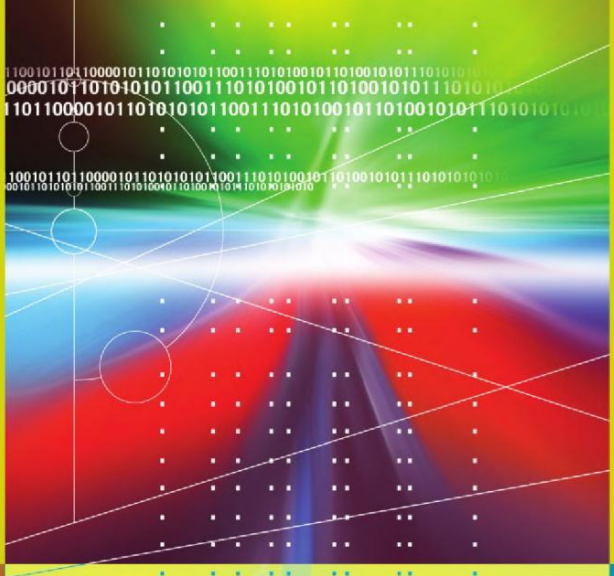


David Salomon

UNDERGRADUATE TOPICS in COMPUTER SCIENCE

Elements of Computer Security

Springer

UTiCS

David Salomon

Elements of Computer Security

Prof. David Salomon (emeritus)
Computer Science Dept.
California State University, Northridge
Northridge, CA 91330-8281
USA
dsalomon@csun.edu

ISBN 978-0-85729-005-2 e-ISBN 978-0-85729-006-9
DOI 10.1007/978-0-85729-006-9
Springer London Dordrecht Heidelberg New York

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Control Number: 2010933120

Printed on acid-free paper.

Springer is part of Springer Science+Business Media (www.springer.com)

Contents

LIFF (n.). A book, the contents of which are totally belied by its cover. For instance, any book the dust jacket of which bears the words. "This book will change your life."

—Douglas Adams, *The Meaning of Liff* (1984)

Introduction

The first microprocessors appeared in the early 1970s and were very quickly employed in personal computers. A popular question in those early years was: Why would anyone want a computer at home? Typical answers were: To balance your checking account, to store your recipes, and to help you compute your taxes. It was only a few years later, when many already owned personal computers, that computer owners discovered the real answer. We buy and use personal computers mainly because they provide us with communications and entertainment.

Games, initially primitive, were implemented for early personal computers and became a powerful selling tool in the hands of computer salespersons because of the entertainment they provided. The development of email in the 1970s and of the World Wide Web in the 1980s have turned computers into tools for communications, which is why they became the common household appliances they are today. Most owners of home computers use their computers to play games, to watch movies and television, and to communicate, to send and receive email, and to browse the Internet. Relatively few users are interested in computations, employ a word processor, benefit from a personal data base, or know how to use a spreadsheet.

Once personal computers became a part of our lives, it had quickly been realized that like many other technological advances, computers and data networks have their dark side. Security problems in the form of malicious programs, loss of privacy, destruction of data, attacks on Web sites and servers, and floods of unwanted advertisement and spam, have popped up immediately and have become a way of life for virtually every computer user.

◇ **Exercise Intro.1:** What industry is the largest user of computers?

Definitions. The dictionary defines security as "the quality or state of being free from danger" or "measures taken to guard against espionage or sabotage, crime, attack, or escape." This book explores some of the ways computers and computer networks are put at risk by perpetrators, hackers, and other wrongdoers. The terms "attack" and "threat" are used here to

identify any activity that aims to gain access to computers for malicious purposes. The terms "security hole," "weakness," and "vulnerability" refer to a state that can be exploited for such an attack (some would even say that a security hole *invites* an attack).

For the purposes of computer security, there are two types of people, insiders (employees) and outsiders (nonemployees). Figure Intro.1 shows the three classes of computer security and crime caused by each of the two types plus the special class of threats that are not directly caused by humans, namely accidents.

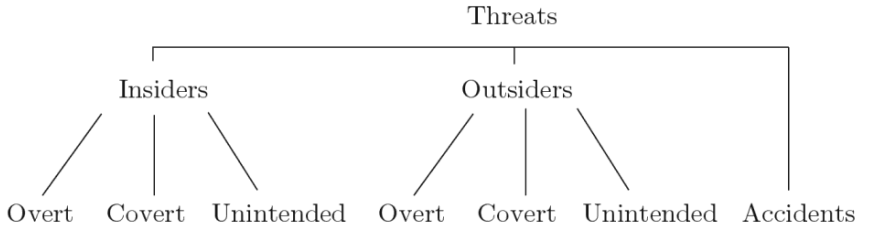


Figure Intro.1: Seven Classes of Computer Security and Crime.

The seven classes are as follows:

- Insiders overt. Overt actions by insiders are often performed by disgruntled employees and result in destruction of data and equipment. However, this class is small compared to the other six.

- Insiders covert. Generally, insiders have more information about a place of work than outsiders, which is why they can wreak more havoc. Thus, this class corresponds to serious threats and criminal actions.

- Insiders unintended. Employees make errors and can also neglect their duties. Consequently, this class encompasses actions such as wrong inputs, wrong data, damage as a result of extreme temperatures or other harsh conditions, and interruption of vital services.

- Outsiders overt. Physical attacks on computer and network facilities belong in this class, as do also DoS attacks (page 199).

- Outsiders covert. This wide class consists of the various types of rogue software sent from the outside to a personal computer, a mobile device, or to a large computer facility.

- Outsiders unintended. It is fairly rare that an outsider will harm a computer or data unintentionally.

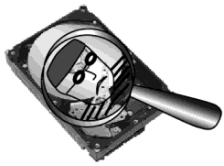
- Finally, there are accidents. They always happen, not just in the computing field. Accidents are caused either by nature, such as earthquake or flood, or indirectly by humans (see the "insiders unintended" class).

> History is a jangle of accidents, blunders, surprises and absurdities, and so is our knowledge of it, but if we are to report it at all we must impose some order upon it.
>
> —Henry Steele Commanger, *The Nature and the Study of History*, 1966.

There are many different types of computer security threats and problems, but they can be classified into three large classes as follows:

- Physical security. A personal computer can be stolen. A large computer center can be broken into and equipment taken. Fire, electrical surges, and floods can damage computer hardware and network connections and cause loss of data. These and other physical threats are discussed in Chapter 1.

- Rogue software. We have all heard of computer viruses. Small, sneaky programs that invade our computers and spread quickly and silently. Viruses are just one aspect of the general threat posed by rogue software. This topic, which also includes worms and Trojan horses, is discussed in Chapters 2 through 6.



- Most computers are connected to networks, and most local networks are connected to the Internet. Thus, there is a large class of computer security threats that are related to networks and fall under the category of network security. This wide area of security includes threats such as port scanning, spoofing, password cracking, spyware, and identity theft and is the topic of Chapters 7 through 9.

