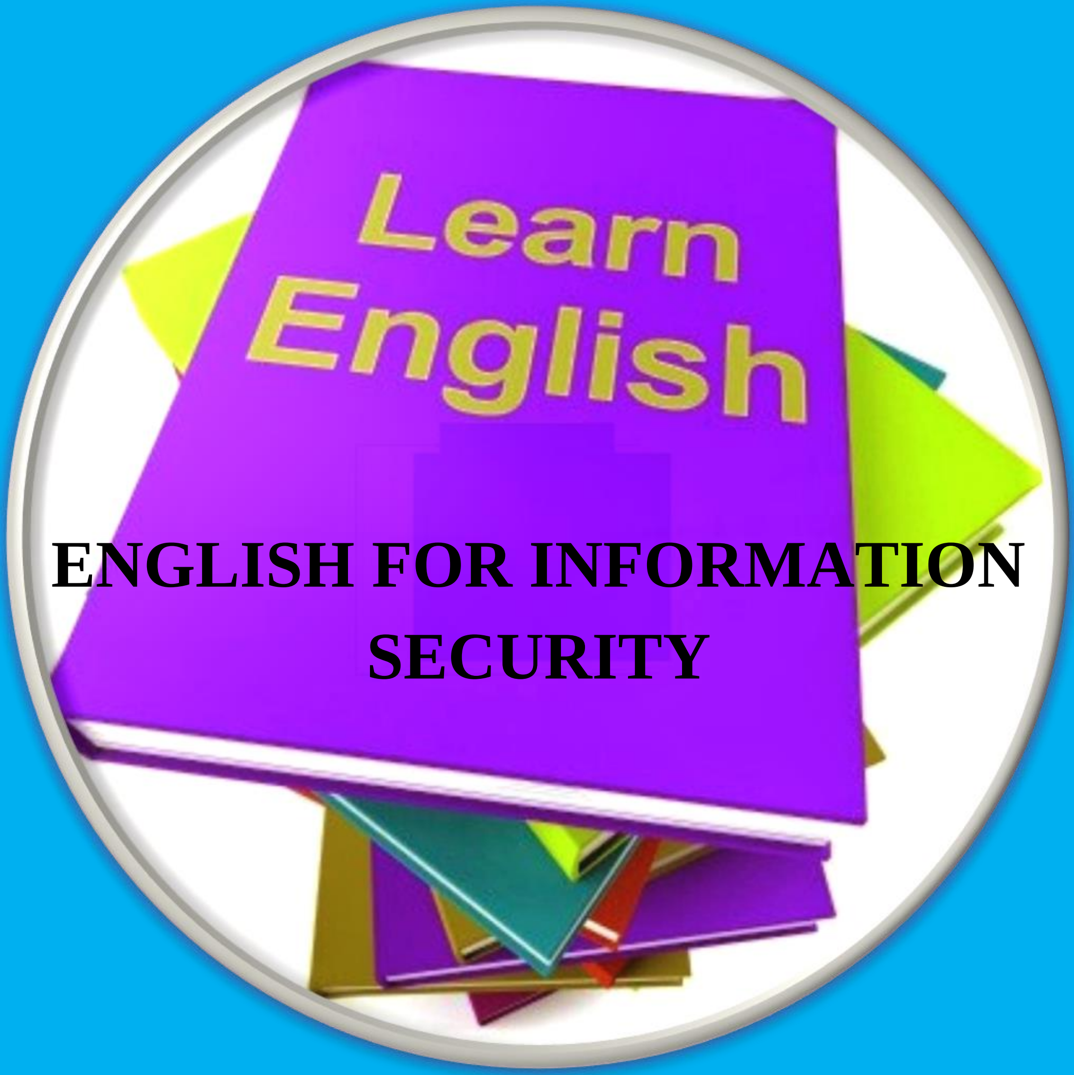
ACADEMY OF CRYPTOGRAPHY TECHNIQUES

MA. MAI THI HAO (Editor)
MA. PHAN BICH THUAN



ENGLISH FOR INFORMATION SECURITY

ACADEMY OF CRYPTOGRAPHY TECHNIQUES

MA. MAI THI HAO (Editor)
MA. PHAN BICH THUAN

ENGLISH FOR INFORMATION SECURITY

(FOR CONFIDENTIAL AND INTERNAL CIRCULATION)

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

The authors would like to express our sincere thanks to the Faculty of Information Security, the lecturers in the faculty, doctors and experts majoring in information security for their great help in compiling this course book. Also, we would like to express our special thanks to professor and doctor of philosophy Luong The Dung who provided us a very useful material and helped us to fulfil the research.

The authors also would like to express our deep gratitude to Board of Directors of the Academy of Cryptography Techniques, the Faculty of Basic Sciences and the Division of English Language for their thorough support in compilation of this course book.

Though the English for Information Security course book is compiled for the second time, unexpected mistakes can not help being made. Therefore, comments from all readers on this book are always welcome and highly appreciated.

The authors

INTRODUCTION

This is the second compilation of the English for Information Security course book with new and outstanding features. Firstly, the knowledge in the book is not too difficult for students and teachers. Secondly, ***the grammar structures, word formation, and the knowledge of parts of speech provided though General English learnt in English 1, English 2, and English 3 are not provided.*** Thirdly, this book helps students improve different language skills in which ***reading comprehension, translation, and speaking are the first priority***. Futher more, the topics in the book are very close to students, especially they relate to almost fundamental knowledge in the information security, which helps to motivate them in class English learning. Finally, skillful combination of four language skills including Reading, Speaking, Listening and Writing is also introduced.

This course book is compiled for the fourth year students of the Academy of Cryptography Techniques majoring in information security, who have completed the syllabus of General English.

In addition, this material provides students with a great number of texts with a variety of basic vocabularies commonly used in the information security, which helps them approach the specialized knowledge. Activities are given before, while and after each text so that students are able to read, comprehend, discuss the topics of their major in English and confidently communicate with each other, which helps them avoid the feelings of being new and strange when they discuss or attend seminars in English. Besides, students can practise summarizing the reading texts in their own words and present a quickview of the contents they are provided in class.

The course book is divided into 8 units with different themes. Each unit is about a specific one and focuses on the different language skills as follow:

1. **READING AND SPEAKING**: This section has from 3 to 4 texts relating to different topics. A pre-reading task with different questions is given before each text, which enables students to be accustomed to the topic of the unit that they are going to deal with later. While-reading and post-reading tasks with activities are also provided after each text on purpose of helping students develop their reading comprehension and communication skills.

2. **WRITING AND SPEAKING**: This section includes tasks or activities relating to the topics and contents of each unit which enable students to develop writing and speaking skills

3. LISTENING: Some video links are given at the end of each unit so that students are able not only to consolidate the knowledge in the lesson but also to improve their listening skill.

Materials used for compiling this course book are taken from the books written by British and American authors to ensure accuracy and standard literal style of native speakers or taken from academic websites and journals.

UNIT 1: INTRODUCTION TO INFORMATION SECURITY

READING AND SPEAKING 1

1. Discuss the questions

1. Does information need protecting? What information needs protecting?
2. When does that information have to be protected?
3. What fields do you think relate to information security?
4. When was information security born?
5. What historical periods do you think information security has experienced?

2. Read the text and do the tasks below

The History of Information Security

The history of information security begins with **computer security**. The need for computer security - that is, the need to secure physical locations, hardware, and software from threats - arose during World War II when the first mainframes, developed to aid computations for communication code breaking (see Figure 1-1), were put to use. Multiple levels of security were implemented to protect these mainframes and maintain the integrity of their data. Access to sensitive military locations, for example, was controlled by means of badges, keys, and the facial recognition of authorized personnel by security guards. The growing need to maintain national security eventually led to more complex and more technologically sophisticated computer security safeguards.

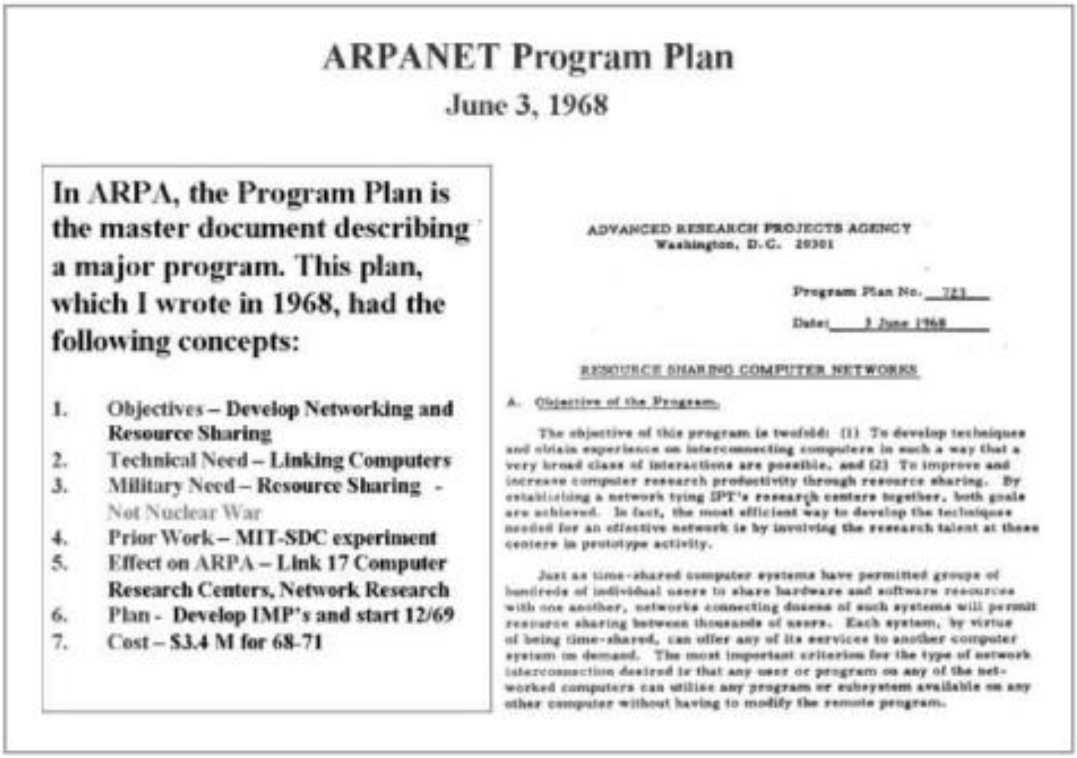
During these early years, information security was a straightforward process composed predominantly of physical security and simple document classification schemes. The primary threats to security were physical theft of equipment, espionage against the products of the systems, and sabotage. One of the first documented security problems that fell outside these categories occurred in the early 1960s, when a systems administrator was working on an MOTD (message of the day) file, and another administrator was editing the password file. A software glitch mixed the two files, and the entire password file was printed on every output file.

Earlier versions of the German code machine Enigma were first broken by the Poles in the 1930s. The British and Americans managed to break later, more complex versions during World War II. The increasingly complex versions of the Enigma, especially the submarine or *Unterseeboot* version of the Enigma, caused considerable anguish to Allied forces before finally being cracked. The information gained from decrypted transmissions was used to anticipate the actions of German armed forces. "Some ask why, if we were reading the Enigma, we did not win the war earlier. One might ask, instead, when, if ever, we would have won the war if we hadn't read it."[1]

Figure 1-1. The Enigma

The 1960s

During the Cold War, many more mainframes were brought online to accomplish more complex and sophisticated tasks. It became necessary to enable these mainframes to communicate via a less cumbersome process than mailing magnetic tapes between computer centers. In response to this need, the Department of Defense's Advanced Research Project Agency (ARPA) began examining the feasibility of a redundant, networked communications system to support the military's exchange of information. Larry Roberts, known as the founder of the Internet, developed the project which was called ARPANET from its inception. ARPANET is the predecessor to the Internet (see figure 1-2. for an except from the ARPA-NET Program Plan).



ARPANET Program Plan

June 3, 1968

In ARPA, the Program Plan is the master document describing a major program. This plan, which I wrote in 1968, had the following concepts:

1. Objectives – **Develop Networking and Resource Sharing**
2. Technical Need – **Linking Computers**
3. Military Need – **Resource Sharing** - Not Nuclear War
4. Prior Work – **MIT-SDC experiment**
5. Effect on ARPA – **Link 17 Computer Research Centers, Network Research**
6. Plan - **Develop IMP's and start 12/69**
7. Cost – **$3.4 M for 68-71**

ADVANCED RESEARCH PROJECTS AGENCY
Washington, D.C. 20301

Program Plan No. 723

Date: 3 June 1968

RESOURCE SHARING COMPUTER NETWORKS

A. Objective of the Program.

The objective of this program is twofold: (1) To develop techniques and obtain experience on interconnecting computers in such a way that a very broad class of interactions are possible, and (2) To improve and increase computer research productivity through resource sharing. By establishing a network tying IPT's research centers together, both goals are achieved. In fact, the most efficient way to develop the techniques needed for an effective network is by involving the research talent at these centers in prototype activity.

Just as time-shared computer systems have permitted groups of hundreds of individual users to share hardware and software resources with one another, networks connecting dozens of such systems will permit resource sharing between thousands of users. Each system, by virtue of being time-shared, can offer any of its services to another computer system on demand. The most important criterion for the type of network interconnection desired is that any user or program on any of the networked computers can utilize any program or subsystem available on any other computer without having to modify the remote program.

Figure 1-2. Development of the ARPANET Program Plan

The 1970s and 80s

During the next decade, ARPANET became popular and more widely used, and the potential for its misuse grew. In December of 1973, Robert M. "Bob" Metcalfe, who is credited with the development of Ethernet, one of the most popular networking protocols, identified fundamental problems with ARPANET security. Individual remote sites did not have sufficient controls and safeguards to protect data from unauthorized remote users. Other problems abounded: vulnerability of password structure and formats; lack of safety procedures for dial-up connections; and nonexistent user identification and authorization to the system. Phone numbers were widely distributed and openly publicized on the walls of phone booths, giving hackers easy access to ARPANET. Because of the range and frequency of computer security violations and the explosion in the numbers of hosts and users on ARPANET, network security was referred to as network insecurity. In 1978, a famous study entitled "Protection Analysis: Final Report" was published. It focused on a project undertaken by ARPA to discover the vulnerabilities of operating system security. For a timeline that includes this and other seminal studies of computer security.

The movement toward security that went beyond protecting physical locations began with a single paper sponsored by the Department of Defense, the Rand Report R-609, which attempted to define the multiple controls and mechanisms necessary for the protection of a multilevel computer system. The document was classified for almost ten years, and is now considered to be the paper that started the study of computer security.

The security-or lack thereof-of the systems sharing resources inside the Department of Defense was brought to the attention of researchers in the spring and summer of 1967. At that time, systems were being acquired at a rapid rate and securing them was a pressing concern for both the military and defense contractors.

In June of 1967, the Advanced Research Projects Agency formed a task force to study the process of securing classified information systems. The Task Force was assembled in October of 1967 and met regularly to formulate recommendations, which ultimately became the contents of the Rand Report R-609.

The Rand Report R-609 was the first widely recognized published document to identify the role of management and policy issues in computer security. It noted that the wide utilization of networking components in information systems in the military introduced security risks that could not be mitigated by the routine practices then used to secure these systems. This paper signaled a pivotal moment in computer security history-when the scope of computer security expanded significantly from the safety of physical locations and hardware to include the following:

- Securing the data
- Limiting random and unauthorized access to that data
- Involving personnel from multiple levels of the organization in matters pertaining to information security

MULTICS

Much of the early research on computer security centered on a system called Multiplexed Information and Computing Service (MULTICS). Although it is now obsolete, MULTICS is noteworthy because it was the first operating system to integrate security into its core functions. It was a mainframe, time-sharing operating system developed in the mid- 1960s by a consortium of General Electric (GE), Bell Labs, and the Massachusetts Institute of Technology (MIT).

In mid-1969, not long after the restructuring of the MULTICS project, several of its developers (Ken Thompson, Dennis Ritchie, Rudd Canada, and Doug McElroy) created a new operating system called UNIX. While the MULTICS system implemented multiple security levels and passwords, the UNIX system did not. Its primary function, text processing, did not require the same level of security as that of its predecessor. In fact, it was not until the early 1970s that even the simplest component of security, the password function, became a component of UNIX.

In the late 1970s, the microprocessor brought the personal computer and a new age of computing. The PC became the workhorse of modern computing, thereby moving it out of the data center. This decentralization of data processing systems in the 1980s gave rise to networking-that is, the interconnecting of personal computers and mainframe computers, which enabled the entire computing community to make all their resources work together.

The 1990s

At the close of the twentieth century, networks of computers became more common, as did the need to connect these networks to each other. This gave rise to the Internet, the first global network of networks. The Internet was made available to the general public in the 1990s, having previously been the domain of government, academia, and dedicated industry professionals. The Internet brought connectivity to virtually all computers that could reach a phone line or an Internet-connected local area network (LAN). After the Internet was commercialized, the technology became pervasive, reaching almost every corner of the globe with an expanding array of uses.

Since its inception as a tool for sharing Defense Department information, the Internet has become an interconnection of millions of networks. At first, these connections were based on de facto **standards**, because industry standards for interconnection of networks did not exist at that time. These de facto standards did little to ensure the security of information though as these precursor technologies were widely adopted and became industry standards, some degree of security was introduced. However, early Internet deployment treated security as a low priority. In fact, many of the problems that plague e-mail on the Internet today are the result of this early lack of security. At that time, when all Internet and e-mail users were (presumably trustworthy) computer scientists, mail server authentication and e-mail encryption did not seem necessary. Early computing approaches relied on security that was built into the physical environment of the data center that housed the computers. As networked computers became the dominant style of computing, the ability to physically secure a networked computer was lost, and the stored information became more exposed to security threats.

2000 to present

Today, the Internet brings millions of unsecured computer networks into continuous communication with each other. The security of each computer's stored information is now contingent on the level of security of every other computer to which it is connected. Recent years have seen a growing awareness of the need to improve information security, as well as a realization that information security is important to national defense. The growing threat of cyber attacks have made governments and companies more aware of the need to defend the computer-controlled control systems of utilities and other critical infrastructure. There is also growing concern about nation-states engaging in information warfare, and the possibility that business and personal information systems could become casualties if they are undefended.

2.1. Answer the questions

1. Who was known as the founder of the Internet? What did he develop?
2. How was access to sensitive military locations controlled during World War II?
3. When was a famous study entitled "Protection Analysis: Final Report" published? What did it focus on? Why?
4. What is the difference between MULTICS system and UNIX system?
5. When has the Internet become an interconnection of millions of networks and why?
6. What led to more complex and more technologically sophisticated computer security safeguards before?

7. When did the technology become pervasive, reaching almost every corner of the globe with an expanding array of uses?
8. What has made governments and companies more aware of the need to defend the computer-controlled control systems of utilities and other critical infrastructure?

2.2. Decide whether the following statements are true (T), false (F) or no information (NI). Correct the false (F)

1. The security of each computer's stored information is now contingent on the level of security of every other computer to which it is connected.

   A. True B. False C. NI

2. Ken Thompson, Dennis Ritchie, Rudd Canada, and Doug McElroy are the Multiplexed Information and Computing Service's inventers.

   A. True B. False C. NI

3. "Protection Analysis: Final Report" was the first widely recognized published document to identify the role of management and policy issues in computer security.

   A. True B. False C. NI

4. Initial planning and development for MULTICS started in 1964, in Cambridge, Massachusetts. Originally it was a cooperative project led by MIT.

   A. True B. False C. NI

5. A task force was built by the Advanced Research Projects Agency so as to study the process of securing classified information system.

   A. True B. False C. NI

6. Access to the ARPANET was expanded in 1981, when the National Science Foundation funded the Computer Science Network.

   A. True B. False C. NI

2.3. Choose the best answer for the following questions and statements

1. ...., networks of computers became more common, as did the need to connect these networks to each other.

   A. At the close of the 20th century C. In the mid-1960s.

B.In the late 1970s. D. During the Cold War

2. The primary threats to security were ....

   A. sabotage

   B. physical theft of equipment

   C. espionage against the products of the systems

   D. All are correct

3. .... primary function, text processing, did not require the same level of security as that of its predecessor.

   A. ARPANET’s C. MULTICS’

   B. ARPA’s D. UNIX’s

4. Early computing approaches relied on ....

   A. information security theory and cryptography.

   B. security that was built into the physical environment of the data center that housed the computers.

   C. the growing threat of cyber attacks.

   D. the level of security of every computer.

5. Network security was referred to as network insecurity...............the range and frequency of computer security violations and the explosion in the numbers of hosts and users on ARPANET.

   A. Because of C. Therefore

   B. However D. Although

3. Speaking

1. Which main information in each period of the history of information security do you get?

2. Present a brief history of information security.

READING AND SPEAKING 2

1. Discuss the questions

1. What is security?
2. What is information security?
3. What components of information security do you know?
4. What areas does information security relate to?

2. Read a brief history of cryptography and do the tasks below

What is security?

In general, **security** is “the quality or state of being secure to be free from danger.”. In other words, protection against adversaries from those who would do harm, intentionally or otherwise is the objective. National security, for example, is a multilayered system that protects the sovereignty of a state, its assets, its resources, and its people. Achieving the appropriate level of security for an organization also requires a multifaceted system. A successful organization should have the following multiple layers of security in place to protect its operations:

- **Physical security**, to protect physical items, objects, or areas from unauthorized access and misuse
- **Personnel security**, to protect the individual or group of individuals who are authorized to access the organization and its operations
- **Operations security**, to protect the details of a particular operation or series of activities
- **Communications security**, to protect communications media, technology, and content
- **Network security**, to protect networking components, connections, and contents
- **Information security**, to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness, and technology.

The Committee on National Security Systems (CNSS) defines information security as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information. Figure 1-3 shows that information security includes the broad areas of information security management, computer and data security, and network security. The CNSS model of information security evolved from a concept developed by the computer security industry called the C.I.A. triangle. The **C.I.A. triangle** has been the industry standard for computer security since the development of the mainframe. It is based on the three characteristics of information that give it value to organizations: confidentiality, integrity, and availability. The security of these three characteristics of information is as important today as it has always been, but the C.I.A. triangle model no longer adequately addresses the constantly changing environment. The threats to the confidentiality, integrity, and availability of information have evolved into a vast collection of events, including accidental or intentional damage, destruction, theft, unintended or unauthorized modification, or other misuse from human or nonhuman threats. This new environment of many constantly evolving threats has prompted the development of a more robust model that addresses the complexities of the current information security environment.

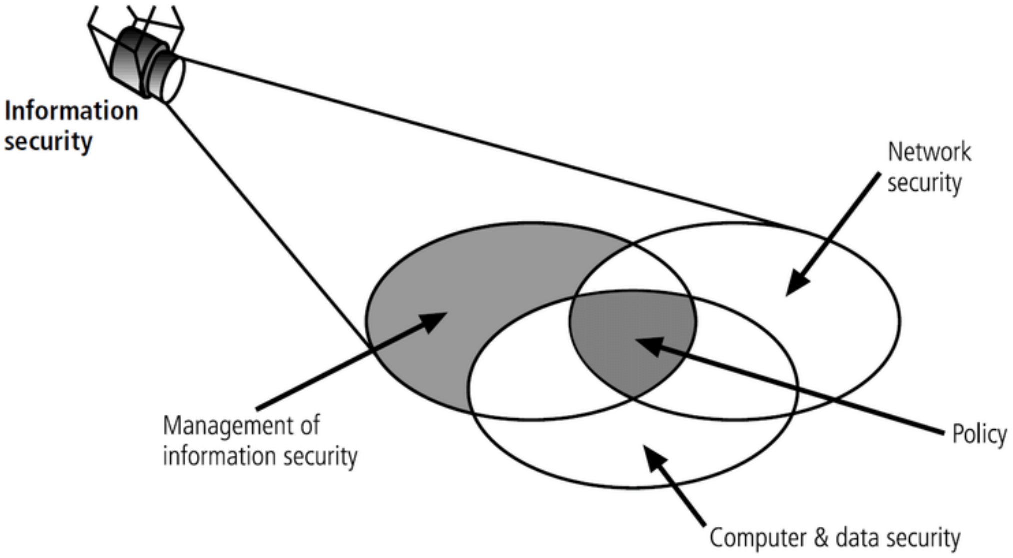


Figure 1-3: Components of Information security

Key Information Security Terms and Concepts

- ***Access:*** A subject or object’s ability to use, manipulate, modify, or affect another subject or object. Authorized users have legal access to a system, whereas hackers have illegal access to a system. Access controls regulate this ability.

- ***Asset*****:** The organizational resource that is being protected. An asset can

be logical, such as a Web site, information, or data; or an asset can be physical, such as a person, computer system, or other tangible object. Assets, and particularly information assets, are the focus of security efforts; they are what those efforts are attempting to protect.

- ***Attack*****:** An intentional or unintentional act that can cause damage to or

otherwise compromise information and/or the systems that support it. Attacks can be active or passive, intentional or unintentional, and direct or indirect. Someone casually reading sensitive information not intended for his or her use is a passive attack.

A hacker attempting to break into an information system is an intentional attack. A lightning strike that causes a fire in a building is an unintentional attack. A direct attack is a hacker using a personal computer to break into a system. An indirect attack is a hacker compromising a system and using it to attack other systems, for example, as part of a botnet (slang for robot network). This group of compromised computers, running software of the attacker's choosing, can operate autonomously or under the attacker's direct control to attack systems and steal user information or conduct distributed denial-of-service attacks. Direct attacks originate from the threat itself. Indirect attacks originate from a compromised system or resource that is malfunctioning or working under the control of a threat.

- ***Control, safeguard,*** *or* ***countermeasure*****:** Security mechanisms,

policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve the security within an organization.

- ***Exploit*****:** A technique used to compromise a system. This term can be a

verb or a noun. Threat agents may attempt to exploit a system or other information by using it illegally for their personal gain. Or, an exploit can be a documented process to take advantage of a vulnerability or exposure, usually in software, that is either inherent in the software or is created by the attacker. Exploits make use of existing software tools or custom-made software components.

- ***Exposure*****:** A condition or state of being exposed. In information

security, exposure exists when a vulnerability known to an attacker is present.

- ***Loss*****:** A single instance of an information asset suffering damage or

unintended or unauthorized modification or disclosure. When an organization's information is stolen, it has suffered a loss.

- ***Protection profile*** *or* ***security posture*****:** The entire set of controls and

safeguards, including policy, education, training and awareness, and technology, that the organization implements (or fails to implement) to protect the asset. The terms are sometimes used interchangeably with the term *security program*, although the security program often comprises managerial aspects of security, including planning, personnel, and subordinate programs.

- ***Risk*****:** The probability that something unwanted will happen.

Organizations must minimize risk to match their **risk appetite**—the quantity and nature of risk the organization is willing to accept.

- ***Subjects*** and ***objects*****:** A computer can be either the **subject** of an

attack—an agent entity used to conduct the attack—or the **object** of an attack—the target entity, as shown in *Figure 1-4***.** A computer can be both the subject and object of an attack, when, for example, it is compromised by an attack (object), and is then used to attack other systems (subject).

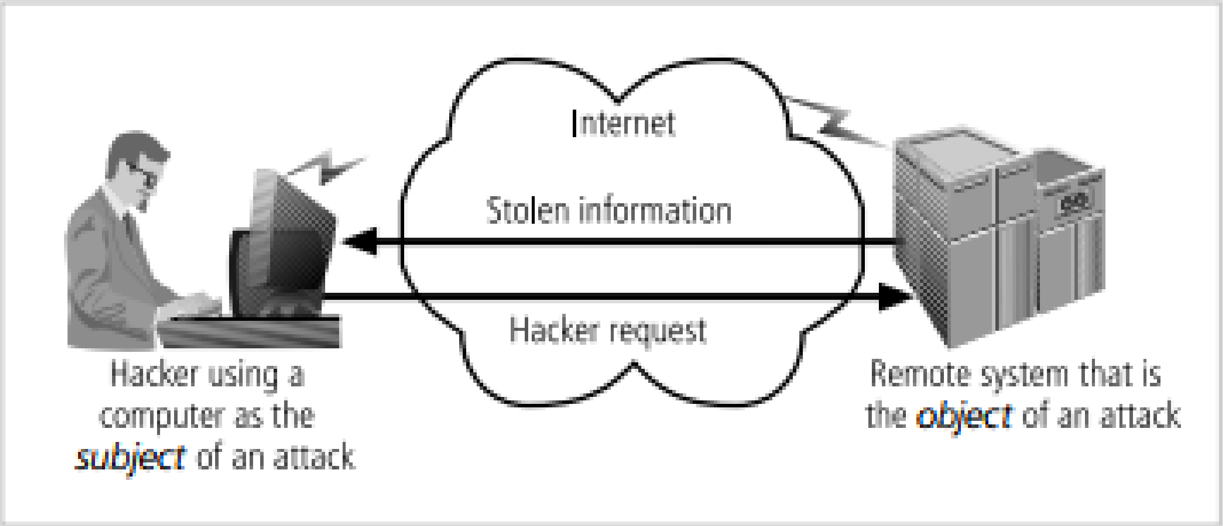

Internet
Stolen information
Hacker request
Hacker using a computer as the subject of an attack
Remote system that is the object of an attack

Figure 1-4. Computer as the Subject and Object of an Attack

- ***Threat*:** A category of objects, persons, or other entities that presents a

danger to an asset. Threats are always present and can be purposeful or undirected. For example, hackers purposefully threaten unprotected information systems, while severe storms incidentally threaten buildings and their contents.

- ***Threat agent*:** The specific instance or a component of a threat. For

example, all hackers in the world present a collective threat, while Kevin Mitnick, who was convicted for hacking into phone systems, is a specific threat agent. Likewise, a lightning strike, hailstorm, or tornado is a threat agent that is part of the threat of severe storms.

- ***Vulnerability*:** A weaknesses or fault in a system or protection

mechanism that opens it to attack or damage. Some examples of vulnerabilities are a flaw in a software package, an unprotected system port, and an unlocked door. Some **well-known vulnerabilities** have been examined, documented, and published; others remain latent (or undiscovered).

2.1. Answer the questions

1. Which areas does information security include?
2. Why does the C.I.A. triangle model no longer adequately address the constantly changing environment?
3. What is security? What is information security?
4. How many fundamental characteristics does information have? What are they?
5. Since when has the C.I.A triangle been industry standard for computer security? What is it based on?
6. What should a successful organization have to protect its operation?
7. What is attack? What types of attack are mentioned in the passages?
8. What is vulnerability? Give some examples of vulnerabilities.

2.2. Decide whether the following statements are true (T), false (F) or no information (NI). Correct the false (F)

1. Network security is to protect the individual or group of individuals who are authorized to access the organization and its operations.

A. True B. False C. NI

2. Information security threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, and identity theft.

   A. True B. False C. NI

3. The C.I.A. triangle model still has adequately addressed the constantly changing environment up to now.

   A. True B. False C. NI

4. Operations security is a process that identifies critical information to determine if friendly actions can be observed by enemy intelligence.

   A. True B. False C. NI

5. The CNSS model of information security evolved from a concept developed by the computer security industry called the C.I.A. triangle.

   A. True B. False C. NI

6. Organizations must minimize risk to match their risk appetite - the quantity and nature of risk the organization is willing to accept.

   A. True B. False C. NI

7. Risk is a weaknesses or fault in a system or protection mechanism that opens it to attack or damage.

   A. True B. False C. NI

8. A successful organization should have mono layer of security in place to protect its operations.

   A. True B. False C. NI

2.3. Choose the best answer to complete the following statements

1. ....is a category of objects, persons, or other entities that presents a danger to an asset.

   A. Threat C. Risk

   B. Security posture D. Vulnerability

2. ...., is a multilayered system that protects the sovereignty of a state, its assets, its resources, and its people.

A. Personnel security C. Network security

B. National security D. Physical security

3. Someone casually reading sensitive information not intended for his or her use is ....

A. intentional attack C. direct attack

B. a passive attack D. active attack

4. ....can be a documented process to take advantage of a vulnerability or exposure, usually in software, that is either inherent in the software or is created by the attacker.

A. A protection profile C. An exploit

B. A threat agent D. An asset

5. Authorized users have .... to a system, whereas hackers have ....to a system.

A. illegal access/ legal access C. lawful/illicit

B. legal access/ illegal access D. B&C are correct

6. ....attacks originate from the threat itself. .... attacks originate from a compromised system or resource that is malfunctioning or working under the control of a threat.

A. Direct/Indirect C. B&C are correct

B. Passive/Active D. Indirect/Passive

7. In information security, ...exists when a vulnerability known to an attacker is present.

A. safeguard C. risk

B. exposure D. security posture

8. When an organization’s information is stolen, it has suffered a ....

A. casualty C. damage

B. loss D. All are correct

3. Speaking

1. What key information security concepts or terminologies do you know? Give their definition in your own way.
2. Present components of information security.

READING AND SPEAKING 3

1. Discuss the questions

1. How many critical characteristics of information do you know? What are they?
2. Which critical characteristics of information is the most important? Why?

2. Read cryptographic goals and do the tasks below

Critical Characteristics of Information

Availability**:** **Availability** enables authorized users—persons or computer systems—to access information without interference or obstruction and to receive it in the required format. Consider, for example, research libraries that require identification before entrance. Librarians protect the contents of the library so that they are available only to authorized patrons. The librarian must accept a patron's identification before that patron has free access to the book stacks. Once authorized patrons have access to the contents of the stacks, they expect to find the information they need available in a useable format and familiar language, which in this case typically means bound in a book and written in English.

Accuracy**:** Information has **accuracy** when it is free from mistakes or errors and it has the value that the end user expects. If information has been intentionally or unintentionally modified, it is no longer accurate. Consider, for example, a checking account. You assume that the information contained in your checking account is an accurate representation of your finances. Incorrect information in your checking account can result from external or internal errors. If a bank teller, for instance, mistakenly adds or subtracts too much from your account, the value of the information is changed. Or, you may accidentally enter an incorrect amount into your account register. Either way, an inaccurate bank balance could cause you to make mistakes, such as bouncing a check.

Authenticity**:** **Authenticity** of information is the quality or state of being genuine or original, rather than a reproduction or fabrication. Information is authentic when it is in the same state in which it was created, placed, stored, or transferred. Consider for a moment some common assumptions about e-mail. When you receive e-mail, you assume that a specific individual or group created and transmitted the e-mail—you assume you know the origin of the e-mail. This is not always the case. **E-mail spoofing**, the act of sending an e-mail message with a modified field, is a problem for many people today, because often the modified field is the address of the originator. Spoofing the sender's address can fool e-mail recipients into thinking that messages are legitimate traffic, thus inducing them to open e-mail they otherwise might not have. Spoofing can also alter data being transmitted across a network, as in the case of user data protocol (UDP) packet spoofing, which can enable the attacker to get access to data stored on computing systems.

Confidentiality**:** Information has **confidentiality** when it is protected from disclosure or exposure to unauthorized individuals or systems. Confidentiality ensures that *only* those with the rights and privileges to access information are able to do so. When unauthorized individuals or systems can view information, confidentiality is breached. To protect the confidentiality of information, you can use a number of measures, including the following:

- Information classification
- Secure document storage
- Application of general security policies
- Education of information custodians and end user

Confidentiality, like most of the characteristics of information, is interdependent with other characteristics and is most closely related to the characteristic known as privacy.

The value of confidentiality of information is especially high when it is personal information about employees, customers, or patients. Individuals who transact with an organization expect that their personal information will remain confidential, whether the organization is a federal agency, such as the Internal Revenue Service, or a business. Problems arise when companies disclose confidential information. Sometimes this disclosure is intentional, but there are times when disclosure of confidential information happens by mistake—for example, when confidential information is mistakenly e-mailed to someone *outside* the organization rather than to someone *inside* the organization. Several cases of privacy violation are outlined in Offline: Unintentional Disclosures.

Integrity

Information has **integrity** when it is whole, complete, and uncorrupted. The integrity of information is threatened when the information is exposed to corruption, damage, destruction, or other disruption of its authentic state. Corruption can occur while information is being stored or transmitted. Many computer viruses and worms are designed with the explicit purpose of corrupting data. For this reason, a key method for detecting a virus or worm is to look for changes in file integrity as shown by the size of the file. Another key method of assuring information integrity is **file hashing**, in which a file is read by a special algorithm that uses the value of the bits in the file to compute a single large number called a **hash value**. The hash value for any combination of bits is unique. If a computer system performs the same hashing algorithm on a file and obtains a different number than the recorded hash value for that file, the file has been compromised and the integrity of the information is lost. Information integrity is the cornerstone of information systems, because information is of no value or use if users cannot verify its integrity.

File corruption is not necessarily the result of external forces, such as hackers. Noise in the transmission media, for instance, can also cause data to lose its integrity. Transmitting data on a circuit with a low voltage level can alter and corrupt the data. Redundancy bits and check bits can compensate for internal and external threats to the integrity of information. During each transmission, algorithms, hash values, and the error-correcting codes ensure the integrity of the information. Data whose integrity has been compromised is retransmitted.

Utility

The **utility** of information is the quality or state of having value for some purpose or end. Information has value when it can serve a purpose. If information is available, but is not in a format meaningful to the end user, it is not useful. For example, to a private citizen U.S. Census data can quickly become overwhelming and difficult to interpret; however, for a politician, U.S. Census data reveals information about the residents in a district, such as their race, gender, and age. This information can help form a politician’s next campaign strategy.

Possession

The **possession** of information is the quality or state of ownership or control. Information is said to be in one's possession if one obtains it, independent of format or other characteristics. While a breach of confidentiality always results in a breach of possession, a breach of possession does not always result in a breach of confidentiality.

2.1. Answer the questions

1. When is information authentic?
2. When is information considered inaccurate?
3. When has information confidentiality?
4. How many critical characteristics does information have? What are they?
5. Why is a key method given in the integrity of information?
6. Why is information integrity the cornerstone of information systems?
7. When is the integrity of information threatened?
8. What can you use to protect the confidentiality of information?

2.2. Decide whether the following statements are true (T), false (F) or no information (NI). Correct the false (F).

1. Once authorized patrons have access to the contents of the stacks, they expect to find the information they need available in a useable format and familiar language.

   A. True B. False C. NI

2. When unauthorized individuals or systems can view information, confidentiality is breached

   A. True B. False C. NI

3. The value of authenticity of information is especially high when it is personal information about employees, customers, or patients.

   A. True B. False C. NI

4. Confidentiality ensures that only those with the rights and privileges to access information are able to do so.

   A. True B. False C. NI

5. If a computer system performs the different hashing algorithm on a file and obtains a different number than the recorded hash value for the file, the file has been compromised and the integrity of the information is lost.

A. True B. False C. NI

6. Within economics the concept of utility is used to model worth or value, but its usage has evolved significantly over time.

A. True B. False C. NI

2.3. Choose the best answer to complete the following questions and statements

1. Which critical characteristics of information is the quality or state of being genuine or original, rather than a reproduction or fabrication?

   A. Authenticity C. Accuracy

   B. Confidentiality D. Utility

2. Why is an E-mail spoofing a problem for many people today?

   A. Because often the modified field is the address of the originator.

   B. Since often the modified field is the address of the originator.

   C. A & B are correct

   D. Because of often the modified field is the address of the originator.

3. The ....is the quality or state of having value for some purpose or end.

   A. integrity C. availability

   B. utility of information D. A&B are correct

4. ....is the quality or state of ownership or control.

   A. The utility of information

   B. The availability of information

   C. The confidentiality of information

   D. The possession of information

5. Incorrect information in your checking account can result from external or internal ....

   A. access C. report

B. errors D. transmission

6. If a bank teller mistakenly adds or subtracts too much from your account, ...

A. The value of hash is unchanged.

B. The availability of information is useless.

C. the value of the information is changed.

D. The confidentiality of information is stolen.

7. You can use ....measures to protect the confidentiality of information.

A. information classification, application of general security policies

B. secure document storage

C. education of information custodians and end user

D. All are correct

3. Speaking

1. Present critical characteristics of information.

2. Choose one of critical characteristics of information and present it.

READING AND SPEAKING 4

1. Discuss the questions

1. What components of an information system do you know?
2. Which component is the most important and why?
3. What is software? Which software do you know?
4. What is hardware? List some hardware components you know.

2. Read the text and do the tasks below

Components of an Information System

As shown in Figure 1-5, an **information system (IS)** is much more than computer hardware; it is the entire set of software, hardware, data, people, procedures, and networks that make possible the use of information resources in the organization. These six critical components enable information to be input, processed, output, and stored. Each of these IS components has its own strengths and weaknesses, as well as its own characteristics and uses. Each component of the information system also has its own security requirements.

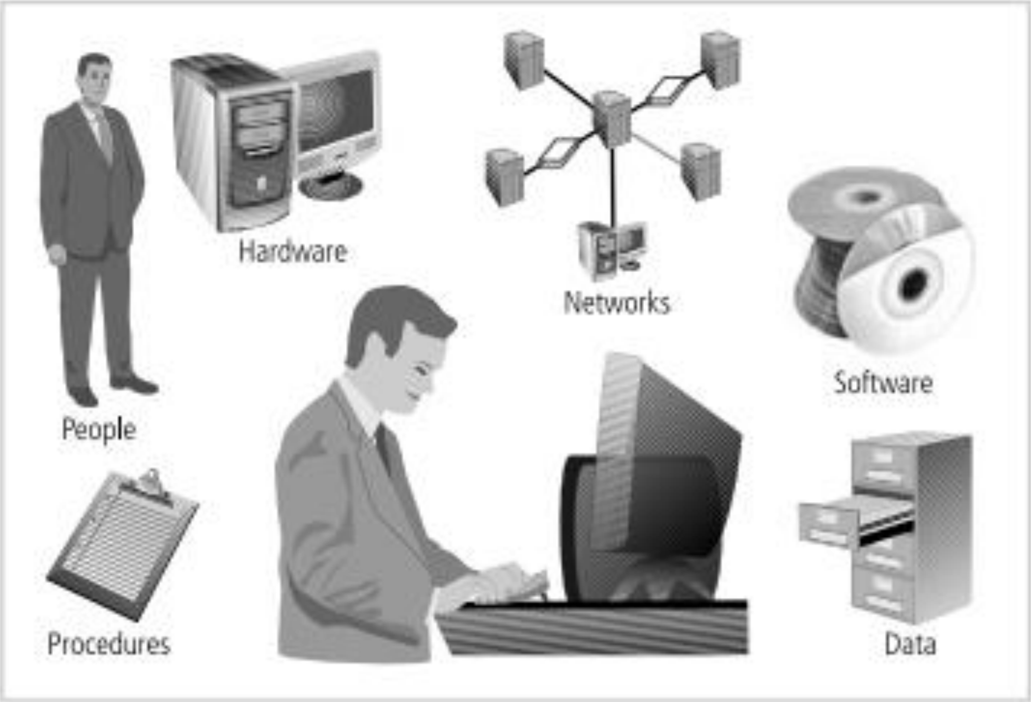


Figure 1-5. Components of an Information System

Software

The software component of the IS comprises applications, operating systems, and assorted command utilities. Software is perhaps the most difficult IS component to secure. The exploitation of errors in software programming accounts for a substantial portion of the attacks on information. The information technology industry is rife with reports warning of holes, bugs, weaknesses, or other fundamental problems in software. In fact, many facets of daily life are affected by buggy software, from smartphones that crash to flawed automotive control computers that lead to recalls.

Software carries the lifeblood of information through an organization. Unfortunately, software programs are often created under the constraints of project management, which limit time, cost, and manpower. Information security is all too often implemented as an afterthought, rather than developed as an integral component from the beginning. In this way, software programs become an easy target of accidental or intentional attacks

Hardware

Hardware is the physical technology that houses and executes the software, stores and transports the data, and provides interfaces for the entry and removal of information from the system. Physical security policies deal with hardware as a physical asset and with the protection of physical assets from harm or theft. Applying the traditional tools of physical security, such as locks and keys, restricts access to and interaction with the hardware components of an information system. Securing the physical location of computers and the computers themselves is important because a breach of physical security can result in a loss of information. Unfortunately, most information systems are built on hardware platforms that cannot guarantee any level of information security if unrestricted access to the hardware is possible.

Before September 11, 2001, laptop thefts in airports were common. A two-person team worked to steal a computer as its owner passed it through the conveyor scanning devices. The first perpetrator entered the security area ahead of an unsuspecting target and quickly went through. Then, the second perpetrator waited behind the target until the target placed his/her computer on the baggage scanner. As the computer was whisked through, the second agent slipped ahead of the victim and entered the metal detector with a substantial collection of keys, coins, and the like, thereby slowing the detection process and allowing the first perpetrator to grab the computer and disappear in a crowded walkway.

Data

Data stored, processed, and transmitted by a computer system must be protected. Data is often the most valuable asset possessed by an organization and it is the main target of intentional attacks. Systems developed in recent years are likely to make use of database management systems. When done properly, this should improve the security of the data and the application. Unfortunately, many system development projects do not make full use of the database management system's security capabilities, and in some cases the database is implemented in ways that are less secure than traditional file systems.

People

Though often overlooked in computer security considerations, people have always been a threat to information security. Legend has it that around 200 B.C. a great army threatened the security and stability of the Chinese empire. So ferocious were the invaders that the Chinese emperor commanded the construction of a great wall that would defend against the Hun invaders. Around 1275 A.D., Kublai Khan finally achieved what the Huns had been trying for thousands of years. Initially, the Khan's army tried to climb over, dig under, and break through the wall. In the end, the Khan simply bribed the gatekeeper—and the rest is history. Whether this event actually occurred or not, the moral of the story is that people can be the weakest link in an organization's information security program. And unless policy, education and training, awareness, and technology are properly employed to prevent people from accidentally or intentionally damaging or losing information, they will remain the weakest link.

Procedures

Another frequently overlooked component of an IS is procedures. Procedures are written instructions for accomplishing a specific task. When an unauthorized user obtains an organization's procedures, this poses a threat to the integrity of the information. For example, a consultant to a bank learned how to wire funds by using the computer center's procedures, which were readily available. By taking advantage of a security weakness (lack of authentication), this bank consultant ordered millions of dollars to be transferred by wire to his own account. Lax security procedures caused the loss of over ten million dollars before the situation was corrected. Most organizations distribute procedures to their legitimate employees so they can access the information system, but many of these companies often fail to provide proper education on the protection of the procedures. Educating employees about safeguarding procedures is as important as physically securing the information system. After all, procedures are information in their own right. Therefore, knowledge of procedures, as with all critical information, should be disseminated among members of the organization only on a need-to-know basis.

Networks

The IS component that created much of the need for increased computer and information security is networking. When information systems are connected to each other to form local area networks (LANs), and these LANs are connected to other networks such as the Internet, new security challenges rapidly emerge. The physical technology that enables network functions is becoming more and more accessible to organizations of every size. Applying the traditional tools of physical security, such as locks and keys, to restrict access to and interaction with the hardware components of an information system are still important; but when computer systems are networked, this approach is no longer enough. Steps to provide network security are essential, as is the implementation of alarm and intrusion systems to make system owners aware of ongoing compromises.

2.1. Answer the questions

1. Which tools of physical security are often applied to restrict access to and interaction with the hardware components of an information system?
2. What happens when an unauthorized user obtains an organization’s procedures?
3. When local area networks are connected to other networks such as the Internet, new security challenges rapidly emerge?
4. What is an information system?
5. Why is data the main target of intentional attacks?
6. Which component of Information system is the most difficult to secure?
7. What became common in airport before 2002? Give details.

8. Why do software programs become an easy target of accidental or intentional attacks?

9. Why is securing the physical location of computers and the computers themselves important?

10. Do only software and hardware enable information to be input, processed, output, and stored.? If no, what components enable it to do so?

2.2. Decide whether the following statements are true (T), false (F) or no information (NI). Correct the false (F).

1. Information systems hardware is the part of an information system you can touch – the physical components of the technology.

   A. True B. False [✓ C. NI]

2. The information technology industry is rife with reports warning of holes, bugs, weaknesses, or other fundamental problems in software.

   [✓ A. True] B. False C. NI

3. The physical technology that enables network functions is becoming less and less accessible to organizations of every size.

   A. True [✓ B. False] C. NI

4. The invaders were so ferocious that the Chinese emperor commanded the construction of a great wall that would defend against the Hun invaders.

   [✓ A. True] B. False C. NI

5. Physically securing the information system isn't so important as educating employees about safeguarding procedures.

   A. True [✓ B. False] C. NI

2.3. Choose the best answer to complete the following statements

1. Many system development projects do not make full use of the .... management system's security capabilities, and in some cases the database is .... in ways that are less secure than traditional file systems.

   A. database/executed C. A&B are correct

   [✓ B. database/implemented] D. data/implemented

2. Frequently overlooked component of an IS is .... They are written

instructions for accomplishing a specific task.

A. networks

B. procedures

C. software

D. database

3. The IS component that created much of the need for increased computer and information security is ....

A. software

B. networking

C. hardware

D. data

4. .... of the IS comprises applications, operating systems, and assorted command utilities.

