268
 surge suppressor, 262
 surge suppressors, power
 protection, 260-262
 surveillance, electromagnetic,
 281-283
 Symantec
 address, 92
 AntiVirus for Macintosh
 (SAM), 116-117
 DiskLock, 41
 DiskLock PB, 42
 FastBack Plus backup software,
 164-165
 Norton Backup backup
 software, 166-167
 Norton Encrypt encryption
 software, 88
 Norton Partition access-
 control software, 50
 Norton Wipe Info file erasure
 software, 97
 SyQuest disks, 148
 system access controls, security
 questionnaire, 14
 Systematic Computer Services
 address, 100
 Viper file erasure
 software, 97
 system bombs, virus
 symptoms, 106

system integrity, security
 questionnaire, 13-14
 SysX virus, 137

T
 T4 virus, 133-134
 tapes
See also cartridges
 digital, 149-151, 158
 maintenance of, 157
 temperature fluctuations, data
 dangers, 4
 TEMPEST, electromagnetic
 surveillance, 281-283
 Ten Tile Puzzle game,
 MBDF virus, 131
 terminology, encryption,
 63-64
 Tetracycle game,
 MBDF virus, 131
 Tetris-rotating game,
 MBDF virus, 131
 thieves, data dangers, 4
 tickets, Kerberos authentication
 protocol, 244-245, 248
 time
 decryption speed, 68
 encryption speed, 77-78
 time bombs, virus, 104
 Top Cat virus, 128-129
 TOPS servers, WDEF virus, 127
 traffic analysis, network
 threats, 228
 training
 security questionnaire, 12
 security vulnerability, 17
 Transfinite Systems
 address, 91
 Ft. Knox encryption software,
 86
 Ft. Knox file erasure software,
 97
 tranzorbs, surge suppressors, 260
 TrashGuard
 address, 99
 file erasure software, 96
 TrashMaster
 address, 99
 file erasure software, 96
 Trent Saburo,
 CODE 1 virus, 136
 Trik
 address, 252, 253
 Lookout! network
 security, 249
 triple-DES encryption, 69,
 72, 86
 Trojan horses

described, 104
 MBDF virus, 131
 Mosaic and FontFinder, 136
 Trusted Computer Systems
 Evaluation Criteria, Orange
 Book, 23
 TwintIt
 address, 179
 backup software, 174
 twinning
 described, 144-145
 DiskTwin, 163
 ExpressMirror, 164
 TwintIt backup software, 174

U
 ultraSECURE
 access-control software, 53-55
 address, 62
 ultraSHIELD
 access-control software, 55
 address, 62
 ultrasonic alarms, 184-185
 unclassified data, defined, 9
 unimportant availability, defined,
 9
 Universal Anti-Theft Kit, 207
 UPS (Uninterruptible Power
 Supplies)
 overview, 264-265
 servers, 259
 user awareness and training,
 security questionnaire, 12
 user-friendliness, security
 vulnerability, 16
 user management, A.M.E. (Access
 Managed Environment), 36-
 37
 Users' Guide to Network Security,
 security
 policies, 232
 usrEZ Software
 address, 59
 Camouflage encryption
 software, 84-85
 cypherPAD access-control
 software, 39-40
 ultraSECURE access-control
 software, 53-55
 ultraSHIELD access-control
 software, 55
 Utilitron
 address, 99
 TrashMaster, 96

V

- vaults, Citadel access-control software, 39
- verification, backup safety rules, 152
- ViaCrypt
 - address, 252
 - PGP (Pretty Good Privacy), 245-246
- Viper
 - address, 100
 - file erasure software, 97
- Virex
 - address, 120
 - anti-virus software, 117-118
 - virtual memory, file erasure, 93-94
- VirusBlockade, anti-virus software, 118
- Virus Clinic, Symantec AntiVirus for Macintosh (SAM), 116-117
- VirusDetective, anti-virus software, 118

viruses

- See also* malicious software
- anti-virus software, 113-120
- biological compared to computer, 105
- defined, 104
- described, 101
- detecting, 106-110
- encrypted and polymorphic, 137-138
- last-ditch clean-up
 - procedures, 112-113
- listed, 121-140
- protection hints, 109
- recovering from infections, 111
- seriousness of, 105-106
- signatures, 106
- virus protection
 - MacPassword, 49
 - overview, 101, 103-118
- visitors, personnel security, 275
- voltage
 - fluctuations, 258
 - line conditioners, 263
 - regulators, 262-266
- vulnerabilities
 - network, 228-230
 - risk analysis, 11
- Vult virus, 121-122

