# Undergraduate Topics in Computer Science

Undergraduate Topics in Computer Science (UTiCS) delivers high-quality instructional content for undergraduates studying in all areas of computing and information science. From core foundational and theoretical material to final-year topics and applications, UTiCS books take a fresh, concise, and modern approach and are ideal for self-study or for a one- or two-semester course. The texts are all authored by established experts in their fields, reviewed by an international advisory board, and contain numerous examples and problems. Many include fully worked solutions.

For further volumes:
http://www.springer.com/series/7592

David Salomon

# Elements of Computer Security

Springer

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

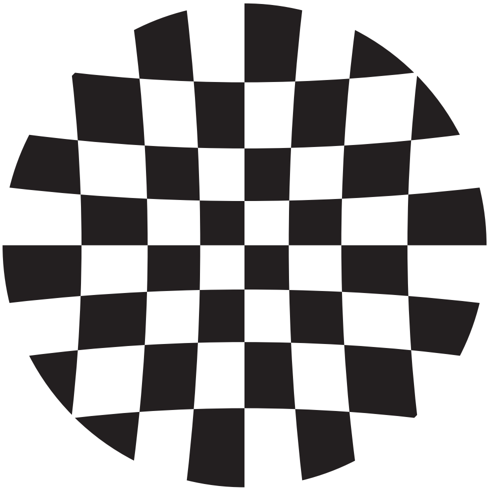
British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Control Number: 2010933120

Printed on acid-free paper.

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

*To the many anonymous cybercriminals and hackers,*
*without whom this book would not have been necessary.*



Now you have given me a security worth
having; and I shall proceed with courage.
—Jane Austen, *Northanger Abbey* (1803)

# Preface

## The Security Challenge: A Global Context

On 21 November 2008, the conficker worm, one of the worst examples of malware in recent years, was first detected. As these words are being written, in February 2010, the worm is still active and is infecting computers worldwide. Various estimates of the number of affected computers range from nine million to 15 million! Encouraged by this "success," the anonymous originator of this worm released four more variants, the last of which was discovered in April 2009. When this malicious piece of software invades a computer, it tries to propagate itself into other computers by exploiting a vulnerability in a network service, a component of the popular Windows operating system. Specifically, the worm looks for computers that do not have recent security updates installed, that employ weak passwords, or that use removable storage such as external disk drives or flash memories. Conficker fully controls an infected computer, but no specific damage has so far been reported.

The conficker worm is just one of many instances of cyber attacks that have been plaguing computer users since the 1980s. Traditionally, such attacks were aimed at computers, but computer security experts predict that future cyber security threats will concentrate more on smart telephones and other mobile devices. Such devices have become so sophisticated and popular in the last few years, that many users claim that they cannot live without them. They are used for online commerce, banking transactions, and sending and receiving sensitive personal information. Malware for the Blackberry and other mobile devices first appeared in 2009 and is likely to become more and more prevalent in the near future.

The conficker worm and the many other threats, attacks, and cyber crimes described in this book explain your interest in it. Computer security has become one of the most important areas in the entire discipline of computing. Computers today are used not only in the home and office, but in a multitude of crucial and sensitive applications. Computers control long distance telephone conversations, the flow of information on the Internet, the distribution of electrical power to cities, and they monitor the operations of nuclear power plants and the performance of space satellites, to name just a few important applications.

We have become used to these small, quiet machines that permeate and enrich our lives and we take them for granted. It is only when they don't perform their tasks, that we suddenly become aware that something has gone wrong. Considering the complexity of today's computers and their functions, and considering especially the physical hazards that abound in the world, it is a wonder that our computers function at all, yet we expect them to be reliable and we entrust them with more and more sensitive, personal, and complex assignments.

It is easy to disrupt a computer. Just brush your elbow accidentally against your desk and you might spill your cup of coffee on your computer. A power loss lasting a fraction of a second may cause a head crash of the hard disk, resulting in a complete loss of the disk drive and all its data. Carelessness on the part of operators or administrators in a large computations center can result in a costly loss of data or physical damage to the equipment. Yet all these dangers (and there are many more) pale in comparison with the many types of intentional criminal harm that we have come to expect and that we collectively associate with the term computer security.