A. The software component

B. The hardware component

C. The network component

D. A&C are correct

5. Physical security policies deal with .... as a physical asset and with the protection of physical assets from harm or theft.

A. software

B. adware

C. spyware

D. hardware

6. .... are often created under the constraints of project management, which limit time, cost, and manpower.

A. software program

B. spyware program

C. hardware program

D. adware program

7. Unfortunately, most information systems are **built** on hardware platforms that cannot **guarantee** any level of information security if unrestricted access to the hardware is possible.

A. designed/make sure

B. designed/ensure

C. A&B are correct

D.implemented/certain

8. By taking .... of a security weakness a bank consultant can order millions of dollars to be transferred by wire to his own account.

A. advantage

B. a flier

C. position

D. opportunity

9. In fact, many .... of daily life are affected by ...., from

smartphones that crash to flawed automotive control computers that lead to recalls.

A. facets/buggy software C. A&B are correct

B. aspects/buggy software D. facets/buggy hardware

10. Knowledge of procedures, as with all critical information, should be .... among members of the organization only on a need-to-know basis.

A. popularized C. generalized

B. disseminated D. all are correct

3. Speaking

1. Present components of an information system.
2. Choose one of the components of an information system and present it in details.
3. Which component of an information system do you think the most important and why?

4. Listening

1. https://www.youtube.com/watch?v=eUxUUarTRW4
2. https://www.youtube.com/watch?v=432IHWNMqJE
3. https://www.youtube.com/watch?v=8caqok3ah8o
4. https://www.youtube.com/watch?v=XlcolUHMnh0

WRITING AND SPEAKING

1. Write about 400 words about one of the following topics in your own words

- A brief history of information security
- Critical characteristics of information
- Components of an information system

2. Present the following contents:

- A brief history of Information security
- Critical characteristics of information
- Components of an information system

FUTHER READING

The Systems Development Life Circle

Information security must be managed in a manner similar to any other major system implemented in an organization. One approach for implementing an information security system in an organization with little or no formal security in place is to use a variation of the systems development life cycle (SDLC): the security systems development life cycle (SecSDLC). To understand a *security* systems development life cycle, you must first understand the basics of the method upon which it is based.

Methodology and Phases

The **systems development life cycle (SDLC)** is a methodology for the design and implementation of an information system. A **methodology** is a formal approach to solving a problem by means of a structured sequence of procedures. Using a methodology ensures a rigorous process with a clearly defined goal and increases the probability of success. Once a methodology has been adopted, the key milestones are established and a team of individuals is selected made accountable for accomplishing the project goals.

The traditional SDLC consists of six general phases. If you have taken a system analysis and design course, you may have been exposed to a model consisting of a different number of phases. SDLC models range from having three to twelve phases, all of which have been mapped into the six presented here. The **waterfall model** pictured in *Figure 1-6.* illustrates that each phase begins with the results and information gained from the previous phase.

At the end of each phase comes a structured review or reality check, during which the team determines if the project should be continued, discontinued, outsourced, postponed, or returned to an earlier phase depending on whether the project is proceeding as expected and on the need for additional expertise, organizational knowledge, or other resources.

Once the system is implemented, it is maintained (and modified) over the remainder of its operational life. Any information systems implementation may have multiple iterations as the cycle is repeated over time. Only by means of constant examination and renewal can any system, especially an information security program, perform up to expectations in the constantly changing environment in which it is placed.

The following sections describe each phase of the traditional SDLC.

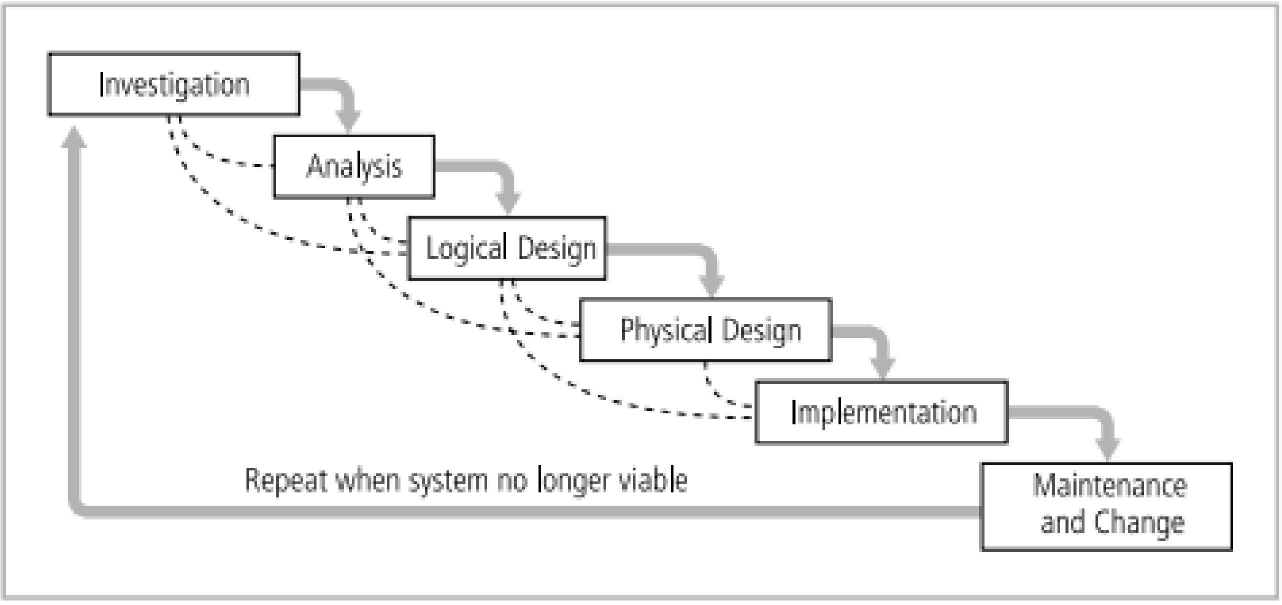


Figure 1-6. SDLC Waterfall Methodology

Investigation

The first phase, investigation, is the most important. What problem is the system being developed to solve? The investigation phase begins with an examination of the event or plan that initiates the process. During the investigation phase, the objectives, constraints, and scope of the project are specified. A preliminary cost-benefit analysis evaluates the perceived benefits and the appropriate levels of cost for those benefits. At the conclusion of this phase, and at every phase following, a feasibility analysis assesses the economic, technical, and behavioral feasibilities of the process and ensures that implementation is worth the organization's time and effort.

Analysis

The analysis phase begins with the information gained during the investigation phase. This phase consists primarily of assessments of the organization, its current systems, and its capability to support the proposed systems. Analysts begin by determining what the new system is expected to do and how it will interact with existing systems. This phase ends with the documentation of the findings and an update of the feasibility analysis.

Logical Design

In the logical design phase, the information gained from the analysis phase is used to begin creating a systems solution for a business problem. In any systems solution, it is imperative that the first and driving factor is the business need. Based on the business need, applications are selected to provide needed services, and then data support and structures capable of providing the needed inputs are chosen. Finally, based on all of the above, specific technologies to implement the physical solution are delineated. The logical design is, therefore, the blueprint for the desired solution. The logical design is implementation independent, meaning Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it. that it contains no reference to specific technologies, vendors, or products. It addresses, instead, how the proposed system will solve the problem at hand. In this stage, analysts generate a number of alternative solutions, each with corresponding strengths and weaknesses, and costs and benefits, allowing for a general comparison of available options. At the end of this phase, another feasibility analysis is performed.

Physical Design

During the physical design phase, specific technologies are selected to support the alternatives identified and evaluated in the logical design. The selected components are evaluated based on a make-or-buy decision (develop the components in-house or purchase them from a vendor). Final designs integrate various components and technologies. After yet another feasibility analysis, the entire solution is presented to the organizational management for approval.

Implementation

In the implementation phase, any needed software is created. Components are ordered, received, and tested. Afterward, users are trained and supporting documentation created. Once all components are tested individually, they are installed and tested as a system. Again a feasibility analysis is prepared, and the sponsors are then presented with the system for a performance review and acceptance test.

Maintenance and Change

The maintenance and change phase is the longest and most expensive phase of the process. This phase consists of the tasks necessary to support and modify the system for the remainder of its useful life cycle. Even though formal development may conclude during this phase, the life cycle of the project continues until it is determined that the process should begin again from the investigation phase. At periodic points, the system is tested for compliance, and the feasibility of continuance versus discontinuance is evaluated. Upgrades, updates, and patches are managed. As the needs of the organization change, the systems that support the organization must also change. It is imperative that those who manage the systems, as well as those who support them, continually monitor the effectiveness of the systems in relation to the organization's environment. When a current system can no longer support the evolving mission of the organization, the project is terminated and a new project is implemented.

Securing the SDLC

Each of the phases of the SDLC should include consideration of the security of the system being assembled as well as the information it uses. Whether the system is custom and built from scratch, is purchased and then customized, or is commercial off-the-shelf software (COTS), the implementing organization is responsible for ensuring it is used securely. This means that each implementation of a system is secure and does not risk compromising the confidentiality, integrity, and availability of the organization's information assets.

UNIT 2: THE NEED FOR SECURITY

READING AND SPEAKING 1

1. Discuss the questions

1. What is threat?
2. What threats in the information area do you know?
3. What do you have to do to avoid those threats?
4. Is threat different from risk or the same as risk? What is their difference? What is their similarity?

2. Read the text and do the tasks below

Threats (1)

Compromises to Intellectual Property

Many organizations create, or support the development of, intellectual property (IP) as part of their business operations. Intellectual property is defined as “the ownership of ideas and control over the tangible or virtual representation of those ideas. Use of another person’s intellectual property may or may not involve royalty payments or permission, but should always include proper credit to the source.” Intellectual property can be trade secrets, copyrights, trademarks, and patents. The unauthorized appropriation of IP constitutes a threat to information security. Employees may have access privileges to the various types of IP, and may be required to use the IP to conduct day-to-day business.

Organizations often purchase or lease the IP of other organizations, and must abide by the purchase or licensing agreement for its fair and responsible use. The most common IP breach is the unlawful use or duplication of software-based intellectual property, more commonly known as **software piracy**. Many individuals and organizations do not purchase software as mandated by the owner’s license agreements. Because most software is licensed to a particular purchaser, its use is restricted to a single user or to a designated user in an organization. If the user copies the program to another computer without securing another license or transferring the license, he or she has violated the copyright.

Deliberate Software Attacks

Deliberate software attacks occur when an individual or group designs and deploys software to attack a system. Most of this software is referred to as **malicious code** or **malicious software**, or sometimes **malware**. These software components or programs are designed to damage, destroy, or deny service to the target systems. Some of the more common instances of malicious code are viruses and worms, Trojan horses, logic bombs, and back doors.

Virus: A computer virus consists of segments of code that perform malicious actions. This code behaves very much like a virus pathogen that attacks animals and plants, using the cell's own replication machinery to propagate the attack beyond the initial target. The code attaches itself to an existing program and takes control of that program's access to the targeted computer. The virus-controlled target program then carries out the virus's plan by replicating itself into additional targeted systems.

One of the most common methods of virus transmission is via e-mail attachment files. Most organizations block e-mail attachments of certain types and also filter all e-mail for known viruses. In earlier times, viruses were slow-moving creatures that transferred viral payloads through the cumbersome movement of diskettes from system to system. Now, computers are networked, and e-mail programs prove to be fertile ground for computer viruses unless suitable controls are in place.

Among the most common types of information system viruses are the **macro virus**, which is embedded in automatically executing macro code used by word processors, spread sheets, and database applications, and the **boot virus**, which infects the key operating system files located in a computer's boot sector.

Worms: Named for the Tapeworm in John Brunner's novel *The Shockwave Rider*, a worm is a malicious program that replicates itself constantly, without requiring another program environment. Worms can continue replicating themselves until they completely fill available resources, such as memory, hard drive space, and network bandwidth.

The complex behavior of worms can be initiated with or without the user downloading or executing the file. Once the worm has infected a computer, it can redistribute itself to all e-mail addresses found on the infected system. Furthermore, a worm can deposit copies of itself onto all Web servers that the infected system can reach, so that users who subsequently visit those sites become infected. Worms also take advantage of open shares found on the network in which an infected system is located, placing working copies of the worm code onto the server so that users of those shares are likely to become infected.

Trojan Horses: Trojan horses *(see Figure 2-1)* are software programs that hide their true nature and reveal their designed behavior only when activated. Trojan horses are frequently disguised as helpful, interesting, or necessary pieces of software, such as readme.exe files often included with shareware or freeware packages. Unfortunately, like their namesake in Greek legend, once Trojan horses are brought into a system, they become activated and can wreak havoc on the unsuspecting user.

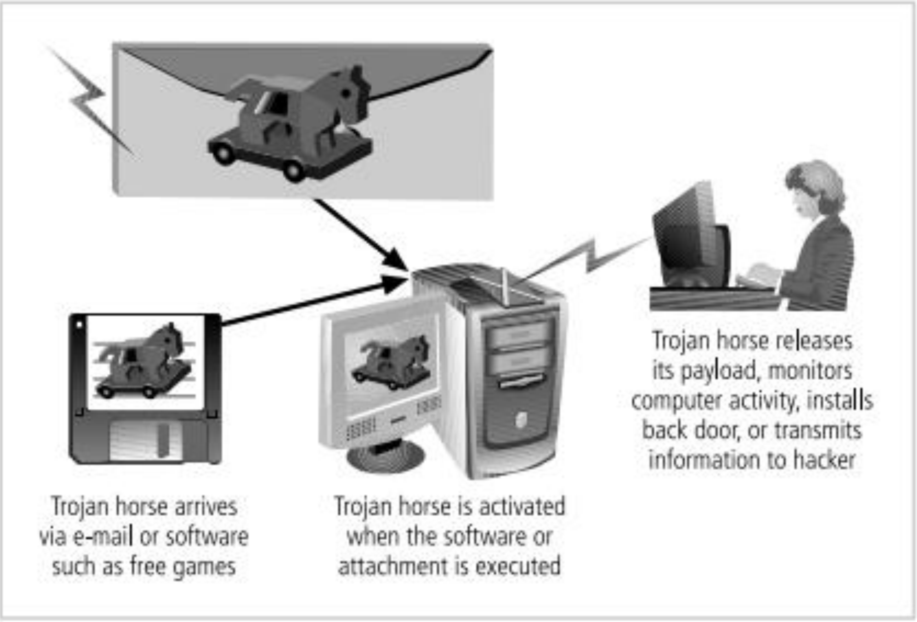

Trojan horse arrives via e-mail or software such as free games
Trojan horse is activated when the software or attachment is executed
Trojan horse releases its payload, monitors computer activity, installs back door, or transmits information to hacker

Figure 2-1. Trojan Horse Attack

Back Door or Trap Door: A virus or worm can have a payload that installs a back door or trap door component in a system, which allows the attacker to access the system at will with special privileges. Examples of these kinds of payloads include Subseven and Back Orifice

Polymorphic Threats: One of the biggest challenges to fighting viruses and worms has been the emergence of polymorphic threats. A polymorphic threat is one that over time changes the way it appears to antivirus software programs, making it undetectable by techniques that look for preconfigured signatures. These viruses and worms actually evolve, changing their size and other external file characteristics to elude detection by antivirus software programs.

Virus and Worm Hoaxes: As frustrating as viruses and worms are, perhaps more time and money is spent on resolving virus hoaxes. Well-meaning people can disrupt the harmony and flow of an organization when they send group e-mails warning of supposedly dangerous viruses that don't exist. When people fail to follow virus-reporting procedures, the network becomes overloaded, and much time and energy is wasted as users forward the warning message to everyone they know, post the message on bulletin boards, and try to update their antivirus protection software.

Espionage or Trespass

Espionage or trespass is a well-known and broad category of electronic and human activities that can breach the confidentiality of information. When an unauthorized individual gains access to the information an organization is trying to protect, that act is categorized as espionage or trespass. Attackers can use many different methods to access the information stored in an information system. Some information gathering techniques are quite legal, for example, using a Web browser to perform market research. These legal techniques are called, collectively, **competitive intelligence**. When information gatherers employ techniques that cross the threshold of what is legal or ethical, they are conducting **industrial espionage**. Many countries considered allies of the United States engage in industrial espionage against American organizations. When foreign governments are involved, these activities are considered espionage and a threat to national security. Some forms of espionage are relatively low tech. One example, called **shoulder surfing** is pictured in *Figure 2-2.*

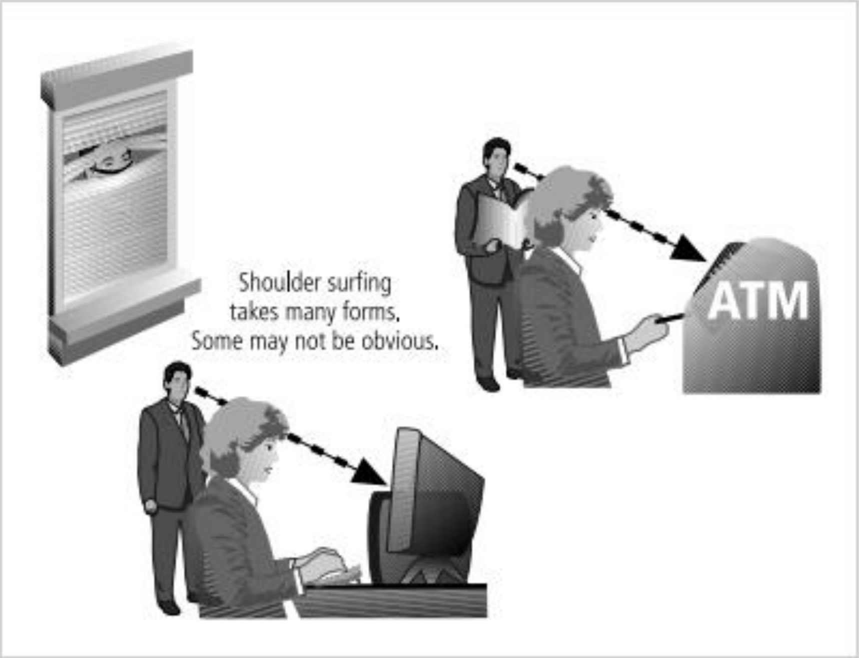


Figure 2-2. ShoulderSurfing

Acts of **trespass** can lead to unauthorized real or virtual actions that enable information gatherers to enter premises or systems they have not been authorized to enter. Controls sometimes mark the boundaries of an organization’s virtual territory. These boundaries give notice to trespassers that they are encroaching on the organization’s cyberspace. Sound principles of authentication and authorization can help organizations protect valuable information and systems. These control methods and technologies employ multiple layers or factors to protect against unauthorized access.

The classic perpetrator of espionage or trespass is the hacker. **Hackers** are “people who use and create computer software to gain access to information illegally.” Hackers are frequently glamorized in fictional accounts as people who stealthily manipulate a maze of computer networks, systems, and data to find the information that solves the mystery or saves the day. Television and motion pictures are inundated with images of hackers as heroes or heroines. However, the true life of the hacker is far more mundane (*see Figure 2-3*). In the real world, a hacker frequently spends long hours examining the types and structures of the targeted systems and uses skill, guile, or fraud to attempt to bypass the controls placed around information that is the property of someone else.

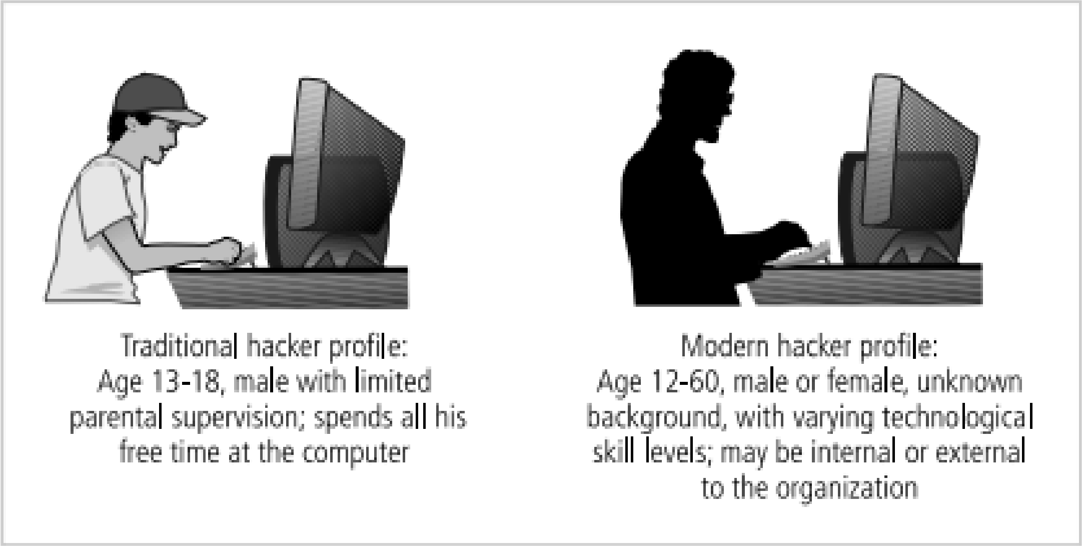

Traditional hacker profile:
Age 13-18, male with limited parental supervision; spends all his free time at the computer
Modern hacker profile:
Age 12-60, male or female, unknown background, with varying technological skill levels; may be internal or external to the organization

Figure 2-3. Hacker Profile

There are generally two skill levels among hackers. The first is the **expert hacker**, or **elite hacker**, who develops software scripts and program exploits used by those in the second category, the novice or **unskilled hacker**. The expert hacker is usually a master of several programming languages, networking protocols, and operating systems and also exhibits a mastery of the technical environment of the chosen targeted system. Once an expert hacker chooses a target system, the likelihood that he or she will successfully enter the system is high. Fortunately for the many poorly protected organizations in the world, there are substantially fewer expert hackers than novice hackers.

2.1. Answer the questions

1. Why don’t any individuals and organizations purchase software as mandated by the owner’s license agreements?
2. Which malicious code software programs that hire their true nature and reveal their designed behavior only when activated?
3. Why are the software components or programs of malicious code designed?
4. What types of software attacks are mentioned in the text?
5. What does IP stand for? What is it?
6. Who is considered an expert hacker?

7. Who are hackers? Which skill levels are divided among hackers?
8. What is one of the most common methods of virus transmission?

2.2. Decide whether the following statements are true (T), false (F) or no information (NI). Correct the false (F).

1. Trade secrets, copyrights, trademarks, and patents are often considered Intellectual property.

   A. True B. False C. NI

2. Before it was easy for viruses to tranfer viral payloads from system to system because there was no e-mail programs.

   A. True B. False C. NI

3. It is not possible for worms to continue replicating themselves until they completely fill available resources, such as memory, hard drive space, and network bandwidth.

   A. True B. False C. NI

4. Before a Trojan horse can infect a machine, the user must download the server side of the malicious application.

   A. True B. False C. NI

5. When an organization places its Web servers in the care of a Web hosting provider, that provider assumes responsibility for all Internet services and for the hardware and operating system software used to operate the Web site.

   A. True B. False C. NI

2.3. Choose the best answer to complete the following questions and statements

1. What is the most common IP breach?

   A. the unlawful use or duplication of software-based intellectual property

   B. the illegally use of software-based intellectual property

   C. A&B are correct

D. the illicit use of software-based intellectual property

2.................. is a well-known and broad category of electronic and human activities that can breach the confidentiality of information.

A. Trojan Horse C. Espionage or trespass

B. A polymorphic threat D. Worm

3. A virus or worm can have a payload that.............a back door or trap door component in a system, which allows the attacker to access the system at will with special privileges.

A. changes C. installs

B. puts D. replaces

4..................is one that over time changes the way it appears to antivirus software programs, making it undetectable by techniques that look for preconfigured signatures.

A. Trojan Horse C. Virus

B. A polymorphic threat D. Worm

5. Worms also take advantage of open shares found on the network in which an infected system is located, placing working copies of the worm code onto the server .... users of those shares are likely to become infected.

A. so as to C. so that

B. in order that D. B&C are correct

6. Which of the followings is a malicious program that replicates itself constantly, without requiring another program environment?

A. Black door C. Virus

B. Worm D. Worm Hoax

3. Speaking

1. What main contents do you get from the text? What do you know about them?
2. Choose one of the threats in the text and present it.

READING AND SPEAKING 2

1. Discuss the questions

1. What natural disasters do you know?
2. Are natural disasters considered threats in the information security? Give an example to support your idea.
3. What is a theft? Which type of theft in the information security do you know?
4. Which threat is the most dangerous in the information security? Why?

2. Read the text and do the tasks below

Threats (2)

Forces of Nature

Forces of nature, force majeure, or acts of God can present some of the most dangerous threats, because they usually occur with very little warning and are beyond the control of people. These threats, which include events such as fires, floods, earthquakes, and lightning as well as volcanic eruptions and insect infestations, can disrupt not only the lives of individuals but also the storage, transmission, and use of information. Some of the more common threats in this group are fire, flood, earthquake, lightning, landslide or mudslide, tornado, hurricane, Tsunami, electrostatic discharge (ESD), and dust contamination.

Human Error or Failure

This category includes acts performed without intent or malicious purpose by an authorized user. When people use information systems, mistakes happen. Inexperience, improper training, and the incorrect assumptions are just a few things that can cause these misadventures. Regardless of the cause, even innocuous mistakes can produce extensive damage.

One of the greatest threats to an organization’s information security is the organization’s own employees. Employees are the threat agents closest to the organizational data. Because employees use data in everyday activities to conduct the organization’s business, their mistakes represent a serious threat to the confidentiality, integrity, and availability of data —even, as *Figure 2-4* suggests, relative to threats from outsiders.

This is because employee mistakes can easily lead to the following: revelation of classified data, entry of erroneous data, accidental deletion or modification of data, storage of data in unprotected areas, and failure to protect information. Leaving classified information in unprotected areas, such as on a desktop, on a Web site, or even in the trash can, is as much a threat to the protection of the information as is the individual who seeks to exploit the information, because one person’s carelessness can create a vulnerability and thus an opportunity for an attacker.

Much human error or failure can be prevented with training and ongoing awareness activities, but also with controls, ranging from simple procedures, such as requiring the user to type a critical command twice, to more complex procedures, such as the verification of commands by a second party. An example of the latter is the performance of key recovery actions in PKI systems. Many military applications have robust, dual-approval controls built in. Some systems that have a high potential for data loss or system outages use expert systems to monitor human actions and request confirmation of critical inputs.

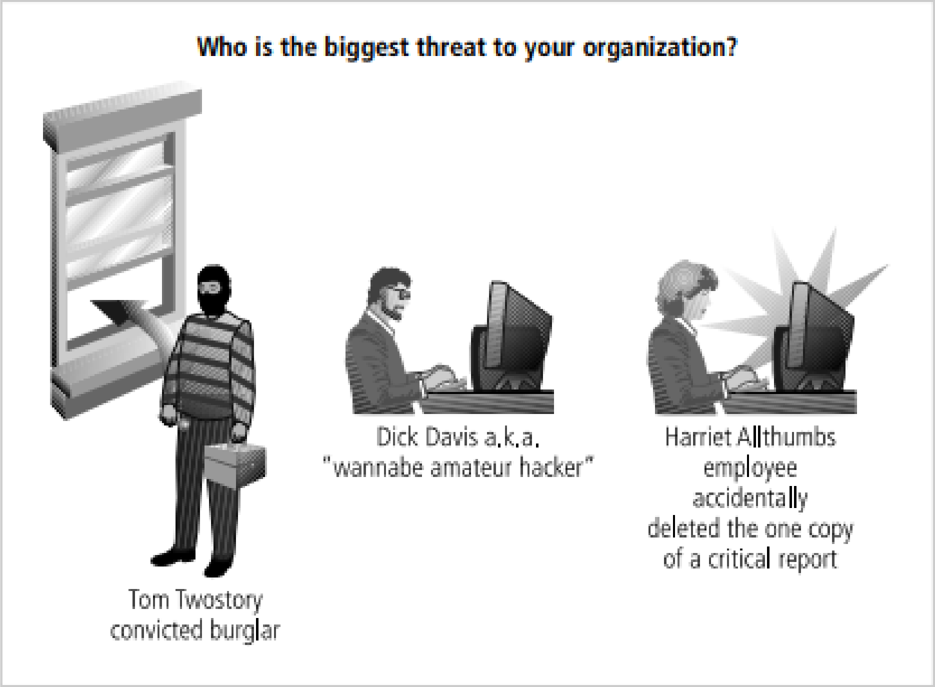


Figure 2-4. Acts of Human Error or Failure

Information Extortion

Information extortion occurs when an attacker or trusted insider steals information from a computer system and demands compensation for its return or for an agreement not to disclose it. Extortion is common in credit card number theft. For example, Web-based retailer CD Universe was the victim of a theft of data files containing customer credit card information. The culprit was a Russian hacker named Maxus, who hacked the online vendor and stole several hundred thousand credit card numbers. When the company refused to pay the $100,000 blackmail, he posted the card numbers to a Web site, offering them to the criminal community. His Web site became so popular he had to restrict access.

Theft

The threat of **theft**—the illegal taking of another's property, which can be physical, electronic, or intellectual—is a constant. The value of information is diminished when it is copied without the owner's knowledge. Physical theft can be controlled quite easily by means of a wide variety of measures, from locked doors to trained security personnel and the installation of alarm systems. Electronic theft, however, is a more complex problem to manage and control. When someone steals a physical object, the loss is easily detected; if it has any importance at all, its absence is noted. When electronic information is stolen, the crime is not always readily apparent. If thieves are clever and cover their tracks carefully, no one may ever know of the crime until it is far too late.

Technical Hardware Failures or Errors

Technical hardware failures or errors occur when a manufacturer distributes equipment containing a known or unknown flaw. These defects can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability. Some errors are terminal—that is, they result in the unrecoverable loss of the equipment. Some errors are intermittent, in that they only periodically manifest themselves, resulting in faults that are not easily repeated, and thus, equipment can sometimes stop working, or work in unexpected ways. One of the best-known hardware failures is that of the Intel Pentium II chip (see *Figure 2-5* , which had a defect that resulted in a calculation error under certain circumstances.

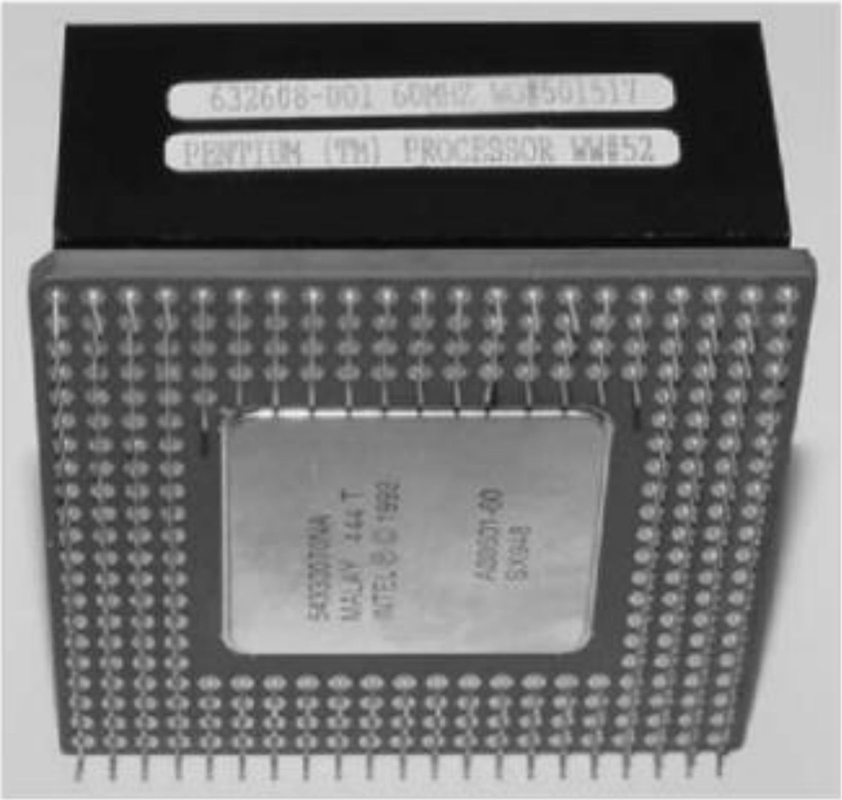


Figure 2-5. Pentium II Chip

Technical Software Failures or Errors

Large quantities of computer code are written, debugged, published, and sold before all their bugs are detected and resolved. Sometimes, combinations of certain software and hardware reveal new bugs. These failures range from bugs to untested failure conditions. Sometimes these bugs are not errors, but rather purposeful shortcuts left by programmers for benign or malign reasons. Collectively, shortcut access routes into programs that bypass security checks are called trap doors and can cause serious security breaches. Software bugs are so commonplace that entire Web sites are dedicated to documenting them. Among the most often used is Bugtraq, found at *www.securityfocus.com*, which provides up-to-the-minute information on the latest security vulnerabilities, as well as a very thorough archive of past bugs.

Apart from the threats mentioned above, missing, inadequate, or incomplete organizational policy or planning; missing, indequate, or incomplete controls; sabotage or vandalism; and technological obsolescence have to be considered.

2.1. Answer the questions

1. Why do employees's mistakes represent a serious threat to the confidentiality, integrity, and availability of data?
2. What threats are mentioned in the text? Which one is the biggest threat to an organization?
3. How can physical theft be controlled?
4. Why is electronic theft a more complex problem to manage and control?
5. Who is Maxus? What did he do? Give details to his act.
6. Can human error or failure be prevented? How can it be protected?
7. Are natural disasters considered threats in the information security? What effects do they cause?
8. Which mistakes do employees often make when they use information systems?

2.2. Decide whether the following statements are true (T), false (F) or no information (NI). Correct the false (F).

1. Experience, proper training, and the incorrect assumptions are just a few things that can cause these misadventures.

   A. True B. False C. NI

2. Much human error or failure can be prevented with training and ongoing awareness activities, but also with controls, ranging from simple procedures.

   A. True B. False C. NI

3. One of the best-known hardware failures is that of the Intel Pentium II chip, which had a defect that resulted in a calculation error under certain circumstances.

   A. True B. False C. NI

4. Large quantities of computer code are written, debugged, published, and sold before all their bugs are detected and resolved.

   A. True B. False C. NI

5. Technical hardware failures or errors has always been one of the most dangerous threads in the information security.

A. True B. False C. NI

2.3. Choose the best answer to complete the following questions and statements

1. …………….. occurs when an attacker or trusted insider steals information from a computer system and demands compensation for its return or for an agreement not to disclose it.

A. Information extortion C. Technical failure

B. Human Error D. B&D are correct

2. Technical hardware failures occur when a manufacturer distributes equipment containing a known or unknown flaw.

A. Technical hardware failures C. Theft

B. inadequate control D. Technological error

3. Which threat is the most dangerous to an organization's information security?

A. Information extortion C. Vandalism

B. An organization's own employees. D. Missing controls

4. The value of information is .... when it is copied without the owner's knowledge.

A. diminished C. A & B are correct

B. lessened D. minimized

5. Large quantities of .... are written, debugged, published, and sold before all their bugs are detected and resolved.

A. software C. computer code

B. hardware D. computer language

6. .... can present some of the most dangerous threats, because they usually occur with very little warning and are beyond the control of people.

A. Force majeure C. Forces of nature

B. Acts of God D. All are correct

3. Speaking

1. What main contents do you get from the text?
2. Choose two of the threats in the text and present it.

READING AND SPEAKING 3

1. Discuss the questions

1. What is an attack?
2. What attacks in the information security do you know? Which one is the most dangerous?
3. What does DDoS stand for? What is it?
4. Do you think your password can be attacked? If yes, how can your password be attacked?

2. Read the text and do the tasks below

Attacks (1)

An **attack** is an act that takes advantage of a vulnerability to compromise a controlled system. It is accomplished by a **threat agent** that damages or steals an organization's information or physical asset. A **vulnerability** is an identified weakness in a controlled system, where controls are not present or are no longer effective. Unlike threats, which are always present, attacks only exist when a specific act may cause a loss. For example, the *threat* of damage from a thunderstorm is present throughout the summer in many places, but an *attack* and its associated risk of loss only exist for the duration of an actual thunderstorm. The following sections discuss each of the major types of attacks used against controlled systems.

Malicious Code

The **malicious code** attack includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information. The state-of-the-art malicious code attack is the polymorphic, or multivector, worm. These attack programs use up to six known attack vectors to exploit a variety of vulnerabilities in commonly found information system devices. Perhaps the best illustration of such an attack remains the outbreak of Nimda in September 2001, which used five of the six vectors to spread itself with startling speed. TruSecure Corporation, an industry source for information security statistics and solutions, reports that Nimda spread to span the Internet address space of 14 countries in less than 25 minutes.

Other forms of malware include covert software applications—**bots** which are often the technology used to implement Trojan Horse, logic bobms, back doors; **spyware** is "any technology that aids in gathering information about a person or organization without their knowledge and it is placed on a computer to secretly gather information about the user and report it"; and **adware**—is "any software program intended for marketing purposes such as that used to deliver and display advertising banners or popups to the user's screen or tracking the user's online usage or purchasing activity.". Each of these hidden code components can be

used to collect information from or about the user which could then be used in a social engineering or identity theft attack.

Hoaxes

A more devious attack on computer systems is the transmission of a virus hoax *with a real virus attached*. When the attack is masked in a seemingly legitimate message, unsuspecting users more readily distribute it. Even though these users are trying to do the right thing to avoid infection, they end up sending the attack on to their coworkers and friends and infecting many users along the way.

Back Doors

Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource through a back door. Sometimes these entries are left behind by system designers or maintenance staff, and thus are called trap doors. A trap door is hard to detect, because very often the programmer who puts it in place also makes the access exempt from the usual audit logging features of the system.

Password Crack

Attempting to reverse-calculate a password is often called **cracking**. A cracking attack is a component of many dictionary attacks (to be covered shortly). It is used when a copy of the Security Account Manager (SAM) data file, which contains hashed representation of the user's password, can be obtained. A password can be hashed using the same algorithm and compared to the hashed results. If they are the same, the password has been cracked.

Brute Force

The application of computing and network resources to try every possible password combination is called a **brute force attack**. Since the brute force attack is often used to obtain passwords to commonly used accounts, it is sometimes called a **password attack**. If attackers can narrow the field of target accounts, they can devote more time and resources to these accounts. That is one reason to always change the manufacturer's default administrator account names and passwords. Password attacks are rarely successful against systems that have adopted the manufacturer's recommended security practices. Controls that limit the number of unsuccessful access attempts allowed per unit of elapsed time are very effective against brute force attacks.

Dictionary

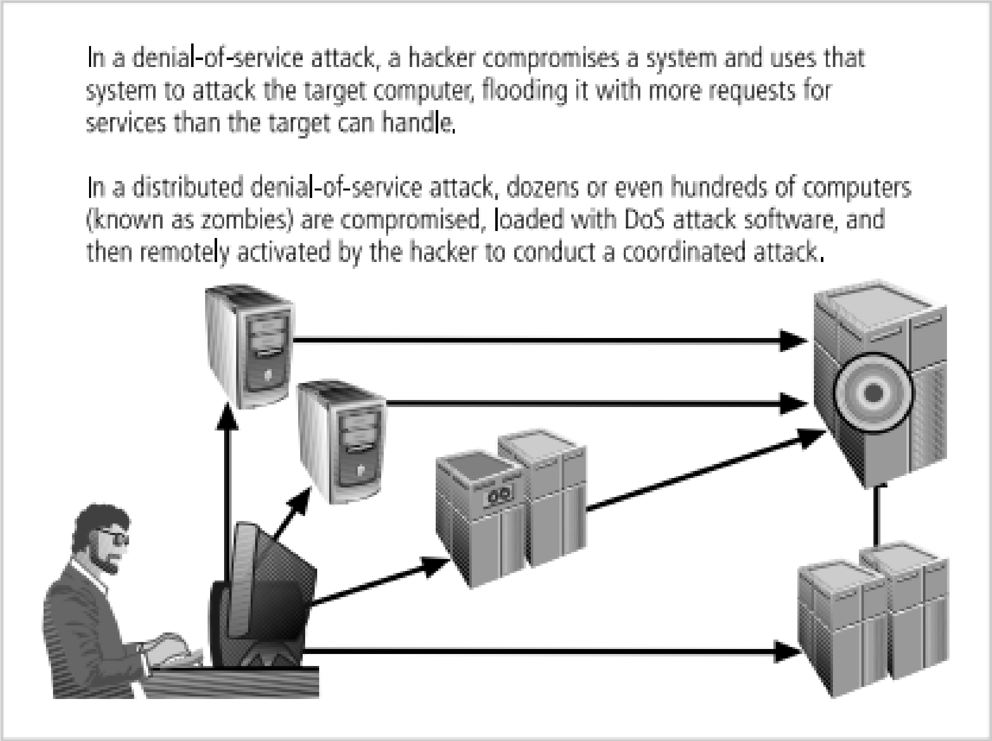
The **dictionary attack** is a variation of the brute force attack which narrows the field by selecting specific target accounts and using a list of commonly used passwords (the dictionary) instead of random combinations. Organizations can use similar dictionaries to disallow passwords during the reset process and thus guard against easy-to-guess passwords. In addition, rules requiring numbers and/or special characters in passwords make the dictionary attack less effective.

Denial-of-Service (DoS) and Distributed

Denial-of-Service (DDoS)

In a **denial-of-service (DoS)** attack, the attacker sends a large number of connection or information requests to a target *(see Figure 2-6).* So many requests are made that the target system becomes overloaded and cannot respond to legitimate requests for service. The system may crash or simply become unable to perform ordinary functions. A **distributed denial-of-service (DDoS)** is an attack in which a coordinated stream of requests is launched against a target from many locations at the same time. Most DDoS attacks are preceded by a preparation phase in which many systems, perhaps thousands, are compromised. The compromised machines are turned into **zombies**, machines that are directed remotely (usually by a transmitted command) by the attacker to participate in the attack. DDoS attacks are the most difficult to defend against, and there are presently no controls that any single organization can apply. There are, however, some cooperative efforts to enable DDoS defenses among groups of service providers; among them is the Consensus Roadmap for Defeating Distributed Denial of Service Attacks. To use a popular metaphor, DDoS is considered a weapon of mass destruction on the Internet. The MyDoom worm attack of early 2004 was intended to be a DDoS attack against *www.sco.com* (the Web site of a vendor of a UNIX operating system) that lasted from February 1, 2004 until February 12, 2004. Allegedly, the attack was payback for the SCO Group's perceived hostility toward the open-source Linux community.

Any system connected to the Internet and providing TCP-based network services (such as a Web server, FTP server, or mail server) is vulnerable to DoS attacks. DoS attacks can also be launched against routers or other network server systems if these hosts enable (or turn on) other TCP services (e.g., echo).



In a denial-of-service attack, a hacker compromises a system and uses that system to attack the target computer, flooding it with more requests for services than the target can handle.

In a distributed denial-of-service attack, dozens or even hundreds of computers (known as zombies) are compromised, loaded with DoS attack software, and then remotely activated by the hacker to conduct a coordinated attack.

Figure 2-6. Denial-of-Service Attacks

2.1. Answer the questions

1. What is a cracking attack? When is it used?
2. What is a distributed denial of-service**?**
3. Why is sometimes the brute force attack called a password attack?
4. Which attack includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information.

5. Why is a trap door hard to detect?

6. Why are always the manufacturer’s default administrator account names and passwords changed?

7. Why are many requests made that the target system becomes overloaded and cannot respond to legitimate requests for service in a DoS attack?

8. What is a vulnerability?

2.2. Decide whether the following statements are true (T), false (F) or no information (NI). Correct the false (F).

1. A lot of systems and users send information on local networks in clear text so sniffers add risk to the network.

A. True B. False [✓ C. NI]

2. It is absolutely imppossible to defend against DDoS attacks becaue they are too dangerous.

A. True [✓ B. False] C. NI

3. Similar dictionaries can be used to allow passwords during the reset process and thus guard against easy-to-guess passwords by organizations.

A. True [✓ B. False] C. NI

4. Many countries were affected by a malicious code named Nimda in a very short time.

[✓ A. True] B. False C. NI

5. A password can be hashed using the same algorithm and compared to the hashed results.

[✓ A. True] B. False C. NI

2.3. Choose the best answer to complete the following questions and statements

1. Which of the following attacks is a variation of the brute force attack?

[✓ A. Dictionary] B. Password crack

C.Back door D. Hoax

2. ....is any technology that aids in gathering information about a person or organization without their knowledge and it is placed on a

computer to secretly gather information about the user and report it.

A. Adware B. Denial-of-Service

C. Dictionary D. Spyware

3. ....attacks are the most difficult to defend against, and there are presently no controls that any single organization can apply.

A. Password crack C. DDoS

B. Dictionary D. Back door

4. ....belong to the state-of-the-art malicious code attack.

A. Polymorphic C. multivector

B. Worm D. All are correct

5. What attack is considered a weapon of mass destruction on the Internet to use a popular metaphor?

A. DDoS C. Back Door

B. Brute force D. Passaword Crack

3. Speaking

1. What main contents do you get from the text? What do you know about them?
2. Choose three of the attacks in the text and present it.

READING AND SPEAKING 4

1. Discuss the questions

1. Have you ever heard *man-in-the-middle*? If yes, what does it mean in your language?
2. What do you know about man-in-the-middle?
3. Have you ever heard *social engineering*? If yes, give some information about it.

2. Read the text and do the tasks below

Attacks (2)

Spoofing

Spoofing is a technique used to gain unauthorized access to computers, wherein the intruder sends messages with a source IP address that has been forged to indicate that the messages are coming from a trusted host. To engage in IP spoofing, hackers use a variety of techniques to obtain trusted IP addresses, and then modify the packet headers to insert these forged addresses. Newer routers and firewall arrangements can offer protection against IP spoofing (see Figure 2-7).

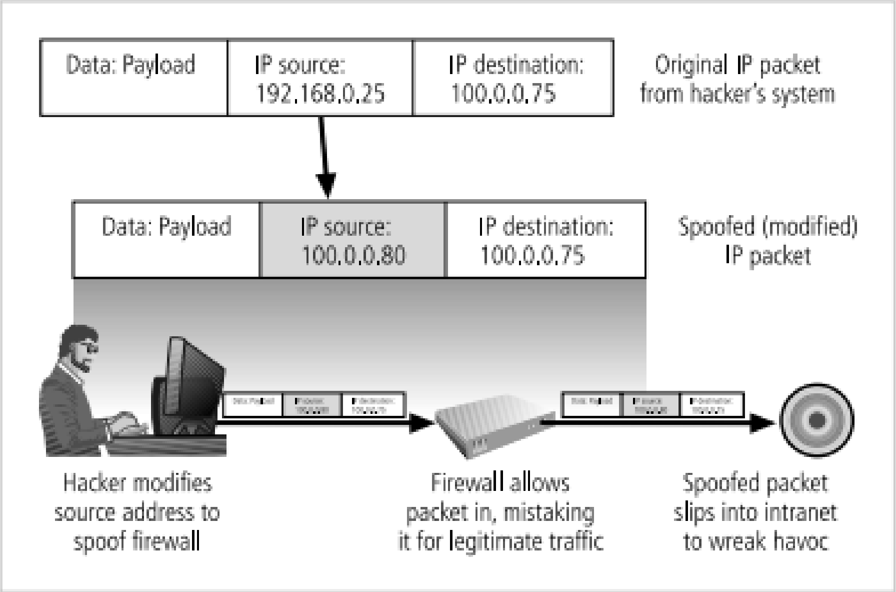

Data: Payload
IP source: 192.168.0.25
IP destination: 100.0.0.75
Original IP packet from hacker's system
Data: Payload
IP source: 100.0.0.80
IP destination: 100.0.0.75
Spoofed (modified) IP packet
Hacker modifies source address to spoof firewall
Firewall allows packet in, mistaking it for legitimate traffic
Spoofed packet slips into intranet to wreak havoc

Figure 2-7. IP Spoofing

Man-in-the-Middle

In the well-known **man-in-the-middle** or **TCP hijacking attack**, an attacker monitors (or sniffs) packets from the network, modifies them, and inserts them back into the network. This type of attack uses IP spoofing to enable an attacker to impersonate another entity on the network. It allows the attacker to eavesdrop as well as to change, delete, reroute, add, forge, or divert data.39 A variant of TCP hijacking, involves the interception of an encryption key exchange, which enables the hacker to act as an invisible man-in-the-middle—that is, an eavesdropper—on encrypted communications. Figure 2-8 illustrates these attacks by showing how a hacker uses public and private encryption keys to intercept messages.

