Chapter 1

1.信息安全定义：Computer security is not a simple concept to define.

If one is referring to a computer, then it can be considered secure when the computer does what it is supposed to do and only what it is supposed to do.

However, the security emphasis has shifted from the computer to the information being processed.

Information security is defined by the information being protected from unauthorized access or alteration and yet is available to authorized individuals when required.

When one begins considering the aspects of information, it is important to realize that information is stored, processed, and transferred between machines, and all of these different states require appropriate protection schemes.

Information assurance is a term used to describe not just the protection of information, but a means of knowing the level of protection that has been accomplished.

2.当今的威胁：As time has gone on, more organized elements of cybercrime （网络威胁）have entered the picture along with nation-states.

From 2009 and beyond, the cyberthreat landscape became considerably more dangerous, with new adversaries（敌手 对手） out to perform one of two functions:

--Deny （否认）the use of your computer systems

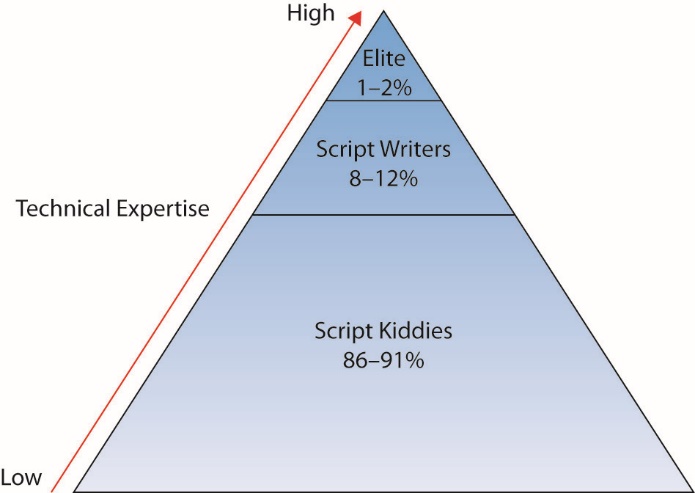
--Use systems for financial gain including theft of intellectual property（知识产权） or financial information including personally identifiable information

Threats to Security：External versus（与） internal threats

Sophistication（复杂 诡辩） of the attacks

--Script（脚本） kiddies versus elite（精英） hackers

Highly structured（结构化） threats to unstructured threats

1. 趋势：

The computing environment has transformed from large mainframes（大型机） to a highly interconnected（相互联系的） network of smaller systems.

There is a switch from a closed operating environment to one in which access to a computer can occur from almost anywhere on the planet.

This has, for obvious reasons, greatly complicated（复杂的） the job of the security professional.

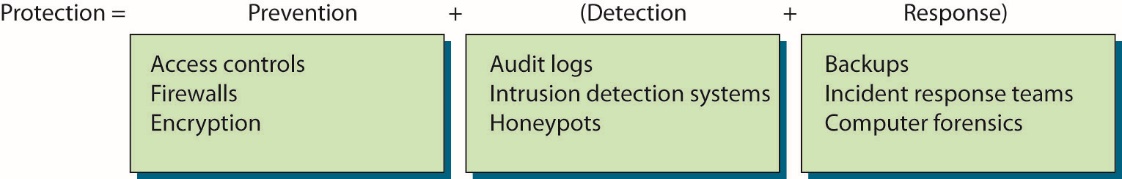
The attackers have become more focused on gain over notoriety（名声）.

The type of individual who attacks a computer system or network has evolved（进化了） over the last 30 years.

Today computer attacks are used to steal and commit fraud（欺诈） and other crimes in the pursuit（追求） of monetary enrichment.（货币浓缩）

Computer crimes are big business today, not just because it is hard to catch the perpetrators（犯罪者）, also because the number of targets is large and the rewards greater than robbing local store.