Almost nonexistent before the 1980s, computer security is now a vast, complex, and important field. This book is just one of many books, articles, reports, and other publications that discuss, explain, and analyze the various aspects of and approaches to computer security. What makes this book special is its reliance on the keyword "compromise." This word is employed here in two meanings as follows:

1. Computer security is a compromise. The more secure a computer, the less convenient it is to use.

2. An attacker has to find only one security weakness to compromise an entire computer installation or many computers worldwide and cause extensive psychological and financial damage to users, their identities, software, and personal and commercial data.

Any security threat or vulnerability described in this book can be reduced, managed, solved, or overcome in some way, but the solution makes it more difficult or less convenient to use the computer, the network, or a particular operating system or program. This view of security as a compromise or a tradeoff is the key to understanding computer and network security.

> Anyone who has ever tried to manage accounts on mainframes or local area networks (LANs) will recognize that there is a constant battle between the aspects of security and user friendliness in computer use. This tension arises from the definition of the two functions. If a computer is easy to use, it is easy to misuse. If a password is hard to guess, it is hard to remember. If access to information is simple for the owner, it is simple for the cracker.
>
> —David Harley et al., *Viruses Revealed*, 2001.

Why does the problem of computer security exist? Why are computers so vulnerable to attacks and so easy to damage? This book offers four reasons, but the reader may come up with more.

Reason 1. Computers are fast, accurate, and powerful in certain tasks such as computing, searching, and manipulating data, while being inadequate and inefficient in other tasks, most notably in anything requiring intelligence.

The field of artificial intelligence is almost as old as the modern electronic computer. Researchers have been trying since the 1950s to teach computers how to solve real-world problems such as recognizing patterns, playing games against a human opponent, and translating natural languages, all without success. Today, after more than half a century of effort, computers can recognize handwriting, can identify speech commands, and can prove certain types of mathematical theorems, but are not good at any of these tasks. Computers have recently become good at beating chess masters at their own game, but only because they (the computers) are fast enough to analyze every possible move in a reasonable time, not because they understand chess.

Thus, computers are fast, reliable, and very useful, but are not very intelligent, which makes them victims of (computer) crime. Even humans, who are much more intelligent, often (perhaps too often) fall prey to clever schemes designed to take their money, so it is no wonder that the problem of computer security is serious and is getting worse.

◇ **Exercise Intro.2:** Computers are fast, reliable, and very useful, but are not very intelligent. With this in mind, can they be trusted?

Reason 2. It is easier to break computer security than to build fully secure computers. A modern computer has many security weaknesses and a hacker has to find only one in order to do harm. A security worker, on the other hand, has to find and correct *all* the security holes, a virtually impossible task. This situation is a special case of the general rule discussed in the answer to exercise 2.15.

Reason 3. A computer is controlled by its operating system and modern operating systems are extremely complex. A systems programmer designs an operating system with a view towards making it easy to use, but as we already know, the easier it is to use a computer, the less secure it is. Today's modern graphical user interface (GUI) operating systems are designed around several layers where the user interacts with the highest level and the hardware is controlled by the lowest level. Each level controls the one below it and it is this organization in levels that allows malware to hide from the user and perform its operations in relative obscurity and safety.

At the time of this writing (mid 2010), operating systems have become so complex that hackers constantly find ways to exploit vulnerabilities and security holes in them. Quite often, such holes are discovered by honest users who then notify the maker of the operating system, resulting in a patch or an update being promptly issued to solve that problem, only for a new hole to be quickly discovered. The following example, found on the Internet in early 2010, is typical. It illustrates the number and variety of security holes that have to be dealt with in just one security update. Don't worry about the details, just keep in mind that this announcement is typical.

Security Update 2010-001, for Mac OS X 10.5, Mac OS X 10.6.
1. Impact: Playing a maliciously crafted mp4 audio file may lead to an unexpected application termination or arbitrary code execution.
Description: A buffer overflow exists in the handling of mp4 audio files. Playing a maliciously crafted mp4 audio file may lead to an unexpected application termination or arbitrary code execution. This issue is addressed through improved bounds checking. Credit to Tobias Klein of trapkit.de for reporting this issue.
2. Impact: A remote attacker may cause an unexpected application termination of cupsd.
Description: A use-after-free issue exists in cupsd. By issuing a maliciously crafted get-printer-jobs request, an attacker may cause a remote denial of service. This is mitigated through the automatic restart of cupsd after its termination. This issue is addressed through improved connection use tracking.
3. Impact: Multiple vulnerabilities in Adobe Flash Player plug-in.
Description: Multiple issues exist in the Adobe Flash Player plug-in, the most serious of which may lead to arbitrary code execution when viewing a maliciously crafted web site. The issues are addressed by updating the Flash Player plug-in to version 10.0.42. Further information is available via the Adobe web site at.... Credit to an anonymous researcher and....
4. Impact: Viewing a maliciously crafted TIFF image may lead to an unexpected application termination or arbitrary code execution.
Description: A buffer underflow exists in ImageIO's handling of TIFF images. Viewing a maliciously crafted TIFF image may lead to an unexpected application termination or arbitrary code execution. This issue is addressed through improved bounds checking. For Mac OS X v10.6 systems, this issue is addressed in Mac OS X v10.6.2.
5. Impact: Viewing a maliciously crafted DNG image may lead to an unexpected application termination or arbitrary code execution.
Description: A buffer overflow exists in Image RAW's handling of DNG images. Viewing a maliciously crafted DNG image may lead to an unexpected application termination or arbitrary code execution. This issue is addressed through improved bounds checking. Credit to... for reporting this issue.
6. Impact: An attacker with a privileged network position may capture data or change the operations performed in sessions protected by SSL.

Description: A man-in-the-middle vulnerability exists in the SSL and TLS protocols. Further information is available at.... A change to the renegotiation protocol is underway within the IETF. This update disables renegotiation in OpenSSL as a preventive security measure. The issue does not affect services using Secure Transport as it does not support renegotiation. Credit to... for reporting this issue.

Reason 4. In addition to the complexity and vulnerability of operating systems, there is another factor that affects the behavior of a computer, namely the Internet and its protocols. Most personal computers and many mobile devices are connected to the Internet and enjoy the benefits of communications that it confers. In order for many computers to communicate, there is a need for communications standards, which is why various communications protocols had to be developed. Such a protocol is a set of rules that specify the individual steps of a complete Internet session. Thus, all the computers that send, forward, and receive email have to execute the same protocol. Similarly, transferring files between computers requires a protocol. The point is that the important Internet protocols were developed in the 1970s and 1980s, before Internet security became a global concern. This is why the security features included in the protocols are often weak. These protocols were examined by many experts and users who made contributions and proposed changes, but once such a protocol is approved and many programs are written to implement it, there is no way to go back and modify it. When a security hole is discovered, warnings are issued and programs are patched, but the underlying protocol is known to be weak.