A term closely related to computer security is computer crime. A computer crime is an incident of computer security in which a law is broken. Traditionally, computer crime has had a low profile. After all, in a computer crime there are no smoking guns, no blood-stained victims, and no getaway cars. Often, such a crime is solved just by sheer accident. In contrast, computer security is a high-visibility discipline because it affects so many people.

Experience has shown that the more sophisticated a civilization is, the more vulnerable it is to natural or man-made disruptions. A tree that fell on power lines in Ohio in August 2004 plunged 50 million people from Detroit to New York into darkness. A computer glitch on 26 December 2004 (the day this paragraph was written) caused the cancellation of 1100 flights of Comair, a subsidiary of Delta Air Lines, and similar examples abound. Our civilization depends highly on computers, which is why any disruption of our computers is at least inconvenient and at worst catastrophic.

In the past, computer security violations, such as viruses and DoS (denial of service, Section 7.5) attacks were caused by hackers, most of whom were believed to be young adults who did this for fun or enjoyed the feeling of power and notoriety. However, this situation has now changed completely. Security experts are warning that future attacks on computers may be planned and funded by terrorists (better called cyberterrorists) and may be devastating. A powerful hurricane, a huge earthquake, or a tsunami may kill many and wreak untold havoc, but a large-scale, concerted attack on key computers may bring the economy of an entire country to its knees, even though no one may actually get killed.

The reason for such dire predictions is our experience with computer security in the last three decades. We know that a single computer virus, perhaps written and released by a teenager living in a remote town in a distant country, can propagate quickly, infect a vast number of computers within hours, and cause economic damage in the billions (of Dollars, Euros, or whatever currency is affected).

Today, computers are responsible for the distribution of electrical power and for routing telephone conversations. They store information on passenger and cargo flights, on large cash transfers between banks, and on military plans, to name just a few crucial applications. It is generally agreed that a well-organized attack that takes over several important, sensitive computers may cause at least a temporary collapse of an entire country.

What makes this kind of attack attractive to organized terrorists is that it can be carried out from the comfort of their homes. There is no need to actually go anywhere, to obtain and use dangerous nuclear or chemical materials, or to smuggle anything across international borders. The fact that we depend so much on computers and digital communications may be crucial to our future survival, and the least that we can do now is to learn as much as possible about potential threats to computers and how to defend against them.

> Virus writing is a crazy activity. People who write viruses just don't consider the consequences of their actions. At the same time, I believe in the American constitution, and the first amendment, which gives people freedom to write and to talk, so I don't have a problem in the larger sense of people discussing or studying viruses.
>
> —Peter Tippett (Symantec) in [Virus bulletin 05] May 1994 issue.

There is an ongoing debate about whether newly-discovered security holes and vulnerabilities in operating systems and communications software should be made public. Publicizing a security weakness allows users to avoid it until a patch is issued or a solution is found. On the other hand, it gives the bad guys ideas. So far, advocates of public exposure have had the upper hand, with the result that any item of news about a new computer security problem ignites a race between attackers and defenders. The following is a list of a few typical recent races:

- November 2009. Windows 7 vulnerability. Microsoft discovered a serious denial-of-service (DoS) vulnerability in the protocol that handles messages between devices on a network for its new Windows 7 operating system.

- September 2009. SMB flaw. Microsoft advised customers that attacks have been detected against a zero-day flaw affecting its FTP Service in Microsoft Internet Information Services (IIS). A new exploit code surfaced at the same time, targeting a zero-day vulnerability in Microsoft Server Message Block (SMB).

- September 2009. A flaw in the BlackBerry certificate handling may invite SMS attacks. Research In Motion (RIM) issued an advisory about a certificate handling flaw that makes it easy for an attacker to trick users into visiting a malicious website.

- April 2009. A newly discovered zero-day flaw in the popular Microsoft PowerPoint application attracts attackers. A malicious PowerPoint file is sent to an unsuspecting user. When the file is opened, the flaw allows the execution of remote code.

- March 2009. Windows kernel flaws patched. Microsoft has issued patches for eight critical vulnerabilities in the Windows kernel. These flaws pertain to several versions of Windows and Windows server. They could be remotely exploited by an attacker to gain control of a computer.