W

- warranties, anti-theft locking devices, 186
- wattage, line conditioners, 263
- WDEF virus, 126-127
- worms, virus, 104

Z

- zero virus, 122-123
- zone access, access control, 233-234
- Zucchini, Don Ernesto, ZUC virus, 127-128
- ZUC virus, 127-128



About the Author

Bruce Schneier is president of Counterpane Systems, an Oak Park, Illinois-based consulting firm specializing in computer security and cryptography. He holds an MS in Computer Science from American University, and has over 10 years experience in working with cryptography and data security with several public and private concerns. Mr. Schneier has written articles on computer security for a variety of magazines, including *MacWeek* and *Macworld*, and has lectured extensively on the subject. His first book, *Applied Cryptography*, was published by John Wiley & Sons. This is his second book.

Protect Your Mac with Citadel and Virex!

Your Mac is constantly exposed to security breaches, whether it's someone tampering with your computer or a virus silently infiltrating your files. You need protection that's potent, yet easy to use. By purchasing *Protect Your Macintosh*, you are already on the way to a safe and secure computer. Here's your chance to boost your system security with two of the best Macintosh utilities available, now at an unheard of price!



SPECIAL OFFER #1: Save \$50 off Citadel with Shredder!

Whether you need access control, DES file encryption, audit trails or even file shredding, Citadel is the only choice for your home or office!

Purchase Citadel with this offer for only **\$49.95** - \$50 off the suggested retail price!



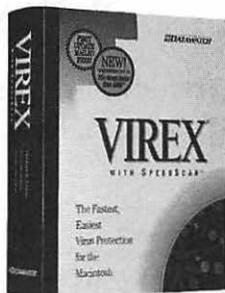
OR

SPECIAL OFFER #2: Save over \$100 by purchasing both Virex AND Citadel!

You've read about the damage viruses cause, protect yourself NOW with Virex! Virex includes the patent-pending technology of SpeedScan that scans for viruses in a fraction of the

time it takes others, allowing you to quickly and effectively protect your Mac against the virus threat. With this offer you'll get Virex AND

Citadel with Shredder for only **\$79.95!** This powerful combination will keep you virus free AND secure from unwelcome access to your Mac.



This special offer is only available to owners of this book.

Act now to get the protection your Macintosh deserves!

DATAWATCH

FOR MORE INFORMATION OR TO ORDER CALL:

(919) 549-0711 (weekdays 9 am to 5:45 pm, est)

OR FAX (919) 549-0065

“CryptoMactic – the best encryption program you can buy for the Macintosh - bar none.” — Bruce Schneier, Author, *Protect Your Macintosh*



CryptoMactic™

With EasyTrash and  Incinerate

**SPECIAL
OFFER
\$39.95**

With this coupon

(Includes shipping; Suggested Retail: \$99.00)

Buy directly from us for \$39.95 or return this coupon with proof of purchase for a \$10 rebate. Fax orders accepted for credit card purchases.

Name: _____ Organization: _____

Address: _____

City, State, Zip: _____

Phone: _____ Fax: _____

I wish to purchase _____ copy(ies) of CryptoMactic at \$39.95 each (limit 5).
 Amount Enclosed _____ (Texas residents, please add 8.25% Sales Tax)
 Card # _____ Visa MC AmEx Exp. Date _____
 Name On Card _____ Signature _____

I have purchased CryptoMactic. Please send my \$10 rebate. (Enclose proof of purchase)

Mail or Fax to:

Kent+Marsh, 3260 Sul Ross, Houston, TX 77098

Fax (713) 522-8965 Sales: (800) 325-3587

SAVE \$100

Encryption, Shredding, Virus Protection, Access Control, Folder Locking, Full 68000 And PowerPC Compatibility, Plus Much, Much More!

ultraSHIELD™ has more access control and security features than any competitive product. It's perfect for protecting personal and competitively-sensitive information in the office, home, or while traveling.