The Ten Immutable Laws of Security (From [technet 04]).

Microsoft security workers investigate countless security reports every year and the ten immutable laws of security [technet 04] listed here are based on their experience. The security issues discussed here are general and stem from the main weakness of computers, namely the lack of intelligence. They show that the best way to minimize security risks is to use common sense. Here is a summary of the ten laws:

1: If someone can persuade you to run his program on your computer, it's not your computer anymore.

2: If someone can alter the operating system on your computer, it's not your computer anymore.

3: If someone has unrestricted physical access to your computer, it's not your computer anymore.

4: If you allow someone to upload programs to your Web site, it's not your Web site anymore.

5: Weak passwords defeat strong security.

6: A computer is only as secure as its owner/user is trustworthy.

7: Encrypted data is only as secure as the decryption key.

8: An out-of-date virus scanner is only a little better than none at all.

9: Absolute anonymity isn't practical, in real life or on the Web.

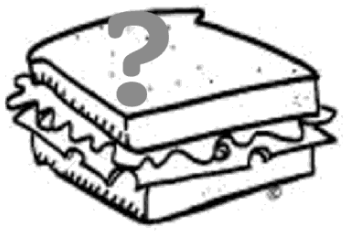
10: Technology is not a panacea.

And here are the same laws in more detail:

Law 1: If someone can persuade you to run his program on your computer, it's not your computer anymore.

It doesn't take much knowledge to understand that when a computer program runs, it will do exactly what it is programmed to do, even if it is programmed to be harmful. When you elect to run a program, you let it control your computer. Once a program is running, it can do anything that a user program can do on the computer. It could collect your keystrokes and save them or send them outside. It could open your text files and change all the occurrences of "will" to "won't" in some of them. It could send rude emails to all your addressees. It could install a virus or other rogue software. It could create a backdoor that lets a fraudster control your computer remotely. It could dial up a long-distance number and leave you stuck with the bill. It could even erase your hard disk.

Which is why it is important to never run, or even download, a program from an untrusted source, where "source," means the person who wrote it, not the person who gave it to you. There's a nice analogy between running a program and eating a sandwich. If a stranger walked up to you and offered you a sandwich, would you eat it? Probably not. How about if your best friend gave you a sandwich? Maybe you would, maybe you wouldn't, it depends on whether she made it or found it lying in the street. Using common sense in the security of your computer means to apply the same critical thought to a program that you would to a sandwich.



Law 2: If someone can alter the operating system on your computer, it's not your computer anymore.

An operating system is a program (rather, a set of programs) that provide important services and also supervise users. As such, the operating system must be more powerful than users' programs. Thus, letting someone modify your operating system is like letting them have more power in your computer than you do. Operating system routines must be powerful, which implicitly makes them trusted. The owner and users of the computer must trust those routines, which is why anyone who manages to corrupt them can gain complete control.

A perpetrator gaining operating system privileges can log into the computer locally or remotely, obtain users' passwords, change users' privileges, and in general do anything in the computer. The conclusion is again to use sound judgement before you let anyone mess with your operating system.

Law 3: If someone has unrestricted physical access to your computer, it's not your computer anymore.

Someone who has access to your computer can deny you your computer's services simply by smashing it (this is an example of stone-age denial of service). More likely, the computer would be stolen, or even held for ransom.

Having physical access makes it easy to install spyware, change the administrator's password, copy data off the hard disk, or do any other type of damage that's difficult or impossible to do from a distance. Any protection provided by the operating system is moot when a stranger has physical access to the computer.

◇ **Exercise Intro.3:** Think of an example of such damage.

Thus, a computer, personal or multiuser, should be physically protected in a way compatible with its value, but it's important to consider the value of the data in the computer, not just the market value of the hardware. Computers used in business and sensitive computers such as servers should be kept in a locked room and be physically protected. The list on Page 22 has more information on this topic.

Laptop computers are very handy and popular, but not only with their owners. Thieves target those machines because of their high price and also because they are easy to steal. A laptop is normally taken out by its owner while traveling and is used in public places, thereby making it a potentially easy item to steal. Section 1.3 has more on laptop security.

Here are two examples of spying that someone who has access to your computer can do.

1. The stealth iBot PC monitor is a small, portable USB spying device. Anyone who has access to your computer, even for only a few seconds, can plug this device into a USB port. In five seconds, the iBot embeds its spying software in the operating system and can then be unplugged. This software records up to 1 GB of everything done on the computer by any of its users, including text, screen shots, and Web sites visited. When the spy has another chance of accessing your computer, he simply plugs in the same iBot again for five seconds, which is all the time it needs to download the stolen data. This type of spying is especially easy if the spy is one of the users of the computer.

2. The eBlaster software acts as a general spy. Once installed on a computer, it records all activities, including text typed, Web sites visited, instant messages sent and received, Internet searches made, and email sent and received. eBlaster can even send its owner email messages about such events in real time (right after an even occurred) and it allows its owner to access, remotely or locally, the computer usage logs it creates.

These products are made by the same company, are advertised and sold online, and are legal.

Law 4: If you allow someone to upload programs to your Web site, it's not your Web site any more.

We already know that it is dangerous to let someone upload a program to your computer, but in most of these cases, the program is uploaded to a Web site and the uploader is permitted by the site's owner to run it. Long

experience shows that Web site owners often allow visitors, out of the goodness of their heart or out of carelessness, to upload software and run it; a risky habit.

Security dictates that the owner of a Web site should limit the freedom of visitors. This is especially true in cases where the Web site is hosted by a large server that also hosts other sites. In such a case, a hacker who takes control of one site can extend his control to all the Web sites on the server. The owner of a large, shared server who wants to avoid trouble should therefore be security conscious.

Law 5: Weak passwords defeat strong security.

Section 8.3 discusses passwords, how they provide remote identification and authentication, and how important it is to select strong passwords. If you have an account on a remote computer and you select a weak password, chances are that someone will manage to crack or guess it. The strong security on the computer wouldn't protect you in such a case. If someone logs in as you, then the operating system treats him as you.

Security experts keep stating the surprising fact that many computer accounts have extremely weak passwords, such as the null password or one of the words "guest," "password," "admin," and "test."

The conclusion is obvious and unavoidable (but still ignored by many users). Select a strong password! It should include letters (both lowercase and uppercase), digits, and some punctuation marks. It should be long, and should be replaced often. Try not to write your password anywhere and don't tell it to anyone. Many current keyboards include modifier keys with names such as command, option, and control. A password can be made stronger if it includes characters modified by those keys, such as §, ¶, †, ‡, CMD-V, and OPTION-U.

Section 8.3 also shows why it is important to select passwords that do not appear in a dictionary, because such passwords can be cracked by a dictionary attack.