Three types of persons are involved in computer security: experts and researchers who study this field and recommend preventive measures and solutions, the general public, which suffers from the breakdown of computer security, and the (mostly anonymous) perpetrators of the various misdeeds and attacks. Most of these perpetrators are known as *hackers*, which is why this important, popular term is discussed in Appendix A.

From the dictionary

Expert: someone widely recognized as a reliable source of knowledge or skill whose judgement is accorded authority and status by the public or their peers.

Not all computer crime and attacks are perpetrated by hackers. Much harm is done by insiders, trusted employees who do it for a variety of reasons. This is the human side of computer security. The history of computer crime is riddled with stories about users who take their frustration out on the computer. They drop it on the floor, shoot it, pound it with a hammer, and even urinate on it, just to vent their feelings and frustration. Some employees strike at their machines as a way to get back at the boss, while others act out of political convictions and allow their fellow party members to sabotage equipment. However, the main reason for insider computer crime is money. An employee or a trusted consultant suddenly realize they have enough knowledge to induce a computer into printing a check, transferring money to their account, or releasing information (such as a mailing list or credit card numbers) that can later be sold, and this temptation may prove too much. Such a treacherous insider suddenly turns into a living Trojan horse, as dangerous as those discussed in Chapter 4. The best an employer can do to defend against such employees is to compartmentalize information, to make sure an employee knows only as much as he or she needs to know for their jobs. This policy is difficult to implement in practice, it adversely affects employees' morale and productivity, and it is not full proof.

We have all heard of bank robbers, but one of the most notorious bank robbers, one who kept the title "biggest computer fraud" in the Guinness Book of World Records [Guinness 04] from 1978 to 1999, was someone called Stanley Rifkin, a name most of us would have trouble recognizing. He is virtually forgotten today, perhaps because he didn't use a gun in his exploit and didn't even hack the bank's computer. He was a consultant to the now defunct Security Pacific National Bank in Los Angeles and in this capacity he learned some of the codes used by bank personnel to make large money transfers. He used this knowledge to call the employees in the wire transfer room, pretending to be Mike Hansen, a member of the bank's international department, and con them into transferring ten million dollars to a temporary account that he had previously opened. He later transferred the money to Switzerland and used it to buy diamonds that he then smuggled back to the United States. He was caught by the FBI very quickly, but only because he had bragged about his exploit to his lawyer, trusting the confidentiality of attorney-client relations. The lawyer notified the FBI and Rifkin was arrested. The final twist of this story is that the bank didn't even miss the money when notified by the FBI of the successful solution of this crime.

◇ **Exercise Pre.1:** Imagine that you are an operator of a large computer. You've been with the company for years, and you have suddenly been switched to the night shift, forcing you to sleep during the day so you rarely get to see your family. You don't want to quit, because in just a few years you'd be eligible for retirement. What can you do to improve your lot?

FBI: Why do you rob banks?
Willie Sutton: Because that's where the money is.
`http://www.fbi.gov/libref/historic/famcases/sutton/sutton.htm.`

### Computer Security: an Example

One of the largest and most sophisticated attacks by cyber criminals started in late 2009 and was discovered in January 2010. More than 75,000 computers belonging to about 2500 companies around the world (374 in the United States) have been compromised. The list of victims includes Fortune 500 companies, US local, state, and federal government agencies, energy companies, ISPs, and educational institutions.

The perpetrators lured company employees by free (infected) software and baited them into opening infected email attachments. Once compromised, a computer was searched for sensitive corporate documents, login information, IPs and URLs of friends and colleagues, and passwords. The computer was then added to a botnet (dubbed Kneber), and employed to spread its "message" to other machines. The Kneber botnet is so large that it is controlled by no fewer than 20 command and control servers worldwide (mostly in China but also in the Ukraine, Korea, Panama, and the United States). It is also possible that this "operation" is being executed and coordinated by more than one group of perpetrators,

This attack has been so widespread, successful, and sophisticated, that one security expert had this to say about it, "it is significant in its scale and in its apparent demonstration that the criminal groups' sophistication in cyberattacks is approaching that of nation states such as China and Russia."