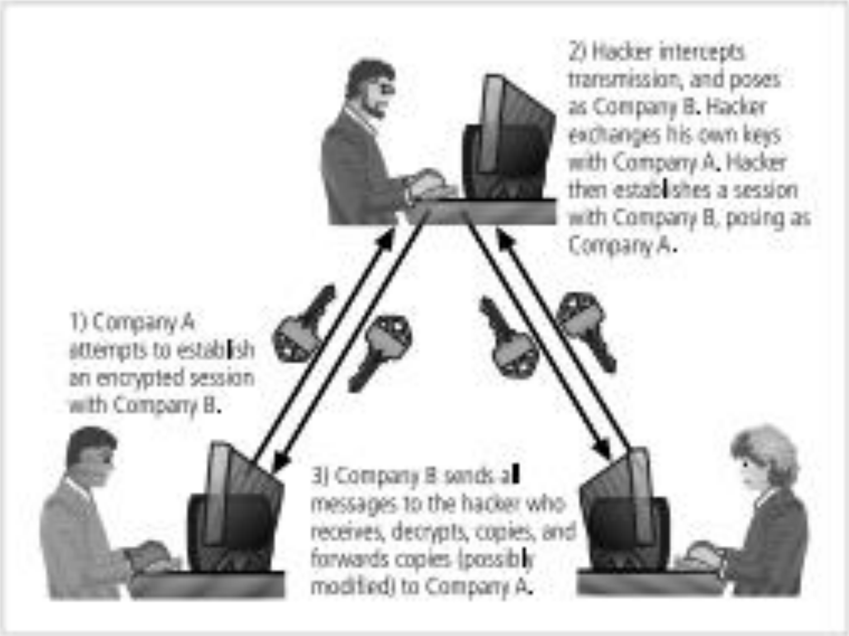

2) Hacker intercepts transmission, and poses as Company B. Hacker exchanges his own keys with Company A. Hacker then establishes a session with Company B, posing as Company A.
1) Company A attempts to establish an encrypted session with Company B.
3) Company B sends all messages to the hacker who receives, decrypts, copies, and forwards copies (possibly modified) to Company A.

Figure 2-8. Man-in-the-middle

Spam

Spam is unsolicited commercial e-mail. While many consider spam a trivial nuisance rather than an attack, it has been used as a means of enhancing malicious code attacks. In March 2002, there were reports of malicious code embedded in MP3 files that were included as attachments to spam. The most significant consequence of spam, however, is the waste of computer and human resources. Many organizations attempt to cope with the flood of spam by using e-mail filtering technologies. Other organizations simply tell the users of the mail system to delete unwanted messages.

Mail Bombing

Another form of e-mail attack that is also a DoS is called a **mail bomb**, in which an attacker routes large quantities of e-mail to the target. This can be accomplished by means of social engineering (to be discussed shortly) or by exploiting various technical flaws in the Simple Mail Transport Protocol (SMTP). The target of the attack receives an unmanageably large volume of unsolicited e-mail. By sending large e-mails with forged header information, attackers can take advantage of poorly configured e-mail systems on the Internet and trick them into sending many e-mails to an address chosen by the attacker. If many such systems are tricked into participating in the event, the target e-mail address is buried under thousands or even millions of unwanted e-mails.

Sniffers

A **sniffer** is a program or device that can monitor data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information. Unauthorized sniffers can be extremely dangerous to a network's security, because they are virtually impossible to detect and can be inserted almost anywhere. This makes them a favorite weapon in the hacker's arsenal. Sniffers often work on TCP/IP networks, where they're sometimes called **packet sniffers**. Sniffers add risk to the network, because many systems and users send information on local networks in clear text. A sniffer program shows all the data going by, including passwords, the data inside files—such as word-processing documents—and screens full of sensitive data from applications.

Social Engineering

In the context of information security, social engineering is the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker. There are several social engineering techniques, which usually involve a perpetrator posing as a person higher in the organizational hierarchy than the victim. To prepare for this false representation, the perpetrator may have used social engineering tactics against others in the organization to collect seemingly unrelated information that, when used together, makes the false representation more credible. For instance, anyone can check a company's Web site, or even call the main switchboard to get the name of the CIO; an attacker may then obtain even more information by calling others in the company and asserting his or her (false) authority by mentioning the CIO's name. Social engineering attacks may involve individuals posing as new employees or as current employees requesting assistance to prevent getting fired. Sometimes attackers threaten, cajole, or beg to sway the target.

There are many other attacks that involve social engineering. One of them is **Phishing -** an attempt to gain personal or financial information from an individual, usually by posing as a legitimate entity. A variant is ***spear phishing***, a label that applies to any highly targeted phishing attack. While normal phishing attacks target as many recipients as possible, a spear phisher sends a message that appears to be from an employer, a colleague, or other legitimate correspondent, to a small group or even one specific person. This attack is sometimes used to target those who use a certain product or Web site. Phishing attacks use three primary techniques, often in combination with one another: URL manipulation, Web site forgery, and phone phishing.

Pharming

Pharming is "the redirection of legitimate Web traffic (e.g., browser requests) to an illegitimate site for the purpose of obtaining private information. Pharming often uses Trojans, worms, or other virus technologies to attack the Internet browser's address bar so that the valid URL typed by the user is modified to that of the illegitimate Web site. Pharming may also exploit the Domain Name System (DNS) by causing it to transform the legitimate host name into the invalid site's IP address; this form of pharming is also known as **DNS cache poisoning**.

Timing Attack

A timing attack explores the contents of a Web browser's cache and stores a malicious cookie on the client's system. The cookie (which is a small quantity of data stored by the Web browser on the local system, at the direction of the Web server) can allow the designer to collect information on how to access password-protected sites. Another attack by the same name involves the interception of cryptographic elements to determine keys and encryption algorithms.

2.1. Answer the questions

1. What is phishing? What is its variant?

2. How may pharming also exploit the Domain Name System?

3. What do sometimes attackers do to sway the target for social engineering?

4. In which attack does an attacker monitor packets from the network, modify them, and insert them back into the network?

5. Why does pharming often use Trojans, worms, or other virus technologies
to attack the Internet browser's address bar?

6. What do hackers use to engage in IP spoofing?

7. In Which attack can the cookie allow the designer to collect information
on how to access password-protected sites?

2.2. Decide whether the following statements are true (T), false (F) or no information (NI). Correct the false (F).

1. Phishing is a technique of fraudulently obtaining private information.

   A. True B. False C. NI

2. Just a few attacks are preceded by a preparation phase in which many systems, perhaps thousands, are compromised.

   A. True B. False C. NI

3. Sniffers add risk to the network, because many systems and users send information on local networks in clear text.

   A. True B. False C. NI

4. Pharming and timing attack belong to social engineering attacks.

   A. True B. False C. Ni

5. One of the techniques which spoofing attaker used to gain unauthorized access to computers is forging a source IP address.

   A. True B. False C. NI

2.3. Choose the best answer to complete the following questions and statements

1. Sending large e-mails with forged header information, ...can take advantage of poorly configured e-mail systems on the Internet and trick them into sending many e-mails to an address chosen by the attacker.

   A.attackers C. users

   B. Organizers D. programmers

2................explores the contents of a Web browser’s cache and ....
a malicious cookie on the client’s system.

C.Pharming/uses C. A timing attack/ stores

D.Spam/contains D. None is correct

3...........can be used both for legitimate network management functions and for stealing information.

A. Spyware C. Brute force

B. Sniffers D. Dictionary

4. Many organizations attempt **to cope with** the flood of spam by using e-mail filtering technologies.

A. to deal with C. keep up with

B. get on well D. put on with

5. Which attacks can be accomplished by exploiting various technical flaws in the Simple Mail Transport Protocol.

A. Man-the-middle C. Mail Boming

B. Phishing D. Pharming

6...............is an attempt to gain personal or financial information from an individual, usually by posing as a legitimate entity.

A. Dictionary C. Sniffer

B. Phishing D. Hoax

3. Speaking

1. What main contents do you get from the text? What do you know about them?
2. Choose three of the attacks in the text and present them.

4. Listening

1. https://www.youtube.com/watch?v=MIzKq8_Q0ro
2. https://www.youtube.com/watch?v=jIDmqDhsi7k
3. https://www.youtube.com/watch?v=n8mbzU0X2nQ
4. https://www.youtube.com/watch?v=-Z3pp14oUiA
5. https://www.youtube.com/watch?v=M2kExUGSDEo
6. https://www.youtube.com/watch?v=yAnthlVHxbk

WRITING AND SPEAKING

1. Write about 400 words about one of the following contents in your own words.

    - Threats in the information security.
    - Attacks in the information security

2. Present attacks in the information security.
3. Present threats in the information security.

FUTHER READING

Cyberattacks

In computers and computer networks an **attack** is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an asset. A **cyberattack** is any type of offensive maneuver that targets computer information systems, infrastructures, computer networks, or personal computer devices. An attacker is a person or process that attempts to access data, functions or other restricted areas of the system without authorization, potentially with malicious intent. Depending on context, cyberattacks can be part of cyberware or cyberterrorism. A cyberattack can be employed by sovereign states, individuals, groups, society or organizations, and it may originate from an anonymous source.

A cyberattack may steal, alter, or destroy a specified target by hacking into a susceptible system. Cyberattacks can range from installing spyware on a personal computer to attempting to destroy the infrastructure of entire nations. Legal experts are seeking to limit the use of the term to incidents causing physical damage, distinguishing it from the more routine data breaches and broader hacking activities. Cyberattacks have become increasingly sophisticated and dangerous

Types of cyberattack

An attack can be *active* or *passive*.

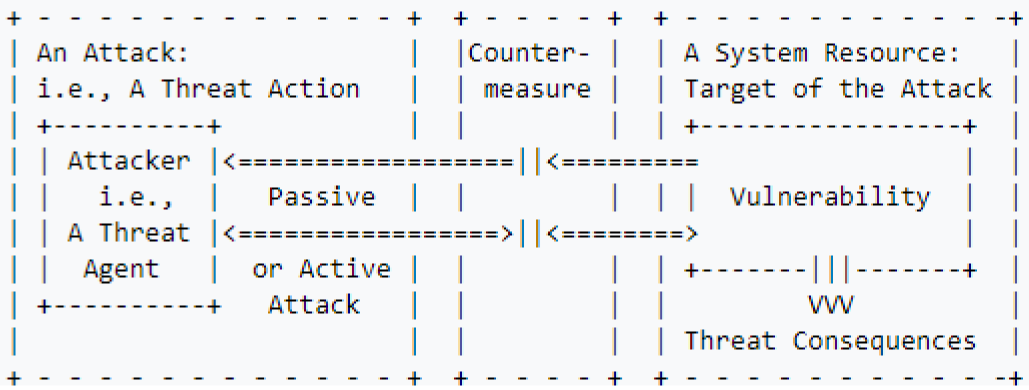
- An "active attack" attempts to alter system resources or affect their operation.
  - ➢ Denial-of-service attack
  - ➢ Spoofing
  - ➢ Mixed threat attack
  - ➢ Network (Man-in-the-middle, Man-in-the-browser, ARP poisoning, Ping flood, Ping of death, and Smurf attack)
  - ➢ Host (Buffer overflow, Heap overflow, Stack overflow, Format string attack
- A "passive attack" attempts to learn or make use of information from the system but does not affect system resources.

- ➢ Computer and network surveillance
- ➢ Network (Wiretapping, Fiber tapping, Port scan, and Idle scan)
- ➢ Host (Keystroke logging, Data scraping, Backdoor

An attack can be perpetrated by an *insider* or from *outside* the organization;

- An "inside attack" is an attack initiated by an entity inside the security perimeter (an "insider"), i.e., an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization.
- An "outside attack" is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an "outsider"). In the Internet, potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

The term "attack" relates to some other basic security terms as shown in the following diagram:



```
+ - - - - - - - - - - - - +  + - - - - +  + - - - - - - - - - - -+
| An Attack:              |  |Counter- |  | A System Resource:   |
| i.e., A Threat Action   |  | measure |  | Target of the Attack |
| +----------+            |  |         |  | +-----------------+  |
| | Attacker |<==================||<=========                 |  |
| |   i.e.,  |   Passive  |  |         |  | |  Vulnerability  |  |
| | A Threat |<=================>||<========>                 |  |
| |  Agent   |  or Active |  |         |  | +-------|||-------+  |
| +----------+   Attack   |  |         |  |         VVV          |
|                         |  |         |  | Threat Consequences  |
+ - - - - - - - - - - - - +  + - - - - +  + - - - - - - - - - - -+
```

A resource (both physical or logical), called an asset, can have one or more vulnerabilities that can be exploited by a threat agent in a threat action. As a result, the confidentiality, integrity or availability of resources may be compromised. Potentially, the damage may extend to resources in addition to the one initially identified as vulnerable, including further resources of the organization, and the resources of other involved parties (customers, suppliers).

UNIT 3: FIREWALLS

READING AND SPEAKING 1

1. Discuss the questions

1. What is a firewall in computing?
2. Is the term "firewall" only used in computing?
3. What are the advantages of firewalls?
4. How many types of firewall do you know ? What are they?
5. Do firewalls always have advantages? If not, what are its disadvantages?

2. Read the text and do the tasks below

A firewall and its history

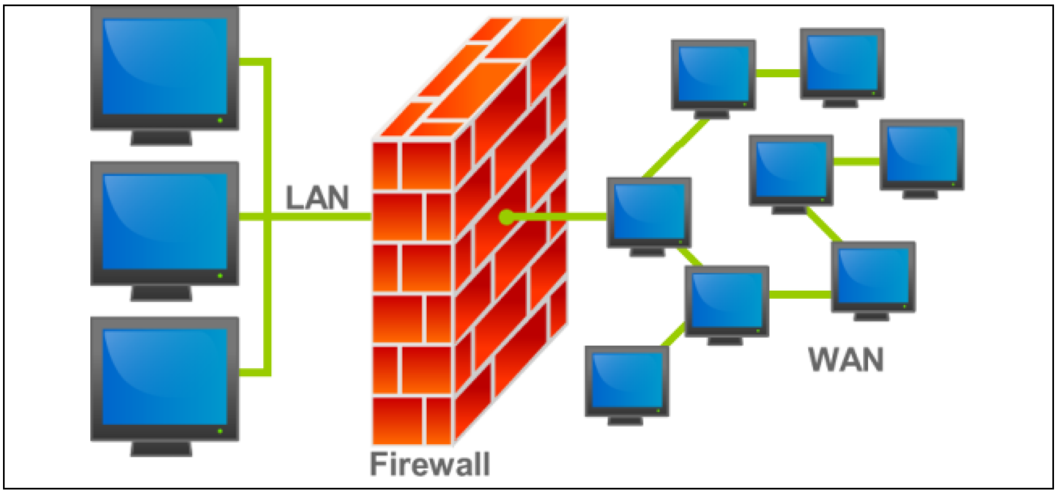


Figure 3-1. Firewalls

In commercial and residential construction, firewalls are concrete or masonry walls that run from the basement through the roof, to prevent a fire from spreading from one section of the building to another. In aircraft and automobiles, a firewall is an insulated metal barrier that keeps the hot and dangerous moving parts of the motor separate from the inflammable interior where the passengers sit. A **firewall** in an information security program is similar to a building's firewall in that it prevents specific types of information from moving between the outside world, known as the **untrusted network** (for example, the Internet), and the inside world, known as the **trusted network**. The firewall may be a separate computer system, a software service running on an existing router or server, or a separate network containing a number of supporting devices. In computing, a **firewall** is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet. Firewalls can be categorized by processing mode, development era, or structure.

The term *firewall* originally referred to a wall intended to confine a fire within a line of adjacent buildings. Later uses refer to similar structures, such as the metal sheet separating the engine compartment of a vehicle or aircraft from the passenger compartment. The term was applied in the late 1980s to network technology that emerged when the Internet was fairly new in terms of its global use and connectivity. The predecessors to firewalls for network security were the routers used in the late 1980s, because they separated networks from one another, thus halting the spread of problems from one network to another.

Before it was used in real-life computing, the term appeared in the 1983 computer-hacking movie WarGames, and possibly inspired its later use.

First generation: packet filters

The first reported type of network firewall is called a packet filter. Packet filters act by inspecting packets transferred between computers. When a packet does not match the packet filter's set of filtering rules, the packet filter either drops (silently discards) the packet, or rejects the packet (discards it and generates an Internet Control Message Protocol notification for the sender) else it is allowed to pass. Packets may be filtered by source and destination network addresses, protocol, source and destination port numbers. The bulk of Internet communication in 20th and early 21st century used either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) in conjunction with well-known ports, enabling firewalls of that era to distinguish between, and thus control, specific types of traffic (such as web browsing, remote printing, email transmission, file transfer), unless the machines on each side of the packet filter used the same non-standard ports.

The first paper published on firewall technology was in 1987, when engineers from Digital Equipment Corporation (DEC) developed filter systems known as packet filter firewalls. At AT&T Bell Labs, Bill Cheswick and Steve Bellovin continued their research in packet filtering and developed a working model for their own company based on their original first generation architecture.

Second generation: stateful filters

From 1989–1990, three colleagues from AT&T Bell Laboratories, Dave Presotto, Janardan Sharma, and Kshitij Nigam, developed the second generation of firewalls, calling them circuit-level gateways.

Second-generation firewalls perform the work of their first-generation predecessors but also maintain knowledge of specific conversations between endpoints by remembering which port number the two IP addresses are using at layer 4 (transport layer) of the OSI model for their conversation, allowing examination of the overall exchange between the nodes.

This type of firewall is potentially vulnerable to denial-of-service attacks that bombard the firewall with fake connections in an attempt to overwhelm the firewall by filling its connection state memory.

Third generation: application layer

Marcus Ranum, Wei Xu, and Peter Churchyard released an application firewall known as Firewall Toolkit (FWTK) in October 1993. This became the basis for Gauntlet firewall at Trusted Information Systems.

The key benefit of application layer filtering is that it can understand certain applications and protocols (such as File Transfer Protocol (FTP), Domain Name System (DNS), or Hypertext Transfer Protocol (HTTP)). This is useful as it is able to detect if an unwanted application or service is attempting to bypass the firewall using a disallowed protocol on an allowed port, or detect if a protocol is being abused in any harmful way

As of 2012, the so-called next-generation firewall (NGFW) is a wider or deeper inspection at the application layer. For example, the existing deep packet inspection functionality of modern firewalls can be extended to include:

- Intrusion prevention systems (IPS)
- User identity management integration (by binding user IDs to IP or MAC addresses for "reputation")

- Web application firewall (WAF). WAF attacks may be implemented in the tool "WAF Fingerprinting utilizing timing side channels"

2.1. Answer the questions

1. What is a firewall in computing?
2. Where does the term firewall derive from?
3. Is a firewall in an information security program the same as or different from a building's firewall? What is their similarity or difference?
4. What are the functions of stateful filters?
5. How can firewalls be categorized?
6. What are the predecessors to firewalls for network security?
7. What is the most important benefit of application layer filtering?
8. What are the benefits of firewalls in aircraft and automobiles?

2.2. Decide whether the following statements are true (T), false (F) or no information (NI). Correct the false one

1. Packet filters operates by inspecting packets transferred between computers.

[✓ A. True] B. False C. NI

2. Firewall Toolkit was invented by Marcus Ranum, Wei Xu, and Peter Churchyard.

A. True [✓ B. False] C. NI

3. Circuit-level gateways are the first generation of firewalls

A. True [✓ B. False] C. NI

4. Firewalls are built between or through buildings, structures, or electrical substation transformers, or within an aircraft or vehicle.

[✓ A. True] B. False C. NI

5. Firewalls can be used to subdivide a building into separate fire areas and are constructed in accordance with the locally applicable building codes.

A. True B. False [✓ C. NI]

2.3. Choose the best answer for the following questions and statements

1..............is typically established between a trusted internal network and untrusted external network in ....

A. a panel/computing B. a wall/construction

C. a shield/computing D. A&C are correct

2. When was Firewall was applied and what was it applied for?

A. In 1987/ firewall technology

B. in the late 1980s/ network technology

C. In early 21st century/IP address

D. In October 1993/ Information systems

3. The benefit of firewalls ....is preventing a fire from spreading from one section of the building to another.

A. In commercial and residential construction

B. in an information security program

C. In computing

C. A&C are correct

4. What is WarGames and when was it made?

A. Third generation firewall/in 2012

B. Packet filters/in early 21st century

C. A computer-hacking movie/in the 1983

D. stateful filters/ from 1989-1990

5. What became the basis for Gauntlet firewall at Trusted Information Systems?

A. Hypertext Transfer Protocol B. Firewall Toolkit

C. User Datagram Protocol D. transport layer

3. Speaking

1. What main information do you get from the text?
2. Present a firewall and its history.

READING AND SPEAKING 2

1. Discuss the questions

1. What does the word “*appliance*” mean?
2. What does SOHO stand for? What does it mean?
3. How are firewalls classified?

2. Read the text and do the tasks below

Firewalls Categorized by Structure

Firewalls can also be categorized by the structures used to implement them. Most commercial-grade firewalls are dedicated *appliances*. Specifically, they are stand-alone units running on fully customized computing platforms that provide both the physical network connection and firmware programming necessary to perform their function, whatever that function (static packet filtering, application proxy, etc.) may be. Some firewall appliances use highly customized, sometimes proprietary hardware systems that are developed exclusively as firewall devices. Other commercial firewall systems are actually off-the-shelf general purpose computer systems that run custom application software on standard operating systems like Windows or Linux/Unix, or on specialized variants of these operating systems. Most small office or residential-grade firewalls are either simplified dedicated appliances running on computing devices or application software installed directly on the user’s computer.

Commercial-Grade Firewall Appliances

Firewall appliances are stand-alone, selfcontained combinations of computing hardware and software. These devices frequently have many of the features of a general-purpose computer with the addition of firmwarebased instructions that increase their reliability and performance and minimize the likelihood of their being compromised. The customized software operating system that drives the device can be periodically upgraded, but can only be modified via a direct physical connection or after running extensive authentication and authorization protocols. The firewall rule sets are stored in nonvolatile memory, and thus they can be changed by technical staff when necessary but are available each time the device is restarted.

These appliances can be manufactured from stripped-down general purpose computer systems, and/or designed to run a customized version of a general-purpose operating system. These variant operating systems are tuned to meet the type of firewall activity built into the application software that provides the firewall functionality.

Commercial-Grade Firewall Systems

A commercial-grade firewall system consists of application software that is configured for the firewall application and run on a general-purpose computer. Organizations can install firewall software on an existing general purpose computer system, or they can purchase hardware that has been configured to specifications that yield optimum firewall performance. These systems exploit the fact that firewalls are essentially application software packages that use common general purpose network connections to move data from one network to another.

Small Office/Home Office (SOHO) Firewall Appliances

As more and more small businesses and residences obtain fast Internet connections with digital subscriber lines (DSL) or cable modem connections, **they** become more and more vulnerable to attacks. What many small business and work-from-home users don't realize is that, unlike dial-up connections, these high-speed services are always on; therefore, the computers connected to them are much more likely to be visible to the scans performed by attackers than those connected only for the duration of a dial-up session. One of the most effective methods of improving computing security in the SOHO setting is by means of a SOHO or residential-grade firewall. These devices, also known as broadband gateways or DSL/cable modem routers, connect the user's local area network or a specific computer system to the Internetworking device—in this case, the cable modem or DSL router provided by the Internet service provider (ISP). The SOHO firewall serves first as a stateful firewall to enable inside-to-outside access and can be configured to allow limited TCP/IP port forwarding and/or screened subnet capabilities. *(see Figure 3-2)*

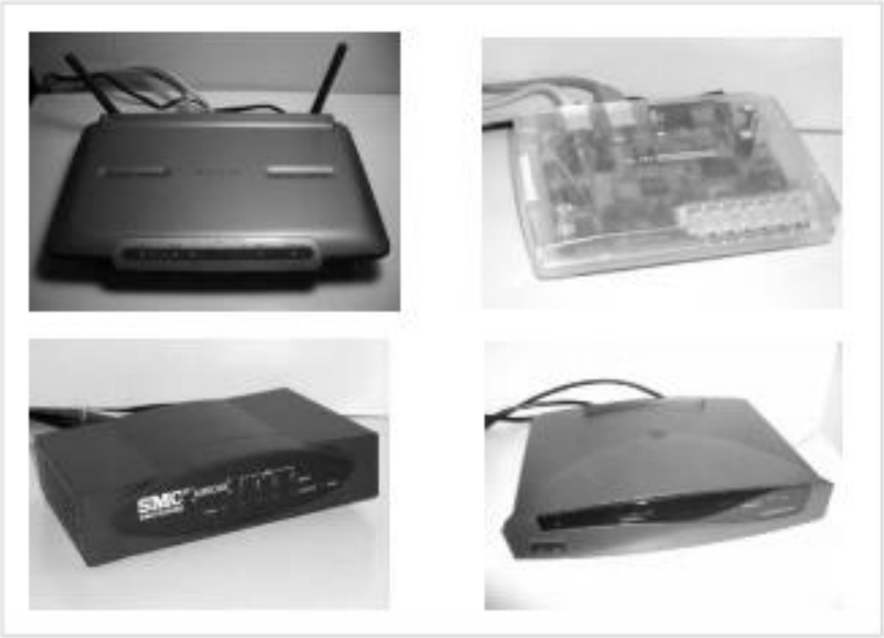


Figure 3-2. SOHO Firewall Device

Residential-Grade Firewall Software

Another method of protecting the residential user is to install a software firewall directly on the user's system. Many people have implemented these residential-grade software-based firewalls (some of which also provide antivirus or intrusion detection capabilities), but, unfortunately, they may not be as fully protected as they think.

Software Versus Hardware: The SOHO Firewall Debate

So which type of firewall should the residential user implement? Many users swear by their software firewalls. Personal experience will produce a variety of opinionated perspectives. Ask yourself this question: *Where* would you rather defend against the attacker? The software option allows the hacker inside your computer to battle a piece of software (free software, in many cases) that may not be correctly installed, configured, patched, upgraded, or designed. If the software happens to have a known vulnerability, the attacker could bypass it and then have unrestricted access to your system. With a hardware firewall, even if the attacker manages to crash the firewall system, your computer and information are still safely behind the now disabled connection. The hardware firewall's use of no routable addresses further extends the protection, making it virtually impossible for the attacker to reach your information. A former student of one of the authors responded to this debate by installing a hardware firewall, and then visiting a hacker chat room. He challenged the group to penetrate his system. A few days later, he received an e-mail from a hacker claiming to have accessed his system. The hacker included a graphic of a screen showing a C:\ prompt, which he claimed was from the student's system. After doing a bit of research, the student found out that the firewall had an image stored in firmware that was designed to distract attackers. It was an image of a command window with a DOS prompt. The hardware (NAT) solution had withstood the challenge.

2.1. Answer the questions

1. What does a commercial-grade firewall system consist of?
2. Why can the firewall rule sets be changed by technical staff when necessary ?
3. What are most small office or residential-grade firewalls?
4. What is one of the most effective methods of improving computing security in the SOHO setting?
5. What method is used for protecting the residential user?
6. What are Windows or Linux/Unix?
7. Why do more and more small businesses and residences become more and more vulnerable to attacks?

2.2. Decide whether the following statements are true (T), false (F) or no information (NI)

1. Broadband gateways or DSL/cable modem routers are commercial-Grade Firewall Appliances.

   A. True B. False C. NI

2. If the residental users install a software firewall directly on the their system, their computer completely is protected.

   A.True B. False C. NI

3. Firewalls can also be categorized by the structures used to implement them. Most commercial-grade firewalls are dedicated *appliances*.

   A. True B. False C. NI

4. All firewall devices can be configured in a number of network connection

architectures.

A.True B. False C. NI

5. The hardware firewall's use of no routable addresses further extends the protection, making it virtually impossible for the attacker to reach your information.

A.True B. False C. NI

2.3. Choose the best answer for the following statements

1. ....are stand-alone, selfcontained combinations of computing hardware and software.

A. Firewall appliances B. Firewall architectures

C. Firewall systems D. Firewall software

2. Organizations can install ....on an existing general purpose computer system.

A. firewall hardware B. firewall architecture

C. firewall software D. firewall devices

3. Which of the following does the word "**they**" in the paragraph 4 refer to?

A. digital subscriber lines B. Internet connections

C. cable modem connections D. businesses and residences

4. Which of the following helps your computer still be safe nomatter how hard the atackers manage?

A. An intivirus software program B. A strong password

C. A hardware firewall D. SOHO

5. The SOHO firewall serves first as a stateful firewall to enable ....access.

A. inside-to-outside B. outside-to-inside

C. A&B are correct D. None is correct

3. Speaking

1. What main contents do you get from the text?

2. Choose one of the contents in the text and present it.

READING AND SPEAKING 3

1. Discuss the questions

1. What does the word “architecture? mean? List some words that go with it?
2. What do you know about firewall architectures in computing?
2. What does NIC stand for? What does it mean?

2. Read the text and do the tasks below

Firewall Architectures

All firewall devices can be configured in a number of network connection architectures. These approaches are sometimes mutually exclusive and sometimes can be combined. The configuration that works best for a particular organization depends on three factors: the objectives of the network, the organization’s ability to develop and implement the architectures, and the budget available for the function. Although literally hundreds of variations exist, there are four common architectural implementations: Packet-filtering routers, screened host firewalls, dual-homed firewalls, and screened subnet firewalls.

Packet-Filtering Routers

Most organizations with an Internet connection have some form of a router at the boundary between the organization’s internal networks and the external service provider. Many of these routers can be configured to reject packets that the organization does not want to allow into the network. This is a simple but effective way to lower the organization’s risk from external attack. The drawbacks to this type of system include a lack of auditing and strong authentication.

Screened Host Firewalls (see Figure 3-3)

Screened host firewalls combine the packet-filtering router with a separate, dedicated firewall, such as an application proxy server. This approach allows the router to prescreen packets to minimize the network traffic and load on the internal proxy. The application proxy examines an application layer protocol, such as HTTP, and performs the proxy services. This separate host is often referred to as a **bastion host**; it can be a rich target for external attacks and should be very thoroughly secured. Even though the bastion host/application proxy actually contains only cached copies of the internal Web documents, it can still present a promising target, because compromise of the bastion host can disclose the configuration of internal networks and possibly provide attackers with internal information. Since the bastion host stands as a sole defender on the network perimeter, it is commonly referred to as the **sacrificial host**. To its advantage, this configuration requires the external attack to compromise two separate systems before the attack can access internal data. In this way, the bastion host protects the data more fully than the router alone.

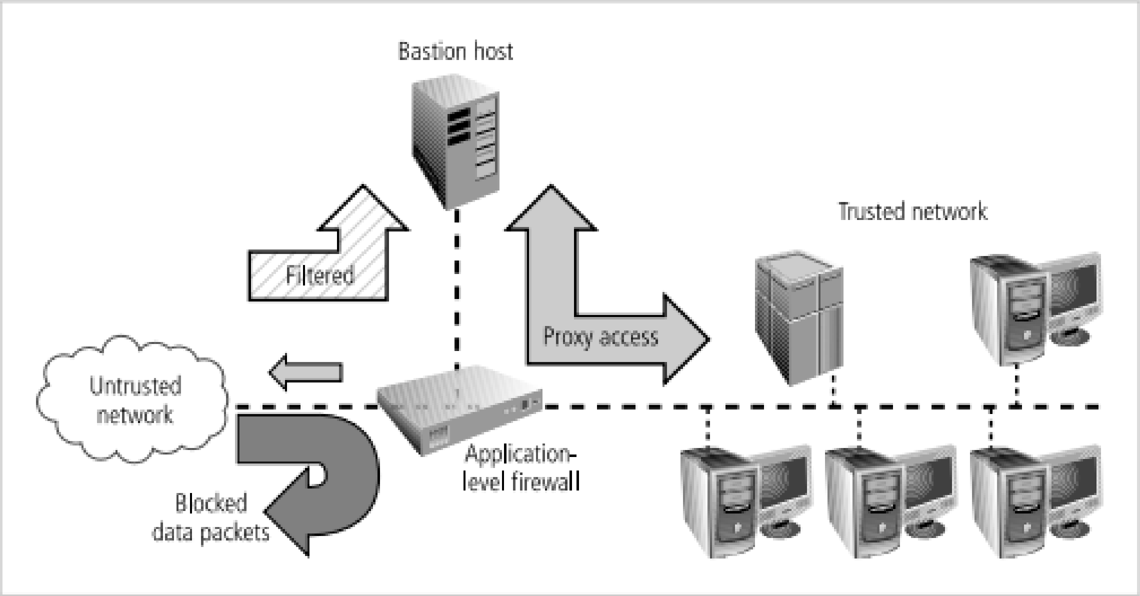


Figure 3-3. Screened Host Firewalls

Dual-Homed Host Firewalls (see Figure 3-4)

The next step up in firewall architectural complexity is the dual-homed host. When this architectural approach is used, the bastion host contains two NICs (network interface cards) rather than one, as in the bastion host configuration. One NIC is connected to the external network, and one is connected to the internal network, providing an additional layer of protection. With two NICs, all traffic *must* physically go through the firewall to move between the internal and external networks. Implementation of this architecture often makes use of NAT.

NAT is a method of mapping real, valid, external IP addresses to special ranges of no routable internal IP addresses, thereby creating yet another barrier to intrusion from external attackers. The internal addresses used by NAT consist of three different ranges. Taking advantage of this, NAT prevents external attacks from reaching internal machines with addresses in specified ranges. If the NAT server is a multi-homed bastion host, it translates between the true, external IP addresses assigned to the organization by public network naming authorities and the internally assigned, no routable IP addresses. NAT translates by dynamically assigning addresses to internal communications and tracking the conversations with sessions to determine which incoming message is a response to which outgoing traffic. Figure 6-13 shows a typical configuration of a dual-homed host firewall that uses NAT and proxy access to protect the internal network. Another benefit of a dual-homed host is its ability to translate between many different protocols at their respective data link layers, including Ethernet, token ring, Fiber Distributed Data Interface (FDDI), and asynchronous transfer mode (ATM). On the downside, if this dual-homed host is compromised, it can disable the connection to the external network, and as traffic volume increases it can become overloaded. However, compared to more complex solutions this architecture provides strong overall protection with minimal expense

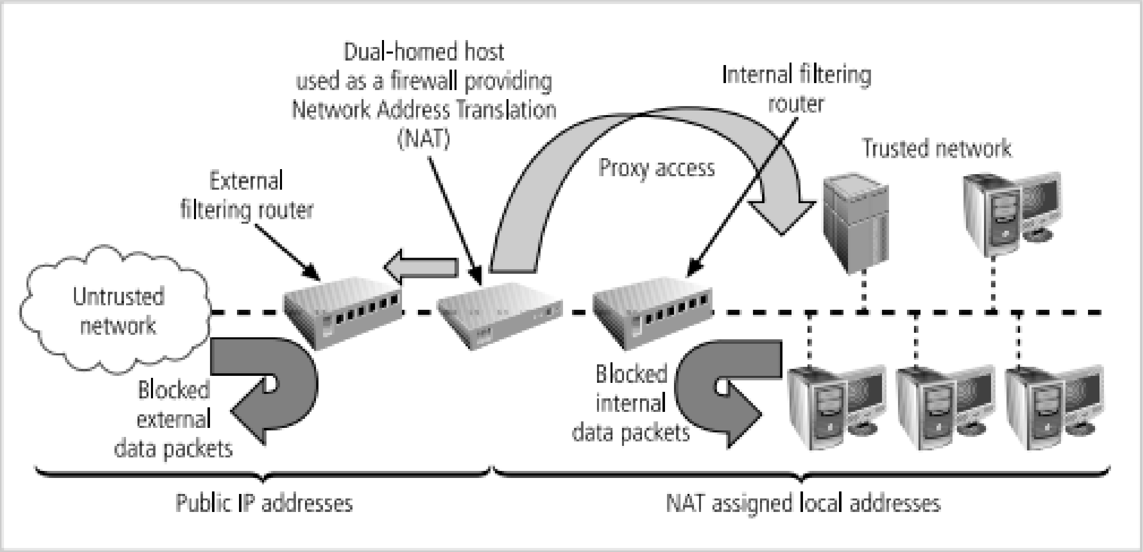

Dual-homed host used as a firewall providing Network Address Translation (NAT)
Internal filtering router
Trusted network
Proxy access
External filtering router
Untrusted network
Blocked external data packets
Blocked internal data packets
Public IP addresses
NAT assigned local addresses

Figure 3-4. Dual-Homed Host Firewalls

Screened Subnet Firewalls (with DMZ) (see Figure 3-5)

The dominant architecture used today is the screened subnet firewall. The architecture of a screened subnet firewall provides a DMZ. The DMZ can be a dedicated port on the firewall device linking a single bastion host, or it can be connected to a screened subnet, as shown in Figure 6-14. Until recently, servers providing services through an untrusted network were commonly placed in the DMZ. Examples of these include Web servers, file transfer protocol (FTP) servers, and certain database servers. More recent strategies using proxy servers have provided much more secure solutions.

A common arrangement finds the subnet firewall consisting of two or more internal bastion hosts behind a packet-filtering router, with each host protecting the trusted network. There are many variants of the screened subnet architecture. The first general model consists of two filtering routers, with one or more dual-homed bastion hosts between them. In the second general model, the connections are routed as follows:

- Connections from the outside or untrusted network are routed through an external filtering router.
- Connections from the outside or untrusted network are routed into—and then out of—a routing firewall to the separate network segment known as the DMZ.
- Connections into the trusted internal network are allowed only from the DMZ bastion host servers.

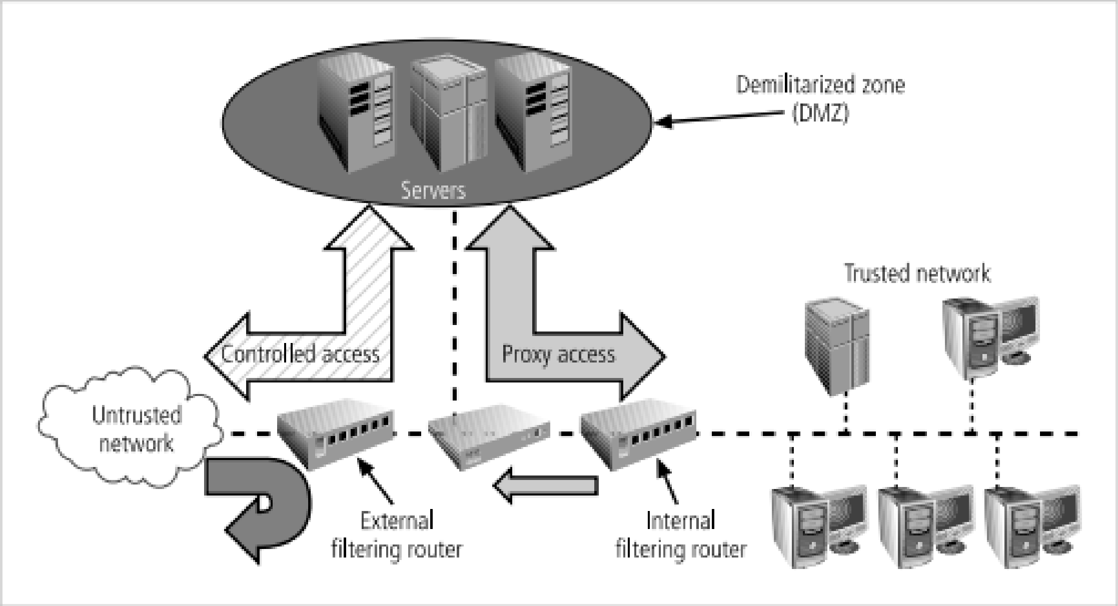


Figure 3-5. Screened Subnet Firewalls (with DMZ)

SOCKS Servers

Deserving of brief special attention is the SOCKS firewall implementation. SOCKS is the protocol for handling TCP traffic via a proxy server. The SOCKS system is a proprietary circuit-level proxy server that places special SOCKS client-side agents on each workstation. The general approach is to place the filtering requirements on the individual workstation rather than on a single point of defense (and thus point of failure). This frees the entry router from filtering responsibilities, but it requires that each workstation be managed as a firewall detection and protection device. A SOCKS system can require support and management resources beyond those of traditional firewalls since it entails the configuration and management of hundreds of individual clients, as opposed to a single device or small set of devices.

2.1. Answer the questions

1. What common architectural implementations are mentioned in the text?
2. Why do most organizations with an Internet connection have some form of a router at the boundary between the organization's internal networks and the external service provider?
3. Which approach allows the router to prescreen packets to minimize the network traffic and load on the internal proxy?
4. What is the protocol for handling TCP traffic via a proxy server?
5. Are there many variants of the screened subnet architecture? What does the first general model consist of?
6. How many NICs does the bastion host contain? What are they?
7. Why is NAT able to prevent external attacks from reaching internal machines with addresses in specified ranges?
8. Why is the bastion host often refered to as the sacrificial host?

2.2. Decide whether the following statements are true (T), false (F) or no information (NI)

1. There are three advantages of NAT montioned in the text.

A. True B. False C. NI

2. A method of mapping real, valid, external IP addresses to special ranges of no routable internal IP addresses is NAT.

A. True B. False C. NI

3. The application proxy examines an application layer protocol, such as HTTP, and performs the proxy services.

A. True B. False C. NI

4. Having some form of a router at the boundary between the organization's internal networks and the external service provider is always has benefits for organizations with an Internet connection.

A. True B. False C. NI

5. Firewall architecture is responsible for the standards and frameworks associated with the architecture of sub-networks

A. True B. False C. NI

2.3. Choose the best answer for the following statements

1. .... combine the packet-filtering router with a separate, dedicated firewall, such as an application proxy server.

B. Screened host firewalls B. Firewall systems

C. Dual-home host firewalls D. Screen subnet firewalls

2. All firewall devices can be configured in .... network connection architectures.

A. a wide range of B. just a few

C. a variety of D. A&C are correct

3. The dominant architecture used today is the .... firewall.

A. screen host B. dual-home host

C. screened subnet D. C&B are correct

4. The configuration that works best for a particular organization depends on ....

A. the organization's ability to develop and implement the architectures

B. the objectives of the network

C. the budget available for the function

D. All are correct

5. The benefit of a ....is its ability to translate between many different protocols at their respective data link layers.

A. dual-homed host	B. screen host
C. SOCKS Server	D. screen subnet firewall

3. Speaking

1. What main contents do you get from the text? What do you know about them?
2. Choose one of the contents in the text and present it.

READING AND SPEAKING 4

1. Discuss the questions

1.What types of firewall have you learnt?

2. What does the phrase "*firewall processing mode*" mean?

3. What firewall processing modes do you know? Give some information to surport your answer.

2. Read the text and do the tasks below

Firewall Processing Modes (1)

Firewalls fall into five major processing-mode categories: packet-filtering firewalls, application gateways, circuit gateways, MAC layer firewalls, and hybrids.1 Hybrid firewalls use a combination of the other four modes, and in practice, most firewalls fall into this category, since most firewall implementations use multiple approaches. In this part only the packet-filtering firewall is discussed and the rest are mentioned later in the futher reading.

The **packet-filtering firewall**, also simply called a filtering firewall, examines the header information of data packets that come into a network. A packet-filtering firewall installed on a TCP/IP- based network typically functions at the IP level and determines whether to drop a packet (deny) or forward it to the next network connection (allow) based on the rules programmed into the firewall. Packet-filtering firewalls examine every incoming packet header and can selectively filter packets based on header information such as destination address, source address, packet type, and other key information. Figure 3-6 shows the structure of an IPv4 packet.

Packet-filtering firewalls scan network data packets looking for compliance with or violation of the rules of the firewall's database. Filtering firewalls inspect packets at the network layer, or Layer 3, of the Open Systems Interconnect (OSI) model, which represents the seven layers of networking processes. (The OSI model is shown later in this chapter in Figure 3-6.) If the device finds a packet that matches a restriction, it stops the packet from traveling from one network to another. The restrictions most commonly implemented in packet-filtering firewalls are based on a combination of the following:

- IP source and destination address
- Direction (inbound or outbound)
- Protocol (for firewalls capable of examining the IP protocol layer)
- Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source and destination port requests (for firewalls capable of examining the TCP/UPD layer

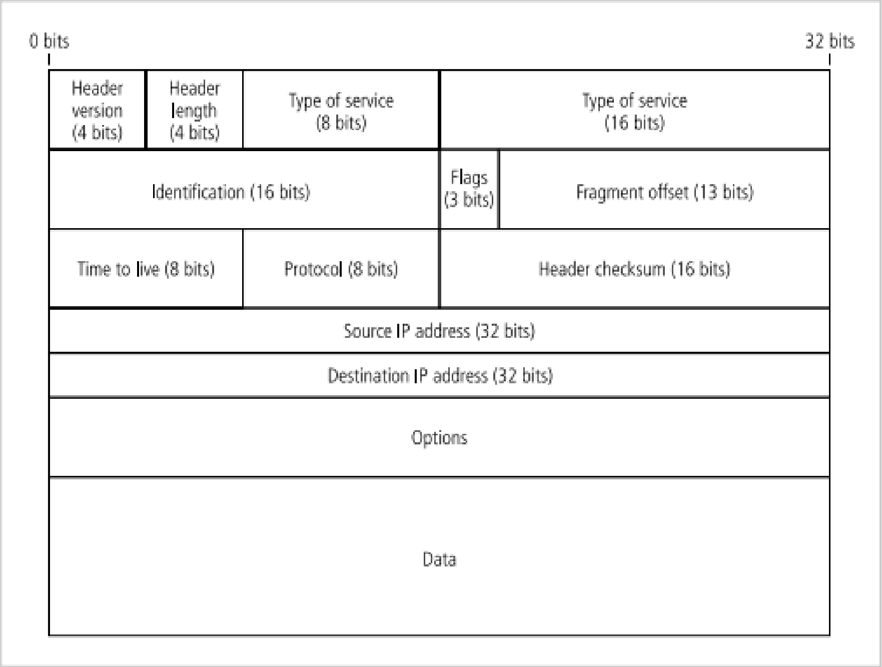


Figure 3-6. IP Packet Structure

Packet structure varies depending on the nature of the packet. The two primary service types are TCP and UDP (as noted above).

Simple firewall models examine two aspects of the packet header: the destination and source address. **They** enforce address restrictions, rules designed to prohibit packets with certain addresses or partial addresses from passing through the device. They accomplish this through ACLs, which are created and modified by the firewall administrators. *Figure 3-7* shows how a packet-filtering router can be used as a simple firewall to filter data packets from inbound connections and allow outbound connections unrestricted access to the public network.

There are three subsets of packet-filtering firewalls: static filtering, dynamic filtering, and stateful inspection. *Static filtering* requires that the filtering rules be developed and installed with the firewall. The rules are created and sequenced either by a person directly editing the rule set, or by a person using a programmable interface to specify the rules and the sequence. Any changes to the rules require human intervention. This type of filtering is common in network routers and gateways.

A *dynamic filtering firewall* can react to an emergent event and update or create rules to deal with that event. This reaction could be positive, as in allowing an internal user to engage in a specific activity upon request, or negative, as in dropping all packets from a particular address when an increase in the presence of a particular type of malformed packet is detected. While static filtering firewalls allow entire sets of one type of packet to enter in response to authorized requests, the dynamic packet-filtering firewall allows only a particular packet with a particular source, destination, and port address to enter. It does this by opening and closing "doors" in the firewall based on the information contained in the packet header, which makes dynamic packet filters an intermediate form between traditional static packet filters and application proxies (which are described later).

Stateful inspection firewalls, also called stateful firewalls, keep track of each network connection between internal and external systems using a state table. A state table tracks the state and context of each packet in the conversation by recording which station sent what packet and when. Like first generation firewalls, stateful inspection firewalls perform packet filtering, but they take it a step further. Whereas simple packet-filtering firewalls only allow or deny certain packets based on their address, a stateful firewall can expedite incoming packets that are responses to internal requests. If the stateful firewall receives an incoming packet that it cannot match in its state table, it refers to its ACL to determine whether to allow the packet to pass. The primary disadvantage of this type of firewall is the additional processing required to manage and verify packets against the state table. This can leave the system vulnerable to a DoS or DDoS attack. In such an attack, the system receives a large number of external packets, which slows the firewall because it attempts to compare all of the incoming packets first to the state table and then to the ACL. On the positive side, these firewalls can track connectionless packet traffic, such as UDP and remote procedure calls (RPC) traffic. Dynamic stateful filtering firewalls keep a dynamic state table to make changes (within predefined limits) to the filtering rules based on events as they happen. A state table looks similar to a firewall rule set but has additional information.