> Two people can keep a secret, but only if one of them is dead.
> —Benjamin Franklin.

Smartcards have been introduced a decade ago and can be used for authentication. Biometric products, such as fingerprint and retina scanners (Section 8.2), are also becoming popular. They used to be too expensive for common use, but this has recently changed. Many current laptops come with a fingerprint scanner and a stand-alone USB unit can be had for less than $50. Even PDAs may have such a unit built in because many PDAs are designed for business users who often carry sensitive company data.

Law 6: A computer is only as secure as its administrator is trustworthy.

The owner of a home personal computer is normally its administrator and sole user as well. A large, multiuser computer has many users and may be owned by a commercial entity, but it must have an administrator. The administrator is responsible for managing user accounts, installing software, searching for viruses, establishing security and usage policies, and performing

any other tasks needed for a smooth running of the facility. It is obvious that the administrator is all powerful in the computer and that an untrustworthy administrator can create havoc in the computer installation.

Such an administrator can negate any security measures taken by the users, can install rogue software, can spy on the users, change their privileges and permissions, and turn off any security and protection features the operating system supports. In short, an untrustworthy administrator is the worst thing that can happen to computer security. An organization planning to acquire a large, multiuser computer should therefore start by hiring a trustworthy administrator. This person should have some experience working with large, multiuser computers and with computer security, but should most of all prove trustworthy. The references of each candidate for this position should be carefully checked and a complete background check should also be considered. In short, each candidate should be fully vetted. In addition, periodic checks of the administrator are also recommended.

There are methods to keep administrators countable. Often it is possible to have two, or even several administrators. Each should be assigned a user account, but with full privileges, instead of an administrator account. This way, the owner or an auditor can tell who did what on the computer. It also helps if the operating system allows to write a copy of all log files and audit information on a different computer. Each time software is installed or updated, one administrator should do the job, and another should later act as an auditor, checking the results.

Law 7: Encrypted data is only as secure as the decryption key.

It has long been known that the security of encryption depends on the encryption key, not on the encryption algorithm (this is known as Kerckhoffs' principle). Thus, encryption keys have to be selected carefully and should be kept secret. Such a key should not be kept in the computer unless it is encrypted and protected by another key. When public-key cryptography (see document on cryptography in the book's Web site) is used, the private key should be protected in the same way.

Law 8: An out-of-date virus scanner is only marginally better than no virus scanner at all.

Anti-virus software is discussed on page 158, where it is stressed that this type of software has to be updated regularly, as new viruses are discovered and analyzed. Thus, anti-virus software is not for the lazy. A computer owner should check every day for new updates of this software, download and install them, and run the programs. A delay in installing a new update may mean an infection by a new virus, so a computer owner/user should start each day (as this author does) by looking up new virus information on the Internet. On a day a new virus is discovered, the user should be especially careful. No software should be downloaded and no email attachment opened until a new anti-virus update is issued and run.

Current anti-virus software normally checks for new updates automatically every time it is run. This is an important feature of the software and it shouldn't be disabled by users just to speed up the process of virus checking.

Law 9: Absolute anonymity isn't practical, in real life or on the Web.

Absolute anonymity in real life is impossible. From time to time we hear about people who cherish their privacy and try to avoid contact with others, especially the media. Howard Hughes is a classic example of such a recluse. There are those who try to stay completely anonymous, but even they have to interact with people, with the result that certain facts are eventually found out about them. Perhaps the best known example of an unknown person is the writer B. Traven, also known as Ret Marut, Hal Croves, and Traven Torsvan. He is the author of *The Treasure of the Sierra Madre* and many other novels. He lived in Mexico from about 1925 until his death in 1969, but despite many efforts to unravel his identity, we still don't know his real name and where and when he was born. Yet even this elusive character had to communicate with his publishers and movie directors, which is why today much is known about his life (see, for example, [Guthke 91]).

> I am freer than anybody else. I am free to choose the parents I want, the country I want, the age I want.
>
> —Rosa Elena Luján (Traven's widow) in the *New York Times*, 6/25/90.

Merely appearing in public reveals your eye color and approximate height, weight, and age. Similarly, a chat with a stranger can reveal facts about yourself, your family, your profession, place of living, and your interests.

◇ **Exercise Intro.4:** What other important fact can such a conversation yield to a stranger?

Identity theft is discussed in Chapter 10, where it is shown that maintaining anonymity and privacy is becoming more difficult and may already be impossible. Here are a few disguising techniques employed by those who are serious about maintaining their anonymity on the Internet. (1) Use network address translation to mask your real IP address. (2) Subscribe to an anonymizing email service (Section 11.2) that forwards your email with a different sender's address. (3) Use different ISPs for different purposes. (4) Visit certain Web sites only from public Internet cafes.

Such techniques and habits make it harder, but not impossible, for identity thieves to locate your personal information. The best way to protect your identity in this age of the Internet is to use common sense and to be careful.

Law 10: Technology is not a panacea.

Technology has been progressing rapidly in the last few decades. There are still those who remember the days without answering machines, cell telephones, or CDs, but their numbers are rapidly dwindling. Yet technology has its downside too. We depend so much on computers that when something goes wrong, it is normally because of a computer glitch. We see our privacy slipping from under out feet. Many, especially the elderly, find it difficult to learn how to use new gadgets. People are baffled by the rising threat of computer security. The phrase "the butler did it," much favored by mystery writers in the past, has been replaced with "it was a computer glitch/bug."

small files and (2) the next step encrypts a random file, thereby making it difficult to break the encryption simply by checking every key.

2. Encrypt B with a secret key to obtain file C. A would-be codebreaker may attempt to decrypt C by writing a program that loops and tries every key, but here is the difficulty. Each time a key is tried, someone (or something) has to check the result. If the result looks meaningful, it may be the decrypted file B, but if the result seems random, the loop should continue. At the end of the loop; frustration.

3. Hide C inside a cover file D to obtain a large file E. Use one of the many steganographic methods for this (notice that many such methods depend on secret keys). One reference for steganography is [Salomon 03], but currently there may be better texts.

4. Hide E in plain sight in your computer by changing its name and placing it in a large folder together with hundreds of other, unfamiliar files. A clever idea is to change the file name to `msLibPort.dll` (or something similar that includes MS and other familiar-looking terms) and place it in one of the many large folders created and used exclusively by Windows, UNIX, and other operating systems. If files in this folder are visible, do not make your file invisible. Anyone looking inside this folder will see hundreds of unfamiliar files and will have no reason to suspect `msLibPort.dll`. Even if this happens, an opponent would have a hard time guessing the three steps above (unless he has read these paragraphs) and the keys used. If file E is large (perhaps more than a few Gbytes), it should be segmented into several smaller files and each hidden in plain sight as described above. This step is important because there are utilities that identify large files and they may attract unwanted attention to your large E.