More than half the machines infected with Kneber are also infected with a peer-to-peer bot called Waledac . It is not uncommon for a computer to be invaded by multiple strains of malware, but this case seems special because the Kneber bot seems to be controlling and watching Waledac and is also downloading Waledac to machines it has invaded. This clever behavior implies that the Kneber bot was planned, implemented, and debugged carefully by experts, and was designed not just to propagate itself and cause harm, but to also be fault tolerant and resilient to removal attempts.

# Overview and Goals

This book is intended as a starting point for those familiar with basic concepts of computers and computations who would like to extend their knowledge into the realm of computer and network security. The book is primarily a textbook for undergraduate classes on computer security. It is mostly nonmathematical and makes no attempt to be complete. The only prerequisite for understanding the material presented here is familiarity with the basic concepts of computers and computations such as (1) the organization of data in bits and bytes, (2) data structures (arrays, trees, and graphs), and (3) network concepts such as IP numbers, input/output ports, and communications protocols.

This book is an up-to-date version of the 2005 text *Foundations of Computer Security.* The material has been brought up to date, old examples of malware and threats have been replaced with new ones, and material that was judged less important was cut out.

Timing. The many phrases "at the time of this writing" found in the book refer to the period from February to June 2010, during which this book was prepared.

Special features that enhance the textbook aspect of the book are the many exercises sprinkled throughout the text (with answers available in the book's Web site), the virus timeline (Appendix C), and the Glossary. Another attractive feature is the jokes (check the index). There are no riddles.

A note on references. The text refers to many resources using notation of the form [Thompson 84] where the 2-digit number is a year. All the references are listed in the Bibliography and many are Web sites. As we all know, Web sites tend to have a frustratingly short life, so by the time this book is in your hands, some of the references may become broken links. However, given the context of a reference, an Internet search will likely locate a cached copy of the original page or a similar page. There is also the Internet wayback machine [wayback 10] where billions of old Web sites are archived. Don't give up easily.

An interesting (and, I believe, also original) feature of this book is its minimal use of the vague term "system." This word is used only (1) in connection with well-defined or commonly-used terms such as "operating system," "file system," and "notational system," (2) when it is part of names of organizations, or (3) when it is included in a quotation or in software code. Many texts use this vague term liberally, thereby confusing the reader. Sentences such as "In addition, the resulting flood may exhaust system memory, resulting in a system crash. The net result is that the system is unavailable or nonfunctional," are confusing. Instead of "system" the author should specify what is being discussed, whether it is a computer, a piece of software, a router, or something else. Here is what William Strunk [Strunk 18] has to say about this term.

System. Frequently used without need.

| | |
|---|---|
| Dayton has adopted the commission system of government | Dayton has adopted government by commission |
| The dormitory system | Dormitories |

—William Strunk Jr., *The Elements of Style.*

While I was at it, I also avoided the use of the cliché "basically," employing "essentially" or "fundamentally" instead.

On the other hand, the term "user" is a favorite in this book.

> Why is it drug addicts and computer aficionados are both called users?
> —Clifford Stoll.

## Organization and Features

- Chapter 1 is a collection of topics that have to do with the physical security of computer hardware, computer networks, and digital data. The topics discussed cover a variety of issues ranging from computer theft and static electricity on carpets to laptop security.

- Chapter 2 is the first of the chapters on rogue software (the term *malware* is often also used). The chapter is devoted to computer viruses, and it covers all the important aspects of this unusual type of software. The various types of viruses, the way viruses propagate, the damage they may inflict (their payload), and the people who write them, are among the topics covered in this chapter.

- Another type of rogue software, namely worms, is the topic of Chapter 3. Techniques for worm propagation are discussed and the historically important Internet worm is described.

- Trojan horses are the topic of Chapter 4. The discussion concentrates on the types of damage done by this type of malware and on how Trojan horses are installed on a computer. Of special interest is Section 4.3 that describes an interesting technique for bugging or rigging a compiler. A Trojan horse can be embedded inside a compiler in such a way that certain programs compiled by it will be infected with the horse, yet nothing suspicious remains in the source code of the compiler itself and even a recompilation of the compiler does not get rid of the malicious software secretly embedded in it.