Chapter 2

1. 安全方法：

➀Ignore security issues

--Minimal amount of security provided with devices

➁Provide host security

--Prevention and detection and response components

➂Provide network-level security

--Prevention and detection and response components

④Combine host and network-level security

--Mature organization uses both in a complementary fashion

⑤Host security takes a granular view of security.

⑥Network Security

1. 访问控制：

Access control is the ability to control whether a subject (such as an individual or a process running on a computer system) can interact（交互） with an object (such as a file or hardware device).

Authentication deals with verifying the identity of a subject.

--It is the process used to verify to the computer system or network that the individual is who they claim to be.

--The most common method to do this is through the use of a user ID and password.

3.授权机制：Access controls define what actions a user can perform or what objects a user is given access.

--Access controls assume that the identity of the user has been verified.

Authentication mechanisms are to ensure that only valid（有效的） users are admitted.

--Authentication is using some mechanism（机制） to prove that you are who you claim to be.

There are three general factors commonly used in authentication.

--Something you know (knowledge factor)

--Something you have (possession factor)

--Something about you (something that you are; inherent factor)

The most common authentication mechanism provides something the valid user should know.

--User ID (or username) and password

The second mechanism for authentication provides something that you have in your possession.

--Magnetic stripe card that contains identifying information

The third mechanism for authentication uses something about you for identification purposes.

--Fingerprint or the geometry of your hand

Chapter 4

1. social engineering

➀Social engineering is the process of convincing an authorized（授权的） individual to provide confidential（保密） information or access to an unauthorized individual.

➁Various deceptive（欺骗的） practices are used to convince the targeted person to take two possible actions:

--Divulge（泄露） information they normally would not divulge

--Convince the target to do something they normally wouldn’t do

➂Social engineering is very successful for two general reasons:

--Most people have a basic desire to be helpful.

--Individuals normally seek to avoid confrontation and trouble.

④Social engineering may also be accomplished using other means besides direct contact between the target and the attacker.

⑤An attacker who is attempting to exploit the natural tendency of people to be helpful may take one of several approaches:

--The attacker may simply ask a question, hoping to immediately obtain the desired information.

--The attacker may first attempt to engage the target in conversation and try to evoke sympathy so that the target feels sorry for the individual and is more prone to provide the information.

--The attacker may appeal to an individual’s ego.

⑥Obtaining insider information

--In 1978, Stanley Mark Rifkin stole $10.2 million from the Security Pacific Bank in Los Angeles.

·Rifkin worked as a computer consultant for the bank.

·He learned details on money transfer.

·He obtained access to electronic funds transfer (EFT) codes by claiming to check on computer equipment.

·Used EFT codes to impersonate a bank officer and ordered the transfer of the $10.2 million.

·The transfer was made with little fanfare.

⑦Hoaxes can be very damaging if it causes users to take some sort of action that weakens security.

--Training and awareness are the best and first line of defense for both users and administrators.

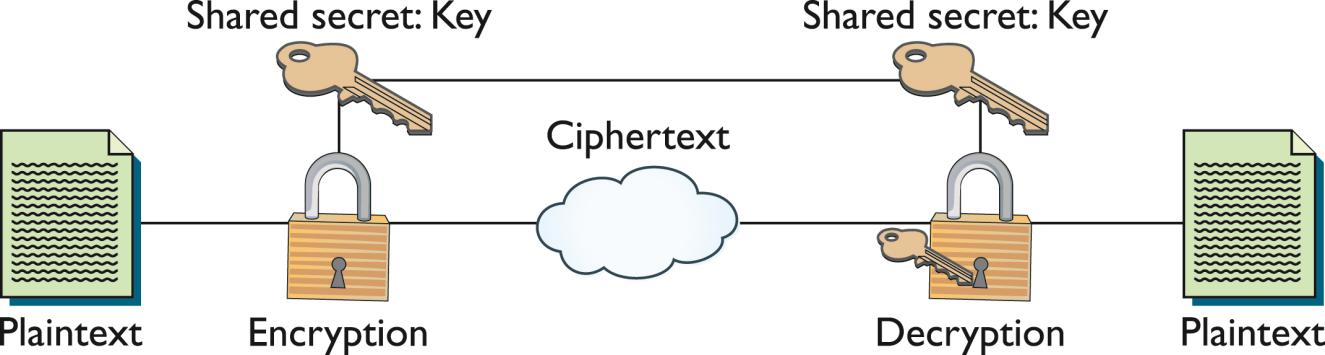
--Users should be trained to be suspicious of unusual e-mails and stories and should know who to contact in the organization to verify their validity when received.