For those who require even greater privacy, here are a few more ideas. (1) A password can be made strong by including in it special characters such §, ¶, †, and ‡. These can be typed with the help of special modifier keys found on most keyboards. (2) Add a step between steps 1 and 2 where file B is recompressed by any compression method. This will not decrease the size of B but will defeat anyone trying to decompress B into meaningful data simply by trying many decompression algorithms. (3) Add a step between steps 1 and 2 where file B is partitioned into segments and random data inserted between the segments. (4) Instead of inserting random data segments, swap segments to create a permutation of the segments. The permutation may be determined by the password used in step 2.

> Until now, the US government's default position has been: If you can't keep data secret, at least hide it on one of 24,000 federal Websites, preferably in an incompatible or obsolete format.
>
> —*Wired*, July 2009.

Resources for Computer Security

For resources and help in computer security, the best place to turn to is the Internet, specifically, the Web. There are Web sites that provide historical information, discuss recent developments and threats, educate computer

users, and offer tools and techniques for protection. It is very common to find in many Web sites security news and warnings such as the one quoted here (from 20 January 2010):

A new vulnerability has been uncovered that affects all 32-bit versions of Windows from Windows 3.11 all the way up to Windows 7. The vulnerability is an attack on the Virtual DOS Machine introduced into Windows Operating Systems in 1993 to run 16-bit applications. The vulnerability was discovered by a member of Google's security team,....

While a patch has not yet been issued by Microsoft, Windows users have a couple of options to seal off this security hole. Administrators of machines running Windows 2003 and newer can edit the Group Policy of a machine to disallow use of 16-bit applications. To do this,....

However, the Word Wide Web also offers resources for hackers. Source code for various types of malicious programs, "success" stories of hackers, and information on weaknesses discovered in various operating systems, servers, and network software are available for the taking. Following is a short list of some "good" sites that offer reliable information and user education. In particular, any software downloaded from these resources stands a good chance of being uncontaminated.

- Perhaps the best overall site is the computer emergency response team, located at `www.cert.org`. This active organization, founded in 1988, is part of the software engineering institute of Carnegie-Mellon University, that receives reports from affected users and network administrators, and is often the first to distribute information on new threats.

- The system administration, networking, and security (SANS), whose mission is to help network administrators with certification, recent news, and training (`www.sans.org`). The conferences on network security it organizes are highly respected.

- COAST—computer operations, audit, and security technology—is a multi project, multiple investigator laboratory in computer security research in the Computer Sciences Department at Purdue University. It functions with close ties to researchers and engineers in major companies and government agencies. This organization is located at `www.cerias.purdue.edu/coast`.

- Counterpane Internet Security, located at `bt.counterpane.com`, is a company that specializes in all aspects of Internet security. It was founded by the well-known security expert Bruce Schneier. The company provides sophisticated surveillance technology and the services of highly trained experts to help network users stay ahead of today's software vulnerabilities, malicious insiders, and attackers from the outside.

- RSA Security, at `http://www.rsa.com/` specializes in cryptography. The company develops new encryption methods and helps organizations protect private information and manage the identities of the people and applications accessing and exchanging that information.

- Some hacker sites (those tend to be either useless or short lived) are the hacker quarterly (`http://www.2600.com/`), the chaos computer club (`http://www.ccc.de/`), and (`http://www.hackernetwork.com/`).

- A useful site with many virus descriptions, statistics, and a virus glossary is [f-secure 05].

- [Webopedia 04] is a useful Web site that describes many Internet security issues.

- [attrition 04] is a Web site maintained by volunteers and dedicated to Internet security. It collects information on many types of attacks, weaknesses, and errors in books on computer security. (This author hopes not to see this book listed in the attrition site.)

- Dr. Richard Ford maintains the website [malware 10] with help, links and FAQs about malware.

- The various Internet search engines always find useful sites. Search under "computer security," "network security," "internet security," or "hacker." For specific threats or to learn more about specific topics, try "Windows security," "virus," "UNIX security," or other key phrases. Much information (in fact, too much) can be had by subscribing to various mailing lists. Search under "security mailing list."

- Needless to say, because of the importance of this topic, there is a huge number of books, in all areas of security, and at all levels. A quick search at `amazon.com` returns more than 12,000 titles for computer security and more than 5,200 for network security (although most of those titles discuss security as a side topic, some are stories of hackers, and many are fiction).

The following is a list of a few popular books:

Security in Computing, (4th ed.), Charles P. Pfleeger and Shari L. Pfleeger, Prentice-Hall, Englewood Cliffs, NJ, 2006.
Exploiting Software: How to Break Code, Greg Hoglund and Gary McGraw, Addison-Wesley Professional, 2004.
Beyond Fear, Bruce Schneier, Copernicus Books, 2003.
Cryptography and Network Security: Principles and Practice (5th ed.), W. Stallings, Prentice-Hall, Englewood Cliffs, NJ, 2011.
Network Security Essentials (2nd ed.), William Stallings, Prentice-Hall, Englewood Cliffs, NJ, 2002.
Computer Security: Art and Science, Matt Bishop, Addison-Wesley Professional, 2002.
Network Security: Private Communication in a Public World, (2nd ed.), Charlie Kaufman, et al, Prentice-Hall, Englewood Cliffs, NJ, 2002.
Network Security: A Beginner's Guide, (2nd ed.), Eric Maiwald, McGraw-Hill Osborne Media, Berkeley, CA, 2003.
Computers Under Attack: Intruders, Worms, and Viruses, Peter J. Denning, ACM Press, New York, N.Y., 1990.

An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12. A 290-page book in PDF format, available online at [NIST Handbook 04].
Applied Cryptography: Protocols, Algorithms, and Source Code in C, Bruce Schneier, John Wiley; (2nd revised ed.), 1996.
Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses, Tom Liston, Prentice Hall, (2nd ed.) 2007.
Security+ Guide to Network Security Fundamentals, Mark Ciampa, Course Technology, (3rd ed.), 2008.

The following books concentrate on computer viruses.

Viruses Revealed, David Harley et al., Osborne/McGraw-Hill, Berkeley, CA, 2001.
Robert Slade's Guide to Computer Viruses, (2nd ed.), Robert M. Slade, Springer-Verlag, 1996.
Dr. Solomon's Virus Encyclopedia, Alan Solomon S&S International, 1995.
A Short Course on Computer Viruses, (2nd ed.), Frederick B. Cohen, New York, NY, John Wiley, 1994.
PC Security and Virus Protection Handbook, Pamela Kane, M&T Books, 1994.
A Pathology of Computer Viruses, David Ferbrache, Springer-Verlag, 1992.
Computer Virus Handbook, Harold J. Highland, Elsevier, 1990 (a little outdated).
Rogue Programs: Viruses, Worms, and Trojans, Lance Hoffman (ed.) Van Nostrand Reinhold, 1990.