- Chapter 5 is full of examples of malware. About a dozen examples of viruses, worms, and Trojans are discussed and described in detail. Many (shorter) descriptions can be found in Appendix C.

- The important topics of preventing malware and defending against it make up Chapter 6. Among the methods discussed in this chapter are backing up files, anti-virus software and its applications, activity monitors, vaccines, and file permissions. The interesting topic of hoaxes is also included here.

- Network security is the topic of Chapters 7 through 10. Chapter 7 starts this important subject with a detailed discussion of important threats that relate to networks. Topics such as port scanning, spoofing, password cracking, firewalls, and denial of service (DoS) are described and analyzed.

- Chapter 8 concentrates on authentication. Both local and remote methods for authentication are included. Of special interest are the biometric authentication techniques of Section 8.2.

- Spyware, the topic of Chapter 9, is a relatively new threat and is already serious enough to merit its own discussion and methods of defense. Material on spyware and terrorism and on remote reporting is also included, as are several varieties of spyware such as adware and researchware.

- Chapter 10 tries to familiarize the reader with the growing crime of identity theft. The topic of phishing is also covered in detail, including examples.

- Privacy and trust in the online world are the topics of Chapter 11. General privacy concerns as well as children's privacy and safety are discussed, together with how to generate trust in visitors to Web sites (and how to keep it). Notice that privacy issues are also discussed in Section 1.5.

- Appendix A discusses the definition, meaning, and history of the term hacker. The appendix also attempts to classify hackers, their techniques, software "products," and motivation.

- Appendix B introduces "l33t Speak" (pronounced "leet"), a language or a notational system widely used by hackers.

- Appendix C is a detailed virus timeline. The history of viruses and other types of rogue software is traced from its infancy in the late 1940s to the present day (early 2010), stressing "firsts" such as the first stealth virus and the first boot sector infector.

## Web and Supplemental Resources

There currently are many useful resources (in the form of books, articles, and websites) for computer security, some of which are listed at the end of the Introduction.

The book's Web site, including a document on cryptography, the answers to the exercises, an errata list, and BibTEX information, is part of the author's Web site, located at `http://www.DavidSalomon.name/`. The author's email address is `dsalomon@csun.edu`, but an alternative address, for emergencies, is ⟨*anyname*⟩`@DavidSalomon.name`.

**Cryptography Introduction**. Cryptography solves many security problems. Without cryptography, the main task of a hacker would be to break into a computer, locate sensitive data, and copy it. Alternatively, the hacker may intercept data sent between computers, analyze it, and help himself to any important or useful “nuggets.” Encrypting sensitive data complicates these tasks, because in addition to obtaining the data, the wrongdoer also has to decrypt it. Cryptography is therefore a very useful tool in the hands of security workers, but it is not a panacea. Even the strongest cryptographic methods cannot prevent a virus from damaging data or deleting files. Similarly, DoS attacks are possible even in environments where all data is encrypted.

Because of the importance of cryptography, a document containing an introduction to this topic has been prepared and is available at the book’s Web site. It discusses the principles and concepts behind the many encryption algorithms used by modern cryptography. It starts with the concepts of cipher and code and follows this with examples of old monoalphabetic and polyalphabetic ciphers. The important method of the one-time pad and the problem of key distribution are discussed next. The chapter continues with the principles of public-key cryptography, RSA encryption, and the all-important secure socket layer (SSL) protocol.

More material on cryptography, including descriptions of algorithms and examples, can be found in [Salomon 03] and in the many excellent texts on cryptography and data hiding that are currently available.

## Acknowledgement

I would like to acknowledge the help provided by my editor, Wayne Wheeler, by Francesca Warren, the copyeditor, and by Giovanni Motta. They went over the final manuscript and made many useful and productive comments, corrections, and suggestions.

**Disclaimer**. This is not a fact-free book. A book like this could not have been written without the help of many people, but this book was! As a result, the author is the only one responsible for both the useful material in the book and for the errors that I hope will not be discovered in the future.

**Disclaimer**. Certain services, software products and Web sites are mentioned in this book. This author does not guarantee the usefulness, quality, or accuracy of claims made by these sites and organizations.