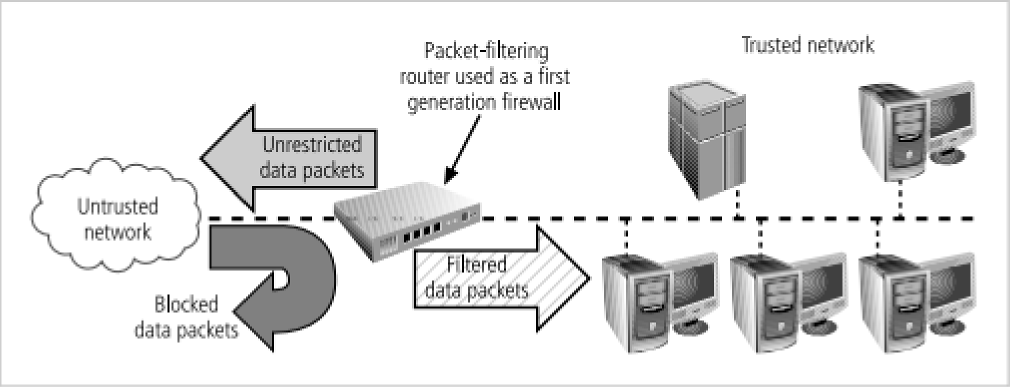


Figure 3-7. Packet - Filter Router

2.1. Answer the questions

1. What type of filtering is common in network routers and gateways?
2. How many subsets of packet-filtering firewalls are mentioned in the text? What are they?
3. How many major processing-mode categories are firewalls categorized? What are they?
4. What do simple firewall models examine?
5. Where do filtering firewalls inspect packets?
6. What does the packet-filtering firewall examine?
7. What is the primary disadvantage of stateful inspection

2.2. Decide whether the following statements are true (T), false (F) or no information (NI). Correct the false one

1. There aren't any drawsback for stateful firewall according to the text.

A. True B. False C. NI

2. The restrictions most commonly implemented in packet-filtering firewalls are based on a combination of IP source and destination address, direction, protocol, and TCP.

A. True B. False C. N

3. Like first generation firewalls, stateful inspection firewalls perform packet filtering, but they take it a step further.

A. True B. False C. NI

4. Auditability makes certain that all actions on a system can be attributed to an authenticated identity.

A. True B. False C. NI

5. According to the text, all firewall proccessing modes are shown.

A. True B. False C. NI

2.3. Choose the best answer for the following statements

1. .... requires that the filtering rules be developed and installed with the firewall.

A. dynamic packet-filtering B. Static filtering

C. stateful filtering D. A&B are correct

2. While static filtering firewalls allow entire sets of one type of packet to enter in response to authorized requests, the ....allows only a particular packet with a particular source, destination, and port address to enter

A. dynamic packet-filtering B. static filtering

C. Stateful filtering D. A&C are correct

3. Packet structure varies depending on the nature of the packet. The two primary service types are ....

A.UDP B. TCP

C. A&B are correct D. IP

4. Which of the following does the word "**they**" in paragraph 4 refer to?

A. two aspects B. Simple firewall model

C. destination and source address D. rules

5. Packet-filtering firewalls examine every incoming packet header and can ....filter packets based on header information.

A. automatically B. typically

C. selectively D. computationally

4. Listening

1. https://www.youtube.com/watch?v=kDEX1HXybrU
2. https://www.youtube.com/watch?v=5cPIukqXe5w

WRITING AND SPEAKING

1. Write about 400 words about one of the following contents in your own words:

   - A firewall and its history
   - Firewall's architecture

2. Present the following topics:

   - A firewall and its history
   - Firewall's architecture

FURTHER READING

Firewall Processing Modes (2)

Application Gateways

The application gateway, also known as an **application-level firewall** or **application firewall**, is frequently installed on a dedicated computer, separate from the filtering router, but is commonly used in conjunction with a filtering router. The application firewall is also known as a **proxy server** since it runs special software that acts as a proxy for a service request. For example, an organization that runs a Web server can avoid exposing the server to direct user traffic by installing a proxy server configured with the registered domain’s URL. This proxy server receives requests for Web pages, accesses the Web server on behalf of the external client, and returns the requested pages to the users. These servers can store the most recently accessed pages in their internal cache, and are thus also called *cache servers*. For one, the proxy server is placed in an unsecured area of the network or in the demilitarized zone (DMZ)—an intermediate area between a trusted network and an untrusted network—so that it, rather than the Web server, is exposed to the higher levels of risk from the less trusted networks. Additional filtering routers can be implemented behind the proxy server, limiting access to the more secure internal system, and thereby further protecting internal systems.

One common example of an application-level firewall (or proxy server) is a firewall that blocks all requests for and responses to requests for Web pages and services from the internal computers of an organization, and instead makes all such requests and responses go to intermediate computers (or proxies) in the less protected areas of the organization’s network. This technique is still widely used to implement electronic commerce functions, although most users of this technology have upgraded to take advantage of the DMZ approach discussed below.

The primary disadvantage of application-level firewalls is that they are designed for one or a few specific protocols and cannot easily be reconfigured to protect against attacks on other protocols. Since application firewalls work at the application layer (hence the name), they are typically restricted to a single application (e.g., FTP, Telnet, HTTP, SMTP, and SNMP). The processing time and resources necessary to read each packet down to the application layer diminishes the ability of these firewalls to handle multiple types of applications.

Circuit Gateways

The **circuit gateway firewall** operates at the transport layer. Again, connections are authorized based on addresses. Like filtering firewalls, circuit gateway firewalls do not usually look at traffic flowing between one network and another, but they do prevent direct connections between one network and another. They accomplish this by creating tunnels connecting specific processes or systems on each side of the firewall, and then allowing only authorized traffic, such as a specific type of TCP connection for authorized users, in these tunnels. A circuit gateway is a firewall component often included in the category of application gateway, but it is in fact a separate type of firewall.

MAC Layer Firewalls

While not as well known or widely referenced as the firewall approaches above, MAC layer firewalls are designed to operate at the media access control sublayer of the data link layer (Layer 2) of the OSI network model. This enables these firewalls to consider the specific host computer’s identity, as represented by its MAC or network interface card (NIC) address in its filtering decisions. Thus, MAC layer firewalls link the addresses of specific host computers to ACL entries that identify the specific types of packets that can be sent to each host, and block all other traffic.

Figure 6-6 shows where in the OSI model each of the firewall processing modes inspects data.

Hybrid Firewalls

Hybrid firewalls combine the elements of other types of firewalls— that is, the elements of packet filtering and proxy services, or of packet filtering and circuit gateways. A hybrid firewall system may actually consist of two separate firewall devices; each is a separate firewall system, but they are connected so that they work in tandem. For example, a hybrid firewall system might include a packet-filtering firewall that is set up to screen all acceptable requests, then pass the requests to a proxy server, which in turn requests services from a Web server deep inside the organization’s networks. An added advantage to the hybrid firewall approach is that it enables an organization to make a security improvement without completely replacing its existing firewalls.

FURTHER READING

Content Filters

Another utility that can help protect an organization's systems from misuse and unintentional denial-of-service problems, and which is often closely associated with firewalls, is the **content filter**. A content filter is a software filter—technically not a firewall—that allows administrators to restrict access to content from within a network. It is essentially a set of scripts or programs that restricts user access to certain networking protocols and Internet locations, or restricts users from receiving general types or specific examples of Internet content. Some refer to content filters as **reverse firewalls**, as their primary purpose is to restrict internal access to external material. In most common implementation models, the content filter has two components: rating and filtering. The rating is like a set of firewall rules for Web sites and is common in residential content filters. The rating can be complex, with multiple access control settings for different levels of the organization, or it can be simple, with a basic allow/ deny scheme like that of a firewall. The filtering is a method used to restrict specific access requests to the identified resources, which may be Web sites, servers, or whatever resources the content filter administrator configures. This is sort of a reverse ACL (technically speaking, a capability table), in that whereas an ACL normally records a set of users that have access to resources, this control list records resources which the user cannot access.

The first content filters were systems designed to restrict access to specific Web sites, and were stand-alone software applications. These could be configured in either an exclusive or inclusive manner. In an exclusive mode, certain sites are specifically excluded. The problem with this approach is that there may be thousands of Web sites that an organization wants to exclude, and more might be added every hour. The inclusive mode works from a list of sites that are specifically permitted. In order to have a site added to the list, the user must submit a request to the content filter manager, which could be time-consuming and restrict business operations. Newer models of content filters are protocol-based, examining content as it is dynamically displayed and restricting or permitting access based on a logical interpretation of content.

The most common content filters restrict users from accessing Web sites with obvious nonbusiness related material, such as pornography, or deny incoming spam e-mail. Content filters can be small add-on software programs for the home or office, such as Net Nanny or Surf Control, or corporate applications, such as the Novell Border Manager. The benefit of implementing content filters is the assurance that employees are not distracted by nonbusiness material and cannot waste organizational time and resources. The downside is that these systems require extensive configuration and ongoing maintenance to keep the list of unacceptable destinations or the source addresses for incoming restricted e-mail up-to-date. Some newer content filtering applications (like newer antivirus programs) come with a service of downloadable files that update the database of restrictions. These applications work by matching either a list of disapproved or approved Web sites and by matching key content words, such as “nude” and “sex.” Creators of restricted content have, of course, realized this and work to bypass the restrictions by suppressing these types of trip words, thus creating additional problems for networking and security professionals.

UNIT 4: SECURITY TECHNOLOGY

READING AND SPEAKING 1

1. Discuss the questions

1. What does IDPS stand for? What does it mean in your own language?
2. What do you about IDPS?
3. What is IDPS used for?
4. What does the word "*intrusion*" mean?

2. Read the text and do the tasks below

Intrusion Detection and Prevention Systems

An **intrusion detection system** (**IDS**) (see Figure 4-1) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any malicious activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms.

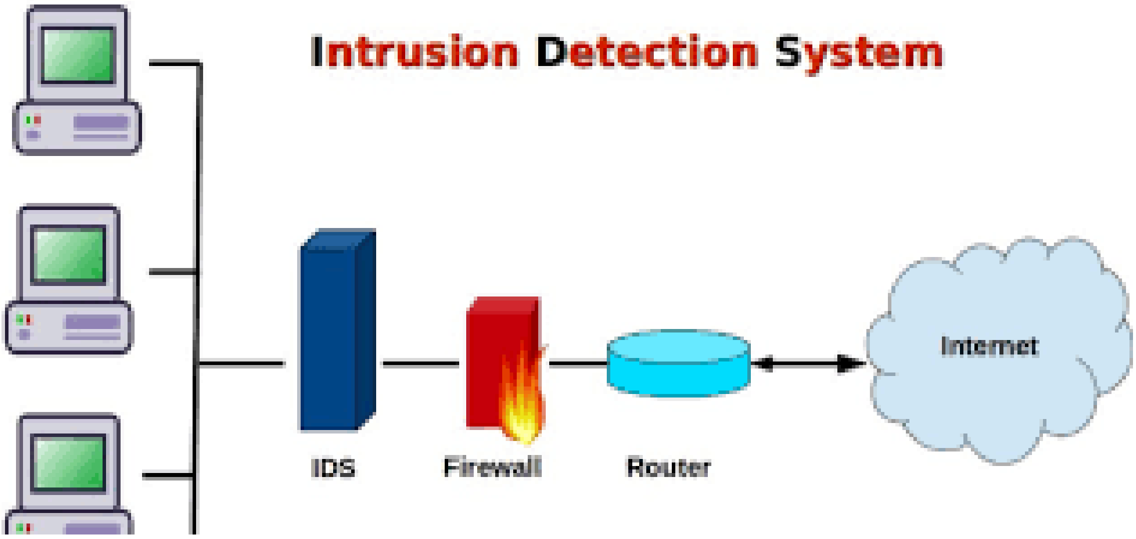


Figure 4-1. Intrusion Detection System

Information security **intrusion detection systems (IDSs)** became commercially available in the late 1990s. An IDS works like a burglar alarm in that it detects a violation (some system activity analogous to an opened or broken window) and activates an alarm. This alarm can be audible and/or visual (producing noise and lights, respectively), or it can be silent (an e-mail message or pager alert). With almost all IDSs, system administrators can choose the configuration of the various alerts and the alarm levels associated with each type of alert. Many IDSs enable administrators to configure the systems to notify them directly of trouble via e-mail or pagers. The systems can also be configured—again like a burglar alarm—to notify an external security service organization of a "break-in." The configurations that enable IDSs to provide customized levels of detection and response are quite complex. A current extension of IDS technology is the **intrusion prevention system (IPS)**, which can detect an intrusion and also prevent that intrusion from successfully attacking the organization by means of an active response. Because the two systems often coexist, the combined term **intrusion detection and prevention system (IDPS)** is generally used to describe current anti-intrusion technologies.

Why Use an IDPS?

1. According to the NIST documentation on industry best practices, there are several compelling reasons to acquire and use an IDPS:
   To prevent problem behaviors by increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse the syste
2. To detect attacks and other security violations that are not prevented by other security measures
3. To detect and deal with the preambles to attacks (commonly experienced as network probes and other "doorknob rattling" activities)
4. To document the existing threat to an organization
5. To act as quality control for security design and administration, especially in large and complex enterprises
6. To provide useful information about intrusions that do take place, allowing improved diagnosis, recovery, and correction of causative factors

One of the best reasons to install an IDPS is that they serve as deterrents by increasing the fear of detection among would-be attackers. If internal and external users know that an organization has an intrusion detection and prevention system, they are less likely to probe or attempt to compromise it, just as criminals are much less likely to break into a house that has an apparent burglar alarm. Another reason to install an IDPS is to cover the organization when its network cannot protect itself against known vulnerabilities or is unable to respond to a rapidly changing threat environment. There are many factors that can delay or undermine an organization's ability to secure its systems from attack and subsequent loss.

IDPSs can also help administrators detect the preambles to attacks. Most attacks begin with an organized and thorough probing of the organization's network environment and its defenses. This initial estimation of the defensive state of an organization's networks and systems is called *doorknob rattling* and is accomplished by means of *footprinting* (activities that gather information about the organization and its network activities and assets) and *fingerprinting* (activities that scan network locales for active systems and then identify the network services offered by the host systems). A system capable of detecting the early warning signs of footprinting and fingerprinting functions like a neighborhood watch that spots would-be burglars testing doors and windows, enabling administrators to prepare for a potential attack or to take actions to minimize potential losses from an attack.

A fourth reason for acquiring an IDPS is threat documentation. The implementation of security technology usually requires that project proponents document the threat from which the organization must be protected. IDPSs are one means of collecting such data. (To collect attack information in support of an IDPS implementation, you can begin with a freeware IDPS tool such as Snort).

Finally, even if an IDPS fails to prevent an intrusion, it can still assist in the after-attack review by providing information on how the attack occurred, what the intruder accomplished, and which methods the attacker employed. This information can be used to remedy deficiencies and to prepare the organization's network environment for future attacks. The IDPS can also provide forensic information that may be useful should the attacker be caught and prosecuted or sued.

2.1. Answer the questions

1. When were information security intrusion detection systems commercially available?
2. What do many IDSs assist administrators to do?
3. What is IPS? What can it do?
4. What is an intrusion detection system?
5. How does an IDS work?
6. How many reasons does an IDPS need installing?
7. What is one of the most important reasons to install an IDPS?
8. Give some descriptions of an IDS.

2.2. Decide whether the following statements are true (T), false (F) or no information (NI)

1. An IDS works like an alarm clock in that it detects a violation (some system activity analogous to an opened or broken window) and activates an alarm.

   1. True B. False C. NI

2. According to the text four reasons are given to indicate that IDSs need installing.

   A. True B. False C. NI

3. When malicious activity or violation appears, an administrator is ussually informed in someway.

   A. True B. False C. NI

4. Writing and implementing good enterprise information security policy are important intrusion prevention activities.

   A. True B. False C. NI

5. Delaying or undermining an organization’s ability to secure its systems from attack and subsequent loss depends on many factors.

   A. True B. False C. NI

2.3. Choose the best answer to complete the following statements

1. Which system combines outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms?

   A. An IDPS system B. A SIEM system

   C. An IDP D. A&C are correct

2. To collect attack information in support of an IDPS implementation, you can begin with ....such as Snort.

   A. hardware IDPS B. firmware IDPS

   C. a freeware IDPS tool D. software package

3. What is the term IDPS and IPS generally used for?

   A. to describe anti-virus programs

   B. to describe current anti-intrusion technologies

   C. to describe IDPS modes

   D. to describe current anti-intrusion technologies

4. The IDPS can also provide forensic information that may be useful should the attacker be ....

   A.arrected B. sued

   C. prosecuted D. all are correct

5. A current extension of IDS ....is the intrusion prevention system.

   A.system B. technology

   C. detection D. intrusion

3. Speaking

1. Present intrusion detection and prevention systems (IDPS)

2. Present the reasons why an IDPS is installed.

READING AND SPEAKING 2

1. Discuss the questions

1. What does NIDS stand for? What does it mean?
2. What does HIDS stand for? What does it mean?
3. What are NIDS and HIDS used for?
4. What does the phrase *Artificial Neural Network* mean?

2. Read the text and do the tasks below

NIDP & HIDS

Network intrusion detection systems (NIDS) are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator. An example of an NIDS would be installing it on the subnet where firewalls are located in order to see if someone is trying to break into the firewall. Ideally one would scan all inbound and outbound traffic, however doing so might create a bottleneck that would impair the overall speed of the network. OPNET and NetSim are commonly used tools for simulating network intrusion detection systems. NID Systems are also capable of comparing signatures for similar packets to link and drop harmful detected packets which have a signature matching the records in the NIDS. When we classify the design of the NIDS according to the system interactivity property, there are two types: on-line and off-line NIDS, often referred to as inline and tap mode, respectively. On-line NIDS deals with the network in real time. It analyses the Ethernet packets and applies some rules, to decide if it is an attack or not. Off-line NIDS deals with stored data and passes it through some processes to decide if it is an attack or not.

NIDS can be also combined with other technologies to increase detection and prediction rates. Artificial Neural Network based IDS are capable of analyzing huge volumes of data, in a smart way, due to the self-organizing structure that allows INS IDS to more efficiently recognize intrusion patterns. Neural networks assist IDS in predicting attacks by learning from mistakes; INN IDS help develop an early warning system, based on two layers. The first layer accepts single values, while the second layer takes the first's layers output as input; the cycle repeats and allows the system to automatically recognize new unforeseen patterns in the network. This system can average 99.9% detection and classification rate, based on research results of 24 network attacks, divided in four categories: DOS, Probe, Remote-to-Local, and user-to-root.

A **host-based intrusion detection system** (**HIDS**) is an intrusion detection system that is capable of monitoring and analyzing the internals of a computing system as well as the network packets on its network interfaces, similar to the way a network-based intrusion detection system (NIDS) operates. This was the first type of intrusion detection software to have been designed, with the original target system being the mainframe computer where outside interaction was infrequent.

A host-based IDS is capable of monitoring all or parts of the dynamic behavior and the state of a computer system, based on how it is configured. Besides such activities as dynamically inspecting network packets targeted at this specific host (optional component with most software solutions commercially available), a HIDS might detect which program accesses what resources and discover that, for example, a word-processor has suddenly and inexplicably started modifying the system password database. Similarly a HIDS might look at the state of a system, its stored information, whether in RAM, in the file system, log files or elsewhere; and check that the contents of these appear as expected, e.g. have not been changed by intruders.

One can think of a HIDS as an agent that monitors whether anything or anyone, whether internal or external, has circumvented the system's security policy.

Protecting the HIDS

A HIDS will usually go to great lengths to prevent the object-database, checksum-database and its reports from any form of tampering. After all, if intruders succeed in modifying any of the objects the HIDS monitors, nothing can stop such intruders from modifying the HIDS itself – unless security administrators take appropriate precautions. Many worms and viruses will try to disable anti-virus tools, for example.

Apart from crypto-techniques, HIDS might allow administrators to store the databases on a CD-ROM or on other read-only memory devices (another factor militating for infrequent updates...) or storing them in some off-system memory. Similarly, a HIDS will often send its logs off-system immediately – typically using VPN channels to some central management system.

One could argue that the trusted platform module comprises a type of HIDS. Although its scope differs in many ways from that of a HIDS, fundamentally it provides a means to identify whether anything/anyone has tampered with a portion of a computer. Architecturally this provides the ultimate (at least at this point in time) host-based intrusion detection, as depends on hardware external to the CPU itself, thus making it that much harder for an intruder to corrupt its object and checksum databases.

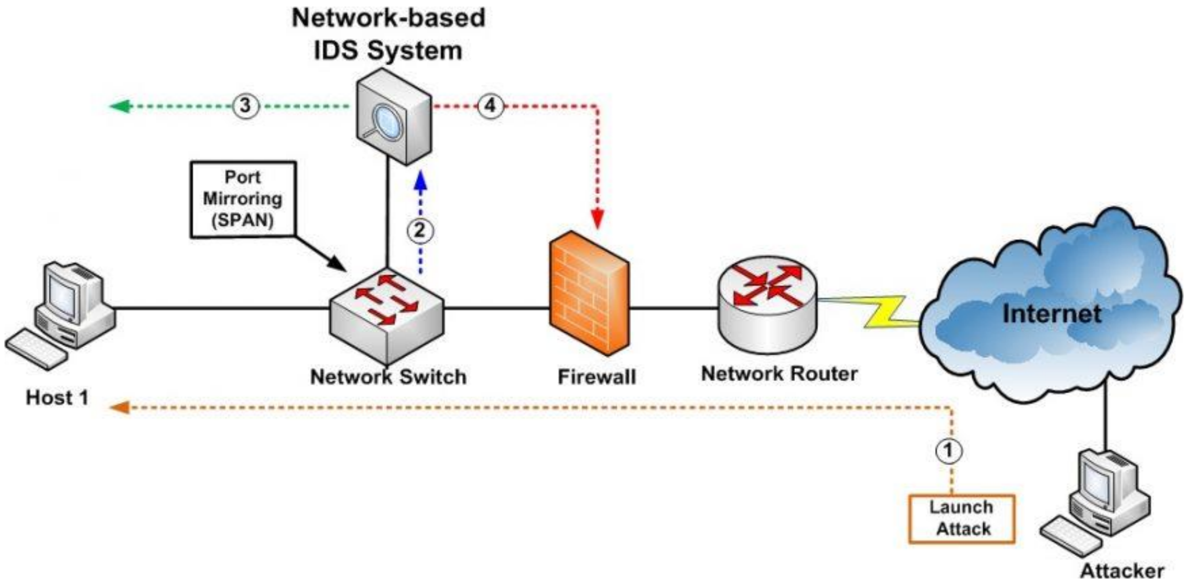


Figure 4-2. Network-based Intrusion Detection System

2.1. Answer the questions

1. What is NIDS's function?
2. What is the difference between on-line NIDS and off-line NIDS?
3. What is a host-based intrusion detection system?
4. What is a host-based IDS capable of doing?
5. What are OPNET and NetSim? What are they used for?
6. What can happen if intruders succeed in modifying any of the objects the HIDS monitors?

7. What HIDS might do apart from crypto-techniques?

8. What types of NIDS are mentioned in the text? What do you rely on to categorize the design of NIDS?

2.2. Decide whether the following statements are true (T), false (F) or no information (NI)

1. According to the text, thanks to Neural networks, IDS can predict attacks when they appear.

A. True B. False C. NI

2. Administrator himself ia able to identify an attack without intrusion detection systems.

A. True B. False C. NI

3. In order to control traffic to and from all devices on the network Network intrusion detection systems are put at a strategic point or points within the network.

A. True B. False C. NI

4. Commercially available software solutions often do correlate the findings from NIDS and HIDS in order to find out about whether a network intruder has been successful or not at the targeted host.

A. True B. False C. NI

5. Both NIDS and HIDS have their own capability to do different functions.

A. True B. False C. NI

2.3. Choose the best answer to complete the following questions and statements

1. How many types does NIDS have according to the system interactivity property? What are they?

A. It has two types: on-line and off-line NIDS

B. It has one: off-line NIDS

C. It has only one: on-line NIDS

D. B&C are correct

2. Why are Network intrusion detection systems placed at a strategic point or points within the network?

A.To control traffic to and from all devices on the network.

B. To monitor traffic to and from all devices on the network.

C. To supervise traffic from and to all devices on the network.

D. B&C are correct

3. NID Systems ....comparing signatures for similar packets to link and drop harmful detected packets which have a signature matching the records in the NIDS.

A. are also able to B. are responsible for

C. are also capable of D. A & C are correct

4. ....can be also combined with other technologies to increase detection and prediction rates.

A. HIDS B. NIDS

C. INN IDS D. ANN

5. Why will a HIDS usually go to great lengths?

A. To prevent the object-database, checksum-database

B. To reports from any form of tampering.

C. A&B are correct

D. To detect the object-database, checksum-database

3. Speaking

1. What main contents do you get from the text?

2. Present the following contents:

- NIDS
- HIDS
- The differences between NIDS and HIDS

READING AND SPEAKING 3

1. **Discuss the questions**

   1. What does the word *method* mean?
   2. What IDPS method do you know?
   3. How many IDPS methods do you know? What are they?
   4. What do the terms: *Signature-Based IDPS, Statistical Anomaly-Based IDPS,* and *Stateful Protocol Analysis IDPS* mean in your language?

2. **Read the text and do the tasks below**

IDPS Detection Methods

IDPSs use a variety of detection methods to monitor and evaluate network traffic. Three methods dominate: the signature-based approach, the statistical-anomaly approach, and the stateful packet inspection approach.

Signature-Based IDPS

A signature-based IDPS (sometimes called a **knowledge-based IDPS** or a **misuse-detection IDPS**) examines network traffic in search of patterns that match known **signatures**—that is, preconfigured, predetermined attack patterns. Signature-based IDPS technology is widely used because many attacks have clear and distinct signatures, for example: (1) footprinting and fingerprinting activities use ICMP, DNS querying, and e-mail routing analysis; (2) exploits use a specific attack sequence designed to take advantage of a vulnerability to gain access to a system; (3) DoS and DDoS attacks, during which the attacker tries to prevent the normal usage of a system, overload the system with requests so that the system's ability to process them efficiently is compromised or disrupted.

A potential problem with the signature-based approach is that new attack strategies must continually be added into the IDPS's database of signatures; otherwise, attacks that use new strategies will not be recognized and might succeed. Another weakness of the signature based method is that a slow, methodical attack might escape detection if the relevant IDPS attack signature has a shorter time frame. The only way a signature-based IDPS can resolve this vulnerability is to collect and analyze data over longer periods of time, a process that requires substantially larger data storage capability and additional processing capacity.

Statistical Anomaly-Based IDPS

The statistical anomaly-based IDPS (stat IDPS) or **behavior-based IDPS** collects statistical summaries by observing traffic that is known to be normal. This normal period of evaluation establishes a performance baseline. Once the baseline is established, the stat IDPS periodically samples network activity and, using statistical methods, compares the sampled network activity to this baseline. When the measured activity is outside the baseline parameters—exceeding what is called the **clipping leve**l—the IDPS sends an alert to the administrator. The baseline data can include variables such as host memory or CPU usage, network packet types, and packet quantities.

The advantage of the statistical anomaly-based approach is that the IDPS can detect new types of attacks, since it looks for abnormal activity of any type. Unfortunately, these systems require much more overhead and processing capacity than signature-based IDPSs, because they must constantly compare patterns of activity against the baseline. Another drawback is that these systems may not detect minor changes to system variables and may generate many false positives. If the actions of the users or systems on a network vary widely, with periods of low activity interspersed with periods of heavy packet traffic, this type of IDPS may not be suitable, because the dramatic swings from one level to another will almost certainly generate false alarms. Because of its complexity and impact on the overhead computing load of the host computer as well as the number of false positives it can generate, this type of IDPS is less commonly used than the signature-based type.

Stateful Protocol Analysis IDPS

According to SP 800-94, Stateful protocol analysis (SPA) is a process of comparing predetermined profiles of generally accepted definitions of benign activity for each protocol state against observed events to identify deviations.

Stateful protocol analysis relies on vendor-developed universal profiles that specify how particular protocols should and should not be used." Essentially, the IDPS knows how a protocol, such as FTP, is supposed to work, and therefore can detect anomalous behavior. By storing relevant data detected in a session and then using that data to identify intrusions that involve multiple requests and responses, the IDPS can better detect specialized, multisession attacks. This process is sometimes called *deep packet inspection* because SPA closely examines packets at the application layer for information that indicates a possible intrusion. Stateful protocol analysis can also examine authentication sessions for suspicious activity as well as for attacks that incorporate "unexpected sequences of commands, such as issuing the same command repeatedly or issuing a command without first issuing a command upon which it is dependent, as well as 'reasonableness' for commands such as minimum and maximum lengths for arguments." The models used for SPA are similar to signatures in that they are provided by vendors. These models are based on industry protocol standards established by such entities as the Internet Engineering Task Force, but they vary along with the protocol implementations in such documents. Also, proprietary protocols are not published in sufficient detail to enable the IDPS to provide accurate and comprehensive assessments.

Unfortunately, the analytical complexity of session-based assessments is the principal drawback to this type of IDPS method, which also requires heavy processing overhead to track multiple simultaneous connections. Additionally, unless a protocol violates its fundamental behavior, this IDPS method may completely fail to detect an intrusion. One final issue is that the IDPS may in fact interfere with the normal operations of the protocol it's examining, especially with client- and server-differentiated operations.

2.1. Answer the questions

1. What are the weaknesses of the signature-based approach?
2. What are the disadvantages of the statistical anomly-based approach?
3. Why is Statistical Anomaly-Based IDPS less commonly used than the signature-based type?
4. What is the solution to the weaknesses of the signature-based approach? --
5. What is the benefit of the statistical anomly-based approach?
6. Why is signature-based IDPS technology widely used?
7. What does SPA stand for? What is it?

8. What are the models used for SPA based on?

2.2. Decide whether the following statements are true (T), false (F) or no information (NI)

1. The signature-based, the statistical-anomaly, and the stateful packet inspection are outstanding approaches used by IDPSs.

A. True B. False C. NI

2. Statistical anomaly-based approach is more commonly used than signature –based approach.

A. True B. False C. NI

3. Signature –based IDPS never goes wrong so attackers can not do anything with it.

A. True B. False C. NI

4. An IDPS can be implemented via one of three basic control strategies.

A. True B. False C. NI

5. One of the advantages of Stateful Protocol Analysis IDPS is that the IDPS may in fact interfere with the normal operations of the protocol it's examining, especially with client- and server-differentiated operations.

A. True B. False C. NI

2.3. Choose the best answer to complete the following statements and questions

1. By ....relevant data detected in a session and then using that data to identify intrusions that involve multiple requests and responses, the IDPS can better detect specialized, multisession attacks.

A. storing B. switching

C. transmitting D. processing

2. Which of the following IDPS may not suitable if the actions of the users or systems on a network vary widely, with periods of low activity interspersed with periods of heavy packet traffic?

A. Stateful Protocol Analysis IDPS B. Signature – Based IDPS

C. Statistical Anomaly-Based IDPS D. None is correct

3. Which of the followings is the approach used IDPSs?

   A. The signature-based B. the statistical-anomaly

   C. the stateful packet inspection D. All are correct

4. Sometimes a knowledge-based IDPS has got another name. It is ....

   A. signature-based IDPS B. misuse-detection IDPS

   C. A&B D. None is correct

5. Behavior-based IDPS collects statistical summaries by ....traffic that is known to be normal.

   A. Keeping track B. controling

   C. observing D. B & C are correct

3. Speaking:

1. Choose one of the IDPS detection methods in the text and present it.
2. Present IDPS detection methods

READING AND SPEAKING 4

1. Discuss the questions

1. What powerful security tools do you know?
2. What does the word *padded cell* mean? What do you know about it?
3. What does the word *honeypot* mean? What do you know about it?

2. Read the text and do the tasks below

Honeypots, Honeynets, and Padded Cell Systems

A class of powerful security tools that go beyond routine intrusion detection is known variously as honeypots, honeynets, or padded cell systems. To understand why these tools are not yet widely used, you must first understand how they differ from a traditional IDPS.

Honeypots are decoy systems designed to lure potential attackers away from critical systems. In the industry, they are also known as decoys, lures, and fly-traps. When a collection of honeypots connects several honeypot systems on a subnet, it may be called a honeynet. A honeypot system (or in the case of a honeynet, an entire subnetwork) contains pseudo-services that emulate well-known services, but is configured in ways that make it look vulnerable to attacks. This combination is meant to lure potential attackers into committing an attack, thereby revealing themselves—the idea being that once organizations have detected these attackers, they can better defend their networks against future attacks targeting real assets. In sum, honeypots are designed to do the following:

- Divert an attacker from critical systems
- Collect information about the attacker's activity
- Encourage the attacker to stay on the system long enough for administrators to document the event and, perhaps, respond.

Because the information in a honeypot appears to be valuable, any unauthorized access to it constitutes suspicious activity. Honeypots are instrumented with sensitive monitors and event loggers that detect attempts to access the system and collect information about the potential attacker's activities. A screenshot from a simple IDPS that specializes in honeypot techniques, called Deception Toolkit.

This screenshot shows the configuration of the honeypot as it is waiting for an attack.

A padded cell is a honeypot that has been protected so that that it cannot be easily compromised—in other words, a hardened honeypot. In addition to attracting attackers with tempting data, a padded cell operates in tandem with a traditional IDPS. When the IDPS detects attackers, it seamlessly transfers them to a special simulated environment where they can cause no harm—the nature of this host environment is what gives the approach the name "padded cell." As in honeypots, this environment can be filled with interesting data, which can convince an attacker that the attack is going according to plan. Like honeypots, padded cells are well-instrumented and offer unique opportunities for a target organization to monitor the actions of an attacker. IDPS researchers have used padded cell and honeypot systems since the late 1980s, but until recently no commercial versions of these products were available. The advantages and disadvantages of using the honeypot or padded cell approach are summarized below

Advantages:

- Attackers can be diverted to targets that they cannot damage.
- Administrators have time to decide how to respond to an attacker
- Attackers' actions can be easily and more extensively monitored, and the records can be used to refine threat models and improve system protections.
- Honeypots may be effective at catching insiders who are snooping around a network.

Disadvantages:

- The legal implications of using such devices are not well understood.
- Honeypots and padded cells have not yet been shown to be generally useful security technologies.
- An expert attacker, once diverted into a decoy system, may become angry and

  launch a more aggressive attack against an organization's systems.
- Administrators and security managers need a high level of expertise to use

these systems.

Trap-and-Trace Systems

Trap-and-trace applications are growing in popularity. These systems use a combination of techniques to detect an intrusion and then trace it back to its source. The trap usually consists of a honeypot or padded cell and an alarm. While the intruders are distracted, or trapped, by what they perceive to be successful intrusions, the system notifies the administrator of their presence. The trace feature is an extension to the honeypot or padded cell approach. The trace—which is similar to caller ID—is a process by which the organization attempts to identify an entity discovered in unauthorized areas of the network or systems. If the intruder is someone inside the organization, the administrators are completely within their power to track the individual and turn him or her over to internal or external authorities. If the intruder is outside the security perimeter of the organization, then numerous legal issues arise.

On the surface, trap-and-trace systems seem like an ideal solution. Security is no longer limited to defense. Now security administrators can go on the offense. They can track down the perpetrators and turn them over to the appropriate authorities. Under the guise of justice, some less scrupulous administrators may even be tempted to back hack, or hack into a hacker's system to find out as much as possible about the hacker.

There are more legal drawbacks to trap-and-trace. The trap portion frequently involves the use of honeypots or honeynets. When using honeypots and honeynets, administrators should be careful not to cross the line between enticement and entrapment. Enticement is the act of attracting attention to a system by placing tantalizing information in key locations. Entrapment is the act of luring an individual into committing a crime to get a conviction. Enticement is legal and ethical, whereas entrapment is not.

Active Intrusion Prevention

Some organizations would like to do more than simply wait for the next attack and implement active countermeasures to stop attacks. One tool that provides active intrusion prevention is known as LaBrea. LaBrea is a "sticky" honeypot and IDPS and works by taking up the unused IP address space within a network. When LaBrea notes an ARP request, it checks to see if the IP address requested is actually valid on the network. If the address is not currently being used by a real computer or network device, LaBrea pretends to be a computer at that IP address and allows the attacker to complete the TCP/IP connection request, known as the three-way handshake. Once the handshake is complete, LaBrea changes the TCP sliding window size to a low number to hold open the TCP connection from the attacker for many hours, days, or even months. Holding the connection open but inactive greatly slows down network-based worms and other attacks. It allows the LaBrea system time to notify the system and network administrators about the anomalous behavior on the network.

2.1. Answer the questions

1. What does a honeypot system contain?
2. What is LaBrea? How does it work?
3. How long have IDPS researchers used padded cell and honeypot systems?
4. What should administrators do when using honeypots and honeynets?
5. What are honeypots? What are they designed for?
6. What systems use a combination of techniques to detect an intrusion and then trace it back to its source?
7. What does LaBrea do when it notes an ARP request?

2.2. Decide whether the following statements are true (T), false (F) or no information (NI)

1. A screenshot from a simple IDPS that specializes in honeypot techniques, called Deception Toolkit.

   A. True B. False C. NI

2. Gathering information about the attacker’s activities is one of the Honeypots’s aim.

   A. True B. False C. NI

3. An IDPS is a complex system in that it involves numerous remote monitoring agents that require proper configuration to gain the proper authentication and authorization.

A. True B. False C. NI

4. Both entrapment and enticement are the act of luring an individual into committing a crime to.

A. True B. False C. NI

5. When doing their jobs, hackers have never been trapped.

B. True B. False C. NI

2.3. Choose the best answer to complete the following questions and statements

1. ....the information in a honeypot appears to be valuable, any unauthorized access to it constitutes suspicious activity.

A. However B. Although

C. In order to D. Because

2. Which of the followings is the advantage of honeyport?

A. Attackers can be diverted to targets that they cannot damage

B. The legal implications of using such devices are not well understood

C. Administrators and security managers need a high level of expertise to use these systems.

D. None is correct

3. If the intruder is outside the security perimeter of the organization, then numerous legal issues arise.

A.If B. Unless

C. When D. While

4. .... are instrumented with sensitive monitors and event loggers that detect attempts to access the system and collect information about the potential attacker's activities.

A.Padded cells B. Honeypots

C. Decoys D. B&C are correct

5. A ....is a honeypot that has been protected so that that it cannot be easily compromised.

A. decoy B. honeypot

C. lure D. padded cell

3. **Speaking:**

    1. Choose one of security tools in the text and present it.
    2. Present advantages and disadvantages of honeypots.

4. **Listening**

    1. https://www.youtube.com/watch?v=cMH4yGE73iQ&t=97s
    2. https://www.youtube.com/watch?v=2baGjql0ZCY
    3. https://www.youtube.com/watch?v=mmt4B60xSj0
    4. https://www.youtube.com/watch?v=FihkG72z7MQ

WRITING AND SPEAKING

1. Write about 350-400 words about one of the following topics in your own words:

    - IDPS
    - NIDS
    - HIDS
    - A comparison of NIDS and HIDS

2. Present the following contents:

    - IDPS
    - NIDS
    - HIDS
    - A comparison of NIDS and HIDS

UNIT 5: WHAT IS CRYPTOGRAPHY?

READING AND SPEAKING 1

1. Discuss the questions

1. Have you ever heard of the word "*cryptography*"? If yes, what does it mean in your language?
2. What areas does cryptography relate?
3. In which areas is cryptography applied?
4. What goals does cryptography have?

2. Read the text and do the tasks below

What is cryptography?

The word "*cryptography*" is derived from the Greek words *kryptos*, meaning *hidden*, and *graphien*, meaning to *write*. Historians believe Egyptian hieroglyphics, which began about 1900 B.C.E, to be an early instance of encipherment. The key that unlocked the hieroglyphic secret was the Rosetta Stone, discovered in 1799 in lower Egypt and now located in the British Museum in London. Francois Champollion, using the *Rosetta Stone*, see Figure 5-1 deciphered the hieroglyphics in 1822. Although Egyptian codes are quite anecdotal, history includes many other cryptographic usages. Communication with secrete codes was commonly required for diplomatic, during war, individual or corporate privacy.

Figure 5-1 Rosetta Stone

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.

The unprocessed readable information is called plaintext or plain data. The process of making the information unreadable is called encryption or enciphering. The result of encryption is a ciphertext or cryptogram. Reversing this process and retrieving the original readable information is called decryption or deciphering. To encrypt or decrypt information, an algorithm or so-called cipher is used.

How a cryptographic algorithm works, is controlled by a secret key, sometimes called password or passphrase (on crypto machines, the key is the setting of the machine). The key is known only to those who are authorized to read the information. Without knowing the key, it should be impossible to reverse the encryption process, or the time to attempt to reverse the process should required take so much time that the information would become useless.

Cryptanalysis or crypto-analysis is the study and analysis of existing ciphers or encryption algorithms, (or Cryptanalysis is the process of obtaining the original message (called the **plaintext**) from an encrypted message (called the **ciphertext**) without knowing the algorithms and keys used to perform the encryption) in order to assess their quality, to find weaknesses or to find a way to reverse the encryption process without having the key. Decryption without a key (often also without authorization) is a cryptanalytic attack, referred to as breaking or cracking a cipher.

A cryptanalytic attack can exploit weaknesses in the algorithm or crypto device itself, exploit its implementation procedures, or try out all possible keys (a brute-force attack). In general, there are two types of attack: The ciphertext-only attack, where the cryptanalyst or attacker has access only to the ciphertext, and the known-plaintext attack, where the cryptanalyst has access to both ciphertext and its corresponding plaintext or assumed plaintext, to retrieve the corresponding key.

Cryptology comprises both cryptography (making) and cryptanalysis (breaking). The expressions 'code', 'encoding' and 'decoding' are frequently used in cryptography. Code, however, is a simple replacement of information with other information, and doesn't use an algorithm. Generally, these are code books or tables that convert one value (letters, words or phrases) into another value (letter sequence, numerical value or special symbols). Cryptography, on the other hand, uses an algorithm (often a combination of fractioning, transposition and substitution) to manipulate the information. Although technically wrong, the expression 'encoding' is often used to indicate encryption or enciphering and one should therefore look at the context in which such expressions are used.

Some use the terms cryptography and cryptology interchangeably in English, while others (including US military practice generally) use cryptography to refer specifically to the use and practice of cryptographic techniques and cryptology to refer to the combined study of cryptography and cryptanalysis. English is more flexible than several other languages in which cryptology (done by cryptologists) is always used in the second sense above. In the English Wikipedia the general term used for the entire field is cryptography (done by cryptographers).The study of characteristics of languages which have some application in cryptography (or cryptology), i.e. frequency data, letter combinations, universal patterns, etc., is called cryptolinguistics.

Cryptographic goals

Cryptography is not the only means of providing information security, but rather one set of techniques.

Confidentiality is a service used to keep the content of information from all but those authorized to have it. Secrecy is a term synonymous with confidentiality and privacy. There are numerous approaches to providing confidentiality, ranging from physical protection to mathematical algorithms which render data unintelligible.

Data integrity is a service which addresses the unauthorized alteration of data. To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution.

Authentication is a service related to identification. This function applies to both entities and information itself. Two parties entering into a communication should identify each other. Information delivered over a channel should be authenticated as to origin, date of origin, data content, time sent, etc. For these reasons this aspect of cryptography is usually subdivided into two major classes: entity authentication and data origin authentication. Data origin authentication implicitly provides data integrity (for if a message is modified, the source has changed).

Non-repudiation is a service which prevents an entity from denying previous commitments or actions. When disputes arise due to an entity denying that certain actions were taken, a means to resolve the situation is necessary. For example, one entity may authorize the purchase of property by another entity and later deny such authorization was granted. A procedure involving a trusted third party is needed to resolve the dispute.

A fundamental goal of cryptography is to adequately address these four areas in both theory and practice. Cryptography is about the prevention and detection of cheating and other malicious activities.

2.1. Answer the questions

1. What is cryptography? What is it used for?
2. Where does cryptography derive from and what does it mean?
3. What aspects of information security does cryptography relate?
4. What is cryptanalysis?
5. What is encryption? What is decryption?
6. Why does cryptanalysis study and analyze existing ciphers or encryption algorithms?
7. How many goals does cryptography have? What are they?
8. What major classes of authentication usually subdivided? Why is it subdivided so?

2.2. Decide whether the following statements are true (T), false (F) or no information (NI)

1. Cryptanalysis is the term used for the study of methods for obtaining the meaning of encrypted information without access to the key normally required to do so.

   A.True B. False C. NI

2. In cryptography, a cryptosystem is a suite of cryptographic algorithms needed to implement a particular security service, most commonly for achieving confidentiality.

   A.True B. False C. NI

3. Encryption is the process of encoding information which converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext.

   A. True B. False C. NI

4. There is no need to find any ways to solve the situation when the two parties have strong disputes.

   A. True B. False C. NI

5. The term "*code*" and "*cryptography*" are the same and they are changeable.

   A. True B. False C. NI

2.3. Choose the best answer to complete the following questions and statements

1. Which process needs the key?

   A. encryption B. decryption

   C.A&B are correct D. recovering the original information

2. What types of attacks are mentioned in the text?

   A. Brute force attack B. Ciphertext-only attack

   C. Known - plaintext attack D. All above are correct

3. A ....is to adequately address confidentiality, data integrity, authentication, and non-repudiation in both theory and practice.

   B. fundamental goal of cryptography

   C. general object of cryptography

   D. basic goal of cryptology

   E. general object of cryptanalysis

4. ……………is a service which prevents an entity from denying previous commitments or actions.

   A. Non-repudiation B. Authentication

   C. Data integrity D. Confidentiality

5. What was considered an early instance of encipherment?

   A. Rosetta Stone B. Egyptian hieroglyphics

C.Scytale D. A code book

6. A service related to verification. This function is for both parties and information itself is ………………………...

   A. data integrity B. non-repudiation

   C. authentication D. confidentiality

7. Which of the following attacks that can, in theory, be used to attempt to decrypt any encrypted data?

   A. A brute-force attack B. dictionary attack

   C. A&B are correct D. Man-in the middle attack

8. Which of the followings is the study of analyzing information systems in order to study the hidden aspects of the systems?

   A. Cryptography B. Cryptology

   C. Cryptanalysis D. A&B are correct

1. Speaking

1. What main contents do you get from the text? What do you know about them?
2. Present cryptography and its goals.

READING AND SPEAKING 2

1. **Discuss the questions**

    1. When was cryptography born? Who used it first?
    2. What were the earliest forms of cryptography?
    3. Which historical periods do you think cryptography has experienced?
    4. What does the word *cryptographer* mean?
    5. Do you know or have you ever heard of any famous cryptographers? If yes, give some information to support your answer.

2. **Read the text and do the tasks below**

Foundations of Cryptography

1900 B.C. Egyptian scribes used nonstandard hieroglyphs while inscribing clay tablets; this is the first documented use of written cryptography.

1500 B.C. Mesopotamian cryptography surpassed that of the Egyptians. This is demonstrated by a tablet that was discovered to contain an encrypted formula for pottery glazes; the tablet used symbols that have different meanings than when used in other contexts.

500 B.C. Hebrew scribes writing the book of Jeremiah used a reversed alphabet substitution cipher known as ATBASH.

487 B.C. The Spartans of Greece developed the scytale, a system consisting of a strip of papyrus wrapped around a wooden staff. Messages were written down the length of the staff, and the papyrus was unwrapped. The decryption process involved wrapping the papyrus around a shaft of similar diameter.

50 B.C. Julius Caesar used a simple substitution cipher to secure military and government communications. To form an encrypted text, Caesar shifted the letter of the alphabet three places. In addition to this monoalphabetic substitution cipher, Caesar strengthened his encryption by substituting Greek letters for Latin letters.

Fourth to sixth centuries The Kama Sutra of Vatsayana listed cryptography as the 44th and 45th of the 64 arts (yogas) that men and women should practice: (44) The art of understanding writing in cipher, and the writing of words in a peculiar way; (45) The art of speaking by changing the forms of the word.

725 Abu ‘Abd al-Rahman al-Khalil ibn Ahman ibn ‘Amr ibn Tammam al Farahidi al-Zadi al Yahmadi wrote a book (now lost) on cryptography; he also solved a Greek cryptogram by guessing the plaintext introduction.

855 Abu Wahshiyyaan-Nabati, a scholar, published several cipher alphabets that were used to encrypt magic formulas.

1250 Roger Bacon, an English monk, wrote Epistle of Roger Bacon on the Secret Works of Art and of Nature and Also on the Nullity of Magic, in which he described several simple ciphers.

1392 The Equatorie of the Planetis, an early text possibly written by Geoffrey Chaucer, contained a passage in a simple substitution cipher.

1412 Subhalasha, a 14-volume Arabic encyclopedia, contained a section on cryptography, including both substitution and transposition ciphers, as well as ciphers with multiple substitutions, a technique that had never been used before.

1466 Leon Battista Alberti, the Father of Western cryptography, worked with polyalphabetic substitution and also invented a device based on two concentric discs that simplified the use of Caesar ciphers.

1518 Johannes Trithemius wrote the first printed book on cryptography and invented a steganographic cipher, in which each letter was represented as a word taken from a succession of columns. He also described a polyalphabetic encryption method using a rectangular substitution format that is now commonly used. He is credited with introducing the method of changing substitution alphabets with each letter as it is deciphered.

1553 Giovan Batista Belaso introduced the idea of the passphrase (password) as a key for encryption; this polyalphabetic encryption method is misnamed for another person who later used the technique and is called “The Vigenѐre Cipher” today.