In addition to books, extensive literature on computer security is available online. As an example, the NSA has a number of documents on computer security at [NSA-SEC 05].

Last word: The best line of defense against all types of computer security is education and the use of technology, combined with good old common sense.

Computer security is not a joke.
—Ian Witten

1
Physical Security

What normally comes to mind, when hearing about or discussing computer security, is either viruses or some of the many security issues that have to do with networks, such as loss of privacy, identity theft, or how to secure sensitive data sent on a network. Computer security, however, is a vast discipline that also includes mundane topics such as how to physically protect computer equipment and secure it against fire, theft, or flood. This chapter is a short discussion of various topics that have to do with physical security.

1.1 Side-Channel Attacks

In order to whet the reader's appetite we start with a new, exotic area of physical threats termed *side-channel attacks*. Today it is easy to locate the many references for this area, so we only mention three. Reference [SDattacks 10] maintains a listing of side-channel attack related publications and patents, [Bar-El 10] is a summary of the field, and [Shamir and Tromer 04] discuss several aspects of this topic.

A sensitive, secret computer installation may be made very secure. It may be surrounded by high electrified fences, employ a small army of guards, be protected by powerful firewalls complemented by watchful system programmers working three shifts, and run virus detection software continuously. Yet, it is possible to spy on such an installation "from the side" by capturing and listening to information that is continuously and unintentionally leaked by electronic devices inside. The basis of this approach is the well-known fact that people are nosy and machines are noisy.

First, a bit of history. One of the earliest side-channel attacks took place in 1956 when Britain's military intelligence (MI5) executed operation

D. Salomon, *Elements of Computer Security*, Undergraduate Topics in Computer Science,
DOI 10.1007/978-0-85729-006-9_1, © Springer-Verlag London Limited 2010

Researchers in this field feel that acoustic emanations are important and should be studied and fully understood, because it is harder to stop sound than to absorb electromagnetic waves. A common cold-war spying technique was to listen to a conversation in a closed room by directing a laser beam at a window and measuring its reflection from the glass pane that vibrates because of the sound waves inside.

An important class of side-channel attacks is the so-called *timing attacks*. A timing attack uses the fact that many important computational procedures take an amount of time that depends on the input. Thus, by measuring the time it takes to complete a procedure, a spy can learn something about the input to the procedure. An important example is the RSA encryption algorithm (see document on cryptography in the book's Web site). Part of this algorithm computes an expression of the form a^b where b is the encryption key. A simple method to compute an exponentiation is to multiply a by itself $b-1$ times, so measuring the time it takes to compute a^b may give a spy an idea of the size of b and thus help in breaking a code. For a reference on timing attacks, see [Boneh and Brumley 04].

The idea of a side-channel attack is not limited to emanations from the CPU. The next section discusses an application to keystrokes, and there have also been attempts to exploit the sounds made by certain types of printers to reconstruct the information being printed. For a reference, see [Kuhn 04].

> It has long been a dream of cryptographers to construct a perfect machine... The development in the last twenty years of electronic machines that accumulate data, or "remember" sequences of numbers or letters, may mean that this dream has already been fulfilled. If so, it will be the nightmare to end all nightmares for the world's cryptanalysts. In fact, the people who live in the vicinity of the National Security Agency think that there already are too many cipher and decoding machines in existence. The electronic equipment plays havoc with their television reception.
>
> —From [Moore and Waller 65].

1.1.1 Acoustic Keyboard Eavesdropping

Chapter 9 mentions keystroke loggers (or keystroke recorders) among other examples of spyware. A keystroke logger is a program that records every keystroke the user makes, and stores this data or transmits it to its owner (the spy). A similar concept is a screen capture, a program that periodically takes a snapshot of the monitor screen and saves it or transmits it outside. There are programs that identify and delete spyware, but spying on a computer can also be done physically. A crude idea is to try to spy on a computer user by looking behind their shoulder, but a more practical, more sophisticated technique is to install a miniature radio transmitter inside a keyboard, to transmit keystrokes to a nearby spy (see Exercise Intro.3). Such a transmitter is a physical threat and cannot be detected by spyware-removal software.

An even more sophisticated spying technique records keystrokes by listening to the sounds that individual keys make when pressed. Old timers in the computing field may remember that pressing a key on an old keyboard

often resulted in two or more copies of the key read from the keyboard due to bouncing of the keys. In a modern keyboard, the keys are placed on top of a plastic sheet and different areas of this sheet vibrate differently (and therefore create different air vibrations, sounds) when a key is pressed. Thus, striking different keys generates different sounds (also the timing of keys varies, an A may take the keyboard slightly longer to produce than a B). The ear is not sensitive enough to hear the differences between sounds generated by different keys, but a good quality microphone is.

The idea of acoustic keyboard eavesdropping is for a spy to hide a microphone as close as possible to a keyboard, to record the sound made by the keys when pressed, to digitize the sound, and to send the audio samples to a computer program controlled by the spy. Experiments have demonstrated that a sensitive parabolic microphone can record keyboard sounds reliably from distances of up to 50 feet (about 17 meters) from the keyboard even in the presence of background noise.

Once the program learns to distinguish the individual sounds, it has to be trained so it can tell which key produces a given sound. In principle, the spy has to use another method, such as a keystroke logger, to capture many keystrokes, then feed the (ASCII codes of the) keys and the corresponding sounds to the program. In practice, however, it has been discovered that keyboards of the same make and model produce very similar sounds. Once the spy knows the kind of keyboard used by the victim, he may train his program on a keyboard of the same type, then feed it the sounds created by the poor victim's keyboard. If the program can recognize, say, 80% of the keystrokes of that keyboard, the spy can use his intelligence to guess the remaining keystrokes and employ this information to train the program further.

◇ **Exercise 1.1:** Is it enough for a spy to detect 80% of a password?

Currently, such spying is exotic and (we hope) rare, but it is a dangerous development in the field of computer security because it is a physical threat and it cannot be recognized and blocked by software. Future developments may bring this type of spying to the attention (and the price range) of many would-be eavesdroppers, with unforeseen (and perhaps disastrous) consequences. A spy can often get to within 50 feet of his target's house by parking a car in the street, renting a room in a nearby house or adjacent apartment, or planting the microphone in a plant in the backyard. (Many front- and backyards have low-voltage lines to light the perimeter of the house at night, and this electricity may be tapped into to power the microphone.) In a place of work it may be easy to install a microphone in a desk next to the victim's desk or in an office adjacent to the victim's office, and such spying may be extremely difficult to detect.

At present it seems that computer hackers and criminals are not aware of this threat and continue to break into computers by means of viruses and by breaking firewalls. Admittedly, someone who wants to control a vast

number of computers cannot use this method, but it may prove attractive to certain spies, especially those who currently install and use spyware. A list of potential spyware users can be found at the beginning of Chapter 9.