Lakeside, California David Salomon

> Tis not my study or intent to compose neatly. . . but to express myself readily & plainly as it happens. So that as a River runs sometimes precipitate and swift, then dull and slow; now direct, then winding; now deep, then shallow; now muddy, then clear; now broad, then narrow; doth my style flow; now serious, then light; now comical, then satirical; now more elaborate, then remiss, as the present subject required, or as at the time I was affected.
>
> —Robert Burton, *The Anatomy of Melancholy,* 1621

# 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.

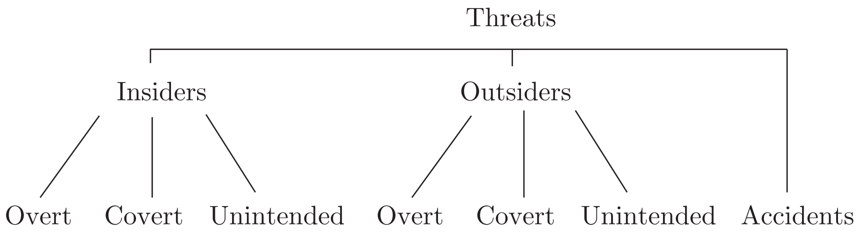


Figure Intro.1: Seven Classes of Computer Security and Crime.

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.

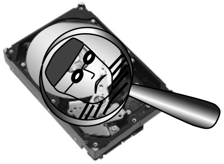
- Finally, there are accidents. They always happen, not just in the computing field. Accidents are caused either by nature, such as earthquake or flood, or indirectly by humans (see the “insiders unintended” class).

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.

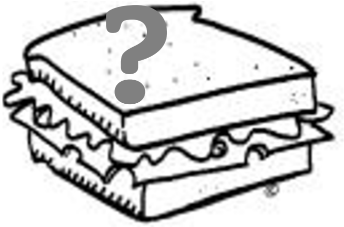
10: Technology is not a panacea.

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."

We simply have to live with the fact that technology is not the answer to all our problems, and that computers, wizards that they are, are not intelligent enough to defend themselves against wrongdoers. Security, especially computer security, must use policy in addition to technology. Security is a combination of technology and how it is used. Pest control professionals always disclaim “we do not exterminate pests, we just control them.” Similarly, technology cannot solve the security problem, it can only keep it under control. We should look at security as a journey, not a destination.

◇ **Exercise Intro.5:** There is nothing magical about ten, so try to come up with another law in the spirit of the above ten. (See also exercise 11.4.)

The discussion here shows that the task of achieving computer security involves common sense, encryption, legal means, various technical means such as passwords, parity bits, CRCs, and checksums, and lastly, keeping secrets. This book discusses the various types of threats to computers and networks and many technical defenses. This is followed by a discussion of the principles of cryptography and current encryption methods and protocols. Common sense is also mentioned several times but this author isn’t going to try to discuss it in any detail or to teach it. Finally, the next paragraph discusses secrets.

Some security problems can be solved or avoided by keeping certain things secret, but experience indicates that keeping secrets is only a temporary solution, because we can tell people all kinds of secrets, but we cannot make them forget the secrets when they move, quit, are laid off, or get promoted. The physical analog is different. When we secure something with a lock and key, we can remove or replace the lock as needed. With human beings, though, secrets are not safe. A secret may be divulged accidentally or intentionally, and on the other hand it cannot be expunged from someone’s memory even by the strictest order issued by a supreme authority. If at all possible, it is preferable to maintain security by technical means rather than by keeping secrets.

> The secret of teaching is to appear to have known all your life what you just learned this morning.
>
> —Anonymous.

### How to Hide Data

The predecessor of this book, *Foundations of Computer Security*, appeared in 1995 and generated considerable interest. In particular, several readers sent me the following question: “I have a small, sensitive data file that I want to hide in my computer, while still having it ready for use at a short notice. I feel that just encrypting the file isn’t secure enough. Can you recommend a safe way to hide it?” Here is what I came up with. Given a data file $A$, consider the following steps:

1. Compress $A$. The result is a file $B$ that is small and also seems random. This has two advantages (1) the remaining steps encrypt and hide

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