1563 Giovanni Battista Porta wrote a classification text on encryption methods, categorizing them as transposition, substitution, and symbol substitution.

1623 Sir Francis Bacon described an encryption method employing one of the first uses of stegano graphy; he encrypted his messages by slightly changing the type-face of a random text so that each letter of the cipher was hidden within the text.

In deed polyalphabetic ciphers were invented by the three main contribution including Johannes Trithemius (1462-1516), Giovanni Battista Porta (1535-1615), and Blaise de Vigenere (1523-1596)

1790s Thomas Jefferson created a 26-letter wheel cipher, which he used for official communications while ambassador to France; the concept of the wheel cipher would be reinvented in 1854 and again in 1913.

1854 Charles Babbage reinvented Thomas Jefferson's wheel cipher. He developed the multiple frequency analysis techniques.

1861–1865 During the U.S. Civil War, Union forces used a substitution encryption method based on specific words, and the Confederacy used a polyalphabetic cipher whose solution had been published before the start of the Civil War.

By the end of the 19th century important steps were made in the development of cryptography. Auguste Kerckhoff was one of the most important men changed cryptography from dark art into a science based on mathematics.

1914–1917 During World War I, the Germans, British, and French used a series of transposition and substitution ciphers in radio communications throughout the war. All sides expended considerable effort to try to intercept and decode communications, and thereby created the science of cryptanalysis. British cryptographers broke the Zimmerman Telegram, in which the Germans offered Mexico U.S. territory in return for Mexico's support. This decryption helped to bring the United States into the war.

1917 William Frederick Friedman, the father of U.S. cryptanalysis, and his wife, Elizabeth, were employed as civilian cryptanalysts by the U.S. government. Friedman later founded a school for cryptanalysis in Riverbank, Illinois.

1917 Gilbert S. Vernam, an AT&T employee, invented a polyalphabetic cipher machine that used a nonrepeating random key. He also invented one-time pad encryption for Telex Traffic.

1919 Hugo Alexander Koch filed a patent in the Netherlands for a rotor-based cipher machine; in 1927, Koch assigned the patent rights to Arthur Scherbius, the inventor of the Enigma machine, which was a mechanical substitution cipher.

1927–1933 During Prohibition, criminals in the U.S. began using cryptography to protect the privacy of messages used in criminal activities.

1937 Event The Japanese developed the Purple machine, which was based on principles similar to those of Enigma and used mechanical relays from telephone systems to encrypt diplomatic messages. By late 1940, a team headed by William Friedman had broken the code generated by this machine and constructed a machine that could quickly decode Purple's ciphers.

1939 -1942 The Allies secretly broke the Enigma cipher, undoubtedly shortening World War II.

1942 Navajo code talkers entered World War II; in addition to speaking a language that was unknown outside a relatively small group within the United States, the Navajos developed code words for subjects and ideas that did not exist in their native tongue.

1948 Claude Elwood Shannon suggested using frequency and statistical analysis in the solution of substitution ciphers. It was Claude Elwood Shannon who laid foundations for modern cryptography and was the father of Information Theory.

1970 Dr. Horst Feistel led an IBM research team in the development of the Lucifer cipher. One of the first block ciphers –encryption performed on block of data bits was the Lucifer cipher, designed by Fiestel and Coppersmith for IBM, and based on what is known as Fiestel network. It was the predecessor of DES.

1976 A design based upon Lucifer was chosen by the U.S. National Security Agency as the Data Encryption Standard and found worldwide acceptance.

1976 Whitefield Diffie and Martin Hellman introduced the idea of public-key cryptography of which algorithms are based on the computational complexity problem. The Diffie–Hellman algorithms are based on the discrete logarithm problem. One of the most significant contribution provided by public-key cryptography is the digital signature.

1977 Ronald Rivest, Adi Shamir, and Leonard Adleman developed a practical public-key cipher for both confidentiality and digital signatures; the RSA family of computer encryption algorithms was born. They invented RSA algorithms which are based on the problem of factorization of large prime. Because of their solution to the secret key distribution problem, the Diffie–Hellman algorithms and RSA are among the most widely used crypto algorithms in the world.

1992 The initial RSA algorithm was published in the Communication of ACM.

1991 Phil Zimmermann released the first version of PGP (Pretty Good Privacy); PGP was released as freeware and became the worldwide standard for public cryptosystems. The first international standard for digital signature (ISO/IES 9796) was adopted.

2000 Rijndael's cipher was selected as the Advanced Encryption Standard. AES is a subset of the Rijndael block cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process.

2.1. Answer the questions

1. When was cryptography changed from dark art into a science based on mathematics? Who changed it?
2. Who was the father of Information Theory?
3. What device was developed and used in the early- to mid-20th century to protect commercial, diplomatic and military communication?
4. Who invented Enigma machine and when was it invented?
5. Who introduced the idea of public-key cryptography? What are its algorithms based on? the computational complexity problem.
6. What device was developed by the Spartans of Greece? When was it developed?
7. What did Leon Battista Alberti invented?
8. Which algorithms are the most widely used in the world among crypto algorithms?

2.2. Decide whether the following statements are true (T), false (F) or no information (NI)

1. Giovan Batista Belaso invented a device based on two concentric discs that simplified the use of Caesar ciphers.

   A. True B. False C. NI

2. The idea of public-key cryptography belongs to Ronald Rivest, Adi Shamir, and Leonard Adleman.

   A. True B. False C. NI

3. Charles Babbage developed the multiple frequency analysis techniques.

   A. True B. False C. NI

4. Leon Battista Alberti was an Italian Renaissance humanist author, artist, architect, poet, priest, linguist, philosopher and cryptographer.

   A. True B. False C. NI

5. Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process are Belgian.

   A. True B. False C. NI

2.3. Choose the best answer for the following questions

1. Who invented one-time pad encryption for Telex Traffic?

   A. Hugo Alexander Koch B. Gilbert S. Vernam

   C. Dr. Horst Feistel D. Charles Babbage

2. What cipher did Julius Caesar use to secure military and government communications?

   A. Monoalphabetic substitution cipher B.A simple substitution cipher

   C.A & B are incorrect D.Tranposition cipher

3. What is one of the most significant contribution provided by public-key cryptography?

   A. The one-time pad B.The key distribution

   C.The frequency analysis D.The digital signature

4. When was the Enigma cipher broken? Who broke it?

   A. In World War II/The Japanese B. In1939 -1942/The Allies

   C. In World War I/The Americans D.In the 1942/The British

5. Which of the followings is one of the first block ciphers?

   A. Caesar cipher B.Wheel cipher

   C.Lucifer cipher D.Vigenère cipher

6. Who broke Japan's Purple's ciphers?

   A. William Friedman B. Gilbert S. Vernam

   C. Horst Feistel D. Phil Zimmermann

7. What types of cipher were used in radio communications during World War I?

   A. Transposition ciphers Substitution ciphers

   C. Enigma cipher D. A&B are correct

8. Why did the United States decide to take part in World War II?

   A.Because the Zimmerman Telegram was broken.

   B. Because the Enigma machine was broken.

   C. Because the Purple machine was used.

D. Because Lucifer cipher was used.

3. Speaking

1. What main contents do you get from the text?
2. Present important historical landmarks of cryptography.
3. Choose four cryptographers who are representative for four historical phrases in the text and present them.

READING AND SPEAKING 3

1. Discuss the questions

1. What does the word *terminology* mean?
2. What is terminology?
3. What is term of cryptography?
4. Which Vietnamese terms of cryptography do you know?
5. Which English terms of cryptography do you know? What do they mean in Vietnamese?

Some basic terminology and concepts

Encryption domains and codomains

- *A* denotes a finite set called the *alphabet of definition*. For example,

A = {0, 1}, the binary alphabet, is a frequently used alphabet of definition. Note that any alphabet can be encoded in terms of the binary alphabet. For example, since there are 32 binary strings of length five; each letter of the English alphabet can be assigned a unique binary string of length five.

- *M* denotes a set called the *message space*. *M* consists of strings of symbols

from an alphabet of definition. An element of *M* is called a *plaintext message* or simply *a plaintext*. For example, *M* may consist of binary strings, English text, computer code, etc.

- C denotes a set called the *ciphertext space*. *C* consists of strings of symbols

from an alphabet of definition, which may differ from the alphabet of definition for *M*. An element of *C* is called a *ciphertext*.

Encryption and decryption transformations

- *K* denotes a set called the *key space.* An element of *K* is called a *key*.
- Each element $e \in K$ uniquely determines a bijection from *M* to *C,* denoted by E_e is called an *encryption function* or an *encryption transformation*. Note that E_e must be a bijection if the process is to be reversed and a unique plaintext message recovered for each distinct *ciphertext*.
- For each $d \in K$, D_d denotes a bijection from *C* to *M* (i.e., $D_d : C \rightarrow M$). D_d is

called a *decryption function* or *decryption transformation*.

- The process of applying the transformation E_e to a message *m*. *M* is usually referred to as *encrypting m* or the *encryption* of *m*.
- The process of applying the transformation D_d to a ciphertext *c* is usually referred to as *decrypting c* or the *decryption* of *c*.
- An *encryption scheme* consists of a set $\{E_e : e \in K\}$ of encryption transformations and a corresponding set $\{D_d : d \in K\}$ of decryption transformations with the property that for each e K there is a unique key $d \in K$ such that $D_d = E_2^{-1}$; that is, $D_d\ (E_e\ (m)) = m$ for all $m \in M$. An encryption scheme is sometimes referred to as *a cipher*.
- The keys *e* and *d* in the preceding definition are referred to as *a key pair* and sometimes denoted by (*e*, *d*). Note that *e* and *d* could be the same.
- To construct an encryption scheme requires one to select a message space *M*, a ciphertext space *C*, a key space *K*, a set of encryption transformations $\{E_e : e \in K\}$ and a corresponding set of decryption transformations $\{D_d : d \in K\}$.

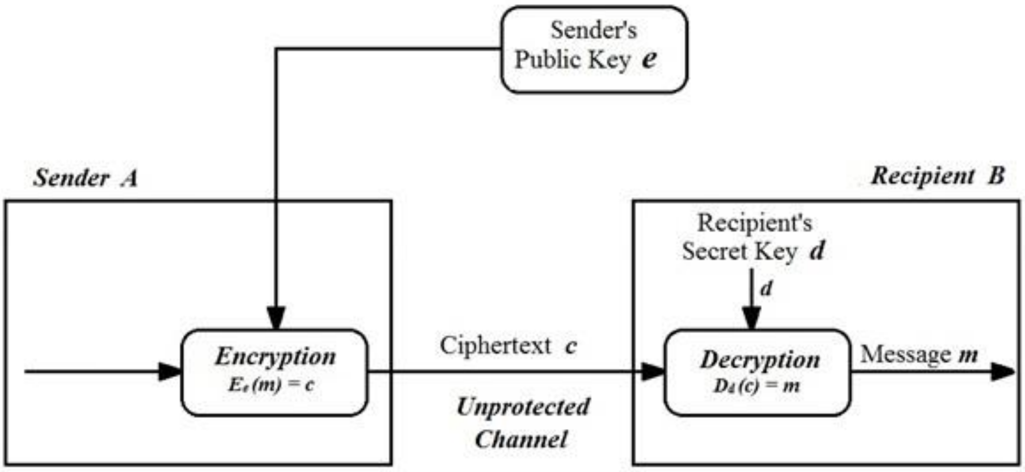


Figure 5-2. Example of Enrcryption Scheme

Achieving confidentiality

An encryption scheme may be used as follows for the purpose of achieving confidentiality. Two parties Alice and Bob first secretly choose or secretly exchange a key pair (*e*, *d*). At a subsequent point in time, if Alice wishes to send a message $m \in M$ to Bob, she computes $c = E_e\ (m)$ and transmits this to Bob. Upon receiving *c*, Bob computes $D_d\ (c) = m$ and hence recovers the original message *m*.

The question arises as to why keys are necessary. (Why not just choose one encryption function and its corresponding decryption function?) Having transformations, which are very similar but characterized by keys means that if some particular encryption/decryption transformation is revealed then one does not have to redesign the entire scheme but simply change the key. It is sound cryptographic practice to change the key (encryption/decryption transformation) frequently. As a physical analogue, consider an ordinary resettable combination lock. The structure of the lock is available to anyone who wishes to purchase one but the combination is chosen and set by the owner. If the owner suspects that the combination has been revealed he can easily reset it without replacing the physical mechanism.

Example (encryption scheme) Let M = {m_1, m_2, m_3} and C = {c_1, c_2, c_3} and. There are precisely 3! = 6 bijections from M to C. The key space K = {*1, 2, 3, 4, 5, 6*} has six elements in it, each specifying one of the transformations. Figure 1 illustrates the six encryption functions which are denoted by E_i, $1\leq i \leq 6$. Alice and Bob agree on a transformation, say E_1. To encrypt the message m_1, Alice computes E_1 (m$_1$) = c_3 and sends c_3 to Bob. Bob decrypts c_3 by reversing the arrows on the diagram for E_1 and observing that c_3 points to m_1.

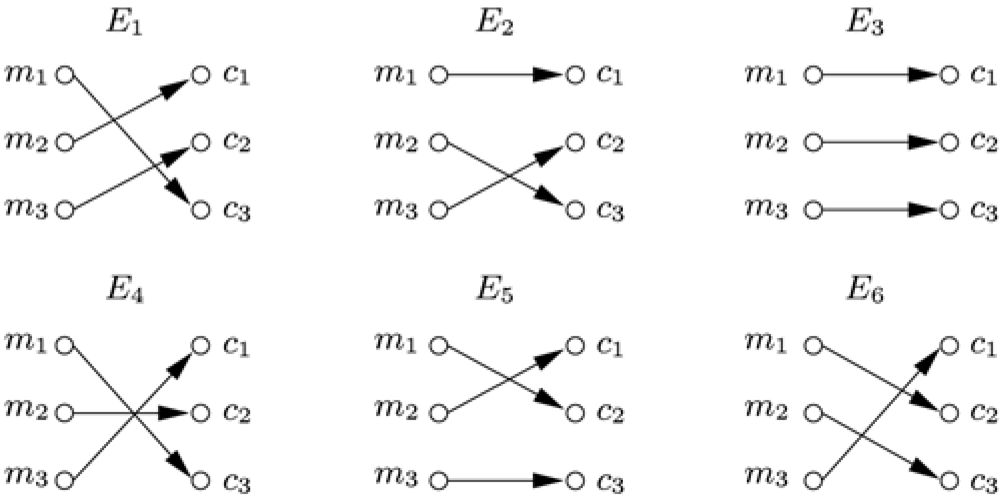


Figure 5-3. Schematic of a simple encryption scheme

When is a small set, the functional diagram is a simple visual means to describe the mapping. In cryptography, the set is typically of astronomical proportions and, as such, the visual description is infeasible. What is required, in these cases, is some other simple means to describe the encryption and decryption transformations, such as mathematical algorithms. Figure 5.4 provides a simple model of a two-party communication using encryption.

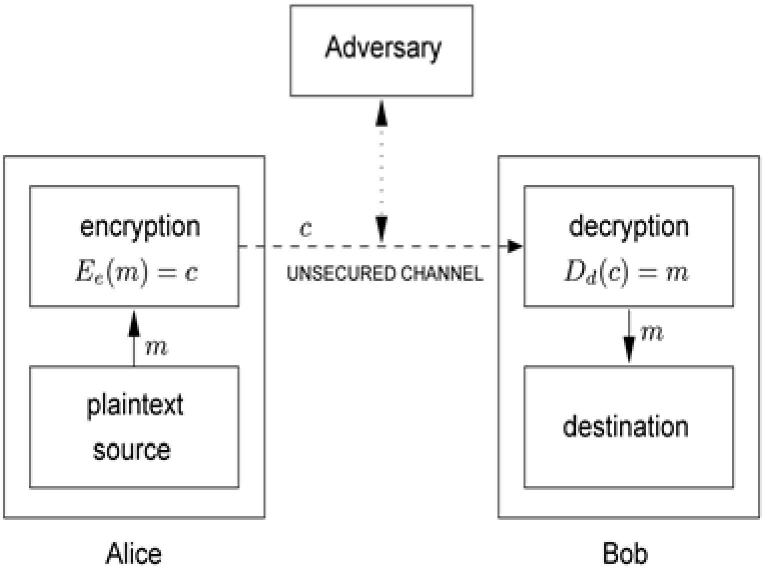


Figure 5-4. Schematic of a two-party communication using encryption

2.1. Answer the questions

1. What do the letter *A,M,C,K* denote?
2. Which letters denote a key pair?
3. What is D_d called?
4. What does an encryption scheme consist of?
5. What does one have to do to construct an encryption scheme?
6. What does the owner of the key do if he suspects that the combination has been revealed?
7. How is an encryption scheme used to achieve confidentiality?

2.2. Decide whether the following statements are true (T), false (F) or no information (NI). Correct the false (F)

1. A letter of the English alphabet can be assigned unique binary strings of length five.

A. True B. False C. NI

2. The structure of the lock is available to anyone who wishes to purchase one

but the combination is chosen and set by the owner.

A. True B. False C. NI

3. M consists of strings of symbols from the binary alphabet.

A. True B. False C. NI

4. There are 23 binary strings of length nine

A. True B. False C. NI

5. A decryption scheme consists of a set $\{E_e : e \quad K\}$ of decryption transformations.

A. True B. False C. NI

2.3. Choose the best answer to complete the following statements

1. An element of *M* is called ……………………..................................

A. a ciphertext space

B. a ciphertext

C. a decryption scheme

D. a plaintext message or simply a plaintext

2. An element of *K* is called ……………..

A. an alphabet of definition B. a key

C. a ciphertext D. a plaintext

3. An element of *C* is called …………………..

A. a ciphertext space B. a decryption scheme

C. a ciphertext D. a key pair

4. One has to ……………… if some particular encryption or decryption transformation is revealed.

A. change the key

B. redesign the entire scheme

C. change the key

D. reset the key

5. The structure of the lock ………………but the combination is chosen and set by the owner.

A. is available to anyone who wants to purchase one

B. is unavailable to anyone who wishes to purchase one

C. A & B are correct

D. All above

6. The diagram in *Figure 5-3.* Schematic of a simple encryption scheme is good for describing an encryption scheme ………………………….

A. when the set is typically of astronomical proportions

B. When the set is small

C. When is a small set

D. B & C are correct

3. Speaking

1. Give definitions to the basic terminologies of cryptography according to the text.
2. Present the following contents:

- Encryption scheme
- How to achieve confidentiality

3. Describe *Figure 5-4*

READING AND SPEAKING 4

1. Discuss the questions

1. How many parties do you think normally participate in a two-way communication? Who are they?
2. What enables them to convey information to each other?
3. Do you think that the information transmitted via a communication channel is always secure? Why and why not?
4. According to you, who can steal that information and are there any means to prevent this problem?

Communication participants

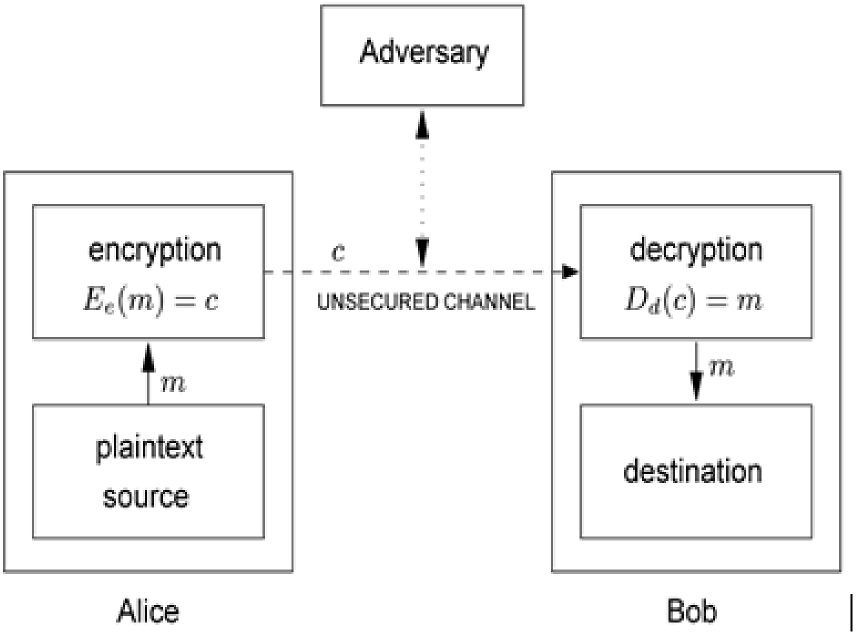


Figure 5-5. Schematic of a two-party communication using encryption

Referring to Figure 2 the following terminology is defined as follow:

• An *entity* or a *party* is someone or something which sends, receives, or manipulates information. Alice and Bob are entities in Example (see figure 5-5). An entity may be a person, a computer terminal, etc.

• A *sender* is an entity in a two-party communication which is the legitimate transmitter of information. In Figure 5-5, the sender is Alice.

• A *receiver* is an entity in a two-party communication which is the intended recipient of information. In Figure 5-5, the receiver is Bob.

- An *adversary* is an entity in a two-party communication which is neither the sender nor receiver, and which tries to defeat the information security service being provided between the sender and receiver. Various other names are synonymous with adversary such as enemy, attacker, opponent, tapper, eavesdropper, intruder, interloper, and interceptor. An adversary will often attempt to play the role of either the legitimate sender or the legitimate receiver.

Channels

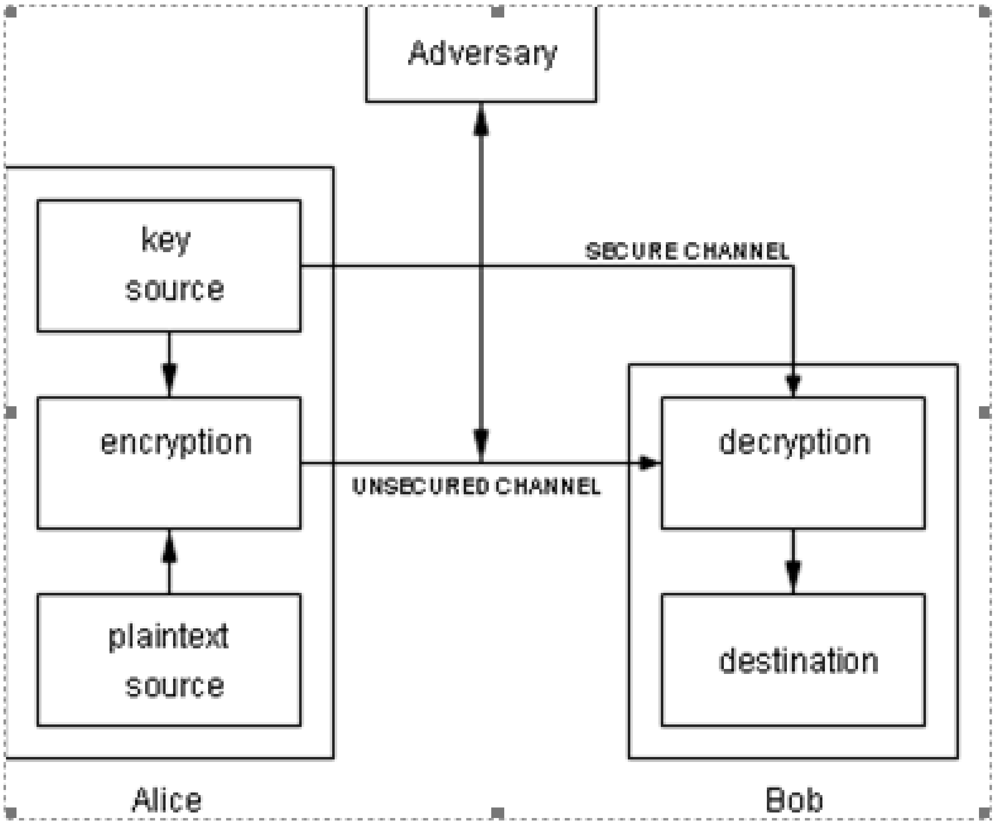


Figure 5-6: Two-party communication using encryption, with a secure channel for key exchange. The decryption key can be efficiently computed from the encryption key.

Referring to Figure 5-6 the following terminology is defined as follow:

- A *channel* is a means of conveying information from one entity to another.
- A *physically secure channel* or *secure channel* is one which is not physically accessible to the adversary.
- An *unsecured channel* is one from which parties other than those for which the information is intended can reorder, delete, insert, or read.
- A *secured channel* is one from which an adversary does not have the ability to reorder, delete, insert, or read.

Security

• A fundamental premise in cryptography is that the sets $M, C, K \{E_e : e \in K\}$, $\{D_d : d \in K\}$ are public knowledge. When two parties wish to communicate securely using an encryption scheme, the only thing that they keep secret is the particular key pair (e, d) which they are using, and which they must select. One can gain additional security by keeping the class of encryption and decryption transformations secret but one should not base the security of the entire scheme on this approach. History has shown that maintaining the secrecy of the transformations is very difficult indeed.

• An encryption scheme is said to be breakable if a third party, without prior knowledge of the key pair (e, d), can systematically recover plaintext from corresponding ciphertext within some appropriate time frame.

An appropriate time frame will be a function of the useful lifespan of the data being protected. For example, an instruction to buy a certain stock may only need to be kept secret for a few minutes whereas state secrets may need to remain confidential indefinitely.

• An encryption scheme can be broken by trying all possible keys to see which one the communicating parties are using (assuming that the class of encryption functions is public knowledge). This is called an *exhaustive search* of the key space. It follows then that the number of keys (i.e., the size of the key space) should be large enough to make this approach computationally infeasible. It is the objective of a designer of an encryption scheme that this be the best approach to break the system.

Information security in general

- *Information security service* is a method to provide some specific aspects of security. For example, integrity of transmitted data is a security objective, and a method to ensure this aspect is an information security service.
- *Breaking* an information security service (which often involves more than simply encryption) implies defeating the objective of the intended service.
- A *passive adversary* is an adversary who is capable only of reading information from an unsecured channel.
- An *active adversary* is an adversary who may also transmit, alter, or delete information on an unsecured channel.

2.1. Answer the questions

1. What is the difference among a sender, a receiver, and an adversary?

2. What are *unsecured channel* and *secured channel*?
3. What is the only thing that the two parties keep secret when using an encryption scheme?
4. Can an encryption scheme be broken? When and how?
5. What is called an *exhaustive search*?
6. What is the objective of a designer of an encryption scheme?
7. What did Kerckhoff articulate in 1883 in his famous literature?
8. What is the difference between an active adversary and a passive adversary?

2.2. Decide whether the following statements are true (T), false (F) or no information (NI). Correct the false (F).)

1. The term *adversary* has five other names including enemy, attacker, opponent, tapper, and eavesdropper.

A. True B. False C. NI

2. An appropriate time frame will never be a function of the useful lifespan of the data being protected.

A. True B. False C. NI

3. Maintaining the secrecy of the transformations is very difficult indeed.

A. True B. False C. NI

4. Point 5 in Kerckhoff's list of requirements allows that the class of encryption transformations being used be publicly known and that the security of the system should reside only in the key chosen.

A. True B. False C. NI

5. An unsecured channel is one from which an adversary does not have the ability to reorder, delete, insert, or read.

A. True B. False C. NI

2.3. Choose the best answer to complete the following questions and statements

1. Which channel is not physically accessible to the adversary?

A. A physically secure channel or secured channel

B. An unsecured channel

C. A secured channel

D. A. secure channel

2. Which role does an adversary attempt to play in a two-way communication?

A. the illegitimate sender or the illegitimate receiver

B. The role of the sender only

C. the legitimate sender or the legitimate receiver

D. The role of the receiver only

3. What is a fundamental premise in cryptography?

A. the set $A, C, K \{E_e : e \quad K\}, \ \{D_d : d \quad K\}$

B. the sets $M, C, K \{E_e : e \quad K\}, \ \{D_d : d \quad K\}$

C. Either A or B

D. Both A and B

4. A/An …………is an entity in a two-party communication which is the legitimate transmitter of information.

A. sender

B. receiver

C. adversary

D. channel

5. A/An …………… is an entity in a two-party communication which is the intended recipient of information.

A. channel

B. adversary

C. sender

D. receiver

6.………………….. an information security service implies defeating the objective of the intended service.

A. Transmitting

B. Defeating

C. Breaking

D. Conveying

7. A/An ………………is an adversary who is capable only of reading information from an unsecured channel.

A. passive adversary

B. active adversary

C. entity

D. party

8. A/An ….. is a means of conveying information from one entity to another.

A. adversary	B. information security service
C. exhaustive search	D. channel

9. An …………is an adversary who may also transmit, alter, or delete information on an unsecured channel.

A. passive adversary	B. entity
C. active adversary	D. party

10…………………is a method to provide some specific aspects of security.

A. Channel	B. Information security service
C. exhaustive search	D. Secure channel

3. Speaking

1. Give definition to the terms in Figure 5-5 and Figure 5-6.

2. Present communication participants and channels.

2. Describe Figure 5-5 and Figure 5-6.

4. Listening

1. https://www.binance.vision/security/history-of-cryptography

2. https://www.youtube.com/watch?v=QqTWyl58Rvw

WRITING AND SPEAKING

1. Write about 350 -400 words about one of the following topics in your own words.

   - Cryptography
   - Goals of cryptography
   - A brief history of cryptography

2. Present the following contents:

   - Cryptography
   - Goals of cryptography
   - A brief history of cryptography

UNIT 6: MODERN CRYPTOGRAPHY

READING AND SPEAKING 1

1. Discuss the questions

1. When was modern cryptography born?
2. Which famous cryptographers have you known? What are their notable distributions in the cryptographic areas
3. What does the phrase *hash function* mean? What is it?
4. What hash functions do you know?

2. Read the text and do the tasks below

Hash functions

Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure.

Up to now a variety of cipher methods have been used such as substitution cipher, transposition cipher, exclusive OR, Vernam cipher, book or running cipher, and hash function. However, in this part only Hash functions are discussed.

Hash functions are mathematical algorithms that generate a message summary or digest (sometimes called a fingerprint) to confirm the identity of a specific message and to confirm that there have not been any changes to the content. While they do not create a ciphertext, hash functions confirm message identity and integrity, both of which are critical functions in e-commerce. **Hash algorithms** are public functions that create a hash value, also known as a message digest, by converting variable-length messages into a single fixed-length value. The **message digest** is a fingerprint of the author’s message that is compared with the recipient’s locally calculated hash of the same message. If both hashes are identical after transmission, the message has arrived without modification. Hash functions are considered one-way operations in that the same message always provides the same hash value, but the hash value itself cannot be used to determine the contents of the message.

Hashing functions do not require the use of keys, but it is possible to attach a **message authentication code (MAC)**—a key-dependent, one-way hash function—that allows only specific recipients (symmetric key holders) to access the message digest. Because hash functions are one-way, they are used in password verification systems to confirm the identity of the user. In such systems, the hash value, or message digest, is calculated based upon the originally issued password, and this message digest is stored for later comparison. When the user logs on for the next session, the system calculates a hash value based on the user's password input, and this value is compared against the stored value to confirm identity.

The **Secure Hash Standard (SHS)** is a standard issued by the National Institute of Standards and Technology (NIST). Standard document FIPS 180-1 specifies SHA-1 (Secure Hash Algorithm 1) as a secure algorithm for computing a condensed representation of a message or data file. SHA-1 produces a 160-bit message digest, which can be used as an input to a digital signature algorithm. SHA-1 is based on principles modeled after MD4 (which is part of the MDx family of hash algorithms created by Ronald Rivest). New hash algorithms (SHA-256, SHA-384, and SHA-512) have been proposed by NIST as standards for 128, 192, and 256 bits, respectively. The number of bits used in the hash algorithm is a measurement of the strength of the algorithm against collision attacks. SHA-256 is essentially a 256-bit block cipher algorithm that creates a key by encrypting the intermediate hash value, with the message block functioning as the key. The compression function operates on each 512-bit message block and a 256-bit intermediate message digest.

A recent attack method called rainbow cracking has generated concern about the strength of the processes used for password hashing. In general, if attackers gain access to a file of hashed passwords, they can use a combination of brute force and dictionary attacks to reveal user passwords. Passwords that are dictionary words or poorly constructed can be easily cracked. Well-constructed passwords take a long time to crack even using the fastest computers, but by using a rainbow table—a database of precomputed hashes from sequentially calculated passwords—the rainbow cracker simply looks up the hashed password and reads out the text version, no brute force required. This type of attack is more properly classified as a **time–memory tradeoff attack**.

To defend against this type of attack, you must first protect the file of hashed passwords and implement strict limits to the number of attempts allowed per login session. You can also use an approach called password hash salting. Salting is the process of providing a non-secret, random piece of data to the hashing function when the hash is first calculated. The use of the salt value creates a different hash and when a large set of salt values are used, rainbow cracking fails since the time-memory tradeoff is no longer in the attacker's favor. The salt value is not kept a secret: it is stored along with the account identifier so that the hash value can be recreated during authentication.

A cryptographic hash function is a hash function; that is, an algorithm that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that any (accidental or intentional) change to the data will change the hash value. The data to be encoded are often called the "message", and the hash value is sometimes called the message digest or simply digest.

The ideal cryptographic hash function has four main properties:

- It is easy to compute the hash value for any given message
- It is infeasible to generate a message that has a given hash
- It is infeasible to modify a message without changing the hash
- It is infeasible to find two different messages with the same hash.

Cryptographic hash functions have many information security applications, notably in digital signatures, message authentication codes (MACs), and other forms of authentication. They can also be used as ordinary hash functions, to index data in hash tables, for fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption. Indeed, in information security contexts, cryptographic hash values are sometimes called (digital) fingerprints, checksums, or just hash values, even though all these terms stand for functions with rather different properties and purposes.

2.1. Answer the questions

1. What are Hash functions?
2. Why are hash functions considered one-way operations?
3. What is the message digest?
4. Why are hash functions widely used in e-commerce?

5. What does SHS stand for? What is it?

6. What are hash algorithms?

7. What is a measurement of the strength of the algorithm against collision attacks?

8. What attack method has become a concern about the strength of the processes used for password hashing?

2.2. Decide whether the following statements are true (T), false (F) or no information (NI). Correct the False (F)

1. No matter how well passwords constructed, they are broken or cracked even using the fastest computers.

   A. True B. False C. NI

2. Rainbow cracking is never cracked so it has become a concern about the strength of the processes used for password hashing.

   A. True B. False C. NI

3. Hash function calculates a hash value based on the user's password input.

   A. True B. False C. NI

4. Users only have to protect the file of hashed passwords and to implement strict limits to the number of attempts allowed per login session in order to prevent rainbow cracking.

   A. True B. False C. NI

5. There are not information-theoretically secure schemes

   A. True B. False C. NI

2.3. Choose the best answer for the following questions and statements

1. Why are hash functions used in password verification systems to confirm the identity of the user?

   A. Because hash functions are mathematical algorithms.

   B. Because hash functions are one-way.

   C. Because hash functions are publish functions.

   D. Because hash functions don't require the use of key.

2. What will attackers do if they gain access to a file of hashed passwords? and.

   A. They can use a combination of brute force

   B. They can use dictionary attacks to reveal user passwords

   C. A&B are correct

   D. They can generate a message summary or digest.

3. What do users have to do to prevent rainbow cracking?

   A. They have to protect the file of hashed passwords

   B. They have to implement strict limits to the number of attempts allowed per login session

   C. They have to use an password hash salting approach

   D. All are correct

4. Which passwords are considered easily to be cracked?

   A. Passwords that are dictionary words

   B. Passwords that are poorly constructed

   C. Passwords that are dictionary words and poorly constructed.

   D. Password that are not long enough.

5. ....is the process of providing a non-secret, random piece of data to the hashing function when the hash is first calculated.

   A. Salting

6. What specifies SHA-1 as a secure algorithm for computing a condensed representation of a message or data file?

   A. Standard document FIPS 180-2

   B. The National Institute of Standards and Technology

   C. A&B are correct

   D. Standard document FIPS 180-1

7. Which applications in the information security do cryptographic hash functions bring?

   A. digital signatures, message authentication codes

B. and other forms of authentication.

C. A&B are correct

D. message authentication codes

8. Which of the following properties that an ideal cryptographic hash function needs to have?

A. It is easy to compute the hash value for any given message

B. It is infeasible to generate a message that has a given hash and to modify a message without changing the hash

C. It is infeasible to find two different messages with the same hash.

D. All are correct

3. Speaking

1. What main contents do you get from the text? What do you know about them?
2. Present hash function

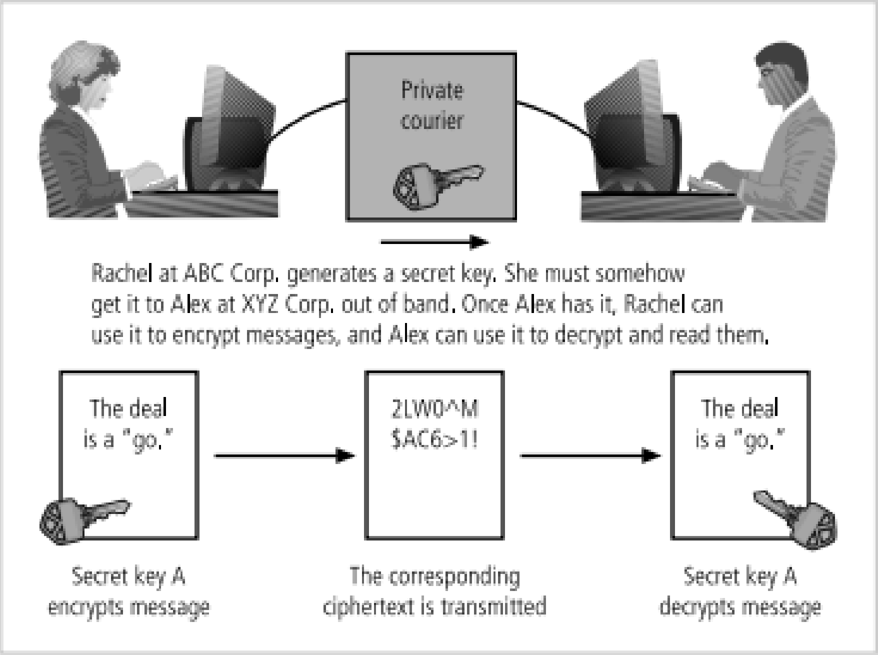
READING AND SPEAKING 2

1. Discuss the questions

1. What does the word *symmetric* mean? List some words that go with it.
2. What does the phrase *symmetric encryption* mean?
3. What do you know about symmetric encryption?
4. Which algorithms are often used in symmetric encryption?

2. Read the text and do the tasks below

Symmetric Encryption



Rachel at ABC Corp. generates a secret key. She must somehow get it to Alex at XYZ Corp. out of band. Once Alex has it, Rachel can use it to encrypt messages, and Alex can use it to decrypt and read them.

Private courier
The deal is a "go."
2LWO^M $AC6>1!
The deal is a "go."
Secret key A encrypts message
The corresponding ciphertext is transmitted
Secret key A decrypts message

Figure 6-1. Example of Symmetric Encryption

In general, cryptographic algorithms are often grouped into two broad categories symmetric and asymmetric—but in practice, today's popular cryptosystems use a hybrid combination of symmetric and asymmetric algorithms. Symmetric and asymmetric algorithms are distinguished by the types of keys they use for encryption and decryption operations.

Symmetric Encryption

Encryption methodologies that require the same **secret key** to encipher and decipher the message are using what is called **private key encryption** or **symmetric encryption**. Symmetric encryption methods use mathematical operations that can be programmed into extremely fast computing algorithms so that the encryption and decryption processes are executed quickly by even small computers. As you can see in Figure 6-1, one of the challenges is that both the sender and the recipient must have the secret key. Also, if either copy of the key falls into the wrong hands, messages can be decrypted by others and the sender and intended receiver may not know the message was intercepted. The primary challenge of symmetric key encryption is getting the key to the receiver, a process that must be conducted out of band (meaning through a channel or band other than the one carrying the ciphertext) to avoid interception.

There are a number of popular symmetric encryption cryptosystems. One of the most widely known is the **Data Encryption Standard (DES)**, which was developed by IBM and is based on the company's Lucifer algorithm, which uses a key length of 128 bits. As implemented, DES uses a 64-bit block size and a 56-bit key. DES was adopted by NIST in 1976 as a federal standard for encryption of non-classified information, after which it became widely employed in commercial applications. DES enjoyed increasing popularity for almost twenty years, until 1997, when users realized that a 56-bit key size did not provide acceptable levels of security. In 1998, a group called the Electronic Frontier Foundation (*www.eff.org*), using a specially designed computer, broke a DES key in less than three days (just over 56 hours, to be precise). Since then, it has been theorized that a dedicated attack supported by the proper hardware (not necessarily a specialized computer) can break a DES key in less than four hours. **Triple DES (3DES)** was created to provide a level of security far beyond that of DES. 3DES was an advanced application of DES, and while it did deliver on its promise of encryption strength beyond DES, it too soon proved too weak to survive indefinitely—especially as computing power continued to double every 18 months. Within just a few years, 3DES needed to be replaced.

The successor to 3DES is the **Advanced Encryption Standard (AES)**. AES is a federal information processing standard (FIPS) that specifies a cryptographic algorithm used within the U.S. government to protect information in federal agencies that are not a part of the national defense infrastructure. (Agencies that are considered a part of national defense use other, more secure methods of encryption, which are provided by the National Security Agency.) The requirements for AES stipulate that the algorithm should be unclassified, publicly disclosed, and available royalty-free worldwide. AES has been developed to replace both DES and 3DES. While 3DES remains an approved algorithm for some uses, its expected useful life is limited. Historically, cryptographic standards approved by FIPS have been adopted on a voluntary basis by organizations outside government entities. The AES selection process involved cooperation between the U.S. government, private industry, and academia from around the world. AES was approved by the Secretary of Commerce as the official federal governmental standard on May 26, 2002.

AES implements a block cipher called the Rijndael Block Cipher with a variable block length and a key length of 128, 192, or 256 bits. Experts estimate that the special computer used by the Electronic Frontier Foundation to crack DES within a couple of days would require approximately 4,698,864 quintillion years (4,698,864,000,000,000,000,000) to crack AES.

2.1. Answer the questions

1. What is the primary challenge of symmetric key encryption?
2. What symmetric encryption cryptosystems is one of the most widely known?
3. What is called symmetric encryption?
4. When was a DES key broken and who broke it?
5. Why do symmetric encryption methods use mathematical operations that can be programmed into extremely fast computing algorithms?
6. What are the disadvantages of symmetric encryption method?
7. Why was Advanced Encryption Standard born?
8. What is the difference between DES and AES?

2.2. Decide whether the following statements are true (T), false (F) or no information (NI). Correct the False (F)

1. 3DES has higher level of security than DES.

A. True B. False C. NI

2. The Secretary of Commerce approved AES as the official federal governmental standard at the end of May, 2002.

A. True B. False C. NI

3. Symmetric encryption method has no drawbacks and it has been sued for a long time.

   A. True B. False C. NI

4. It is only the U.S. government itself selected AES as federal government standard.

   A. True B. False C. NI

5. AES is based on the Rijndael cipher developed by two Russian cryptographers.

   A. True B. False C. NI

2.3. Choose the best answer for the following statements

1. What is Data Encryption Standard based on?

   A. Rijndeal cipher B. Lucifer algorithm

   C. computational hardness D. None is correct

2. The requirements for AES stipulate that the algorithm should ....

   A. be unclassified B. be publicly disclosed.

   C. available royalty-free worldwide D. All are correct

3. When was Data Encryption Standard found unsafe?

   A. In 1976 B. In 1998

   C. In 1997 D. In 2002

4. Which of the following agencies in the U.S are allowed to use AES to protect information?

   A. Agencies that are considered a part of national defense.

   B. Agencies that are not a part of the national defense infrastructure.

   C. A & B are correct

   D. Agencies that are considered a part of national policemen.

5. Which of the followings has the highest level of security?

   A. DES B. Triple DES

   C. AES D. RSA

3. Speaking

1. What main contents do you get from the text? What do you know about them?
2. Present the following contents:

   - Symmetric encryption

   - DES, 3DES, AES

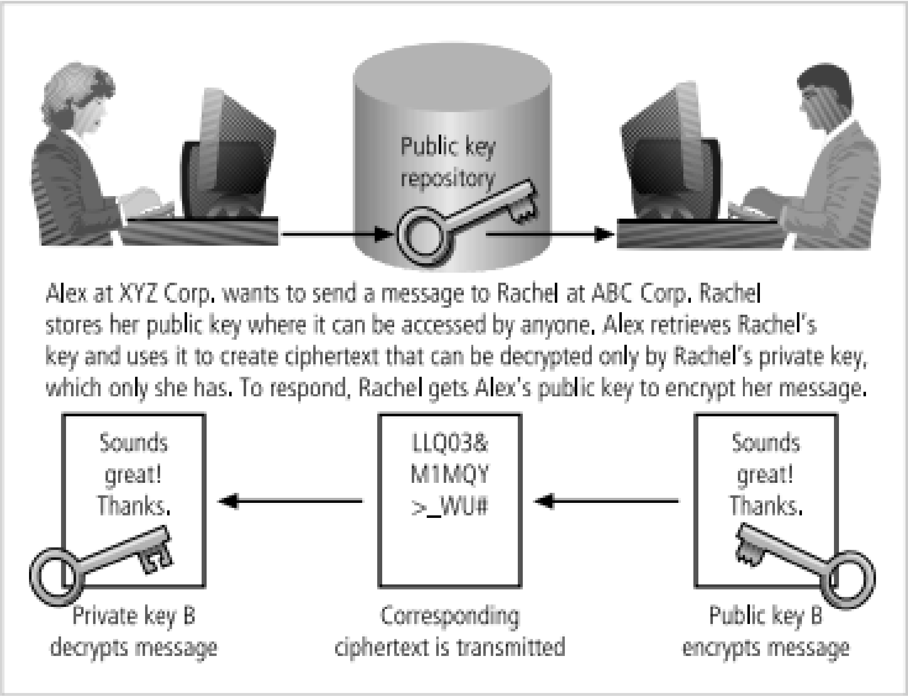
READING AND SPEAKING 3

1. Discuss the questions

1. What does the word *asymmetric* mean? What words that go with it?
2. What is asymmetric encryption? What do you know about it?
3. Have you ever heard "*RSA*" and *trap door*? If yes, so what are they?
4. Give some information about RSA.

2. Read the text and do the tasks below

Asymmetric Encryption



Alex at XYZ Corp. wants to send a message to Rachel at ABC Corp. Rachel stores her public key where it can be accessed by anyone. Alex retrieves Rachel's key and uses it to create ciphertext that can be decrypted only by Rachel's private key, which only she has. To respond, Rachel gets Alex's public key to encrypt her message.

Figure 6-2. Example of Asymmetric Encryption

While symmetric encryption systems use a single key to both encrypt and decrypt a message, **asymmetric encryption** uses two different but related keys, and either key can be used to encrypt or decrypt the message. If, however, key A is used to encrypt the message, only key B can decrypt it, and if key B is used to encrypt a message, only key A can decrypt it. Asymmetric encryption can be used to provide elegant solutions to problems of secrecy and verification. This technique has its highest value when one key is used as a private key, which means that it is kept secret (much like the key in symmetric encryption), known only to the owner of the key pair, and the other key serves as a public key, which means that it is stored in a public location where anyone can use it. This is why the more common name for asymmetric encryption is **public-key encryption**.

Consider the following example, illustrated in Figure 6-2. Alex at XYZ Corporation wants to send an encrypted message to Rachel at ABC Corporation. Alex goes to a public key registry and obtains Rachel's public key. Remember that the foundation of asymmetric encryption is that the same key cannot be used to both encrypt and decrypt the same message. So when Rachel's public key is used to encrypt the message, only Rachel's private key can be used to decrypt the message, and that private key is held by Rachel alone. Similarly, if Rachel wants to respond to Alex's message, she goes to the registry where Alex's public key is held and uses it to encrypt her message, which of course can only be read by Alex's private key. This approach, which keeps private keys secret and encourages the sharing of public keys in reliable directories, is an elegant solution to the key management problems of symmetric key applications.

Asymmetric algorithms are one-way functions. A one-way function is simple to compute in one direction, but complex to compute in the opposite direction. This is the foundation of public-key encryption. Public-key encryption is based on a hash value, which, as you learned earlier in this chapter, is calculated from an input number using a hashing algorithm. This hash value is essentially a summary of the original input values. It is virtually impossible to derive the original values without knowing how those values were used to create the hash value. For example, if you multiply 45 by 235 you get 10,575. This is simple enough. But if you are simply given the number 10,575, can you determine which two numbers were multiplied to determine this number? Now assume that each multiplier is 200 digits long and prime. The resulting multiplicative product would be up to 400 digits long. Imagine the time you'd need to factor that out.