It's easy to operate — just log in your password once, then everything happens automatically and transparently. And ultraSHIELD uses the genuine security technology of ultraSECURE™.

ultraSHIELD includes easy to use, intuitive options for:

- Password Access Control,
- Protection of Partitions, Folders, and Drives,
- Fast and easy Drag & Drop file/folder protection,
- Fast, secure Proprietary Encryption, ■ Automatic Encryption/Decryption,
- Fastest (60 times faster than competition) U.S. Government DES encryption, ■ Virus Protection, ■ Options for Shredding to U.S. Government standards, for drives or TRASH, and ■ Comprehensive activity/audit and tamper logs/records.



"...feature-packed security product, combines practically every security feature you might need into one integrated package, including a lightning-fast version of the U.S. Government data-encryption standard (DES)."

"ultraSHIELD is a great product at a great price."

— MACWORLD, December 1993

Get ultraSHIELD, the security program that's much, much more and save \$100. Send your Check today to:



The Continuing Excellence Corporation
18881 Von Karman Ave., Suite 1270
Irvine, CA 92715

PowerBook Features

ultraSHIELD provides unique PowerBook options too: ■ Genuine Security, ■ Screen Backlight Battery Saver that automatically conserves battery power when the screen saver is turned on, ■ Sleep Lock Out option.

Accelerated for PowerPC

And ultraSHIELD operates smoothly on the Power Macintoshes, PowerBooks and other Macintoshes, as well as all System Software (6.02 and higher). ultraSHIELD's performance is increased greater than five times on the Power Macintosh, as compared to the Quadra 950.



© 1994 usREZ Software, Inc. usREZ, ultraSHIELD and ultraSECURE are trademarks of usREZ Software, Inc. All brand names are trademarks or registered trademarks of their respective holders.

YES! I want to take advantage of the savings and get ultraSHIELD now for only \$49.

Enclosed is my check for \$49.

Charge to my: Visa MasterCard

Credit Card No. Expire Date

Suggested Retail Price: \$149.00.
Direct Sale ONLY; FOB Irvine, CA.

Offer expires April 15, 1995
Send original coupon ONLY; Photocopies not acceptable.

Name

Company

Street

City State Zip

Telephone

PROTECT YOUR MACINTOSH

FROM...

spies, vandals, viruses, thieves, competitors, missile strikes, lightning strikes, your boss, your employees, your colleagues, your kids, your parents, the press, earthquakes, tornadoes, hardware crashes, software glitches, your own mistakes.

Here is the first hands-on, comprehensive guide covering all aspects of Macintosh security, including both stand-alone and networked Macintoshes. It covers the following topics:

▶ **FILE ENCRYPTION**

How encryption works, what products to buy for password protection, how to choose and protect passwords.

▶ **VIRUS PROTECTION**

What you need to know about viruses, an overview of the most common viruses, how to detect and recover from viruses, which virus-protection software works best.

▶ **BACKING UP YOUR FILES**

Backup strategies, how to backup and restore, which backup software to buy.

▶ **PHYSICAL SECURITY**

Overview of anti-theft devices, laptop locks and alarms, other protection products.

▶ **NETWORK SECURITY**

Methods of network security, dial-in security, network protection software.

Bruce Schneier is an independent computer-security consultant in Oak Park, Illinois. His articles on computer security have appeared in Macworld, Network World, LAN Technology, Byte, Computer Language, Dr. Dobbs Journal, and other magazines. He is the author of Applied Cryptography (John Wiley & Sons, 1993).

USER LEVEL



Beginning



Intermediate



Advanced

ISBN 1-56609-101-2



Warehouse - BK15837465

Protect Your Macintosh
Used, Good

(uG) _S_ WF

Self Category
INTOSH



Peachpit Press, Inc.
2414 Sixth St.
Berkeley, CA 94710
510/548-4393
fax: 510/548-5991

9"781566091012

Canada \$33.95