--Hoaxes often also advise the user to send it to their friends so they know about the issue as well—and by doing so, they help spread the hoax.

Chapter 5

1. 加密方法

➀对称加密



Key Management

· Security of the algorithms relies on the key, as such key management is of critical concern.

Includes anything having to do with the exchange, storage, safeguarding, and revocation of keys.

· A key must be current and verified.

· If you have an old or compromised key, you need a way to check to see that the key has been revoked.

➁非对称加密

· Invented by Whitfield Diffie and Martin Hellman in 1975.

· Uses two keys instead of one.

· Commonly known as public key cryptography.（密码学）

· The system uses a pair of keys:

--A private key that is kept secret.

--A public key that can be sent to anyone.

· Security relies upon resistance（阻力） to deducing one key, given the other.

1. 算法

Cryptographic Algorithms（算法）

· Every current encryption scheme is based upon an algorithm.每一个加密组合都基于一个算法

· The cryptographic algorithm — what is commonly called the encryption algorithm or cipher（密码）—is made up of mathematical steps for encrypting and decrypting information.

1. 帕西函数（hashing function）是单向函数

· Hashing functions are commonly used encryption methods.

· A hashing function is a special mathematical function that performs one-way encryption.

· Once the algorithm is processed, there is no feasible（可行的） way to use the ciphertext（密文） to retrieve（检索） the plaintext（明文）.

· There is no feasible way to generate（生成） two different plaintexts that compute to the same hash value.

· Two popular hash algorithms are the Secure Hash Algorithm (SHA) series and Message Digest (MD) hash of varying versions (MD2, MD4, MD5).

summary

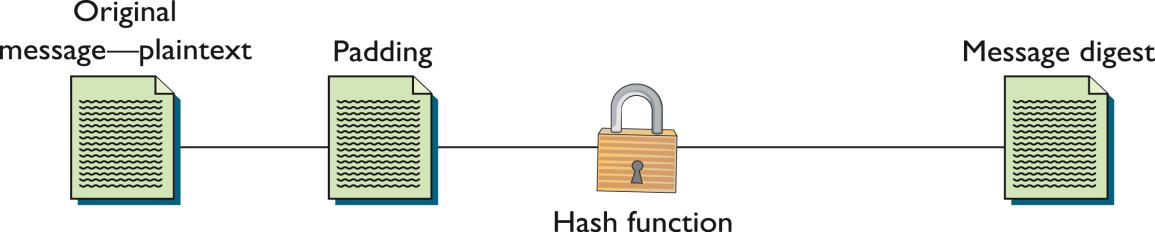
· Hashing functions are very common, and they play an important role in security.

--Storing passwords

--Signing messages

--Maintaining message integrity

· By computing a digest of the message, less data needs to be signed by the more complex asymmetric encryption.