There is a shortcut, however. In mathematics, it is known as a trapdoor (which is different from the software trapdoor). A mathematical **trapdoor** is a "secret mechanism that enables you to easily accomplish the reverse function in a one-way function.". With a trapdoor, you can use a key to encrypt or decrypt the ciphertext, but not both, thus requiring two keys. The public key becomes the true key, and the private key is derived from the public key using the trapdoor.

One of the most popular public key cryptosystems is RSA, whose name is derived from Rivest-Shamir-Adleman, the algorithm's developers. The **RSA algorithm** was the first public key encryption algorithm developed (in 1977) and published for commercial use. It is very popular and has been embedded in both Microsoft and Netscape Web browsers to enable them to provide security for e-commerce applications. The patented RSA algorithm has in fact become the de facto standard for public-use encryption applications. To learn how this algorithm works, see the Technical Details box entitled "RSA Algorithm." The problem with asymmetric encryption, as shown earlier in the example in Figure 8-6, is that holding a single conversation between two parties requires four keys. Moreover, if four organizations want to exchange communications, each party must manage its private key and four public keys. In such scenarios, determining which public key is needed to encrypt a particular message can become a rather confusing problem, and with more organizations in the loop, the problem expands. This is why asymmetric encryption is sometimes regarded by experts as inefficient. Compared to symmetric encryption, asymmetric encryption is also not as efficient in terms of CPU computations. Consequently, hybrid systems, such as those described in the section of this chapter titled "Public-Key Infrastructure (PKI)," are more commonly used than pure asymmetric systems.

2.1. Answer the questions

1. What is asymmetric encryption**?**
2. What symmetric encryption cryptosystems is one of the most popular public key cryptosystems?
3. What is the foundation of public-key encryption?
4. What is the highest value of the asymmetric encryption when one key is used as a private key?
5. What is a mathematical trapdoor?
6. What is public-key encryption based?
7. What can users do and what can't they do with a trapdoor?

2.2. Decide whether the following statements are true (T), false (F) or no information (NI). Correct the False (F)

1. The great advantage of private key cryptography is that any two parties anywhere who have the private key software can securely exchange messages without having to make any prior arrangements.

   A. True B. False C. NI

2. With a trapdoor, encryption and decryption are performed by using the same key.

   A. True B. False C. NI

3. Asymmetric encryption is also called public-key encryption because tin a key pair, one key is stored in a public location where anyone can use it.

   A. True B. False C. NI

4. People who were using public key cryptography had to switch to 150-digit or 200-digit primes if they wanted security.

   A. True B. False C. NI

5. Symmetric encryption method is not as good as asymmetric encryption one, so no methods can replace it.

   A. True B. False C. NI

2.3. Choose the best answer for the following questions and statements

1. Who developed RSA algorithm?

   A. Ron Rivest B. Adi Shamir

   C. Leonard Adleman D. All arec correct

2. What is the disadvantage of RSA?

   A. Holding a single conversation between two parties requires four keys.

   B. Key distribution

   C. Holding a single conversation between two parties requires two pairs of keys.

   D. A&C are correct

3. What must four organizations do if they want to communicate?

   A. Each party must control its public key and four private keys.

   B. Each party must manage its public key and four private keys.

   C. A&B are correct

D. Each party must manage its private key and four public keys.

4. In which of the following uses is RSA useful?

A. Trading use B. Commercial use

B. mathematical use D. computer use

5. Where is RSA embedded?

A. In Netscape Websites

B. In Microsoft

C. In Microsoft and Netscape Web browsers

D. A&C are correct

3. Speaking

1. What main contents do you get from the text? What do you know about them?
2. Present the following contents:

- Asymmetric encryption
- RSA

READING AND SPEAKING 4

1. Discuss the questions

1. What does PKI stand for? What does it mean?
2. What is PKI? What is it used for?
3. What areas is it widely used?

2. Read the text and do the tasks below

Public-key Infrastructure

The ability to conceal the contents of sensitive messages and to verify the contents of messages and the identities of their senders have the potential to be useful in all areas of business. To be actually useful, these cryptographic capabilities must be embodied in tools that allow IT and information security practitioners to apply the elements of cryptography in the everyday world of computing. This section covers a number of the more widely used tools that bring the functions of cryptography to the world of information systems.

Public-key Infrastructure (PKI) is an integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services that enables users to communicate securely. PKI systems are based on public-key cryptosystems and include digital certificates and certificate authorities (CAs).

Digital certificates are public-key container files that allow computer programs to validate the key and identify to whom it belongs. PKI and the digital certificate registries they contain enable the protection of information assets by making verifiable digital certificates readily available to business applications. This, in turn, allows the applications to implement several of the key characteristics of information security and to integrate these characteristics into business across an organization. These processes include the following:

- *Authentication*: Individuals, organizations, and Web servers can validate the identity of each of the parties in an Internet transaction.
- *Integrity:* Content signed by the certificate is known to not have been altered while in transit from host to host or server to client.
- *Privacy:* Information is protected from being intercepted during transmission. Authorization: The validated identity of users and programs

can enable authorization rules that remain in place for the duration of a transaction; this reduces some of the overhead and allows for more control of access privileges for specific transactions.

- *Nonrepudiation:* Customers or partners can be held accountable for transactions, such as online purchases, which they cannot later dispute.

A typical PKI solution protects the transmission and reception of secure information by integrating the following components:

- A *certificate authority (CA),* which issues, manages, authenticates, signs, and revokes users' digital certificates, which typically contain the user name, public key, and other identifying information.
- A *registration authority (RA),* which operates under the trusted collaboration of the certificate authority and can handle day-to-day certification functions, such as verifying registration information, generating end-user keys, revoking certificates, and validating user certificates.
- *Certificate directories,* which are central locations for certificate storage that provide a single access point for administration and distribution.
- *Management protocols,* which organize and manage the communications among CAs, RAs, and end users. This includes the functions and procedures for setting up new users, issuing keys, recovering keys, updating keys, revoking keys, and enabling the transfer of certificates and status information among the parties involved in the PKI's area of authority.
- *Policies and procedures,* which assist an organization in the application and management of certificates, in the formalization of legal liabilities and limitations, and in actual business use.

Common implementations of PKI include systems that issue digital certificates to users and servers; directory enrollment; key issuing systems; tools for managing the key issuance; and verification and return of certificates. These systems enable organizations to apply an enterprise-wide solution that provides users within the PKI's area of authority the means to engage in authenticated and secure communications and transactions.

The CA performs many housekeeping activities regarding the use of keys and certificates that are issues and used in its zone of authority. Each user authenticates himself or herself with the CA, and the CA can issue new or replacement keys, track issued keys, provide a directory of public key values for all known users, and perform other management activities. When a private key is compromised, or when the user loses the privilege of using keys in the area of authority, the CA can revoke the user's keys. The CA periodically distributes a **certificate revocation list (CRL)** to all users. When important events occur, specific applications can make a real-time request to the CA to verify any user against the current CRL.

The issuance of certificates (and the keys inside of them) by the CA enables secure, encrypted, nonrepudiable e-business transactions. Some applications allow users to generate their own certificates (and the keys inside of them), but a key pair generated by the end user can only provide nonrepudiation and not reliable encryption. A central system operated by a CA or RA can generate cryptographically strong keys that are considered by all users to be independently trustworthy, and can provide services for users such as private key backup, key recovery, and key revocation.

The strength of a cryptosystem relies on both the raw strength of its key's complexity and the overall quality of its key management security processes. PKI solutions can provide several mechanisms for limiting access and possible exposure of the private keys. These mechanisms include password protection, smart cards, hardware tokens, and other hardware-based key storage devices that are memory-capable (like flash memory or PC memory cards). PKI users should select the key security mechanisms that provide a level of key protection appropriate to their needs. Managing the security and integrity of the private keys used for nonrepudiation or the encryption of data files is critical to the successful use of encryption and nonrepudiation services within the PKI's area of trust.10

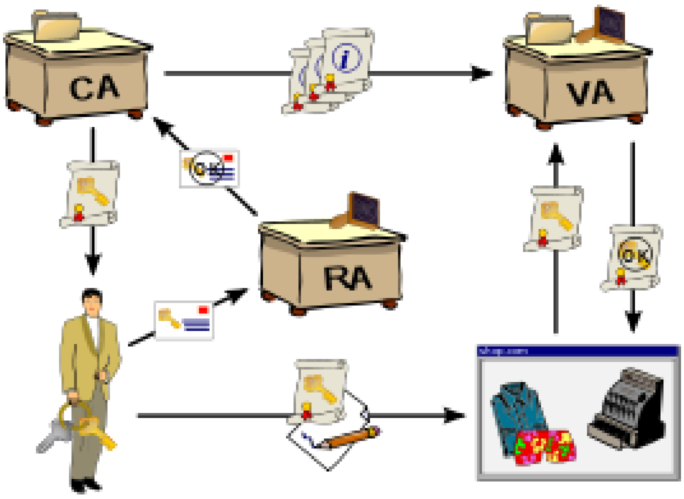


Diagram of a public key infrastructure

2.1. Answer the questions

1. What does PKI stand for? What is it?
2. What components are integrated for a typical solution PKI to protect the transmission and reception of secure information?
3. What do common implementations of PKI include?
4. What does the strength of a cryptosystem rely?
5. What are digital certificates?
6. What is critical to the successful use of encryption and nonrepudiation services within the PKI's area of trust.10?
7. What are Public-key Infrastructure systems based on?
8. What mechanisms can PKI solutions provide for limiting access and possible exposure of the private keys?

2.2. Decide whether the following statements are true (T), false (F) or no information (NI). Correct the False (F)

1. The purpose of a digital certificate is to establish the identity of users within the ecosystem.

   A. True B. False C. NI

2. A certificate authority or certification authority (CA) is an entity that issues digital certificates and it acts as a trusted third party—trusted both by owner of the certificate and by the party relying upon the certificate.

   A. True B. False C. NI

3. The strength of key's complexity and the overall quality of key management are the fundamental factors that are not important for information security protection.

   A. True B. False C. NI

4. The CA provides a certificate revocation list to its users, but it doesn't take their keys when a private key is agreed, or when their privilege of using keys in the area of authority are lost.

   A. True B. False C. NI

5. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.

A. True B. False C. NI

2.3. Choose the best answer for the following questions and statements

1. What can the CA do when the user loses the privilege of using keys in the area of authority?

A. The CA can withdraw the user's keys.

B. The CA can revoke the user's keys.

C. A&B are correct

D. A The CA can destroy the user's keys.

2. What is the function of a central system operated by a CA?

A. It generates cryptographically strong keys that are considered by all users to be independently trustworthy.

B. It provides private key backup, key recovery, and key revocation.

C. A&B are correct

D. It verifies any user against the current certification revocation list.

3. Which mechanisms should PKI users select in digital certification?

A. The key security mechanisms that provide a level of key protection appropriate to their needs.

B. The convenient mechanisms that help them exchange communication quickly.

C. The good transaction mechanisms that enable them do what they need

D. A&C are correct

4. The ....by the CA enables secure, encrypted, nonrepudiable e-business transactions. nen soan lai cau nay

A. policy of certificate B. issuance of certificates

C. mechanisms of certificate D. procedure of certificate

5. How often does the CA distribute a certificate revocation list to all users?

A. Yearly B. Regulary

C. Twice a year D. Monthly

3. Speaking

1. What main contents do you get from the text? What do you know about them?
2. Present processes in performing digital certificate.
3. Present advantages of PKI.

READING AND SPEAKING 5

1. Discuss the questions

1. What does the word *cyberattack* mean?
2. What is a cyberattack?
3. What types of cyberattack do you know?
4. What types of attacks in cryptography do you know?

2. Read the text and do the tasks below

Attacks on Cryptosystems

Historically, attempts to gain unauthorized access to secure communications have used brute force attacks, in which the ciphertext is repeatedly searched for clues that can lead to the algorithm's structure. These ciphertext attacks involve a hacker searching for a common text structure, wording, or syntax in the encrypted message that can enable him or her to calculate the number of each type of letter used in the message. This process, known as frequency analysis, is used along with published frequency of occurrence patterns of various languages and can allow an experienced attacker to crack almost any code quickly with a large enough sample of the encoded text. To protect against this, modern algorithms attempt to remove the repetitive and predictable sequences of characters from the ciphertext. Occasionally, an attacker may obtain duplicate texts, one in ciphertext and one in plaintext, and thus reverse-engineer the encryption algorithm in a **known-plaintext attack** scheme. Alternatively, attackers may conduct a **selected-plaintext attack** by sending potential victims a specific text that they are sure the victims will forward on to others. When the victim does encrypt and forward the message, it can be used in the attack if the attacker can acquire the outgoing encrypted version. At the very least, reverse engineering can usually lead the attacker to discover which cryptosystem is being employed.

Most publicly available encryption methods are generally released to the information and computer security communities to test the encryption algorithm's resistance to cracking. In addition, attackers are kept informed of which methods of attack have failed. Although the purpose of sharing this information is to develop a more secure algorithm, it does prevent attackers from wasting their time, freeing them up to find new weaknesses in the cryptosystem or new, more challenging means of obtaining encryption keys.

In general, attacks on cryptosystems fall into four general categories: man-in-the-middle, correlation, dictionary, and timing.

Man-in-the-Middle Attack

A **man-in-the-middle attack** attempts to intercept a public key or even to insert a known key structure in place of the requested public key. Thus, attackers attempt to place themselves between the sender and receiver, and once they've intercepted the request for key exchanges, they send each participant a valid public key, which is known only to them. To the victims of such attacks, encrypted communication appears to be occurring normally, but in fact the attacker is receiving each encrypted message and decoding it (with the key given to the sending party), and then encrypting and sending it to the intended recipient. Establishing public keys with digital signatures can prevent the traditional man in-the-middle attack, as the attacker cannot duplicate the signatures.

Correlation Attacks

As the complexities of encryption methods have increased, so too have the tools and methods of cryptanalysts. **Correlation attacks** are a collection of brute-force methods that attempt to deduce statistical relationships between the structure of the unknown key and the ciphertext generated by the cryptosystem. Differential and linear cryptanalysis, which are advanced methods of code breaking that are beyond the scope of this text, have been used to mount successful attacks on block cipher encryptions such as DES. If **these** advanced approaches can calculate the value of the public key in a reasonable time, all messages written with that key can be decrypted. The only defense against this attack is the selection of strong cryptosystems that have stood the test of time, thorough key management, and strict adherence to the best practices of cryptography in the frequency of key changes.

Dictionary Attacks

In a **dictionary attack**, the attacker encrypts every word in a dictionary using the same cryptosystem as used by the target in an attempt to locate a match between the target ciphertext and the list of encrypted words. Dictionary attacks can be successful when the ciphertext consists of relatively few characters, as for example files which contain encrypted usernames and passwords. An attacker who acquires a system password file can run hundreds of thousands of potential passwords from the dictionary he or she has prepared against the stolen list. Most computer systems use a well-known one-way hash function to store passwords in such files, but an attacker can almost always find at least a few matches in any stolen password file. After a match is found, the attacker has essentially identified a potential valid password for the system.

Timing Attacks

In a **timing attack**, the attacker eavesdrops on the victim's session and uses statistical analysis of patterns and inter-keystroke timings to discern sensitive session information. While timing analysis may not directly result in the decryption of sensitive data, it can be used to gain information about the encryption key and perhaps the cryptosystem. It may also eliminate some algorithms, thus narrowing the attacker's search and increasing the odds of eventual success. Having broken an encryption, the attacker may launch a **replay attack**, which is an attempt to resubmit a recording of the deciphered authentication to gain entry into a secure source.

Defending Against Attacks

Encryption is a very useful tool in protecting the confidentiality of information that is in storage or transmission. However, it is just that—another tool in the information security administrator's arsenal against threats to information security. Frequently, the uninformed describe information security exclusively in terms of encryption (and possibly firewalls and antivirus software). But encryption is simply the process of hiding the true meaning of information.

Over millennia, mankind has developed dramatically more sophisticated means of hiding information from those who should not see it, but no matter how sophisticated encryption and cryptosystems have become, they retain the flaw that was present in the very first such system: If you discover the key, that is, the method used to perform the encryption, you can read the message. Thus, key management is not so much the management of technology but rather the management of people.

2.1. Answer the questions

1. What are correlation attacks?
2. What method can prevent correlation attacks?
3. What is a man-in-the-middle attack?
4. What method can prevent the traditional man in-the-middle attack?
5. When can dictionary attacks be successful?
6. When may the attacker launch a replay attack in timing attack?
7. What method was used to get unauthorized access to secure communications?
8. What type of attacks are mentioned according to the text?

2.2. Decide whether the following statements are true (T), false (F) or no information (NI). Correct the False (F)

1. An attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other is called a man – in – the –middle attack.

   A. True B. False C. NI

2. Although frequency analysis is the able to permit an inexperienced attacker to crack most any code quickly, modern algorithms can break it.

   A. True B. False C. NI

3. A well-known one-way hash function is used to store passwords, so the attacker is not able to crack it and the information is never stolen.

   A. True B. False C. NI

4. More sophisticated means of hiding information from those who should not see it have been developed increasingly so the information security is always safe.

   A. True B. False C. NI

5. A dictionary attack is based on trying all the strings in a pre-arranged listing, typically derived from a list of words such as in a dictionary.

   A. True B. False C. NI

2.3. Choose the best answer for the following statements and questions

1. What attacks were used to gain unauthorized access to secure communications?

A. Brute force attacks B. known-plaintext attacks

C. selected –plaintex attacks D. All are correct

2. Attackers may conduct a ....by sending potential victims a specific text that they are sure the victims will forward on to others.

A. known-plaintext attack B. selected-plaintext attack

C. Brute force attack D. A &C are correct

3. ....have been used to mount successful attacks on block cipher encryptions such as DES.

A. Differential and linear cryptanalysis B. Differential cryptanalysis

C. Frequency analysis D. Linear cryptanalysis

4. In which attack does the attacker eavesdrop on the victim's session?

A. In a dictionary attack B. In a correlation attack

C. In a man-in-the middle attack D. In a timing attack

5. Which of the following does the word "**these**" in the paragraph 6 refer to?

A. Correlation attacks

B. Brute-force methods

C. Differential and linear cryptanalysis

D. Advanced methods

3. Speaking

1. What main contents do you get from the text? What do you know about them?

2. Present attacks on cryptosystems.

4. Listening

1. https://www.youtube.com/watch?v=cqgtdkURzTE

2. https://www.youtube.com/watch?v=c5rHvmJwFOM

3. https://www.youtube.com/watch?v=2BldESGZKB8
4. https://www.youtube.com/watch?v=JR4_RBb8A9Q
5. https://www.youtube.com/watch?v=Rnn_HLtgJ2M
6. https://www.youtube.com/watch?v=AQDCe585Lnc

WRITING AND SPEAKING

1. Write about 400 words about one of the following topics in your own words.
   - Hash functions
   - Symmetric encryption
   - Asymmetric encryption
   - Attacks on cryptosystems
2. Present the following contents:
   - Hash functions
   - Symmetric encryption
   - Asymmetric encryption
   - Attacks on cryptosystems

FUTHER READING

Digital Signatures

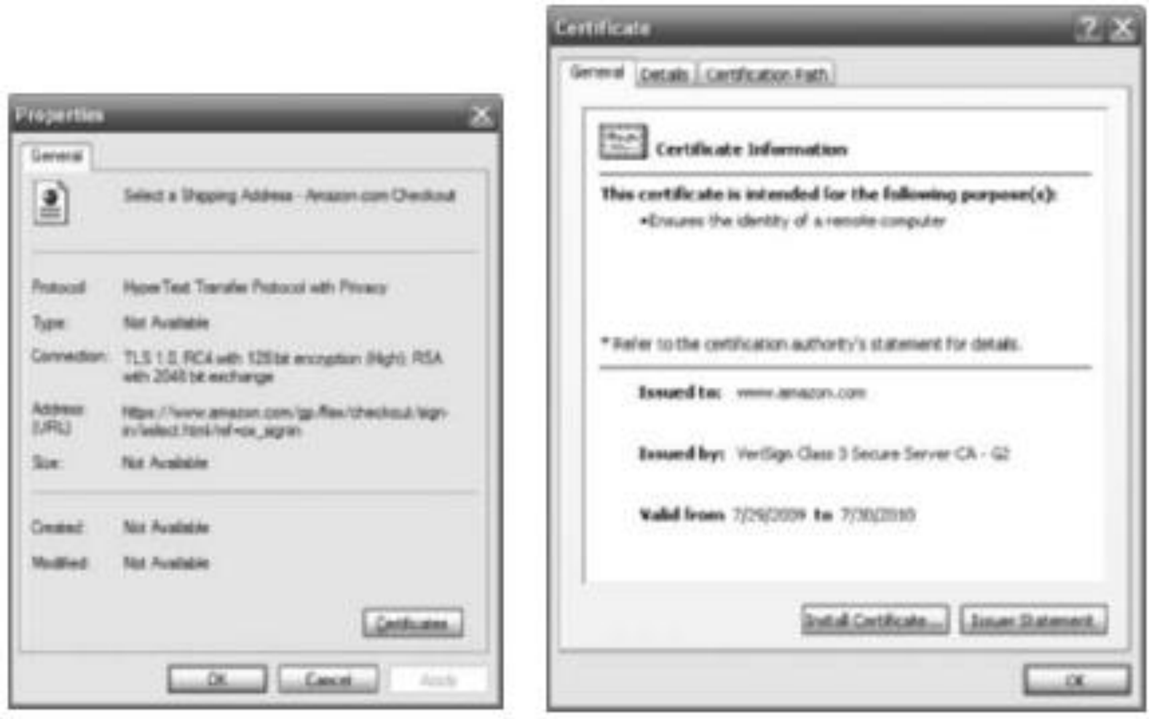
Digital signatures were created in response to the rising need to verify information transferred via electronic systems. Asymmetric encryption processes are used to create digital signatures. When an asymmetric cryptographic process uses the sender's private key to encrypt a message, the sender's public key must be used to decrypt the message. When the decryption is successful, the process verifies that the message was sent by the sender and thus cannot be refuted. This process is known as nonrepudiation and is the principle of cryptography that underpins the authentication mechanism collectively known as a digital signature. Digital signatures are, therefore, encrypted messages that can be mathematically proven authentic.

The management of digital signatures is built into most Web browsers. The Internet Explorer digital signature management screen is shown in Figure 8-7. In general, digital signatures should be created using processes and products that are based on the **Digital Signature Standard** (DSS). When processes and products are certified as DSS compliant, they have been approved and endorsed by U.S. federal and state governments, as well as by many foreign governments, as a means of authenticating the author of an electronic document. NIST has approved a number of algorithms that can be used to generate and verify digital signatures.

These algorithms can be used in conjunction with the sender's public and private keys, the receiver's public key, and the Secure Hash Standard (described earlier in this chapter) to quickly create messages that are both encrypted and nonrepudiable. This process first creates a message digest using the hash algorithm, which is then input into the digital signature algorithm along with a random number to generate the digital signature. The digital signature function also depends upon the sender's private key and other information provided by the CA. The resulting encrypted message contains the digital signature, which can be verified by the recipient using the sender's public key.

Digital Certificates

As you learned earlier in this chapter, a digital certificate is an electronic document or container file that contains a key value and identifying information about the entity that controls the key. The certificate is often issued and certified by a third party, usually a certificate . A digital signature attached to the certificate's container file certifies the file's origin and integrity. This verification process often occurs when you download or update software via the Internet. The window in Figure 6-3 shows, for example, that the downloaded files do in fact come from the purported originating agency, Amazon.com, and thus can be trusted.



Select a Shipping Address - Amazon.com Checkout

Protocol: HyperText Transfer Protocol with Privacy
Type: Not Available
Connection: TLS 1.0, RC4 with 128 bit encryption (High); RSA with 2048 bit exchange
Address (URL): https://www.amazon.com/gp/flex/checkout/sign-in/select.html/ref=ox_signin
Size: Not Available

Created: Not Available
Modified: Not Available

Certificate Information

This certificate is intended for the following purpose(s):
•Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: www.amazon.com

Issued by: VeriSign Class 3 Secure Server CA - G2

Valid from 7/29/2009 to 7/30/2010

Figure 6-3 Digital certificate

Unlike digital signatures, which help authenticate the origin of a message, digital certificates authenticate the cryptographic key that is embedded in the certificate. When used properly these certificates enable diligent users to verify the authenticity of any organization's certificates. This is much like what happens when the Federal Deposit Insurance Corporation issues its FDIC logo to banks to assure customers that their bank is authentic. Different client-server applications use different types of digital certificates to accomplish their assigned functions, as follows

- The CA application suite issues and uses certificates (keys) that identify and establish a trust relationship with a CA to determine what additional certificates (keys) can be authenticated.

- Mail applications use Secure/Multipurpose Internet Mail Extension (S/MIME) certificates for signing and encrypting e-mail as well as for signing forms.
- Development applications use object-signing certificates to identify signers of object oriented code and scripts.
- Web servers and Web application servers use Secure Sockets Layer (SSL) certificates to authenticate servers via the SSL protocol (which is described shortly) in order to establish an encrypted SSL session.
- Web clients use client SSL certificates to authenticate users, sign forms, and participate in single sign-on solutions via SSL.

UNIT 7: PHYSICAL SECURITY

Introduction

Information security requires the protection of both data and physical assets. You have already learned about many of the mechanisms used to protect data, including firewalls, intrusion detection systems, and monitoring software.

Physical security encompasses the design, implementation, and maintenance of countermeasures that protect the physical resources of an organization, including the people, hardware, and supporting system elements and resources that control information in all its states (trans- mission, storage, and processing). Most technology-based controls can be circumvented if an attacker gains physical access to the devices being controlled. In other words, if it is easy to steal the hard drives from a computer system, then the information on those hard drives is not secure. Therefore, physical security is just as important as logical security to an information security program.

In earlier units, you encountered a number of threats to information security that could be classified as threats to physical security. For example, an employee accidentally spilling coffee on a laptop threatens the physical security of the information in the computer—in this case, the threat is an act of human error or failure. A compromise to intellectual property can include an employee without an appropriate security clearance copying a classified marketing plan. A deliberate act of espionage or trespass could be a competitor sneaking into a facility with a camera. Deliberate acts of sabotage or vandalism can be physical attacks on individuals or property. Deliberate acts of theft include employees stealing computer equipment, credentials, passwords, and laptops. Quality of service deviations from service providers, especially power and water, also represent physical security threats, as do various environmental anomalies. In his book, *Fighting Computer Crime*, Donn B. Parker lists the following "Seven Major Sources of Physical Loss":

- Extreme temperature: heat, cold
- Gases: war gases, commercial vapors, humid or dry air, suspended particles
- Liquids: water, chemicals
- Living organisms: viruses, bacteria, people, animals, insects
- Projectiles: tangible objects in motion, powered objects
- Movement: collapse, shearing, shaking, vibration, liquefaction, flow waves, separation, slide
- Energy anomalies: electrical surge or failure, magnetism, static electricity, aging circuitry; radiation: sound, light, radio, microwave, electromagnetic, atomic

As with all other areas of security, the implementation of physical security measures requires sound organizational policy. Physical security policies guide users on the appropriate use of computing resources and information assets, as well as on the protection of their own personal safety in day-to-day operations. Physical security is designed and implemented in several layers. Each of the organization's communities of interest is responsible for components within these layers, as follows:

- General management is responsible for the security of the facility in which the organization is housed and the policies and standards for secure operation. This includes exterior security, fire protection, and building access, as well as other controls such as guard dogs and door locks.
- IT management and professionals are responsible for environmental and access security in technology equipment locations, and for the policies and standards that govern secure equipment operation. This includes access to server rooms, and power conditioning and server room temperature and humidity controls, and more specialized controls like static and dust contamination equipment.

Information security management and professionals are responsible for risk assessments and for reviewing the physical security controls implemented by the other two groups.

READING AND SPEAKING 1

1. **Discuss the questions:**

    1. What is physical security?

    2. What are the primary threats to physical security?

    3. How does physical access control differ from logical access

    control? How is it similar?

    4. Which physical access controls could you identify in our Academy?

    5. Who is in charge of physical access controls in our Academy?

2. **Read the text and do the tasks below**

Physical Access Controls

A number of physical access controls are uniquely suited to governing the movement of people within an organization's facilities—specifically, controlling their physical access to company resources. While logical access to systems, in this age of the Internet, is a very important subject, the control of physical access to the assets of the organization is also of critical importance. Some of the technology used to control physical access is also used to control logical access, including biometrics, smart cards, and wireless enabled keycards.

Before learning more about physical access controls, you need to understand what makes a facility secure. An organization's general management oversees its physical security. Commonly, a building's access controls are operated by a group called **facilities management**. Larger organizations may have an entire staff dedicated to facilities management, while smaller organizations often outsource these duties.

In facilities management, a **secure facility** is a physical location that has in place controls to minimize the risk of attacks from physical threats. The term *secure facility* might bring to mind military bases, maximum-security prisons, and nuclear power plants, but while securing a facility requires some adherence to rules and procedures, the environment does not necessarily have to be that constrained. It is also not necessary that a facility resemble a fortress to minimize risk from physical attacks. In fact, a secure facility can sometimes use its natural terrain, local traffic flow, and surrounding development to enhance its physical security, along with protection mechanisms such as fences, gates, walls, guards, and alarms.

Physical Security Controls

There are a number of physical security controls that an organization's communities of inter- est should consider when implementing physical security inside and outside the facility. Some of the major controls are:

- Walls, fencing, and gates
- Guards
- Dogs
- ID cards and badges
- Locks and keys
- Mantraps
- Electronic monitoring
- Alarms and alarm systems
- Computer rooms and wiring closets
- Interior walls and doors

Walls, Fencing, and Gates Some of the oldest and most reliable elements of physical security are walls, fencing, and gates. While not every organization needs to implement external perimeter controls, walls and fences with suitable gates are an essential starting point for organizations whose employees require access to physical locations the organization owns or controls. These types of controls vary widely in appearance and function, ranging from chain link or privacy fences that control where people should park or walk, to imposing concrete or masonry barriers designed to withstand the blast of a car bomb. Each exterior perimeter control requires expert planning to ensure that it fulfills the security goals and that it presents an image appropriate to the organization.

Guards Controls like fences and walls with gates are static, and are therefore unresponsive to actions, unless they are programmed to respond with specific actions to specific stimuli, such as opening for someone who has the correct key. Guards, on the other hand, can evaluate each situation as it arises and make reasoned responses. Most guards have clear **standard operating procedures (SOPs)** that help them to act decisively in unfamiliar situations. In the military, for example, guards are given general orders (see the Offline on guard duty), as well as special orders that are particular to their posts.

Dogs If an organization is protecting valuable resources, dogs can be a valuable part of physical security if they are integrated into the plan and managed properly. Guard dogs are useful because their keen sense of smell and hearing can detect intrusions that human guards cannot, and they can be placed in harm's way when necessary to avoid risking the life of a person.

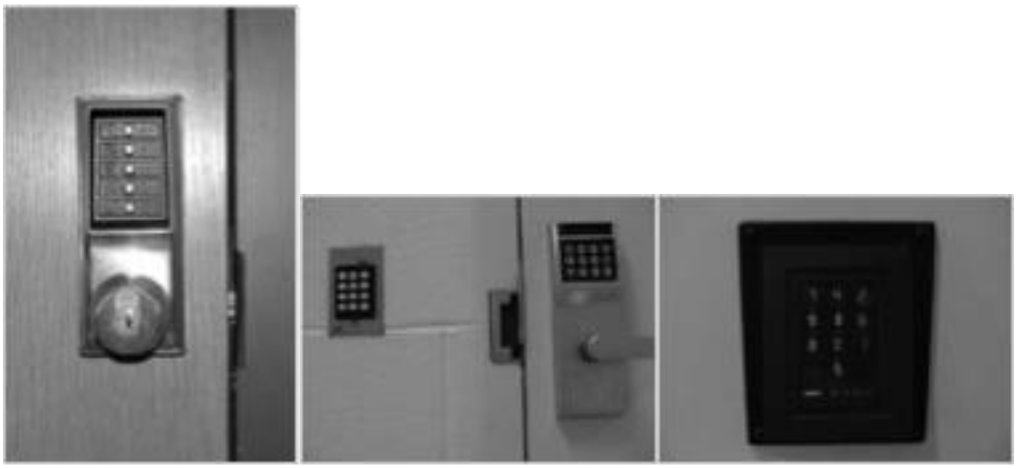
ID Cards and Badges An **identification (ID) card** is typically concealed, whereas a **name badge** is visible. Both devices can serve a number of purposes. First, they serve as simple forms of biometrics in that they use the cardholder's picture to authenticate his or her access to the facility. The cards may be visibly coded to specify which buildings or areas may be accessed. Second, ID cards that have a magnetic strip or radio chip that can be read by automated control devices allow an organization to restrict access to sensitive areas within the facility. ID cards and name badges are not foolproof, however; and even the cards designed to communicate with locks can be easily duplicated, stolen, or modified. Because of this inherent weakness, such devices should not be an organization's only means of controlling access to restricted areas.

Another inherent weakness of this type of physical access control technology is the human factor. **Tailgating** occurs when an authorized person presents a key to open a door, and other people, who may or may not be authorized, also enter. Launching a campaign to make employees aware of tailgating is one way to combat this problem. There are also technological means of discouraging tailgating, such as mantraps (which are discussed in a following section) or turnstiles. These extra levels of control are usually expensive, in that they require floor space and/or construction, and are inconvenient for those required to use them. Consequently, anti-tailgating controls are only used where there is significant security risk from unauthorized entry.

Locks and Keys There are two types of lock mechanisms: mechanical and electromechanical. The **mechanical lock** may rely on a key that is a carefully shaped piece of metal, which is rotated to turn tumblers that release secured loops of steel, aluminum, or brass (as in, for example, brass padlocks). Alternatively, a mechanical lock may have a dial that rotates slotted discs until the slots on multiple disks are aligned, and then retracts a securing bolt (as in combination and safe locks). Although mechanical locks are conceptually simple, some of the technologies that go into their development are quite complex. Some of these modern enhancements have led to the creation of the electromechanical lock. **Electromechanical locks** can accept a variety of inputs as keys, including magnetic strips on ID cards, radio signals from name badges, personal identification numbers **(PINs)** typed into a keypad, or some combination of these to activate an electrically powered locking mechanism.

Locks can also be divided into four categories based on the triggering process: manual, programmable, electronic, and biometric. **Manual locks** such as padlocks and combination locks, are commonplace and well understood. If you have the key (or combination) you can open the lock. These locks are often preset by the manufacturer and therefore unchangeable. In other words, once manual locks are installed into doors, they can only be changed by highly trained locksmiths. Programmable locks can be changed after they are put in service, allowing for combination or key changes without a locksmith and even allowing the owner to change to another access method (key or combination) to upgrade security. Many examples of these types of locks are shown in Figure 7-1. Mechanical push button locks, shown in the left-most photo in Figure 7-1, are popular for securing computer rooms and wiring closets, as they have a code that can be reset and don't require electricity to operate.

Electronic locks can be integrated into alarm systems and combined with other building management systems. Also, these locks can be integrated with sensors to create various combinations of locking behavior. One such combination is a system that coordinates the use of fire alarms and locks to improve safety during alarm conditions (i.e., fires). Such a system changes a location's required level of access authorization when that location is in an alarm condition. Another example is a combination system in which a lock is fitted with a sensor that notifies guard stations when that lock has been activated. Another common form of electronic locks are electric strike locks, which usually require people to announce themselves before being "buzzed" through a locked door. In general, electronic locks lend themselves to uses where they can be activated or deactivated by a switch controlled by an agent, usually a secretary or guard. Electronic push button locks, like their mechanical cousins, have a numerical keypad over the knob, requiring the individual user to enter a personal code and open the door. These locks usually use battery backups to power the keypad in case of a power failure.



Programmable/mechanical **Electronic**

Figure 7-1 *Locks*

Some locks use smart cards, as described previously—keys that contain computer chips. These smart cards can carry critical information, provide strong authentication, and offer a number of other features. Keycard readers based on smart cards are often used to secure computer rooms, communications closets, and other restricted areas. The card reader can track entry and provide accountability. In a locking system that uses smart cards, the access level of individuals can be adjusted according to their current status (i.e., current employee, recently resigned) and thus personnel changes do not require replacement of the lock. A specialized type of keycard reader is the **proximity reader**, which, instead of requiring individuals to insert their cards, allows them simply to place their cards within the reader's range. Some of these readers can recognize the card even when it is inside a pocket.

The most sophisticated locks are **biometric locks**. Finger, palm, and hand readers, iris and retina scanners, and voice and signature readers fall into this category.

The management of keys and locks is fundamental to the fulfillment of general management's responsibility to secure an organization's physical environment. When people are hired, fired, laid off, or transferred, their access controls, whether physical or logical, must be appropriately adjusted. Failure to do so can result in employees cleaning out their offices and taking more than their personal effects. Also, when locksmiths are hired, they should be carefully screened and monitored, as there is a chance that they could have complete access to the facility.

Sometimes locks fail, and thus facilities need to have alternative procedures in place for con- trolling access. These procedures must take into account that locks fail in one of two ways: the door lock fails and the door becomes unlocked—a **fail-safe lock**; or the door lock fails and the door remains locked—a **fail-secure lock**. In practice, the most common reason why technically sophisticated locks fail is loss of power and activation through fire control systems. A fail-safe lock is usually used to secure an exit, where it is essential that in the event of, for instance, a fire, the door is unlocked. A fail-secure lock is used when human safety in the area being controlled is not the dominant factor. One example of this is a situation in which the security of nuclear or biological weapons needs to be controlled; here, preventing a loss of control of these weapons is more critical to security (meaning it is a security issue of greater magnitude) than protecting the lives of the personnel guarding the weapons.

Understanding lock mechanisms is important, because locks can be exploited by an intruder to gain access to the secured location. If an electronic lock is short circuited, it may become fail-safe and allow the intruder to bypass the control and enter the room.

Mantraps A common enhancement for locks in high security areas is the mantrap. A **mantrap** is a small enclosure that has separate entry and exit points. To gain access to the facility, area, or room, a person enters the mantrap, requests access via some form of electronic or biometric lock and key, and if confirmed, exits the mantrap into the facility. Otherwise the person cannot leave the mantrap until a security official overrides the enclosure's automatic locks. Figure 7-2 provides an example of a typical mantrap layout.

Electronic Monitoring Monitoring equipment can be used to record events within a specific area that guards and dogs might miss, or in areas where other types of physical controls are not practical. Although you may not know it, many of you are, thanks to the silver globes attached to the ceilings of many retail stores, already subject to cameras viewing you from odd corners—that is, video monitoring. Attached to these cameras are video cassette recorders (VCRs) and related machinery that capture the video feed. Electronic monitoring includes **closed-circuit television (CCT)** systems. Some CCT systems collect constant video feeds, while others rotate input from a number of cameras, sampling each area in turn.

These video monitoring systems have drawbacks: for the most part they are passive and do not prevent access or prohibited activity. Another drawback to these systems is that people must view the video output, because there are no intelligent systems capable of reliably evaluating a video feed. To determine if unauthorized activities have occurred, a security staff member must constantly review the information in real time or review the information collected in video recordings. For this reason, CCT is most often used as an evidence collection device after an area has been broken into than as a detection instrument. In high-security areas (such as banks, casinos, and shopping centers), however, security personnel monitor CCT systems constantly, looking for suspicious activity.

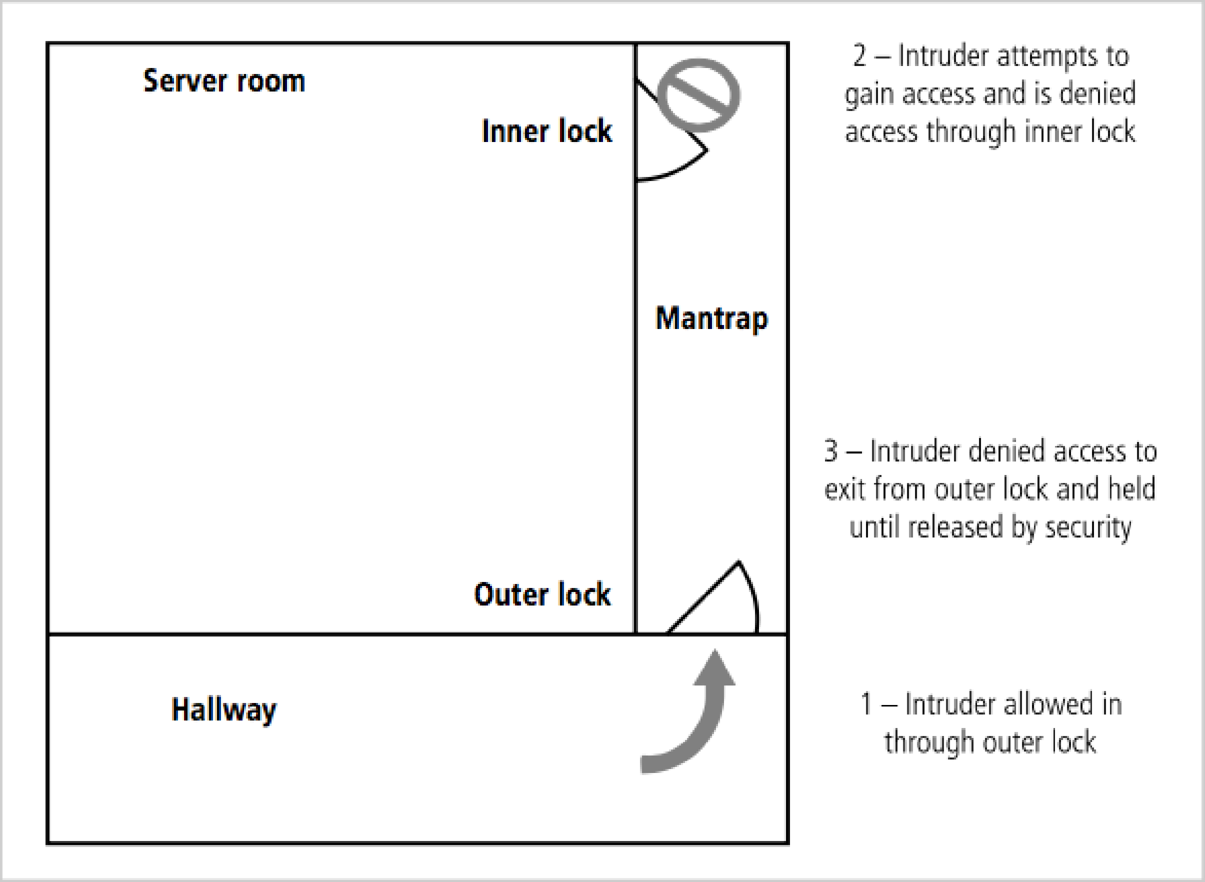

Server room
Inner lock
2 – Intruder attempts to gain access and is denied access through inner lock
Mantrap
3 – Intruder denied access to exit from outer lock and held until released by security
Outer lock
Hallway
1 – Intruder allowed in through outer lock

Figure 7-2 Mantraps

Source: Course Technology/Cengage Learning

Alarms and Alarm Systems Closely related to monitoring are the alarm systems that notify people or systems when a predetermined event or activity occurs. Alarms can detect a *physical* intrusion or other untoward event. This could be a fire, a break-in, an environmental disturbance such as flooding, or an interruption in services such as a loss of power. One example of an alarm system is the burglar alarm commonly found in residential and commercial environments. Burglar alarms detect intrusions into unauthorized areas and notify either a local or remote security agency to react. To detect intrusions, these systems rely on a number of different types of sensors: motion detectors, thermal detectors, glass breakage detectors, weight sensors, and contact sensors. **Motion detectors** detect movement within a confined space and are either active or passive. Some motion sensors emit energy beams, usually in the form of infrared or laser light, ultrasonic sound or sound waves, or some form of electromagnetic radiation. If the energy from the beam projected into the area being monitored is disrupted, the alarm is activated. Other types of motion sensors are passive in that they constantly measure the energy (infrared or ultrasonic) from the monitored space and detect rapid changes in this energy. The passive measurement of these energies can be blocked or disguised and is therefore fallible. **Thermal detectors** measure rates of change in the ambient temperature in the room. They can, for example, detect when a person with a body temperature of 98.6 degrees Fahrenheit enters a room with a temperature of 65 degrees Fahrenheit, because the person's presence changes the room's ambient temperature. Thermal detectors are also used in fire detection (as is described in later sections). **Contact and weight sensors** work when two contacts are connected as, for example, when a foot steps on a pressure- sensitive pad under a rug, or a window is opened, triggering a pin-and-spring sensor. **Vibration sensors** also fall into this category, except that they detect movement of the sensor rather than movement in the environment.

Computer Rooms and Wiring Closets Computer rooms and wiring and communications closets require special attention to ensure the confidentiality, integrity, and avail- ability of information. For an outline of the physical and environmental controls needed for computer rooms, read the Technical Details box entitled "Physical and Environmental Controls for Computer Rooms."

Logical access controls are easily defeated if an attacker gains physical access to the computing equipment. Custodial staff members are often the least scrutinized employees (or nonemployees) who have access to an organization's offices. Yet custodians are given the greatest degree of unsupervised access. They are often handed the master keys to the entire building and then ignored, even though they collect paper from every office, dust many desks, and move large containers from every area. It is, therefore, not difficult for this type of worker to gather critical information and computer media or copy proprietary and classified information. All this is not to say that an organization's custodial staff should be under constant suspicion of espionage, but to note that the wide-reaching access that custodians have can be a vulnerability that attackers exploit to gain unauthorized information. Factual accounts exist of technically trained agents working as custodians in the offices of their competition. Thus, custodial staffs should be carefully managed not only by the organization's general management, but also by IT management.

Interior Walls and Doors The security of information assets can sometimes be com- promised by the nature of the construction of the walls and doors of the facility. The walls in a facility are typically of two types: standard interior and firewall. Building codes require that each floor have a number of **firewalls**, or walls that limit the spread of damage should a fire break out in an office. While the network firewalls discussed in an earlier chapter isolate the logical subnetworks of the organization, physical firewalls isolate the physical spaces of the organization's offices. Between the firewalls, standard interior walls compartmentalize the individual offices. Unlike firewalls, these interior walls reach only part way to the next floor, which leaves a space above the ceiling but below the floor of the next level up. This space is called a **plenum**, and is usually one to three feet to allow for ventilation systems that can inexpensively collect return air from all the offices on the floor. For security, how- ever, this design is not ideal, because it means that an individual can climb over the wall from one office to the other. As a result, all high-security areas, such as computer rooms and wiring closets, must have firewall-grade walls surrounding them. This provides physical security not only from potential intruders, but also from fires.

The doors that allow access into high-security rooms should also be evaluated. Standard office-grade doors provide little or no security. For example, one of the authors of this text- book once locked himself out of his office by accidentally breaking the key off in the lock. When the locksmith arrived, he carried a curious contraption. Instead of disassembling the lock or deploying other locksmith secrets, he carried a long piece of heavy-duty wire, bent into the shape of a bow, with a string tied to each end. He slid one end of this bow through the one-inch gap under the door, stood it on one end and yanked the string. The wire bow slid over the door handle and the string looped over it. When the locksmith yanked the string, the door swung open. (Note: to see this device in action visit *http://gizmodo.com/ 5477600/hotel-locks-defeated-by-piece-of-wire-secured-by-towel*, or search on the term "hotel locks defeated by piece of wire.") This information is not meant to teach you how to access interior offices but to warn you that no office is completely secure. How can you avoid this problem? In most interior offices, you can't. Instead, IT security professionals must educate the organization's employees about how to secure the information and systems within their offices.

To secure doors, install push or crash bars on computer rooms and closets. These bars are much more difficult to open from the outside than the standard door pull handles and thus provide much higher levels of security, but **they** also allow for safe egress in the event of an emergency.

2.1. Answer the questions:

1. How can you define a secure facility?

2. Why are guards considered the most effective form of control for situations that require decisive action in the face of unfamiliar stimuli?

4. When should dogs be used for physical security?

5. What are the weaknesses of ID cards and name badges?

5. What is tailgating?

6. What are the measures to prevent tailgating?

7. List two types of lock mechanism. What is the difference between them?

8. List and describe the four categories of locks. In which situation is each type of lock preferred?

9.What are the two possible modes that locks use when they fail? What implications do these modes have for human safety? In which situation is each mode preferred?