This vulnerability of keyboards can be eliminated by redesigning keyboards such that all keys would generate the same sound or very similar sounds. The technique of acoustic eavesdropping, however, is not limited to keyboards.

For a detailed reference on this approach, see [Asonov and Agrawal 04].

> The idea of eavesdropping on a typewriter keyboard, mentioned as coming from Dmitri Asonov ("Acoustic Keyboard Eavesdropping"), was anticipated decades ago by the National Security Agency. The radio waves created each time a key is struck on the keyboard of a teletypewriter or an electrical cipher machine differ from letter to letter. These can be detected and discriminated, thereby enabling the eavesdropper to understand the message before it is encrypted for transmission. The technique is codenamed Tempest (see the 1972 paper [nsa.tempest 10]).
>
> —David Kahn, *The New York Times*, 23 January 2005.

1.2 Physical Threats

▪ Surges in electrical power, often caused by lightning, may burn out electronic components in the computer. Solution: Use an uninterruptible power supply (UPS). Such a device regulates the incoming voltage and produces a clean output signal. If the voltage gets high, the UPS trims it. If the voltage drops, the UPS uses its internal battery to supply the computer with power for a few minutes, enough to either turn off the computer (typical for a home computer) or to start a generator (typical in a large installation, especially an installation that has to operate continuously, such as a hospital or a telephone exchange).

◇ **Exercise 1.2:** What can go wrong if power to the computer is suddenly turned off?

▪ Physical security of computer facilities. We constantly hear of damage done by computer viruses and other malicious programs, but the best virus protection software cannot prevent a home personal computer from being stolen (although it can help in its recovery, see Section 1.3). Thus, computer security starts by protecting the facilities that house computers and computer data. This problem is especially acute in industry. Many a company can be wiped out if its computers and especially if its sensitive data are stolen or damaged. Damage can be intentional, inflicted by a criminal or a disgruntled employee, or accidental, caused by fire, power failure, or broken air conditioning.

The solution is to physically protect this sensitive asset. A home should have an alarm system and power to the computer should pass through an

uninterrupted power supply (UPS). A commercial entity should have a secure computer facility, with controlled access, heavy doors, card-operated locks, security cameras, and an automatic fire system (using gas instead of water if possible). In addition, special care should be given to unconventional entry points, such as attics and air conditioning ducts. A modern office building often has a large attic above the ceiling of each floor. This space is handy for stringing wires inside the building, but can be used by a person to crawl into an otherwise secure room. A wide air-conditioning duct can be used for the same purpose and should therefore be secured by a heavy screen.

Other items, such as emergency lights, fireproof containers (for storing disks and papers), and proper training of personnel, are also important.

- Traditionally, fire is suppressed by water, but this causes damage to structures and equipment that may exceed the damage caused by the fire. For a while, a gas known as halon was used to extinguish fires in sensitive environments, but this was later found to deplete the ozone layer in the atmosphere. Modern replacements for water and halon are certain fluids that look like water but evaporate quickly. An example is the chemical NOVEC 1230 made by 3M [3M 04]. It can be used to protect delicate objects and electronic equipment from fire without damaging the items themselves.

Heat is only one type of damage caused by a fire. Smoke and soot particles resulting from a fire can compound the damage by contaminating removable disks, ruining the delicate mechanisms of magnetic disk and optical drives, and dirtying the electrical connections in keyboards. A case in point is the explosive eruption of Mount St. Helens in 1980, whose volcanic ash damaged computer equipment at large distances from the mountain.

Case study. The Pentagon is the United States' military headquarters. Located near Washington, D.C., the Pentagon has many computers and extensive networking equipment. Back in the 1970s, someone forgot to turn off a 300-watt light bulb in a vault where computer tapes were stored. The small bulb generated heat that had nowhere to go and started heating up the room and smoldering the ceiling. When the door was finally opened, the fresh air rushing into the room turned the high temperature to fire. The fire spread to several adjoining rooms and caused damage in the millions of dollars.

- Theft should especially be mentioned, because computers and mobile devices are getting smaller and lightweight all the time and are therefore easy to steal. There is a school of thought in law enforcement that says that if you want to catch a thief, you should think like one. We hear about sophisticated hackers who write viruses and spyware, but an unsophisticated thief can cause much harm by stealing computers, because all the data in the computer disappears with the computer. Such data may be slow and expensive to replace and may also be private and sensitive. We should always keep in mind the simple, straightforward brute-force approach that computer thieves often adopt. Simply sneak in, take what you find, and get away quickly.

When a mobile device is stolen, the thief (or whoever bought the device from him) eventually wants to turn it on and use it. Thus, special applications

for remote lock and wipe have been developed for mobile devices. Once such an application is installed in a mobile device, its owner can *remotely* erase all the data on the device (or at least lock it with a password). Once a computer is stolen, the thief can take out the drive and read it from another computer, so the solution in this case is to encrypt sensitive data.

▪ A facility using electronic locks and keys or other physical-identification devices to restrict access to certain areas should consider the following problem, known as piggybacking or tailgating. An intruder may wait at a locked door, perhaps holding disks, paper or other innocuous-looking stuff with both hands, trying to look legitimate and waiting for the door to open. When someone comes out of the restricted room, the intruder slips in while the door is still open. A guard can prevent such a problem, but this is an expensive solution. An alternative is to install a turnstile, or even a mantrap. The latter device is a two-door entrance where a person has to pass through two doors in order to enter or exit a restricted room. To enter, a person must pass through door A into a small space, the mantrap, and then open door B to the restricted room. The point is that door B will not open until door A is fully closed.

Figure 1.1 shows a possible design for a secure and safe computer installation. The operators' room (area 2) has a mantrap-controlled access to the outside and to the other rooms. The processor room (area 4) is easy to keep clean because access to it is through the network router room. Area 5, the disk drives room, is kept even cleaner because access to it is through area 4. This is important because those drives have many moving parts. A lazy Susan (the circle) provides access to removable disks and DVDs from their storage (area 6). Area 7 is a storage room for papers, forms, and spare parts. It also serves as temporary trash storage and houses the all-important shredders. The printers (and perhaps also binders, copiers, and collators), with their noise and paper particles, are insulated in area 8. The only area that contributes to weak security is the loading dock (area 9), because it has another outside access. However, access to the outside is important in cases of emergency, so this outside door is another example of the tradeoff between security and convenience.

◇ **Exercise 1.3:** Basements are easier to protect against unwanted entry. With this in mind, why is a basement a bad choice for a computer facility?