Chapter 8

Physical Security Safeguards

· Walls and guards

· Physical access controls and monitoring

· Convergence

· Policies and procedures

· Environmental control

区分哪些是物理的安全防护（防火墙不是）eg. Door lock camera

防火墙：抵御外部网络攻击

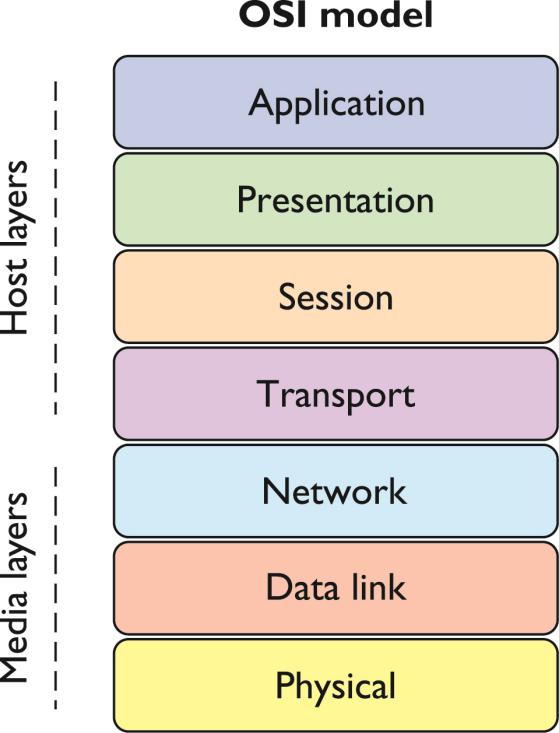
Boot disk 启动盘

Drive imaging :拷贝到另一边

Bios：基本输出系统

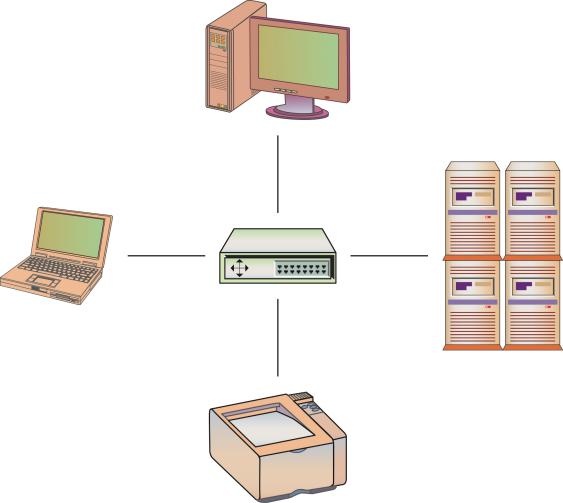
Chapter 9

Osi：七层网络模型

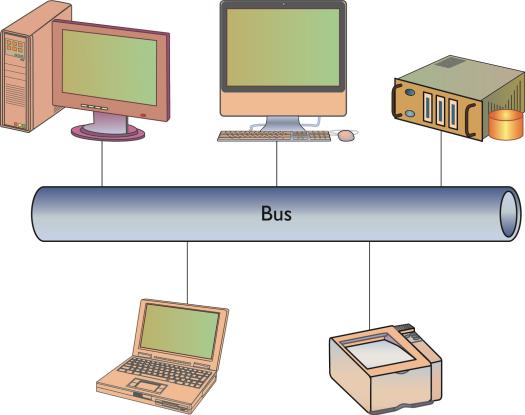


1. top结构：

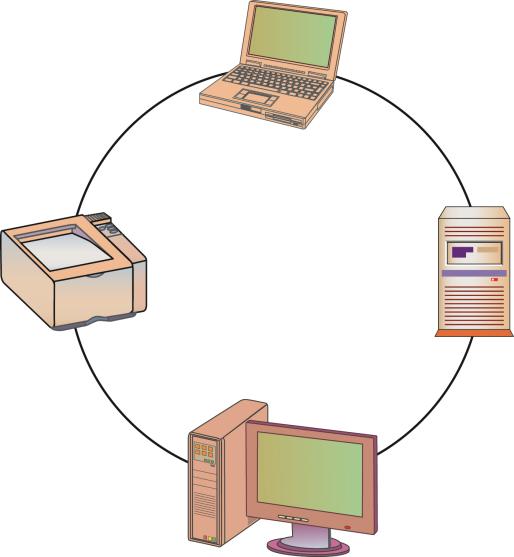
➀star topolohy:Network components are connected to a central point.



➁bus topology:Network components are connected to the same cable（电缆）, often called “the bus” or “the backbone.”



➂ring topology:Network components are connected to each other in a closed loop with each device directly connected to two other devices.