10. What is a mantrap? When should it be used?

11. What are the disadvantages of video monitoring systems?

2.2. Decide whether the following statements are true (T), false (F), or no information (NI)

1. Anti-tailgating controls are common and affordable measures to deploy.

A. True B. False C. NI

2. Only a key that is a carefully shaped piece of metal can be used to open a mechanical lock.

A. True B. False C. NI

3. Manual locks are very popular.

A. True B. False C. NI

4. Electricity is necessary to operate a mechanical push button locks.

A. True B. False C. NI

5. A fail-safe lock could cause more dangers for people than a fail-secure lock.

A. True B. False C. NI

6. CCT is the most often used electronic monitoring equipment.

A. True B. False C. NI

2.3. Choose the best answer for the following questions and statements

1. Which information may NOT be provided on an ID card or name badge?

C. The cardholder’s address

D. The cardholder’s picture

E. The cardholder’s name

F. The building and area the cardholder could access

2. What is considered the most complex type of lock?

A. Electromechanical locks

B. Biometric locks

C. Smart cards

D. Programmable locks

3. What is NOT considered a biometric lock?

A. Iris scanner

B. Palm reader

C. Voice reader

D. Proximity reader

4. Which place may burglar alarms NOT be found?

A. Shopping mall

B. Jewellery store

C. University

D. Home

5. What does the word “**they**” in the last paragraph refer to?

A. push or crash bars

B. computer rooms and closets

C. door pull handles

D. levels of security

3. Speaking

1. Present your understanding about different forms of alarm and give examples from your everyday life.

2. Talk about a physical access control that you might add or improve in our Academy.

READING AND SPEAKING 2

1. **Discuss the questions:**
   1. Which fire suppression system could you identify in your surroundings?
   2. List all fire detection systems that you know about.
2. **Read the text and do the tasks below**

Fire Security and Safety

The most important security concern is the safety of the people present in an organization's physical space—workers, customers, clients, and others. The most serious threat to that safety is fire. Fires account for more property damage, personal injury, and death than any other threat to physical security. As a result, it is imperative that physical security plans examine and implement strong measures to detect and respond to fires and fire hazards.

Fire Detection and Response

Fire suppression systems are devices that are installed and maintained to detect and respond to a fire, potential fire, or combustion danger situation. These systems typically work by denying an environment one of the three requirements for a fire to burn: temperature (ignition source), fuel, and oxygen.

While the temperature of ignition, or **flame point**, depends upon the material, it can be as low as a few hundred degrees. Paper, the most common combustible in the office, has a flame point of 451 degrees Fahrenheit (a fact that is used to dramatic effect in Ray Bradbury's novel *Fahrenheit 451*). Paper can reach that temperature when it is exposed to a carelessly dropped cigarette, malfunctioning electrical equipment, or other accidental or purposeful misadventures.

Water and water mist systems, which are described in detail in subsequent paragraphs, work both to reduce the temperature of the flame in order to extinguish it and to saturate some types of fuels (such as paper) to prevent ignition. Carbon dioxide systems (CO_2) rob fire of its oxygen. Soda acid systems deny fire its fuel, preventing the fire from spreading. Gas-based systems, such as Halon and its Environmental Protection Agency-approved replacements, disrupt the fire's chemical reaction but leave enough oxygen for people to survive for a short time. Before a fire can be suppressed, however, it must be detected.

Fire Detection Fire detection systems fall into two general categories: manual and automatic. **Manual fire detection systems** include human responses, such as calling the fire department, as well as manually activated alarms, such as sprinklers and gaseous systems. Organizations must use care when manually triggered alarms are tied directly to suppression systems, since false alarms are not uncommon. Organizations should also ensure that proper security remains in place until all employees and visitors have been cleared from the building and their evacuation has been verified. During the chaos of a fire evacuation, an attacker can easily slip into offices and obtain sensitive information. To help prevent such intrusions, fire safety programs often designate an individual from each office area to serve as a floor monitor.

There are three basic types of fire detection systems: thermal detection, smoke detection, and flame detection. **Thermal detection systems** contain a sophisticated heat sensor that operates in one of two ways. **Fixed temperature** sensors detect when the ambient temperature in an area reaches a predetermined level, usually between 135 degrees Fahrenheit and 165 degrees Fahrenheit, or 57 degrees Centigrade to 74 degrees Centigrade. **Rate-of-rise** sensors detect an unusually rapid increase in the area temperature within a relatively short period of time. In either case, if the criteria are met, the alarm and suppression systems are activated. Thermal detection systems are inexpensive and easy to maintain. Unfortunately, thermal detectors usually don’t catch a problem until it is already in progress, as in a full-blown fire. As a result, thermal detection systems are not a sufficient means of fire protection in areas where human safety could be at risk. They are also not recommended for areas with high- value items or items that could be easily damaged by high temperatures.

Smoke detection systems are perhaps the most common means of detecting a potentially dangerous fire, and they are required by building codes in most residential dwellings and commercial buildings. Smoke detectors operate in one of three ways. **Photoelectric sensors** project and detect an infrared beam across an area. If the beam is interrupted (presumably by smoke), the alarm or suppression system is activated. **Ionization sensors** contain a small amount of a harmless radioactive material within a detection chamber. When certain by-products of combustion enter the chamber, they change the level of electrical conductivity within the chamber and activate the detector. Ionization sensor systems are much more sophisticated than photoelectric sensors and can detect fires much earlier, since invisible by-products can be detected long before enough visible material enters a photoelectric sensor to trigger a reaction. **Air-aspirating detectors** are sophisticated systems and are used in high-sensitivity areas. They work by taking in air, filtering it, and moving it through a chamber containing a laser beam. If the laser beam is diverted or refracted by smoke particles, the system is activated. These types of systems are typically much more expensive than systems that use photoelectric or ionization sensors; however, they are much better at early detection and are commonly used in areas where extremely valuable materials are stored.

The third major category of fire detection systems is the **flame detector**. The flame detector is a sensor that detects the infrared or ultraviolet light produced by an open flame. These systems compare a scanned area's light signature to a database of known flame light signatures to determine whether or not to activate the alarm and suppression systems. While highly sensitive, flame detection systems are expensive and must be installed where they can scan all areas of the protected space. They are not typically used in areas with human lives at stake; however, they are quite suitable for chemical storage areas where normal chemical emissions might activate smoke detectors.

Fire Suppression Fire suppression systems can consist of portable, manual, or automatic apparatus. Portable extinguishers are used in a variety of situations where direct application of suppression is preferred, or fixed apparatus is impractical. Portable extinguishers are much more efficient for smaller fires, because triggering an entire building's sprinkler systems can do a lot of damage. Portable extinguishers are rated by the type of fire they can combat, as follows:

- Class A fires: Those fires that involve ordinary combustible fuels such as wood, paper, textiles, rubber, cloth, and trash. **Class A fires** are extinguished by agents that interrupt the ability of the fuel to be ignited. Water and multipurpose dry chemical fire extinguishers are ideal for these types of fires.
- Class B fires: Those fires fueled by combustible liquids or gases, such as solvents, gasoline, paint, lacquer, and oil. **Class B fires** are extinguished by agents that remove oxygen from the fire. Carbon dioxide, multipurpose dry chemical, and Halon fire extinguishers are ideal for these types of fires.
- Class C fires: Those fires with energized electrical equipment or appliances. **Class C fires** are extinguished with non-conducting agents only. Carbon dioxide, multipurpose dry chemical, and Halon fire extinguishers are ideal for these types of fires. Never use a water fire extinguisher on a Class C fire.
- Class D fires: Those fires fueled by combustible metals, such as magnesium, lithium, and sodium. **Class D fires** require special extinguishing agents and techniques.

Manual and automatic fire response systems include those designed to apply suppressive agents. These are usually either sprinkler or gaseous systems. All **sprinkler systems** are designed to apply liquid, usually water, to all areas in which a fire has been detected, but an organization can choose from one of three implementations: wet-pipe, dry-pipe, or pre-action systems. A **wetpipe** system has pressurized water in all pipes and has some form of valve in each protected area. When the system is activated, the valves open, sprinkling the area. This is best for areas where the fire represents a serious risk to people, but where damage to property is not a major concern. The most obvious drawback to this type of system is water damage to office equipment and materials. A wet-pipe system is not usually appropriate in computer rooms, wiring closets, or anywhere electrical equipment is used or stored. There is also the risk of accidental or unauthorized activation. Figure 8-3 shows a wet-pipe water sprinkler system that is activated when the ambient temperature reaches 140 degrees Fahrenheit to 150 degrees Fahrenheit, bringing the special liquid in the glass tube to a boil, which causes the tube to shatter and open the valve. Once the valve is open, water flows through the diffuser, which disperses the water over the area.

A **dry-pipe system** is designed to work in areas where electrical equipment is used. Instead of water, the system contains pressurized air. The air holds valves closed, keeping the water away from the target areas. When a fire is detected, the sprinkler heads are activated, the pressurized air escapes, and water fills the pipes and exits through the sprinkler heads. This reduces the risk of accidental leakage from the system. Some sprinkler system, called **deluge systems**, keep open all of the individual sprinkler heads, and as soon as the system is activated, water is immediately applied to all areas. This is not, however, the optimal solution for computing environments, since there are other more sophisticated systems that can suppress the fire without damage to computer equipment.

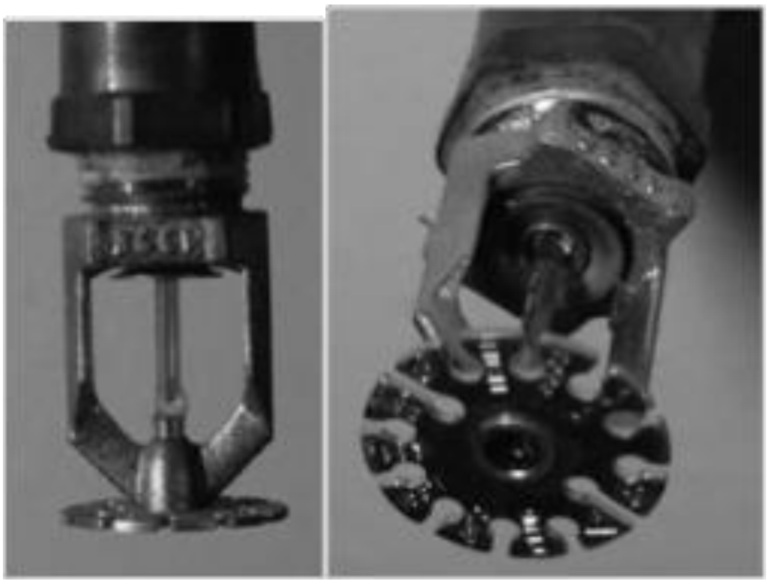


Figure 7-3 Water Sprinkler System *Source: Course Technology/Cengage Learning*

A variation of the dry-pipe system is the **pre-action system**. This approach has a two-phase response to a fire. Under normal conditions, the system has nothing in the delivery pipes. When a fire is detected, the first phase is initiated, and valves allow water to enter the sys- tem. At that point, the system resembles a wet-pipe system. The pre-action system does not deliver water into the protected space until the individual sprinkler heads are triggered, at which time water flows only into the area of the activated sprinkler head.

Water mist sprinklers are the newest form of sprinkler systems and rely on ultra-fine mists instead of traditional shower-type systems. The water mist systems work like traditional water system by reducing the ambient temperature around the flame, therefore minimizing its ability to sustain the necessary temperature needed to maintain combustion. Unlike traditional water sprinkler systems, however, these systems produce a fog-like mist that, because the droplets are much less susceptible to gravity, stays buoyant (airborne) much longer. As a result, a much smaller quantity of water is required; also the fire is extinguished more quickly, which causes less collateral damage. Relative to gaseous systems (which are discussed shortly), water-based systems are low cost, nontoxic, and can often be created by using an existing sprinkler system that may have been present in earlier construction.

A physical security plan requires that every building have clearly marked fire exits and maps posted throughout the facility. It is important to have drills to rehearse fire alarm responses and designate individuals to be in charge of escorting everyone from the location and ensuring that no one is left behind. It is also important to have fire suppression systems that are both manual and automatic, and that are inspected and tested regularly.

2.1.Answer the questions:

1. What is considered the most serious threat within the realm of physical security? Why is it valid to consider this threat the most serious?

2.How do fire suppression systems manipulate the three elements for a fire to burn?

3.What is flame point? In which situation can paper reach its flame point?

4. What is the role of a floor monitor?

5.List and describe the three fire detection technologies covered in the chapter. Which is currently the most commonly used?

6. List three ways in which smoke detectors operate. Which type is the most expensive?

7. List and describe the four classes of fire described in the text. Does the class of a fire dictate how to control the fire?

2.2. Decide whether the following statements are true (T), false (F), or no information (NI)

1. Fire is the most popular danger to human safety in an organization’s physical space.

A. True B. False C. NI

2. Ionization sensors are most usually found in places where highly valuable materials are stored.

A. True B. False C. NI

3. Flame detector is commonly installed in highly populated areas.

A. True B. False C. NI

4. The suitable fire suppression system for small fires is portable extinguisher.

A. True B. False C. NI

5. Fire suppression systems in every building need to be inspected and tested every year.

A. True B. False C. NI

2.3. Choose the best answer for the following questions and statements

1. What is NOT one of the elements must be present for a fire to ignite and continue to burn?

A. oxygen

B. carbon dioxide

C. temperature

D. fuel

2. Which of the following is NOT a fire suppression system?

A. Soda acid system

B. Gas-based system

C. Water mist system

D. Manual detection system

3. Which of the following is NOT a manual fire detection system?

A. human responses

B. automatic system

C. sprinklers

D. gaseous system

4. Among these three smoke detection systems, which is best at early fire detection?

A. Air-aspirating detectors

B. Ionization sensors

C. Photoelectric sensors

D. They are the same

5. What does the word “it” in line 11, paragraph 3 refer to?

A. temperature of ignition

B. paper

C. material

D. None are correct

3. Speaking

1. Present about fire suppression systems being used in different buildings that you know. Why is that specific system selected for that context?

READING AND SPEAKING 3

1. **Discuss the questions:**
   1. Do you think supporting utilities such as heating, ventilation, air conditioning and power system could affect the physical security of an organization?
   2. How can it happen? Give practical examples that you know about.
2. **Read the text and do the tasks below**

Failure of Supporting Utilities and Structural Collapse

Supporting utilities, such as heating, ventilation and air conditioning, power, water, and other utilities, have a significant impact on the safe operation of a facility. Extreme temperatures and humidity levels, electrical fluctuations and the interruption of water, sewage, and garbage services can create conditions that inject vulnerabilities in systems designed to protect information. Thus, each of these utilities must be properly managed in order to prevent damage to information and information systems.

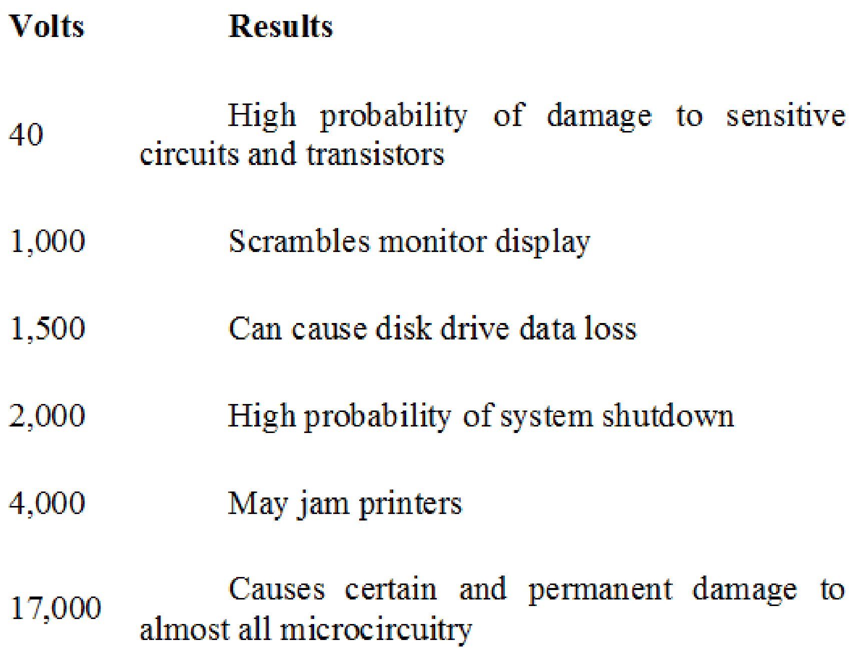
Heating, Ventilation, and Air Conditioning

Although traditionally a facilities management responsibility, the operation of the heating, ventilation, and air-conditioning (HVAC) system can have dramatic impact on information and information systems operations and protection. Specifically, the temperature, filtration, humidity, and static electricity controls must be monitored and adjusted to reduce risks to information systems.

Temperature and Filtration Computer systems are electronic, and as such are subject to damage from extreme temperature and particulate contamination. Temperatures as low as 100 degrees Fahrenheit can damage computer media, and at 175 degrees Fahrenheit, computer hardware can be damaged or destroyed. When the temperature approaches 32 degrees Fahrenheit, media are susceptible to cracking and computer components can actually freeze together. Rapid changes in temperature, from hot to cold or from cold to hot, can produce condensation, which can create short circuits or otherwise damage systems and components. The optimal temperature for a computing environment (and for people) is between 70 and 74 degrees Fahrenheit. Properly installed and maintained systems keep the environment within the manufacturer-recommended temperature range. In the past it was thought necessary to fully filter all particles from the air flow from the HVAC system. Modern computing equipment is designed to work better in typical office environments, and thus the need to provide extensive filtration for air-conditioning is now limited to particularly sensitive environments such as chip fabrication and component assembly areas. In other words, filtration is no longer as significant a factor as it once was for most commercial data processing facilities.

Humidity and Static Electricity Humidity is the amount of moisture in the air. High humidity levels create condensation problems, and low humidity levels can increase the amount of static electricity in the environment. With condensation comes the short-circuiting of electrical equipment and the potential for mold and rot in paper-based information storage. **Static electricity** is caused by a process called **triboelectrification**, which occurs when two materials make contact and exchange electrons, and results in one object becoming more positively charged and the other more negatively charged. When a third object with an opposite charge or ground is encountered, electrons flow again, and a spark is produced. One of the leading causes of damage to sensitive circuitry is **electrostatic discharge (ESD)**. Integrated circuits in a computer are designed to use between two and five volts of electricity; any voltage level above this range introduces a risk of microchip damage. Static electricity is not even noticeable to humans until levels approach 1,500 volts, and the spark can't be seen until the level approaches 4,000 volts. Moreover, a person can generate up to 12,000 volts of static current by merely walking across a carpet. Table 7-1 shows some static charge voltages and the damage they can cause to systems.

In general, ESD damage to chips produces two types of failures. Immediate failures, also known as catastrophic failures, occur right away, are usually totally destructive, and require chip replacement. Latent failures or delayed failures can occur weeks or even months after the damage occurs. The damage may not be noticeable, but the chip may suffer intermittent problems. (It has been observed, however, that with the overall poor quality of some of the current popular operating systems, this type of damage may be hard to notice.) As a result, it is imperative to maintain the optimal level of humidity, which is between 40 percent and 60 percent, in the computing environment.



Volts	Results
40	High probability of damage to sensitive circuits and transistors
1,000	Scrambles monitor display
1,500	Can cause disk drive data loss
2,000	High probability of system shutdown
4,000	May jam printers
17,000	Causes certain and permanent damage to almost all microcircuitry

Table 7-1 Static Charge Damage in Computers

Humidity levels below this range create static, and levels above create condensation. Humidification or dehumidification systems can regulate humidity levels.

Ventilation Shafts While the ductwork in residential buildings is quite small, in large commercial buildings, it may be large enough for a person to climb through. This is one of Hollywood's favorite methods for villains or heroes to enter buildings, but these ventilation shafts aren't quite as negotiable as the movies would have you believe. In fact, with moderate security precautions, these shafts can be completely eliminated as a security vulnerability. In most new buildings, the ducts to the individual rooms are no larger than 12 inches in diameter and are flexible, insulated tubes. The size and nature of the ducts precludes most people from using them, but access may be possible via the plenum. If the ducts are much larger, the security team can install wire mesh grids at various points to compartmentalize the runs.

Power Management and Conditioning Electrical power is another aspect of the organization's physical environment that is usually considered within the realm of physical security. It is critical that power systems used by information-processing equipment be properly installed and correctly grounded. Interference with the normal pattern of the electrical current is referred to as **noise**. Because computers sometimes use the normal 60 Hertz cycle of the electricity in alternating current to synchronize their clocks, noise that interferes with this cycle can result in inaccurate time clocks or, even worse, unreliable internal clocks inside the CPU.

Grounding and Amperage Grounding ensures that the returning flow of current is properly discharged to the ground. If the grounding elements of the electrical system are not properly installed, anyone touching a computer or other electrical device could become a ground source, which would cause damage to equipment and injury or death to the person. Computing and other electrical equipment in areas where water can accumulate must be uniquely grounded, using **ground fault circuit interruption** (GFCI) equipment. GFCI is capable of quickly identifying and interrupting a ground fault—that is, a situation in which a person has come into contact with water and becomes a better ground than the electrical circuit's current source.

Power should also be provided in sufficient amperage to support needed operations. Nothing is more frustrating than plugging in a series of computers, only to have the circuit breaker trip. Consult a qualified electrician when designing or remodeling computer rooms to make sure sufficiently high amperage circuits are available to provide the needed power. Overloading a circuit not only trips circuit breakers, but can also create a load on an electrical cable that is in excess of what the cable is rated to handle, and thus increase the risk of its overheating and starting a fire.

Uninterruptible Power Supply (UPS) The primary power source for an organization's computing equipment is most often the electric utility that serves the area where the organization's buildings are located. This source of power can experience interruptions. Therefore, organizations should identify the computing systems that are critical to their operations (in other words, the systems that must continue to operate during interruptions) and make sure those systems are connected to a device that assures the delivery of electric power without interruption—that is, an uninterruptible power supply (UPS).

The capacity of UPS devices is measured using the volt-ampere (or VA) power output rating. UPS devices typically run up to 1,000 VA and can be engineered to exceed 10,000 VA. A typical PC might use 200 VA, and a server in a computer room may need 2,000 to 5,000 VA, depending on how much running time is needed. Figure 7-4 shows a number of types of UPS. This section describes the following basic configurations: the standby, line- interactive, standby on-line hybrid, standby-ferro, double conversion online (also known as true online), and delta conversion online.

A **standby** or **offline UPS** is an offline battery backup that detects the interruption of power to the equipment and activates a transfer switch that provides power from batteries, through a DC to AC converter, until the power is restored or the computer is shut down. Because this type of UPS is not truly uninterruptible, it is often referred to as a standby power supply (SPS). The advantage of an SPS is that it is the most cost-effective type of UPS. However, the significant drawbacks, such as the limited run time and the amount of time it takes to switch from standby to active, may outweigh the cost savings. Switching time may also become an issue because very sensitive computing equipment may not be able to handle the transfer delay, and may reset and suffer data loss or damage. Also, SPS systems do not provide power conditioning, a feature of more sophisticated UPSs (discussed below). As a result, an SPS is seldom used in critical computing applications and is best suited for home and light office use.

A **ferroresonant standby UPS** improves upon the standby UPS design. It is still an offline UPS, with the electrical service providing the primary source of power and the UPS serving as a battery backup. The primary difference is that a ferroresonant transformer replaces the UPS transfer switch. The transformer provides line filtering to the primary power source, reducing the effect of some power problems and reducing noise that may be present in the power as it is delivered. This transformer also stores energy in its coils, thereby providing a buffer to fill in the gap between the interruption of service and the activation of an alternate source of power (usually a battery backup). This greatly reduces the probability of system reset and data loss. Ferroresonant standby UPS systems are better suited to settings that require a large capacity of conditioned and reliable power, since they are available for uses up to 14,000 VA. With the improvement in other UPS designs, however, many manufacturers have abandoned this design in favor of other configurations.

The **line-interactive UPS** has a substantially different design than the previously mentioned UPS models. In line-interactive UPSs, the internal components of the standby models are replaced with a pair of inverters and converters. The primary power source, as in both the SPS and the ferroresonant UPS, remains the power utility company, with a battery serving as backup. However, the inverters and converters both charge the battery and provide power when needed. When utility power is interrupted, the converter begins supplying power to the systems. Because this device is always connected to the output as opposed to relying on a switch, this model has a much faster response time and also incorporates power conditioning and line filtering.

In a **true online UPS**, the primary power source is the battery, and the power feed from the utility is constantly recharging this battery. This model allows constant use of the system, while completely eliminating power fluctuation. True online UPS can deliver a constant, smooth, conditioned power stream to the computing systems. If the utility-provided power fails, the computer systems are unaffected as long as the batteries hold out. The online UPS is considered the top-of-the-line option and is the most expensive. The only major drawback, other than cost, is that the process of

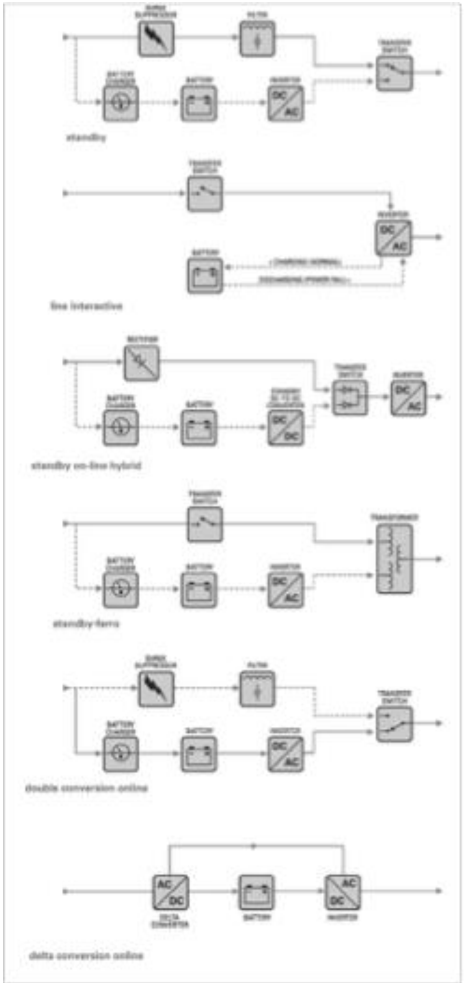


Figure 7-4 Types of Uninterruptible Power Supplies

Source: Courtesy of American Power Conversion Corporation

constantly converting from the AC feed from the utility to the DC used by the battery storage and then converting back to AC for use by the systems generates a lot of heat. An improved model resolves this issue by incorporating a device known as a delta-conversion unit, which allows some of the incoming power to be fed directly to the destination computers, thus reducing the amount of energy wasted and heat generated. Should the power fail, the delta unit shuts off, and the batteries automatically compensate for the increased power draw.

Selecting the best UPS can be a lesson in electrical engineering, because you must calculate the load that the protected systems require from the UPS. This can be quite complex and proves challenging in practice. Fortunately, many UPS vendors provide sample scenarios that can help you select the optimal device. Because a high-quality UPS may cost several thousand dollars, it is advisable to select the smallest UPS necessary to provide the desired effect. To calculate manually the rating needed in a UPS, you should begin by reviewing the computer systems and all connected support equipment to be protected. For example, the back panel of a monitor may indicate that the monitor is rated at 110 volts and 2 amps. Since volts times amps yields the power needs of a device, to calculate the power you need to run this device, you multiply 110 by 2; the production of this equation is the rating of the monitor, 220 VA. Now suppose the computer draws 3 amps at 110 volts, and therefore has a rating of 330 VA. Together the total is 550 VA. Once you have this information, you can select a UPS capable of supporting this power level. Generally, UPS systems provide information on how long they would run at specific VA levels. Some smaller-scale UPSs can run for approximately six minutes at 600 VA at full voltage. You should look for a UPS that provides enough time for the computing equipment to ride out minor power fluctuations, and for the user to shut down the computer safely if necessary.

Emergency Shutoff

One important aspect of power management in any environment is the ability to stop power immediately should the current represent a risk to human or machine safety. Most computer rooms and wiring closets are equipped with an emergency power shutoff, which is usually a large red button that is prominently placed to facilitate access, and has a cover to prevent unintentional use. These devices are the last line of defense against personal injury and machine damage in the event of flooding or sprinkler activation. The last person out of the computer room hits the switch to stop the flow of electricity to the room, preventing the water that might be used to extinguish the fire from short-circuiting the computers. While it is never advisable to allow water to come into contact with a computer, there is a much higher probability of recovering the systems if they were not powered up when they got wet. At a minimum, hard drives and other sealed devices may be recoverable. Some disaster recovery companies specialize in water damage recovery.

Water Problems

Another critical utility infrastructure element is water service. On the one hand, lack of water poses problems to systems, including fire suppression and air-conditioning systems. On the other hand, a surplus of water, or water pressure, poses a real threat. Flooding, leaks, and the presence of water in areas where it should not be is catastrophic to paper and electronic storage of information. Water damage can result in complete failure of computer systems and the structures that house them. It is therefore important to integrate water detection systems into the alarm systems that regulate overall facilities operations.

Structural Collapse

Unavoidable environmental factors or forces of nature can cause failures in the structures that house the organization. Structures are designed and constructed with specific load limits, and overloading these design limits inevitably results in structural failure. Personal injury and potential for loss of life are also likely. Scheduling periodic inspections by qualified civil engineers will enable managers to identify potentially dangerous structural conditions before the structure fails.

Maintenance of Facility Systems

Just as with any phase of the security process, the implementation of the physical security phase must be constantly documented, evaluated, and tested; once the physical security of a facility is established, it must be diligently maintained. Ongoing maintenance of systems is required as part of the systems' operations. Documentation of the facility's configuration, operation, and function should be integrated into disaster recovery plans and standard operating procedures. Testing provides information necessary to improve the physical security in the facility and identifies weak points.

2.1. Answer the questions:

1. Which four physical characteristics of the indoor environment are controlled by a properly designed HVAC system?

2.What are the optimal temperature and humidity ranges for computing systems?

3. Why is air filtration NOT as important as it was in the past?

4. What is the cause of condensation problems? Which consequences may result from them?

5. What do people use to adjust the humidity level?

6. Why is it critical that the grounding elements of the electrical system are installed properly?

7. What are the consequences of overloading a circuit?

8. What is the role of UPS?

9. Why is an emergency power shutoff necessary, especially in computer rooms and wiring closets?

9. What two critical functions are impaired when water is not available in a facility?

2.2. Decide whether the following statements are true (T), false (F), or no information (NI)

1. Nowadays, temperature control is an important factor to protect most commercial data processing facilities.

A. True B. False C. NI

2. Nowadays, extensive filtration for air-conditioning is a must if you want to maintain an optimal environment for most commercial data processing facilities.

A. True B. False C. NI

3. Ten volts of electricity may bring harm to the microchip.

A. True B. False C. NI

4. Ventilation shafts are usually utilized by attackers to break into commercial building nowadays.

A. True B. False C. NI

5. Both lack of water and a surplus of water could damage the computer systems.

A. True B. False C. NI

2.3. Choose the best answer for the following questions and statements

1. Which of the following temperature is the most suitable for a computer?

A. 30 Fahrenheit

B. 73 Fahrenheit

C. 170 Fahrenheit

D. 103 Fahrenheit

2. Which UPS is suitable to use for regular houses?

A. True online UPS

B. Offline UPS

C. Ferroresonant standby UPS

D. Line-interactive UPS

3. At which of the following places is a standby power supply NOT usually used?

A. critical computing applications

B. home

C. office

D. school

4. Which of the following is NOT a water problem?

A. Lack of water

B. Polluted water

C. Flooding

D. Leaks

5. Which system will be affected directly if the amount of water is insufficient?

A. alarm systems

B. water detection systems

C. air-conditioning systems

D. power systems

3. Speaking

1. Present your understanding about four primary types of UPS systems. Which is the most effective and the most expensive, and why?

FURTHER READING

Interception of Data

There are three methods of data interception: direct observation, interception of data transmission, and electromagnetic interception. The first method, *direct observation*, requires that an individual be close enough to the information to breach confidentiality. The physical security mechanisms described in the previous sections limit the possibility of an individual accessing unauthorized areas and directly observing information. There is, however, a risk when the information is removed from a protected facility. If an employee is browsing documents over lunch in a restaurant or takes work home, the risk of direct observation rises substantially. A competitor can more easily intercept vital information at a typical employee's home than at a secure office. Incidences of interception, such as shoulder surfing, can be avoided if employees are prohibited from removing sensitive information from the office or required to implement strong security at their homes.

The second method, *interception of data transmissions*, has become easier in the age of the Internet. If attackers can access the media transmitting the data, they needn't be anywhere near the source of the information. In some cases, the attacker can use sniffer software, which was described in previous chapters, to collect data. Other means of interception, such as tapping into a LAN, require some proximity to the organization's computers or networks. It is important for network administrators to conduct periodic physical inspections of all data ports to ensure that no unauthorized taps have occurred. If direct wiretaps are a concern, the organization should consider using fiber-optic cable, as the difficulty of splicing into this type of cable makes it much more resistant to tapping. If wireless LANs are used, the organization should be concerned about eavesdropping, since an attacker can snoop from a location that can be—depending on the strength of the wireless access points (WAPs)—hundreds of feet outside the organization's building. Since wireless LANs are uniquely susceptible to eaves- dropping, and current generation wireless sniffers are very potent tools, all wireless communications should be secured via encryption. Incidentally, it may interest you to know that the U.S. federal laws that deal with wiretapping do not cover wireless communications, except for commercial cellular phone calls; courts have ruled that users have no expectation of privacy with radio-based communications media.

The third method of data interception, *electromagnetic interception*, sounds like it could be from a *Star Trek* episode. For decades, scientists have known that electricity moving through cables emits electromagnetic signals (EM). It is possible to eavesdrop on these signals and therefore determine the data carried on the cables without actually tapping into them. In 1985, scientists proved that computer monitors also emitted radio waves, and that the image on the screens could be reconstructed from these signals. More recently, scientists have determined that certain devices with LED displays actually emit information encoded in the light that pulses in these LEDs.

Whether devices that emit **electromagnetic radiation** (EMR) can actually be monitored such that the data being processed or displayed can be reconstructed has been a subject of debate (and rumor) for many years. James Atkinson, an electronics engineer certified by the National Security Agency (NSA), says that there is no such thing as practical monitoring of electronic emanations and claims that stories about such monitoring are just urban legends. He goes on to say that most modern computers are shielded to prevent interference with other household and office equipment—not to prevent eavesdropping. Atkinson does concede that receiving emanations from a computer monitor is theoretically possible, but notes that it would be an extremely difficult, expensive, and impractical undertaking.

Legend or not, a good deal of money is being spent by the government and military to protect computers from electronic remote eavesdropping. In fact, the U.S. government has developed a program, named **TEMPEST**, to reduce the risk of EMR monitoring. (In keeping with the speculative fancy surrounding this topic, some believe that the acronym TEMPEST was originally a code word created by the U.S. government in the 1960s, but was later defined as Transient Electromagnetic Pulse Emanation Surveillance Technology or Telecommunications Electronics Material Protected from Emanating Spurious Transmissions.) In general, TEMPEST involves the following procedures: ensuring that computers are placed as far as possible from outside perimeters, installing special shielding inside the CPU case, and implementing a host of other restrictions, including maintaining distances from plumbing and other infrastructure components that carry radio waves. Regardless of whether the threat from eavesdropping on electromagnetic emanations is real, many procedures that protect against emanations also protect against threats to physical security.

Mobile and Portable Systems

Mobile computing requires even more security than the average in-house system. Most mobile computing systems—laptops, handhelds, and PDAs—have valuable corporate information stored within them, and some are configured to facilitate user access into the organization's secure computing facilities. Forms of access include VPN connections, dial-up configurations, and databases of passwords. In addition, many users keep the locations of files and clues about the storage of information in their portable computers. Many users like the convenience of allowing the underlying operating systems to remember their usernames and passwords because it provides easier access and because they frequently have multiple accounts, with different usernames and passwords, to manage. While it is tempting to allow operating systems to enable easier access to frequently used accounts, the downside of setting up these arrangements on a portable system is obvious: loss of the system means loss of the access control mechanisms.

A relatively new technology to help locate lost or stolen laptops can provide additional security. For example, Absolute Software's CompuTrace Laptop Security is computer software that is installed on a laptop, as illustrated in Figure 7-5. Periodically, when the computer is on the Internet, the software reports itself and the electronic serial number of the computer on which it is installed to a central monitoring center. If the laptop is reported stolen, this soft- ware can trace the computer to its current location for possible recovery. The software is undetectable on the system, even if the thief knows the software is installed. Moreover, CompuTrace remains installed even if the laptop's hard drive is formatted and the operating sys- tem is reinstalled.

Also available for laptops are burglar alarms made up of a PC card or other device that contains a motion detector. If the device is armed, and the laptop is moved more than expected, the alarm triggers a very loud buzzer or horn. The security system may also dis- able the computer or use an encryption option to render the information stored in the sys- tem unusable.

For maximum security, laptops should be secured at all times. If you are traveling with a laptop, you should have it in your possession at all times. Special care should be exercised when flying, as laptop thefts are common in airports. The following list comes from the Metropolitan Police of the District of Columbia and outlines steps you can take to prevent your laptop from being stolen or carelessly damaged:

Don't leave a laptop in an unlocked vehicle, even if the vehicle is in your driveway or garage, and never leave it in plain sight, even if the vehicle is locked—that's just inviting trouble. If you must leave your laptop in a vehicle, the best place is in a locked trunk. If you don't have a trunk, cover it up and lock the doors.

Parking garages are likely areas for thefts from vehicles, as they provide numerous choices and cover for thieves. Again, never leave your laptop in plain sight; cover it or put it in the trunk.

Do be aware of the damage extreme temperatures can cause to computers.

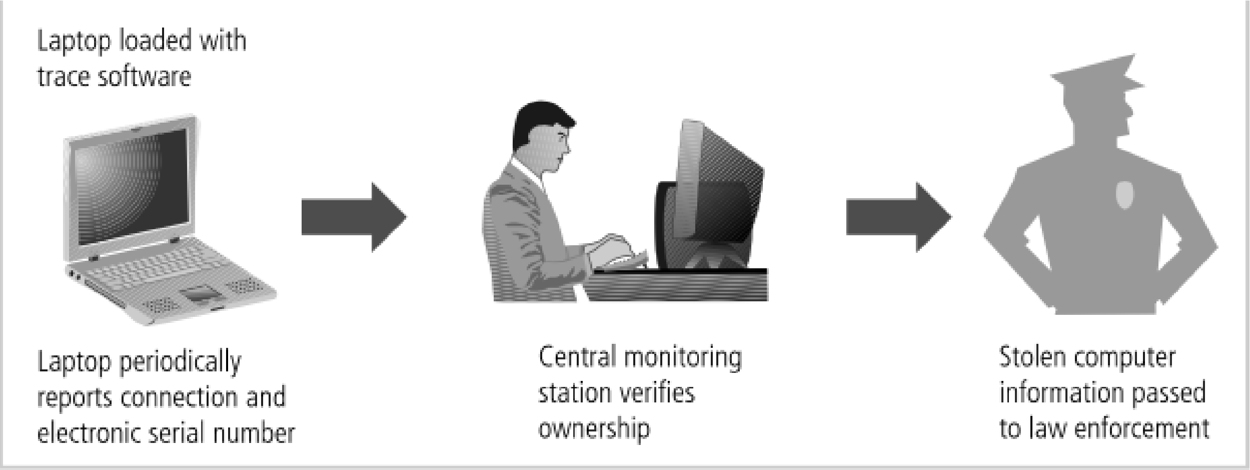


Figure 7-5 Laptop Theft Deterrence *Source: Course Technology/Cengage Learning*

Carry your laptop in a nondescript carrying case, briefcase, or bag when moving about. Placing it in a case designed for computers is an immediate alert to thieves that you have a laptop.

Going to lunch or taking a break? Don’t leave a meeting or conference room without your laptop. Take it with you, or you run the risk that it won’t be there when you return.

Lock the laptop in your office during off-hours. Don’t have your own office? Use a cable lock that wraps around a desk or chair leg, or put the laptop in a locked closet or cabinet.

Don’t let unaccompanied strangers wander around in your workplace. Offer assistance and deliver the visitors to their destinations.

Apply distinctive paint markings to make your laptop unique and easily identifiable. Liquid white-out is a good substance to apply.

Consider purchasing one of the new theft alarm systems specially made for laptops.

Be aware that if your computer is stolen, automatic logins can make it easy for a thief to send inappropriate messages with your account.

Back up your information on disks today, and store the disks at home or the office.

Remote Computing Security

Remote site computing, which is becoming increasingly popular, involves a wide variety of computing sites that are distant from the base organizational facility and includes all forms of telecommuting. **Telecommuting** is off site computing that uses Internet connections, dial- up connections, connections over leased point-to-point links between offices, and other connection mechanisms.

Telecommuting from users’ homes deserves special attention. One of the appeals of telecom- muting for both the employee and employer is that by avoiding physical commuting, tele- commuting employees have more time to focus on the work they do. But as more people become telecommuters, the risk to information traveling via the often unsecured connections that telecommuters use is substantial. The problem is that not enough organizations provide secure connections to their office networks, and even fewer provide secure systems, should the employee’s home computer be compromised. To secure the entire network, the organization must dedicate security resources to protecting these home connections. Although the installation of a VPN may go a long way toward protecting the data in transmission, tele- commuters frequently store office data on their home systems, in home filing cabinets, and on off-site media. To ensure a secure process, the computers that telecommuters use must be made *more* secure than the organization's systems, as they are outside the security perimeter. An attacker breaking into someone's home would probably find a much lower level of security than at an office. Most office systems require users to log in, but the telecommuter's home computer is probably the employee's personal machine, and thus is likely to have a much less secure operating system and may not use a password. Telecommuters must use a securable operating system that requires password authentication, such as Windows XP/ Vista/7 or Server 2003/2008. They must store all loose data in locking filing cabinets and loose media in locking fire safes. They must handle data at home more carefully than they would at the office, since the general level of security for the average home is lower than that of a commercial building.

The same applies to workers using mobile computers on the road. Employees using note- books in hotel rooms should presume that their unencrypted transmissions are being monitored, and that any unsecured notebook computer can be stolen. The off-site worker using leased facilities does not know who else is physically attached to the network and therefore who might be listening to his or her data conversations. VPNs are a must in all off-site- to-on-site communications, and the use of associated advanced authentication systems is strongly recommended.

Although it is possible to secure remote sites, organizations cannot assume that employees will invest their own funds for security. Many organizations barely tolerate telecommuting for a number of reasons, including that telecommuting employees generally require two sets of computing equipment, one for the office and one for the home. This extra expense is difficult to justify, especially when the employee is the only one gaining the benefit from telecommuting. In those rare cases in which allowing an employee or consultant to telecommute is the only way to gain extremely valuable skills, the organization is usually willing to do what is necessary to secure its systems. Only when additional research into telecommuting clearly dis- plays a bottom-line advantage do organizations begin to invest sufficient resources into securing the equipment of their telecommuters. However, there are some organizations that sup- port telecommuting, and these organizations typically fall into one of three groups. The first is the mature and therefore fiscally sound organization with a sufficient budget to support telecommuting and thus enhance its standing with employees and its organizational image. In recent years, the option to telecommute has become a factor in the organizational rankings undertaken by various magazines. Some organizations seek to improve employee work conditions and also improve their position in the best-places-to-work ranking by adding telecom- muting as an option for employees. The second group is the new high-technology company, with a large number of geographically diverse employees who telecommute almost exclusively. These companies use technology extensively and are determined to make the adoption of technology and its use the cornerstone of their organizations. The third group overlaps with the second and is called a virtual organization. A **virtual organization** is a group of individuals brought together for a specific task, usually from different organizations, divisions, or departments. These individuals form a virtual company, either in leased facilities or through 100-percent telecommuting arrangements. When the job is done, the organization is either redirected or dissolved. These organizations rely almost exclusively on remote computing and telecommuting, but they are extremely rare and therefore not well documented or studied.

Special Considerations for Physical Security

There are a number of special considerations to take into account when developing a physical security program. The first of these is the question of whether to handle physical security inhouse or to outsource it. As with any aspect of information security, the make-or-buy decision should not be made lightly. There are a number of qualified and professional agencies that provide physical security consulting and services. The benefits of outsourcing physical security include gaining the experience and knowledge of these agencies, many of which have been in the field for decades. Outsourcing unfamiliar operations always frees an organization to focus on its primary objectives, rather than support operations. The downside includes the expense, the loss of control over the individual components of the physical security solution, and the need to trust another company to perform an essential business function. An organization must not only trust the processes used by the contracted company, but also its ability to hire and retain trustworthy employees who respect the security of the contracting company even though they have no allegiance to it. This level of trust is often the most difficult aspect of the decision to outsource, because the reality of outsourcing physical security is that nonemployees will be providing a safeguard that the organization administers only marginally.

Another physical security consideration is social engineering. As you learned in previous chapters, social engineering involves using people skills to obtain confidential information from employees. While most social engineers prefer to use the telephone or computer to solicit information, some attempt to access the information more directly. As in the previously mentioned cases in which technically proficient agents are placed into janitorial positions at a competitor’s office, there are a number of ways an outsider can gain access to an organization’s resources. Most organizations do not, for example, have very thorough procedures for authenticating and controlling nonemployees who access their facility. When there is no procedure in place, no one gives the wandering repairman, service worker, or city official a second look. It is not difficult to dress like a telephone repairman, construction worker, or building inspector and move freely throughout a building. Some might even say that to go almost anywhere in any building, all one really needs is a clipboard and an attitude. If you look as if you have a mission and appear competent, most people will leave you alone. How can organizations combat this type of attack? By requiring that all individuals entering the facility display appropriate visitor badges and be escorted when they are in restricted areas.

Inventory Management

Like other organizational resources, computing equipment should be inventoried and inspected on a regular basis. The management of computer inventory is an important part of physical security. How else can corporate security know if an employee has been pilfering computer supplies or a former employee has taken organizational equipment home? Similarly, classified information should also be inventoried and managed. In the military, whenever a classified document needs is reproduced, a stamp is placed on the original before it is copied. This stamp states the document's classification level and the text imprint "of " so that the person making the copies can mark the sequence number for each copy as well as the total number of copies being made. If, for example, twenty-five copies are to be made, the person responsible for copying the document writes "26" in the right blank, makes copies, and then numbers them. Why 26 and not 25? The original is always document number one. After the numbering, each classified copy is issued to the assigned person, who signs for it. While this procedure may be overkill for most organizations, it does ensure that the inventory management of classified documents is secure at all times. Also, the formality of having to sign for a document cements its worth in the mind of the recipient.

1. Answer the questions

1. List and describe the three fundamental ways that data can be intercepted. How does a physical security program protect against each of these data interception methods?
2. What can you do to reduce the risk of laptop theft?
3. What is the pros and cons of outsourcing physical security?
4. What should people do to control nonemployees accessing their facility?

2. Speaking (Work in group). Research a real case of physical security attack. What happened? Which physical security systems were involved? What was the result? Present about them to the class.

UNIT 8: IMPLEMENTING INFORMATION SECURITY

Introduction

First and foremost, an information security project manager must realize that implementing an information security project takes time, effort, and a great deal of communication and coordination. This chapter and the next discuss the two stages of the **security systems development life cycle** (SecSDLC) implementation phase and describe how to successfully execute the infor- mation security blueprint. In general, the implementation phase is accomplished by changing the configuration and operation of the organization's information systems to make them more secure. It includes changes to the following:

Procedures (for example, through policy)

People (for example, through training)

Hardware (for example, through firewalls)

Software (for example, through encryption)

Data (for example, through classification)

As you may recall from earlier chapters, the SecSDLC involves collecting information about an organization's objectives, its technical architecture, and its information security environment. These elements are used to form the information security blueprint, which is the foundation for the protection of the confidentiality, integrity, and availability of the organization's information.

During the implementation phase, the organization translates its blueprint for information security into a **project plan**. The project plan instructs the individuals who are executing the implementation phase. These instructions focus on the security control changes that are needed to improve the security of the hardware, software, procedures, data, and people that make up the organization's information systems. The project plan as a whole must describe how to acquire and implement the needed security controls and create a setting in which those controls achieve the desired outcomes.

Before developing a project plan, however, management should coordinate the organization's information security vision and objectives with the communities of interest involved in the execution of the plan. This type of coordination ensures that only controls that add value to the organization's information security program are incorporated into the project plan. If a statement of the vision and objectives for the organization's security program does not exist, one must be developed and incorporated into the project plan. The vision statement should be concise. It should state the mission of the information security program and its objectives. In other words, the project plan is built upon the vision statement, which serves as a compass for guiding the changes necessary for the implementation phase. The components of the project plan should never conflict with the organization’s vision and objectives.

READING AND SPEAKING 1

1. **Discuss the questions:**
    1. Have you ever participated in planning a project? How was it executed?
    2. What do you think are the characteristics of a good plan?
2. **Read the text and do the tasks below**

Information Security Project Management

Organizational change is not easily accomplished. The following sections discuss the issues a project plan must address, including project leadership; managerial, technical, and budgetary considerations; and organizational resistance to the change.

The major steps in executing the project plan are as follows:

- Planning the project
- Supervising tasks and action steps
- Wrapping up

The project plan can be developed in any number of ways. Each organization has to determine its own project management methodology for IT and information security projects. Whenever possible, information security projects should follow the organization’s project management practices.

Developing the Project Plan

Planning for the implementation phase requires the creation of a detailed project plan. The task of creating such a project plan is often assigned to either a project manager or the project champion. This individual manages the project and delegates parts of it to other decision makers. Often the project manager is from the IT community of interest, because most other employees lack the requisite information security background and the appropriate management authority and/or technical knowledge.