▪ Magnetic fields. Hard disks are magnetic storage. Data is recorded in small magnetic dots on the disk and is therefore sensitive to magnetic fields. (In contrast, CDs and DVDs are optical storage and are not sensitive to magnetism.) Experience shows that it is not enough to place a small magnet in your pocket and walk into a computer room, hoping to harm computers and data. Stronger fields are needed in order to adversely affect magnetic storage, but such fields exist. An old story, from the 1960s, tells of a computer tape storage room where tapes were always going bad. It took months until someone observed that the trouble affected only the tapes stored on the lower shelves. It turned out that the floor was cleaned periodically with a powerful vacuum cleaner that affected only those tapes.

from a terrible disaster (fire, earthquake, flood, terrorism, computer virus) in a short period of time. [Maiwald and Sieglein 02] is one of many references that discuss such a plan and how to implement it.

> An armed society is a polite society. Manners are good when one may have to back up his acts with his life.
>
> —Robert A. Heinlein.

- Hard copy. The media has been touting the paperless office for several decades, but we still use paper. In fact, we use it more and more. Security workers know that criminals often collect papers thrown away carelessly and scrutinize them for sensitive information such as credit card numbers and passwords to computer accounts. This behavior is part of the general practice of dumpster diving. The solution is to shred sensitive documents, and even not-so-sensitive papers. See Chapter 10 and especially Section 10.2 for more on shredding and related topics.

- Spying. Spyware, an important threat, is the topic of Chapter 9, but spying can also be done in the traditional way, by person. You, the reader probably haven't walked around your neighbor's or your ex-spouse's house at night, trying to look in windows and catch a glimpse of a computer screen with passwords, bank logins, or forbidden pictures, but others do that all the time. Industrial espionage and spying conducted by governments are very real. A commercial organization often decides that spying on its competitors is the only way for it to stay active, healthy, and competitive. Spying on computer users can be done by looking over someone's shoulder, peeping through a keyhole, setting a small security camera, planting spyware in a computer, and also in other ways, as described in Section 1.1.

- Data integrity. Digital data consists of bits. Text, images, sound, and movies can be digitized and converted to strings of zeros and ones. When data is stored, in memory or on a storage device, or when it is transmitted over a communication line, bits may get corrupted. Keeping each bit at its original value is referred to as data integrity and it is an aspect of computer security.

Before we look at solutions, it is important to discuss the significance of this problem (see also exercise 2.11). Text is represented in a text file as individual characters, each coded in ASCII (8 bits) or Unicode (16 bits). Thus, each bad bit in a text file changes one character of text to another character. Quite often, this is not a problem. If the file is the text of a book, a personal letter, or someone's homework, one bad character (or even a few bad characters) isn't considered a serious problem. If, however, the file is a legal, medical, or commercial document, the change of even one character may change the meaning of a sentence and may significantly alter the meaning of a paragraph or even the entire document.

An image consists of small dots called pixels (from picture element). Each pixel is represented as a number, the code of the pixel's color. A bad

bit therefore corrupts the color of one pixel. If the bit is one of the least significant (i.e., it is on the right-hand side of the number) the change in color may be insignificant. Even if the color of one pixel is changed significantly, a viewer may not notice it, because the entire image may have millions of pixels. Thus, in general, a few bad bits in an image do not pose a problem, but there are exceptions. An X-ray image, an image created by a telescope, or an image taken by a spy satellite may be examined carefully by experts who may draw important conclusions from the colors of individual pixels. Such images must therefore keep their integrity when transmitted or stored. A movie is a string of images, so one bad bit affects one pixel in one frame of the movie. It may be noticeable as a momentary flicker and may not be a serious problem. An audio file consists of audio samples, each a number that relates to the intensity of the sound at a certain moment. There are typically about 44,000 audio samples for each second of sound, so one bad sample, caused by one bad bit, may be audible, but may not detract from the enjoyment of listening to music or prevent a listener from understanding spoken text.

The conclusion is that the amount of data integrity that's required depends on the data in question and ranges from no integrity at all (for unimportant data or data that can easily be reacquired) to maximum integrity (for crucial data that cannot be replaced). Data integrity is provided by error-detecting and error-correcting (in general, error-control) codes, and the basic principles of this discipline are described in many texts.

- The three principles of security management. Three simple principles can significantly reduce the security threats posed by employees in a large computer installation. Perhaps the most important of the three is the separation of duties. This principle, employed by many spy, anti-spy, and secret organizations, says that an employee should be provided only with the knowledge and data that are absolutely necessary for the performance of their duties. What an employee does not know, cannot be disclosed by him or leaked to others. The second principle is to rotate employees periodically. An employee should be assigned from time to time to different shifts, different work partners, and different jobs. Also, regular annual vacations should always be mandatory for those in security-related positions.

Every time a person is switched to another job or task, they have to be retrained, which is why this principle adversely affects the overall efficiency of the organization. Also, when an employee is switched from task A to task B, they have to be given the data and knowledge associated with both tasks, which contradicts the principle of separation of duties. In spite of this, it is important to rotate employees because a person left too long in the same position may get bored with it and a bored security worker is a potentially

Some software makers offer theft tracking or tracing software combined with a service that can help in tracking any stolen computer, not just a laptop. You purchase the software, install it, and give it an email address to report to. Every time the computer is started or is reset, it sends a stealth message with the computer's current IP number to that address. If the computer is stolen, there is an excellent chance that the thief would connect to the Internet, so its new IP number will be sent to that email address. Both the software maker and the police are then notified and try to locate the computer from its IP number.

◇ **Exercise 1.4:** How is such tracking done?

The whole point about such software is that it somehow has to be embedded "deep" in the computer, such that formatting the hard drive (even a low-level formatting) or reinstalling the operating system would not erase the software. Current examples of such security software for both Windows and the Macintosh platforms are [PCPhoneHome 04], [sweetcocoa 05], and [absolute 05]. Because the security software is on the hard drive, replacing the drive removes this protection.

[business.com 04] has a list of various security devices and software for computers. The PDF document at `http://www.rufy.com/laptop.pdf` offers useful information on protecting a Macintosh.

A good idea is to encrypt all sensitive software on a laptop, just in case.

The following simple precautions go a long way in securing your computer so it remains yours:

- With an electric engraving pen, write your name and either your permanent email or telephone number (but not your social security number or address) on the computer case. For a large computer, write it in several places. The thief knows from experience that selling such a marked machine takes time, so they may try to steal someone else's computer. A car is sometimes stolen for its parts, but computer parts are generally inexpensive enough to deter a thief from the effort of stealing, taking the machine apart, and selling individual parts.

- A laptop can be hidden when traveling if it is carried in a nonstandard case, especially one with a distinctive color that makes it noticeable.

- When traveling by car, place the laptop on the floor in the passenger side and throw a rag or a towel over it. This place has the most comfortable temperature in the car, and the rag may camouflage the laptop so it does not attract the attention of passers by. Generally, a computer should not be left in a car for a long period because cars tend to get hot even when the outside temperature is not high.

- When flying, take the laptop with you. Never check it in as luggage. There is much information on the Internet about airport scams where a team of two or more criminals confuse you at the x-ray checkpoint and end up with your bag(s).