1. 网络协议（IP协议）

An IP packet, often called a datagram, has two main sections: the header and the data section (sometimes called the payload).

The header section contains all of the information needed to describe the packet.

TCP：Transmission Control Protocol

UDP：User Datagram Protocol

ICMP:Internet Control Message Protocol

1. IPv4 和IPv6

IPv6优点:It has security features built into the base protocol series.IPv6 has a simplified packet header（数据包包头） and new addressing scheme.(计划)

区别：IPv6地址有3.4\*10（38）次方nodes

1. Packet Delivery（包传送）

· Packet delivery can be divided into two sections: local and remote packet delivery.

--Local delivery applies to packets being sent out on a local network

--Remote delivery applies to packets being delivered to a remote system, such as across the Internet

· Ultimately, packets may follow a local delivery, remote delivery, local delivery pattern before reaching their intended destination.

DNS：Domain Name System（域名服务）（由sina.com转化为123.172.123）

DNS translates names into IP addresses. When you enter the name of your favorite web site into the location bar of your web browser and press ENTER, the computer has to figure out what IP address belongs to that name.

Chapter 11

1.ACL：Access control list

is used in more than one manner in the field of computer security.

--Routers and firewalls: An ACL is a set of rules used to control traffic flow into or out of an interface（接口） or network.

--System resources: An ACL lists permissions attached to an object.

· An access control matrix provides the simplest framework for illustrating the process.

--Seldom used in computer systems because it is extremely costly in terms of storage space and processing.

远程访问的过程→验证真实性（MAC）→访问控制

Mandatory access control (MAC) is the process of controlling access to information based on the sensitivity of that information and whether or not the user is operating at the appropriate sensitivity level and has the authority to access that information.

2.Kerberos：系统设计上采用客户端/服务器结构与DES加密技术，并且能够进行相互认证，即客户端和服务器端均可对对方进行身份认证。可以用于防止窃听、防止replay攻击、保护数据完整性等场合，是一种应用对称密钥体制进行密钥管理的系统。支持SSO

Chapter 13

1. IDS分两大类：➀HIDS:Host-based IDS

This examines activity on an individual system, such as a mail server, web server, or individual PC. It is concerned only with an individual system and usually has no visibility into the activity on the network or systems around it.

Advantages:

--Can be very operating system-specific（特别操作系统）

--Can reduce false-positive rates

--Can be very application specific

--Can determine how an alarm will impact a system

Disadvantage:

--Must process information on every system you want to watch

--May have a high cost of ownership and maintenance

--Uses local system resources

--A focused view and cannot relate to activity around it

➁NIDS:Network-based IDS

This examines activity on the network itself. It has visibility only into the traffic crossing the network link it is monitoring and typically has no idea of what is happening on individual systems.

Advantages of NIDS

--Providing IDS coverage requires fewer systems.

--Deployment, maintenance, and upgrade costs are usually lower.

--A NIDS has visibility into all network traffic and can correlate attacks among multiple systems.

Disadvantages of NIDS

--It is ineffective（无效果的） when traffic is encrypted.（加密）

--It can’t see traffic that does not cross it.

--It doesn’t know about activity on the hosts themselves.

1. Signatures

➀Content-based signatures：基于内容的

--Matching characters or strings

--Easy to build and look for simple things, such as a certain string of characters or a certain flag set in a TCP packet

E.g. On certain older versions of sendmail, sending an e-mail message to “decode” would cause the system to execute the contents of the e-mail.

➁Context-based signatures:基于上下文的

--Matching patterns of activity

--Generally more complex

E.g. A potential intruder may use a port scanner to look for any systems accepting connections on port 80.

3.False positives

--A match generates a response for benign traffic

False negatives

--Malicious activity goes undetected

Chapter 15

1. Malicious Code：恶意代码

名词解释

ACL：Access control list

DES：data encryption standard

ECC：Error Correction Code

UEFI：Unified Extensible Firmware Interface