The project plan can be created using a simple planning tool such as the **work breakdown structure (WBS)**. To use the WBS approach, you first break down the project plan into its major tasks. The major project tasks are placed into the WBS, along with the following attributes for each:

- Work to be accomplished (activities and deliverables)
- Individuals (or skill set) assigned to perform the task
- Start and end dates for the task (when known)
- Amount of effort required for completion in hours or work days
- Estimated capital expenses for the task
- Estimated noncapital expenses for the task
- Identification of dependencies between and among tasks

Each major task on the WBS is then further divided into either smaller tasks (subtasks) or specific action steps. Given the variety of possible projects, there are few formal guidelines for deciding what level of detail—that is, at which level a task or subtask should become an action step—is appropriate. There is, however, one hard-and-fast rule you can use to make this determination: a task or subtask becomes an action step when it can be completed by one individual or skill set and has a single deliverable.

The WBS can be prepared with a simple desktop PC spreadsheet program. The use of more complex project management software tools often leads to **projectitis**, wherein the project manager spends more time documenting project tasks, collecting performance measurements, recording project task information, and updating project completion forecasts than in accomplishing meaningful project work.

Work to Be Accomplished The work to be accomplished encompasses both activities and deliverables. A **deliverable** is a completed document or program module that can either serve as the beginning point for a later task or become an element in the finished project. Ideally, the project planner provides a label and thorough description for the task. The description should be complete enough to avoid ambiguity during the later tracking process, yet not so detailed as to make the WBS unwieldy. For instance, if the task is to write firewall specifications for the preparation of a **request for proposal** (RFP), the planner should note that the deliverable is a specification document suitable for distribution to vendors.

Assignees The project planner should describe the skill set or person, often called a **resource**, needed to accomplish the task. The naming of individuals should be avoided in the early planning efforts. Instead of assigning individuals, the project plan should focus on organizational roles or known skill sets. For example, if any of the engineers in the networks group can write the specifications for a router, the assigned resource would be noted as "network engineer" on the WBS. As planning progresses, however, the specific tasks and action steps can and should be assigned to individuals. For example, when *only* the manager of the networks group can evaluate the responses to the RFP and make an award for a contract, the project planner should identify the network manager as the resource assigned to this task.

Start and End Dates In the early stages of planning, the project planner should attempt to specify completion dates only for major project milestones. A **milestone** is a specific point in the project plan when a task that has a noticeable impact on the progress of the project plan is complete. For example, the date for sending the final RFP to vendors is a milestone, because it signals that all RFP preparation work is complete. Assigning too many dates to too many tasks early in the planning process exacerbates projectitis. Planners can avoid this pitfall by assigning only key or milestone start and end dates early in the process. Later in the planning process, planners may add start and end dates as needed.

Amount of Effort Planners need to estimate the effort required to complete each task, subtask, or action step. Estimating effort hours for technical work is a complex process. Even when an organization has formal governance, technical review processes, and change control procedures, it is always good practice to ask the people who are most familiar with the tasks or with similar tasks to make these estimates. After these estimates are made, all those assigned to action steps should review the estimated effort hours, understand the tasks, and agree with the estimates.

Estimated Capital Expenses Planners need to estimate the capital expenses required for the completion of each task, subtask, or action item. While each organization budgets and expends capital according to its own established procedures, most differentiate between capital outlays for durable assets and expenses for other purposes. For example, a firewall device costing $5,000 may be a capital outlay for an organization, but the same organization might not consider a $5,000 software package to be a capital outlay because its accounting rules classify all software as expense items, regardless of cost.

Estimated Noncapital Expenses Planners need to estimate the noncapital expenses for the completion of each task, subtask, or action item. Some organizations require that this cost include a recovery charge for staff time, while others exclude employee time and only project contract or consulting time as a noncapital expense. As mentioned earlier, it is important to determine the practices of the organization for which the plan is to be used. For example, at some companies a project to implement a firewall may charge only the costs of the firewall hardware as capital and consider all costs for labor and software as expense, regarding the hardware element as a durable good that has a lifespan of many years. Another organization might use the aggregate of all cash outflows associated with the implementation as the capital charge and make no charges to the expense category. The justification behind using this aggregate, which might include charges for items similar to hardware, labor, and freight, is that the newly implemented capability is expected to last for many years and is an improvement to the organization's infrastructure. A third company may charge the whole project as expense if the aggregate amount falls below a certain threshold, under the theory that small projects are a cost of ongoing operations.

Task Dependencies Planners should note wherever possible the dependencies of other tasks or action steps on the task or action step at hand. Tasks or action steps that come before the specific task at hand are called **predecessors**, and those that come after the task at hand are called **successors**. There can be more than one type of dependency, but such details are typically covered in courses on project management and are beyond the scope of this text.

2.1.Answer the questions:

1. List and describe the three major steps in executing the project plan.
2. What is a work breakdown structure (WBS)? Is it the only way to organize a project plan?
3. List and define the common attributes of the tasks of a WBS.
4. How does a planner know when a task has been subdivided to an adequate degree and can be classified as an action step?
5. What is a deliverable? Name two uses for deliverables.
6. How could you determine whether a task or subtask can become an action step?
7. What is a resource? What are the two types?
8. What is a milestone? and why is it significant to project planning?
9. Who is the best judge of effort estimates for project tasks and action steps? Why?

2.2. Decide whether the following statements are true (T), false (F), or no information (NI)

1. A simple desktop PC spreadsheet program is an inefficient tool to prepare the WBS.

A. True B. False C. NI

2. The name of the person assigned for the task should be mentioned clearly at the beginning of the planning effort.

A. True B. False C. NI

3. Projectitis can be alleviated by assigning more dates to each task.

A. True B. False C. NI

4. It is the most suitable for the planners and managers to estimate the effort hours for technical work.

A. True B. False C. NI

5. Different companies have different ways to charge when it comes to capital and

expense.

A. True B. False C. NI

2.3. Choose the best answer for the following questions and statements.

1. Which of the followings should be take into consideration when creating a project plan?

A. Budget

B. Project leadership

C. Organizational resistance to the change.

D. All are correct.

2. Who is often responsible for creating a detailed project plan?

A. the director

B. the network engineer

C. the network manager

D. the project manager

3. Which of the following attributes is NOT included in the WBS?

A. assignees

B. technical knowledge

C. start and end dates

D. estimated expenses

4. Which is the word "determination" in line 34 closest in meaning to?

A. stamina

B. decision

C. perseverance

D. discovery

5. What does the word “those” in the last paragraph refer to?

A. Predecessors

B. Tasks or action steps

C. Planners

D. Details

2. Speaking

1.Present about the common attributes of the tasks of a WBS.

2. (Work in group) Creating a WBS of a project plan in your class.

READING AND SPEAKING 2

1. **Discuss the questions:**

   1. Have you ever worked on any projects?
   2. What are usually considered when working on a project?

2. **Read the text and do the tasks below:**

Project Planning Considerations

As the project plan is developed, adding detail is not always straightforward. The following sections discuss factors that project planners must consider as they decide what to include in the work plan, how to break tasks into subtasks and action steps, and how to accomplish the objectives of the project.

Financial Considerations Regardless of an organization's information security needs, the amount of effort that can be expended depends on the available funds. A **cost benefit analysis (CBA)**, typically prepared in the analysis phase of the SecSDLC, must be reviewed and verified prior to the development of the project plan. The CBA determines the impact that a specific technology or approach can have on the organization's information assets and what it may cost.

Each organization has its own approach to the creation and management of budgets and expenses. In many organizations, the information security budget is a subsection of the overall IT budget. In others, information security is a separate budget category that may have the same degree of visibility and priority as the IT budget. Regardless of where in the budget information security items are located, monetary constraints determine what can (and can- not) be accomplished.

Public organizations tend to be more predictable in their budget processes than private organizations, because the budgets of public organizations are usually the product of legislation or public meetings. This makes it difficult to obtain additional funds once the budget is determined. Also, some public organizations rely on temporary or renewable grants for their budgets and must stipulate their planned expenditures when the grant applications are written. If new expenses arise, funds must be requested via new grant applications. Also, grant expenditures are usually audited and cannot be misspent. However, many public organizations must spend all budgeted funds within the fiscal year—otherwise, the subsequent year's budget is reduced by the unspent amount. As a result, these organizations often conduct end-of-fiscal-year spend-a-thons. This is often the best time to acquire, for example, that remaining piece of technology needed to complete the information security architecture.

Private (for-profit) organizations have budgetary constraints that are determined by the marketplace. When a for-profit organization initiates a project to improve security, the funding comes from the company’s capital and expense budgets. Each for-profit organization determines its capital budget and the rules for managing capital spending and expenses differently. In almost all cases, however, budgetary constraints affect the planning and actual expenditures for information security. For example, a preferred technology or solution may be sacrificed for a less desirable but more affordable solution. The budget ultimately guides the information security implementation.

To justify the amount budgeted for a security project at either a public or for-profit organization, it may be useful to benchmark expenses of similar organizations. Most for-profit organizations publish the components of their expense reports. Similarly, public organizations must document how funds are spent. A savvy information security project manager might find a number of similarly sized organizations with larger expenditures for security to justify planned expenditures. While such tactics may not improve this year’s budget, they could improve future budgets. Ironically, attackers can also help information security project planners justify the information security budget. If attacks successfully compromise secured information systems, management may be more willing to support the information security budget.

Priority Considerations In general, the most important information security controls in the project plan should be scheduled first. Budgetary constraints may have an effect on the assignment of a project’s priorities. The implementation of controls is guided by the prioritization of threats and the value of the threatened information assets. A less-important control may be prioritized if it addresses a group of specific vulnerabilities and improves the organization’s security posture to a greater degree than other individual higher-priority controls.

Time and Scheduling Considerations Time and scheduling can affect a project plan at dozens of points—consider the time between ordering and receiving a security control, which may not be immediately available; the time it takes to install and configure the control; the time it takes to train the users; and the time it takes to realize the return on the investment in the control. For example, if a control must be in place before an organization can implement its electronic commerce product, the selection process is likely to be influenced by the speed of acquisition and implementation of the various alternatives.

Staffing Considerations The need for qualified, trained, and available personnel also constrains the project plan. An experienced staff is often needed to implement technologies and to develop and implement policies and training programs. If no staff members are trained to configure a new firewall, the appropriate personnel must be trained or hired.

Procurement Considerations There are often constraints on the equipment and services selection processes—for example, some organizations require the use of particular service vendors or manufacturers and suppliers. These constraints may limit which technologies can be acquired. For example, in a recent budget cycle, the authors' lab administrator was considering selecting an automated risk analysis software package. The leading candidate promised to integrate everything, including vulnerability scanning, risk weighting, and control selection. Upon receipt of the RFP, the vendor issued a bid to accomplish the desired requirements for a heart-stopping $75,000, plus a 10 percent annual maintenance fee. If an organization has an annual information security capital budget of $30,000, it must eliminate a package like this from consideration—despite how promising the software's features are. Also, consider the chilling effect on innovation when an organization requires elaborate sup- porting documentation and/or complex bidding for even small-scale purchases. Such procurement constraints, designed to control losses from occasional abuses, may actually increase costs when the lack of operating agility is taken into consideration.

Organizational Feasibility Considerations Whenever possible, security-related technological changes should be transparent to system users, but sometimes such changes require new procedures, for example additional authentication or validation. A successful project requires that an organization be able to assimilate the proposed changes. New technologies sometimes require new policies, and both require employee training and education. Scheduling training after the new processes are in place (that is, after the users have had to deal with the changes without preparation) can create tension and resistance, and might undermine security operations. Untrained users may develop ways to work around unfamiliar security procedures, and their bypassing of controls may create additional vulnerabilities. Conversely, users should not be prepared so far in advance that they forget the new training techniques and requirements. The optimal time frame for training is usually one to three weeks before the new policies and technologies come online.

Training and Indoctrination Considerations The size of the organization and the normal conduct of business may preclude a single large training program on new security procedures or technologies. If so, the organization should conduct a phased-in or pilot implementation, such as roll-out training for one department at a time. When a project involves a change in policies, it may be sufficient to brief supervisors on the new policy and assign them the task of updating end users in regularly scheduled meetings. Project planners must ensure that compliance documents are also distributed and that all employees are required to read, understand, and agree to the new policies.

Scope Considerations

Project scope describes the amount of time and effort-hours needed to deliver the planned features and quality level of the project deliverables. The scope of any given project plan should be carefully reviewed and kept as small as possible given the project's objectives. To control project scope, organizations should implement large information security projects in stages, as in the bull's-eye approach discussed later in this chapter.

There are several reasons why the scope of information security projects must be evaluated and adjusted with care. First, in addition to the challenge of handling many complex tasks at one time, the installation of information security controls can disrupt the ongoing operations of an organization, and may also conflict with existing controls in unpredictable ways. For example, if you install a new packet filtering router and a new application proxy firewall at the same time and, as a result, users are blocked from accessing the Web, which technology caused the conflict? Was it the router, the firewall, or an interaction between the two? Limiting the project scope to a set of manageable tasks does not mean that the project should only allow change to one component at a time, but a good plan carefully considers the number of tasks that are planned for the same time in a single department.

The Need For Project Management

Project management requires a unique set of skills and a thorough understanding of a broad body of specialized knowledge. Realistically, most information security projects require a trained project manager—a CISO or a skilled IT manager who is trained in project management techniques. Even experienced project managers are advised to seek expert assistance when engaging in a formal bidding process to select advanced or integrated technologies or outsourced services.

Supervised Implementation Although it is not an optimal solution, some organizations designate a champion from the general management community of interest to supervise the implementation of an information security project plan. In this case, groups of tasks are delegated to individuals or teams from the IT and information security communities of interest. An alternative is to designate a senior IT manager or the CIO of the organization to lead the implementation. In this case, the detailed work is delegated to cross-functional teams. The optimal solution is to designate a suitable person from the information security community of interest. In the final analysis, each organization must find the project leadership that best suits its specific needs and the personalities and politics of the organizational culture.

Executing the Plan Once a project is underway, it is managed using a process known as a **negative feedback loop** or cybernetic loop, which ensures that progress is measured periodically. In the negative feedback loop, measured results are compared to expected results. When significant deviation occurs, corrective action is taken to bring the deviating task back into compliance with the project plan, or else the projection is revised in light of new information. See Figure 8-1 for an overview of this process.

Corrective action is taken in two basic situations: either the estimate was flawed, or performance has lagged. When an estimate is flawed, as when the number of effort-hours required is underestimated, the plan should be corrected and downstream tasks updated to reflect the change. When performance has lagged, due, for example, to high turnover of skilled employees, corrective action may take the form of adding resources, making longer schedules, or reducing the quality or quantity of the deliverable. Corrective action decisions are usually expressed in terms of trade-offs. Often a project manager can adjust one of the three following planning parameters for the task being corrected:

Effort and money allocated
Elapsed time or scheduling impact
Quality or quantity of the deliverable

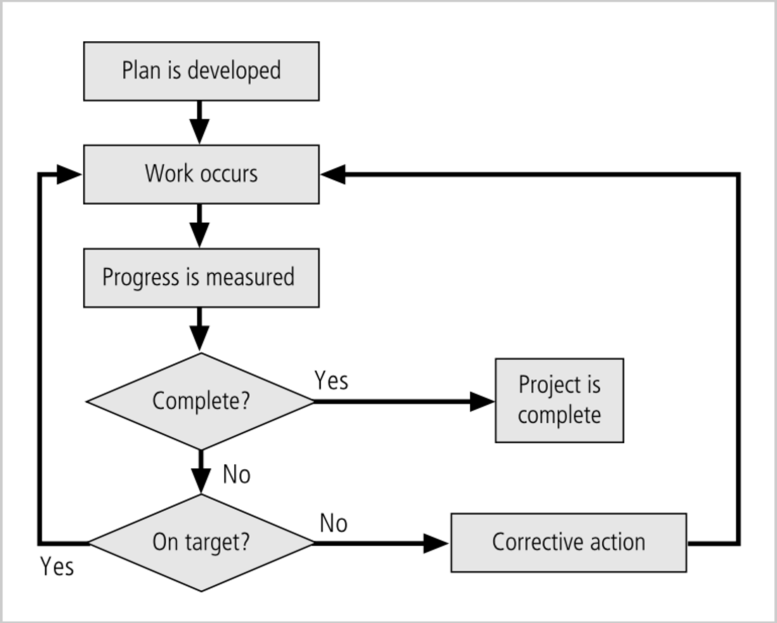


Figure 8-1 *Negative Feedback Loop*

When too much effort and money is being spent, you may decide to take more time to complete the project tasks or to lower the deliverable quality or quantity. If the task is taking too long to complete, you should probably add more resources in staff time or money or else lower deliverable quality or quantity. If the quality of the deliverable is too low, you must usually add more resources in staff time or money or take longer to complete the task. Of course, there are complex dynamics among these variables, and these simplistic solutions do not serve in all cases, but this simple trade-off model can help the project manager to analyze available options.

Project Wrap-up Project wrap-up is usually handled as a procedural task and assigned to a mid-level IT or information security manager. These managers collect documentation, finalize status reports, and deliver a final report and a presentation at a wrap-up meeting. The goal of the wrap-up is to resolve any pending issues, critique the overall project effort, and draw conclusions about how to improve the process for the future.

2.1. Answer the questions:

1. What is the role of a cost benefit analysis (CBA)?
2. Why do many public organizations often spend a considerable amount of money at the end of the fiscal year?
3. When should users be trained before the new policies and technologies come online?
4. What is project scope? Why does it have to be carefully evaluated
5. What is a negative feedback loop? How is it used to keep a project in control?
6. When a task is not being completed according to the plan, what two circumstances are likely to be involved?
7. Which parameter can a project manager adjust to correct the task when significant deviation occurs?
8. What are the objectives of project wrap-up?

2.2. Decide whether the following statements are true (T), false (F), or no information (NI)

1. The available funds play a decisive role in determining the amount of effort spent in information security projects in every organization.

   A. True B. False C. NI

2. In every organization, the information security budget is a subsection of the overall IT budget.

   A. True B. False C. NI

3. Most of organizations lack of qualified and trained personnel to implement information security project.

A. True B. False C. NI

4. Time and scheduling only affects a project at the beginning of the planning.

A. True B. False C. NI

5. A negative feedback loop assures that progress is measured every two-year.

A. True B. False C. NI

2.3. **Choose the best answer for the following questions and statements**.

1. Which of the following is closest in meaning to the word “accomplished” in line 16, paragraph 3?

   A. Concluded

   B. Attained

   C. Allocated

   D. Trained

2. Where does information security budget of public organizations NOT come from?

   A. Legislation

   B. Public meeting

   C. Renewable grant

   D. Their own expense budget

3. Which of the followings may NOT likely affect the budget for a security project of a for-profit organization?

   A. Earlier successful attacks on secured information systems

   B. Benchmark expenses of similar organizations

   C. The staff training program

   D. The marketplace

4. In an organization, who should be selected to supervise the implementation of an information security project plan?

   A. a champion from the general management community of interest

B. a suitable person from the information security community of interest

C. the CIO of the organization

D. a senior IT manager of the organization

5. Which of the following is one of the objectives of a wrap-up meeting?

A. Discussing next year project

B. Evaluating the overall effort

C. Completing the final task of the project

D. Estimating the amount of budget left

4. Speaking

Present your understanding about the trade-off model in situations when corrective actions have to be taken. Give examples.

FURTHER READING

Technical Aspects of Implementation

Some aspects of the implementation process are technical in nature and deal with the applica- tion of technology, while others deal instead with the human interface to technical systems. In the following sections, conversion strategies, prioritization among multiple components, out- sourcing, and technology governance are discussed.

Conversion Strategies

As the components of the new security system are planned, provisions must be made for the changeover from the previous method of performing a task to the new method. Just like IT systems, information security projects require careful conversion planning. In both cases, four basic approaches used for changing from an old system or process to a new one are:

- Direct changeover: Also known as going "cold turkey," a **direct changeover** involves stopping the old method and beginning the new. This could be as simple as having employees follow the existing procedure one week and then use a new procedure the next. Some cases of direct changeover are simple, such as requiring employees to use a new password (which uses a stronger degree of authentication) beginning on an announced date; some may be more complex, such as requiring the entire company to change procedures when the network team disables an old firewall and activates a new one. The primary drawback to the direct changeover approach is that if the new sys- tem fails or needs modification, users may be without services while the system's bugs are worked out. Complete testing of the new system in advance of the direct change- over reduces the probability of such problems.
- Phased implementation: A **phased implementation** is the most common conversion strategy and involves a measured rollout of the planned system, with a part of the whole being brought out and disseminated across an organization before the next piece is implemented. This could mean that the security group implements only a small portion of the new security profile, giving users a chance to get used to it and resolving issues as they arise. This is usually the best approach to security project implementation. For example, if an organization seeks to update both its VPN and IDPS systems, it may first introduce the new VPN solution that employees can use to connect to the organization's network while they're traveling. Each week another department will be allowed to use the new VPN, with this process continuing until all departments are using the new approach. Once the new VPN has been phased into operation, revisions to the organization's IDPS can begin.

- Pilot implementation: In a **pilot implementation**, the entire security system is put in place in a single office, department, or division, and issues that arise are dealt with before expanding to the rest of the organization. The pilot implementation works well when an isolated group can serve as the "guinea pig," which prevents any problems with the new system from dramatically interfering with the performance of the organization as a whole. The operation of a research and development group, for example, may not affect the real-time operations of the organization and could assist security in resolving issues that emerge.
- Parallel operations: The **parallel operations** strategy involves running the new methods alongside the old methods. In general, this means running two systems concurrently; in terms of information systems, it might involve, for example, running two firewalls concurrently. Although this approach is complex, it can reinforce an organization's information security by allowing the old system(s) to serve as backup for the new systems if they fail or are compromised. Drawbacks usually include the need to deal with both systems and maintain both sets of procedures.

The Bull's-Eye Model

A proven method for prioritizing a program of complex change is the **bull's-eye method**. This methodology, which goes by many different names and has been used by many organizations, requires that issues be addressed from the general to the specific, and that the focus be on systematic solutions instead of individual problems. The increased capabilities—that is, increased expenditures—are used to improve the information security program in a systematic and measured way. As presented here and illustrated in Figure 8-2, the approach relies on a process of project plan evaluation in four layers:

1. Policies: This is the outer, or first, ring in the bull's-eye diagram. The critical importance of policies has been emphasized throughout this textbook.

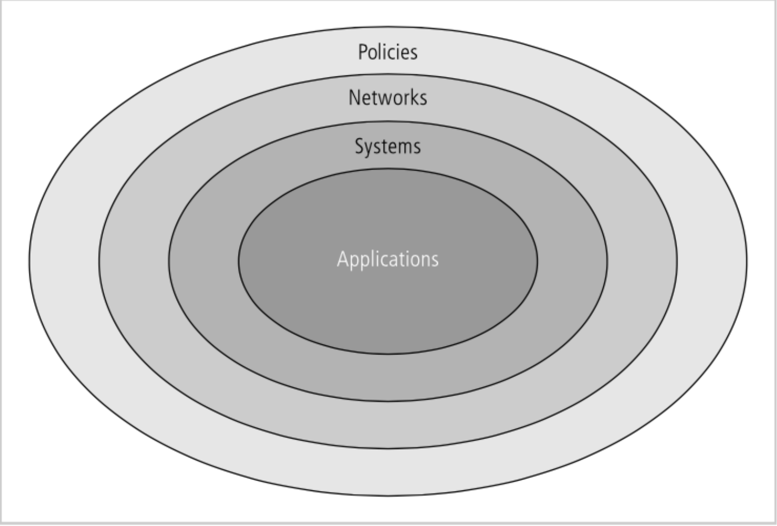


Figure 8-2 The Bull's-Eye Model

The foundation of all effective information security programs is sound information secu- rity and information technology policy. Since policy establishes the ground rules for the use of all systems and describes what is appropriate and what is inappropriate, it enables all other information security components to function correctly. When deciding how to implement complex changes and choose from conflicting options, you can use policy to clarify what the organization is trying to accomplish with its efforts.

2. Networks: In the past, most information security efforts focused on this layer, and so until recently information security was often considered synonymous with network security. In today's computing environment, implementing information security is more complex because networking infrastructure often comes into contact with threats from the public network. Those organizations new to the Internet find (as soon as their policy environment defines how their networks should be defended) that designing and implementing an effective DMZ is the primary way to secure an organization's networks. Secondary efforts in this layer include providing the necessary authentication and authorization when allowing users to connect over public networks to the organization's systems.

3. Systems: Many organizations find that the problems of configuring and operating information systems in a secure fashion become more difficult as the number and complexity of these systems grow. This layer includes computers used as servers, desktop computers, and systems used for process control and manufacturing systems.

4. Applications: The layer that receives attention last is the one that deals with the application software systems used by the organization to accomplish its work. This includes packaged applications, such as office automation and e-mail programs, as well as high- end enterprise resource planning (ERP) packages than span the organization. Custom application software developed by the organization for its own needs is also included.

By reviewing the information security blueprint and the current state of the organization's information security efforts in terms of these four layers, project planners can determine which areas require expanded information security capabilities. The bull's-eye model can also be used to evaluate the sequence of steps taken to integrate parts of the information security blueprint into a project plan. As suggested by its bull's-eye shape, this model dictates the following:

- Until sound and useable IT and information security policies are developed, communi- cated, and enforced, no additional resources should be spent on other controls.
- Until effective network controls are designed and deployed, all resources should go toward achieving this goal (unless resources are needed to revisit the policy needs of the organization).

- After policies and network controls are implemented, implementation should focus on the information, process, and manufacturing systems of the organization. Until there is well-informed assurance that all critical systems are being configured and operated in a secure fashion, all resources should be spent on reaching that goal.
- Once there is assurance that policies are in place, networks are secure, and systems are safe, attention should move to the assessment and remediation of the security of the organization's applications. This is a complicated and vast area of concern for many organizations. Most organizations neglect to analyze the impact of information security on existing purchased and their own proprietary systems. As in all planning efforts, attention should be paid to the most critical applications first.

To Outsource or Not

Not every organization needs to develop an information security department or program of its own. Just as some organizations outsource part of or all of their IT operations, so too can organizations outsource part of or all of their information security programs. The expense and time required to develop an effective information security program may be beyond the means of some organizations, and therefore it may be in their best interest to hire professional services to help their IT departments implement such a program.

When an organization outsources most or all IT services, information security should be part of the contract arrangement with the supplier. Organizations that handle most of their own IT functions may choose to outsource the more specialized information security functions. Small- and medium-sized organizations often hire outside consultants for penetration testing and information security program audits. Organizations of all sizes frequently outsource net- work monitoring functions to make certain that their systems are adequately secured and to gain assistance in watching for attempted or successful attacks.

Technology Governance and Change Control

Other factors that determine the success of an organization's IT and information security programs are technology governance and change control processes.

Technology governance, a complex process that organizations use to manage the effects and costs of technology implementation, innovation, and obsolescence, guides how frequently technical systems are updated and how technical updates are approved and funded. Technology governance also facilitates communication about technical advances and issues across the organization.

Medium- and large-sized organizations deal with the impact of technical change on the operation of the organization through a **change control** process. By managing the process of change, the organization can do the following:

- Improve communication about change across the organization
- Enhance coordination between groups within the organization as change is scheduled and completed
- Reduce unintended consequences by having a process to resolve conflict and disruption that change can introduce
- Improve quality of service as potential failures are eliminated and groups work together
- Assure management that all groups are complying with the organization's policies regarding technology governance, procurement, accounting, and information security

Effective change control is an essential part of the IT operation in all but the smallest organizations. The information security group can also use the change control process to ensure that the essential process steps that assure confidentiality, integrity, and availability are followed when systems are upgraded across the organization.

Nontechnical Aspects of Implementation

Some aspects of the information security implementation process are not technical in nature, and deal instead with the human interface to technical systems. In the sections that follow, the topic of creating a culture of change management and the considerations for organizations facing change are discussed.

The Culture of Change Management

The prospect of change, the familiar shifting to the unfamiliar, can cause employees to build up, either unconsciously or consciously, a resistance to that change. Regardless of whether the changes are perceived as good (as in the case of information security implementations) or bad (such as downsizing or massive restructuring), employees tend to prefer the old way of doing things. Even when employees embrace changes, the stress of actually making the changes and adjusting to the new procedures can increase the probability of mistakes or create vulnerabilities in systems. By understanding and applying some of the basic tenets of change management, project managers can lower employee resistance to change and can even build resilience to change, thereby making ongoing change more palatable to the entire organization.

The basic foundation of change management requires that those making the changes under- stand that organizations typically have cultures that represent their mood and philosophy. Disruptions to this culture must be properly addressed and their effects minimized. One of the oldest models of change is the Lewin change model, which consists of:

- Unfreezing
- Moving

- Refreezing

Unfreezing involves thawing hard-and-fast habits and established procedures. Moving is the transition between the old way and the new. Refreezing is the integration of the new methods into the organizational culture, which is accomplished by creating an atmosphere in which the changes are accepted as the preferred way of accomplishing the necessary tasks.

Considerations for Organizational Change

Steps can be taken to make an organization more amenable to change. These steps reduce resistance to change at the beginning of the planning process and encourage members of the organization to be more flexible as changes occur.

Reducing Resistance to Change from the Start The level of resistance to change affects the ease with which an organization is able to implement procedural and managerial changes. The more ingrained the existing methods and behaviors are, the more difficult making the change is likely to be. It's best, therefore, to improve the interaction between the affected members of the organization and the project planners in the early phases of an information security improvement project. The interaction between these groups can be improved through a three-step process in which project managers communicate, educate, and involve.

Communication is the first and most critical step. Project managers must communicate with the employees, so that they know that a new security process is being considered and that their feedback is essential to making it work. You must also constantly update employees on the progress of the SecSDLC and provide information on the expected completion dates. This ongoing series of updates keeps the process from being a last-minute surprise and primes people to accept the change more readily when it finally arrives.

At the same time, you must update and educate employees about exactly how the proposed changes will affect them individually and within the organization. While detailed information may not be available in earlier stages of a project plan, details that can be shared with employees may emerge as the SecSDLC progresses. Education also involves teaching employees to use the new systems once they are in place. This, as discussed earlier, means delivering high-quality training programs at the appropriate times.

Finally, project managers can reduce resistance to change by involving employees in the project plan. This means getting key representatives from user groups to serve as members of the SecSDLC development process. In systems development, this is referred to as **joint application development**, or JAD. Identifying a liaison between IT and information security implementers and the general population of the organization can serve the project team well in early planning stages, when unforeseen problems with acceptance of the project may need to be addressed.

Developing a Culture that Supports Change An ideal organization fosters resilience to change. This means the organization understands that change is a necessary part of the culture, and that embracing change is more productive than fighting it. To develop such a culture, the organization must successfully accomplish many projects that require change. A resilient culture can be either cultivated or undermined by management's approach. Strong management support for change, with a clear executive-level champion, enables the organization to recognize the necessity for and strategic importance of the change. Weak management support, with overly delegated responsibility and no champion, sentences the project to almost-certain failure. In this case, employees sense the low priority that has been given to the project and do not communicate with representatives from the development team because the effort seems useless.

Answer the questions:

1. List and describe the four basic conversion strategies (as described in the chapter) that are used when converting to a new system. Under which circumstances is each of these the best approach?
2. What is technology governance? What is change control? How are they related?

Word list

abbreviation (n): sự rút gọn

abacus (n): bàn tính.

access control (n): kiểm soát truy cập

accomplish (v): thực hiện

addition (n): phép cộng

Advanced Encryption Standard (AES): chuẩn mã hóa dữ liệu tiên tiến

Advanced Research Projects Agency Network (ARPANET): mạng lưới cơ quan với các đề án nghiên cứu tân tiến.

Advanced Research Projects Agency (ARPA): Cơ quan Chỉ đạo các Dự án Nghiên cứu Tiên tiến

adversary (n): kẻ thù

algorithm (n): thuật toán

allocate (v): phân phối.

analysis (n): sự phân tích

analog (n, adj): tương tự.

American National Standard Institute (ANSI):Viện tiêu chuẩn Quốc gia Mỹ

alphanumeric data (n): dữ liệu chữ số

alphabetical catalog (n): mục lục xếp theo trật tự chữ cái

appliance (n): thiết bị, máy móc

application (n): ứng dụng

Application-Level Gateway (ALG): cổng cấp ứng dụng

appropriate (adj): thích hợp

approximation (n): xấp xỉ

arise (v): xuất hiện, nảy sinh

arithmetic (adj): số học

assort (v): chia loại, phân loại

asymmetric-key (n): khóa phi đối xứng

asymmetric algorithm (n): thuật toán phi đối xứng

authentication (n): sự xác thực

authenticator (n): kí hiệu xác nhận

authentication protocol (n): giao thức xác thực

authorized user (n): người dùng hợp pháp

available (adj): có sẵn, dùng được, có hiệu lực

backdoor (n): tấn công cửa sau

binary (adj/n): thuộc về nhị phân/ số nhị phân.

bijection (n): ánh xạ

binary alphabet (n): bảng nhị phân

bit-string (n): xâu bít

block cipher (n): mã khối

boot (v): khởi động

broad classification (n): phân loại tổng quát

brute force attack (n): tấn công vét cạn

capability (n): khả năng

cataloging (n): công tác biên mục

cipher (n): mật mã

ciphertext (n): bản mã

Circuit Level Gateway: cổng mạch

ciphertext-only scenario (n): trường hợp chỉ biết bản mã

cipher feedback mode (CFB): chế độ phản hồi mã

cipher block chaining mode (CBC): chế độ liên kết khối mã

certification (n): giấy chứng nhận

certification authority (n): cơ quan chứng nhận

Circuit Level Gate (CLG): cổng mạch

clarify (v): làm dễ hiểu.

cluster controller (n): bộ điều khiển trùm

complex (adj): phức tạp

component (n): thành phần, thiết bị

computerize (v): tin học hóa

computer-controlled instrumentation (n): dụng cụ điều khiển bằng điện toán

Compromised-Key Attack (n): tấn công phá mã khóa

command (v/n): ra lệnh/ lệnh

compile (v): biên dịch

cookie (n): một tệp nhỏ, được lưu trên máy tính của bạn bởi trình duyệt

coin-tossing (n): phép tung đồng xu

coincide (v): xảy ra đồng thời

C.I.A triangle (Confidentiality Integrity Availability): tam giác bảo mật

conceal (v): giấu, che đậy

configuration (n): cấu hình

compatible (adj): tương thích

consultant (n): cố vấn

convert (v): chuyển đổi

confidentiality (n): tính bí mật

concept (n): khái niệm

cryptanalysis (n): phân tích mật mã

cryptanalyst (n): người làm công tác thám mã

cryptography (n): mật mã

cryptosystem (n): hệ mật

cryptanalytic technique (n): kĩ thuật thám mã

crypto-communication (n): truyền tin bí mật

cryptographic algorithm (n): thuật toán mật mã

cryptography hash function (n): hàm băm mật mã

character-by character (n): từng kí tự

coefficient (n): hệ số

columnar transposition (n): biến đổi cột

commute (v): thay thế, giao hoán

corresponding row (n): hàng tương ứng

corresponding plaintext block (n): khối bản rõ tương ứng

cryptographic system (n): hệ mật

data packet (n): gói dữ liệu

data compression function (n): hàm nén dữ liệu

database (n): cơ sở dữ liệu

Data Encryption Standard (DES): chuẩn mã hóa dữ liệu

deal (v): giao dịch

deliberate software attack (n): tấn công phần mềm có chủ ý

demagnetize (v): khử từ hóa

device (n): thiết bị

detect (v): dò tìm

dependable (adj): có thể tin cậy được.

devise (v): phát minh.

decipher (v): giải mã

demand (n): yêu cầu

detail (adj): chi tiết

develop (v): phát triển

Distributed denial-of-service: tấn công từ chối dịch vụ phân tán

distribute manually (n): sự phân phối bằng tay

disk (n): đĩa

division (n): phép chia

drawback (n): trở ngại, hạn chế

decoding technique (n): kỹ thuật giải mã

Defense Advanced Research Projects Agency (DARPA): Cơ quan Chỉ đạo các Dự án Nghiên cứu Quốc phòng Tiên tiến,

dial-in modem (n): modem quay số

dial-up connection (n): việc quay số

differential attack (n): tấn công lượng sai

digital (adj): thuộc về số

digital signature (n): chữ ký số

Digital Signature Algorithm (DSA): thuật toán chữ ký số

digital signature (n): chữ ký điện tử, chữ ký số

discrete (adj): rời rạc

discrete logarithm (np): logarit rời rạc

divisor (n): ước số

domain name (n): tên miền

Domain Name System (DNS) cache poisoning: tấn công khai thác lỗ hổng trong hệ thống tên miền

dummy run (n): việc chạy thử

dynamic packet-filtering firewall (n): tường lửa bộ lọc gói động

eavesdrop (v): nghe trộm

effective (adj): có hiệu lực

efficient (adj): có hiệu suất cao

embed (v): gắn vào, nhúng vào

encryption (n): mã hóa

encrypting key (n): khóa mã hóa

encryption device (n): thiết bị mã hóa

encipher (v): mã hóa

encryption (n): việc mã hóa

entity’s identity (n): danh tính/sự nhận dạng của đối tượng/đối tác

elite (adj): ưu tú, giỏi

error-correcting codes (n): mã sửa các sai số

espionage (n): do thám

expertise (v): thành thạo, tinh thông

exhaustive key (n): khóa tìm bằng phương pháp vét cạn

exclusive-or operation (n) : phép toán xor loại trừ

exhaustive trial (n): thử vét cạn

exhaustive (adj): thuộc về vét cạn

exhaustive key search (n): phương pháp tìm khóa vét cạn

factor (n): thừa số

factor (v): phân tích

ferrite ring (n): vòng nhiễm từ

frequency analysis (n): phân tích tần số freeware (n): phần mềm được cung cấp miễn phí

firewall (n): tường lửa

FOSSFree and Open Source Software: phần mềm Nguồn mở và Miễn phí

function (n): hàm

fundamental (adj): cơ bản

hacker (n): tin tặc

hash function (n): hàm băm

hand-held personalized calculator (n): máy tính cầm tay cá nhân

hand-written signature (n): chữ kí bằng tay

hierarchy (n): phân cấp

hieroglyphics (n): hệ thống chữ viết tượng hình

Host-based Intrusion Detection System (HIDS): hệ thống bảo vệ chống xâm nhập dựa vào máy chủ

hybrid system (n): hệ lai ghép

identifier (n): thiết bị nhận dạng

impersonate (v): giả mạo, mạo danh

implement (v): công cụ, phương tiện

implementation (n): sự thực thi, việc thực hiện

impractical (adj): không thực tế

index column (n): cột chỉ số

index row (n): hàng chỉ số

individual (adj/n): thuộc về cá nhân/ cá nhân

inertia (n): quán tính.

infeasible (adj): không thể làm được

irregularity (n): sự bất thường, không theo quy tắc.

instruction (n): chỉ thị, chỉ dẫn

insurance (n): bảo hiểm

integrate (v): hợp nhất, sáp nhập

integrated firewalls (nph): tường lửa tích hợp

integrity (n): sự toàn vẹn

intelligence (n): tình báo

integer factorization: phân tích số nguyên

integer factorization (n): phân tích số nguyên

Internet Protocol address (n): một địa chỉ giao thức Internet

install (v): cài đặt

intercept (v): chặn

intranet (n): mạng nội bộ

Intrusion Prevention Systems (IPS): hệ thống phòng chống xâm nhập

Internet Service Provider (ISP): nhà cung cấp dịch vụ Internet

graphics (n): đồ họa

goal (n): mục tiêu

gadget (n): đồ phụ tùng nhỏ

Global Positioning System (GPS***)***: hệ thống định vị toàn cầu

key distribution problem (n): bài toán phân phối khóa

key length: độ dài khóa

linear equation (n): phương trình tuyến tính

linear feedback generator (n): bộ sinh phản hồi tuyến tính

linear mathematical function (n): hàm số toán học tuyến tính

linear relationship (n): mối quan hệ tuyến tính

linear transformation (n): biến đổi tuyến tính

linear cryptanalysis: phương pháp thám mã tuyến tính

logarithm (n): logarit

maintain (v): duy trì

Massachusetts Institute of Technology (MIT): Viện Khoa học công nghệ Massachusetts

matrix (adj/n): ma trận

malware (n): phần mềm độc hại

malicious code (n): mã độc

memory (n): bộ nhớ

message authentication code (n): mã xác thực bản thông tin message of the day (MODT): tin nhắn trong ngày

message authentication code (n): mã xác thực thông báo

microprocessor (n): bộ vi xử lý

minicomputer (n): máy tính mini

monitor (v): giám sát

multi-task (n): đa nhiệm.

multiplication (n): phép nhân

negotiate (v): thương lượng

Network Instrusion Detection System (NIDS): hệ thống bảo vệ chống xâm nhập mạng

next-generation firewalls (NGFW): tường lửa thế hệ tiếp theo

non-repudiation (n): sự không từ chối

National Security Agency NSA: cơ quan an ninh quốc gia của Mỹ

numeric (adj): số học, thuộc về số học

occur (v): xảy ra, xảy đến

ogin (v): đăng nhập

operation (n): thao tác

operating system (n): hệ điều hành

Open System Interconnection (OSI): kết nối các hệ thống mở

outcomming interface of packet: cổng gói tin đi

oversee (v): quan sát

Packet- Filtering Router: bộ định tuyến bộ lọc gói tin

Packet filtering (n): bộ lọc gói tin

perform (v): thực hiện

permutation (n): phép hoán vị

period of the sequence (nph): chu kì của chuỗi

permute (v): hoán vị

pinpoint (v): chỉ ra một cách chính xác, xác định chính xác

phone booth (n): trạm điện thoại

physical threat (n): mối đe dọa vật lý

plaintext (n): bản rõ

polyalphabetic cipher (n): hệ mật đa biểu

polymath: nhà thông thái, học giả

polymorphic (adj): đa dạng

power supply (n): bộ lưu điện

principle (n): nguyên tắc

priority (n): Sự ưu tiên.

process (v): xử lý

process (n): quá trình, tiến trình

product (n): tích

product of two numbers (n): tích của hai số

Point-to-Point Protocol (PPP): giao thức kết nối Internet 1-1

productivity (n): hiệu suất.

protocol (n): Giao thức

proxy-based firewall: tường lửa dựa trên proxy

proxy server (n): máy chủ ủy nhiệm

port (n): cổng

prime factorization (n): phân tích ra thừa số nguyên tố

prime number (n): số nguyên tố

private key (n): khóa bí mật

public key: khóa công khai

physical process (n): xử lí vật lí

prime number (n): số nguyên tố

prior arrangement (n): sắp xếp ưu tiên

private key cryptography (n): mật mã khóa bí mật

pseudorandom (adj): thuộc về giả ngẫu nhiên

public key cryptography (n): mật mã khóa công khai

public – key infrustructure (PKI): cơ sở hạ tầng khóa công khai

public key (n): khóa công khai

pulse (n): xung

random (adj): ngẫu nhiên

real-time (adj): thời gian thực

relative frequency (n): tần số quan hệ

relative shift (n): dịch chuyển quan hệ

resource (n): nguồn

remote access (n): truy cập từ xa

respond (v): phản hồi

rotor machine (n): máy rotor

router (n): bộ định tuyến

security identifcation (n): nhận dạng an toàn

secure password database (n): cơ sở dữ liệu mật khẩu bảo mật

secrecy (n): bí mật

Secure Sockets Layer (SSL): tầng socket bảo mật (một tiêu chuẩn của công nghệ bảo mật)

security certificate (n): xác thực bảo mật

security policy (n): chính sách bảo mật

security cable (n): khóa an toàn

server (n): máy chủ

SIM card (n): một thẻ nhớ di động

signal (n): tín hiệu

simultaneous (adj): đồng thời

solution (n): giải pháp, lời giải

solve (v): giải quyết

stateful firewall: tường lửa có trạng thái

stateful inspection firewall: tường lửa kiểm tra trạng thái

steganography (n): ngụy trang

stream cipher (n): mã dòng

Serial Direct Cable Connection (n): kết nối cáp trực tiếp nối tiếp

sequence (n): chuỗi

scheme (n): sơ đồ

shift value (n): giá trị dịch chuyển

signing algorithm (n): thuật toán ký

signature verifying algorithm (n): thuật toán kiểm tra chữ ký

space (n): khoảng trống, không gian

specific algorithm (n): thuật toán riêng biệt

spybot (n): chương trình chống phần mềm gián điệp miễn phí

storage (n): lưu trữ

store (v): lưu trữ

string (n): chuỗi

sub-cryptogram (n): đoạn mã con

substitution (n): sự thay thế

subtraction (n): phép trừ

substantial (adj): tính thực tế

sufficient (adj): đủ, có khả năng

swap file (n): tệp đệm

switch (n/v): công tắc, chuyển

symmetric key (n): khóa đối xứng

terminal (n): điểm cuối, máy trạm

terminology (n): thuật ngữ

triangle (n): hình tam giác

trade off (adj: đánh đổi

transmit (v): truyền

transposition cipher (n): mã chuyển vị

Transmission Control Protocol/ Internet Protocol (TCP/IP)”: bộ giao thức cho phép kết nối các hệ thống mạng không đồng nhất với nhau

Transport Layer Security (TLS): Bảo mật tầng giao vận

trap door (n): cửa sập

trap-and-trace system (n): hệ thống kiểm tra và theo dõi

trespass (n): xâm lấn

statistical astronomy: thiên văn học thống kê unbreakable (adj): không thể phá vỡ

union catalog (n): mục lục liên hợp.

vulnerability: sự tổn thương

vulnerable (adj): có thể bị tấn công

wiping (n): tiến trình xóa triệt vĩnh viễn thông tin bảo mật

Web application firewall (WAF): Tường lửa ứng dụng web

References

[1]. A. Menezes, P. van Oorschot and S. Vastone, *Handbook of applied cryptography*, CRC Press Inc, 1997.

[2]. Andress, J, *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*, Syngress, 2014.

[3]. Bergstra, J, *The History of Information Security: A Comprehensive Handbook.* DeNardis, L. Oxford University Press, 2008.

[4]. Fred Cohen, *A short history of cryptography*, Fred Cohen – All rights Reserved, 1990, 1995.

[5]. Fred Piper and Sean Murphy, *Cryptography: A very short introduction,* Oxford University Press, 2002.

[6]. Fred Piper,Simon Blake-Wilson, and John Mitchell, *Digital Signatures: Information Systems Audit and Control*, ISACA, 2000.

[7]. ISO/IEC 27000, *Information technology – Security techniques – Information security management systems*, 2009.

[8]. Michael E Whitman, Herbert, J. Marttord, *Principles of Information Security*, Fourth Edition, Course Technology, 20 Channel Center**,** Boston, MA 02210**,** USA, 2011.

[9]. Newsome, B, *A Practical Introduction to Security and Risk Management*. SAGE Publications, 2013.

[10]. Roland van Rijswijk and Martijn Oostdijk, *Application of modern cryptography*, SURFnet B.V, 2010.

[11]. Serge Vaudenay, *A classical introduction to modern cryptography,* Science and Business Media Inc, 2006.

[12]. Vacca, John R, *Computer and information security handbook*, SAGE Publications, 2009.

ENGLISH FOR INFORMATION SECURITY

Chịu trách nhiệm xuất bản

GIÁM ĐỐC-TBT: NGUYỄN THỊ THU HÀ

Biên tập: **Ngô Mỹ Hạnh**
Nguyễn Long Biên

Mã số: GD 44 Hm13

NHÀ XUẤT BẢN THÔNG TIN VÀ TRUYỀN THÔNG

Trụ sở: Số 9, Ngõ 90, Phố Ngụy Như Kom Tum, Quận Thanh Xuân, TP. Hà Nội
ĐT Biên tập: 04.35772143 ĐT Phát hành: 04.35772138
E-mail: nxb.tttt@mic.gov.vn Fax: 04.35772194, 04.35579858
Website: www.nxbthongtintruyenthong.vn

Chi nhánh TP. Hồ Chí Minh: 8A đường D2, P25, Quận Bình Thạnh, TP. Hồ Chí Minh
Điện thoại: 08.35127750, 08.35127751 Fax: 08.35127751
E-mail: cnsg.nxbtttt@mic.gov.vn

Chi nhánh TP. Đà Nẵng: 42 Trần Quốc Toản, Quận Hải Châu, TP. Đà Nẵng
Điện thoại: 0511.3897467 Fax: 08.35127751
E-mail: cndn.nxbtttt@mic.gov.vn

In: 300 bản, khổ: 20x30 cm tại XN 951-Ban Cơ yếu Chính phủ

Số đăng ký kế hoạch xuất bản 1925-2013/CXB/43-776/TTTT

Số quyết định xuất bản: 387/QĐ-NXB TTTT ngày 28 tháng 1 năm 2019

In xong và nộp lưu chiểu Quý I năm 2020