E. G. S. Pillay Engineering College, Nagapattinam
Computer Science and Engineering

Elective II **IT 2042 INFORMATION SECURITY** **VIII Sem CSE**

QUESTION BANK - UNIT-V

1) What are firewalls?

Firewalls

- A firewall is any device that prevents a specific type of information from moving between the untrusted network outside and the trusted network inside
- There are five recognized generations of firewalls
- The firewall may be:
  - a separate computer system
  - a service running on an existing router or server
  - a separate network containing a number of supporting devices

2) **Explain different generations of firewalls**.

First Generation

- Called packet filtering firewalls
- Examines every incoming packet header and selectively filters packets based on
  - address, packet type, port request, and others factors
- The restrictions most commonly implemented are based on:
  - IP source and destination address
  - Direction (inbound or outbound)
  - TCP or UDP source and destination port-requests

Second Generation

- Called application-level firewall or proxy server
- Often a dedicated computer separate from the filtering router
- With this configuration the proxy server, rather than the Web server, is exposed to the outside world in the DMZ
- Additional filtering routers can be implemented behind the proxy server
- The primary disadvantage of application-level firewalls is that they are designed for a specific protocol and cannot easily be reconfigured to protect against attacks on protocols for which they are not designed

Third Generation

- Called stateful inspection firewalls
- Keeps track of each network connection established between internal and external systems using a state table which tracks the state and context of each packet in the conversation by recording which station sent what packet and when
- If the stateful firewall receives an incoming packet that it cannot match in its state table, then it defaults to its ACL to determine whether to allow the packet to pass
- The primary disadvantage is the additional processing requirements of managing and verifying packets against the state table which can possibly expose the system to a DoS attack
- These firewalls can track connectionless packet traffic such as UDP and remote procedure calls (RPC) traffic

Fourth Generation

- While static filtering firewalls, such as first and third generation, allow entire sets of one type of packet to enter in response to authorized requests, a dynamic packet filtering firewall allows only a particular packet with a particular source, destination, and port address to enter through the firewall
- It does this by understanding how the protocol functions, and opening and closing "doors" in the firewall, based on the information contained in the packet header. In this manner, dynamic packet filters are an intermediate form, between traditional static packet filters and application proxies

Fifth Generation

- The final form of firewall is the kernel proxy, a specialized form that works under the Windows NT Executive, which is the kernel of Windows NT
- It evaluates packets at multiple layers of the protocol stack, by checking security in the kernel as data is passed up and down the stack

3) **How firewalls are categorized by processing mode?**
   The five processing modes are
   1) Packet filtering
   2) Application gateways
   3) Circuit gateways
   4) MAC layer firewalls
   5) Hybrids

4) **Explain packet filtering router.**
Packet-filtering Routers

- Most organizations with an Internet connection have some form of a router as the interface at the perimeter between the organization's internal networks and the external service provider
- Many of these routers can be configured to filter packets that the organization does not allow into the network
- This is a simple but effective means to lower the organization's risk to external attack
- The drawback to this type of system includes a lack of auditing and strong authentication
- The complexity of the access control lists used to filter the packets can grow and degrade network performance

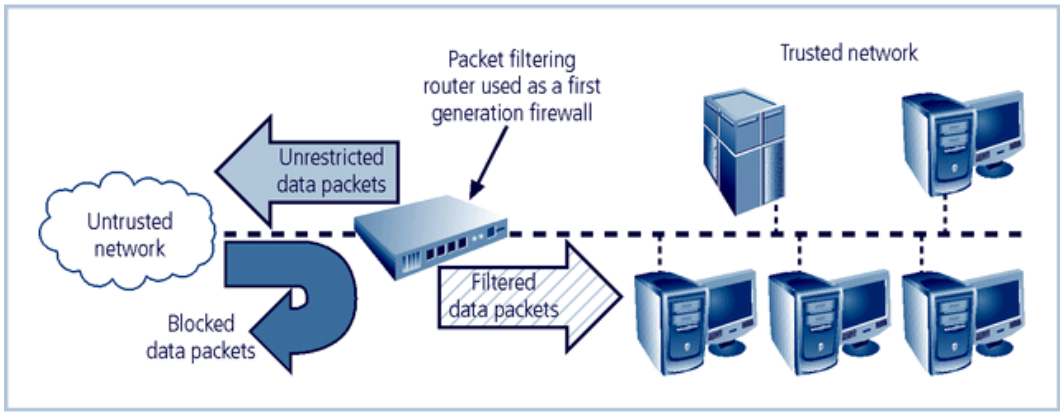


FIGURE 8-2 Packet Filtering Firewall

5) **Explain screen Host firewalls.**

Screened-Host Firewall Systems

- Combine the packet-filtering router with a separate, dedicated firewall such as an application proxy server
- Allows the router to pre-screen packets to minimize the network traffic and load on the internal proxy
- 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, as it represents a single, rich target for external attacks, and should be very thoroughly secured

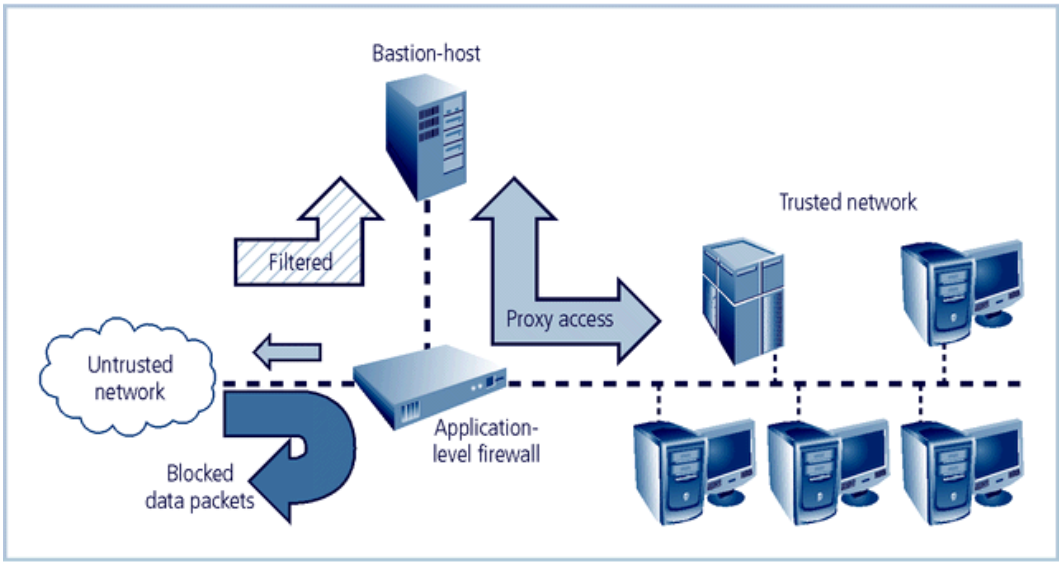


FIGURE 8-3 Screened Host Firewall

6) What are dual homed host firewalls?

Dual-homed Host Firewalls

- The bastion-host contains two NICs (network interface cards)
- One NIC is connected to the external network, and one is connected to the internal network
- With two NICs all traffic must physically go through the firewall to move between the internal and external networks
- A technology known as network-address translation (NAT) is commonly implemented with this architecture to map from real, valid, external IP addresses to ranges of internal IP addresses that are non-routable

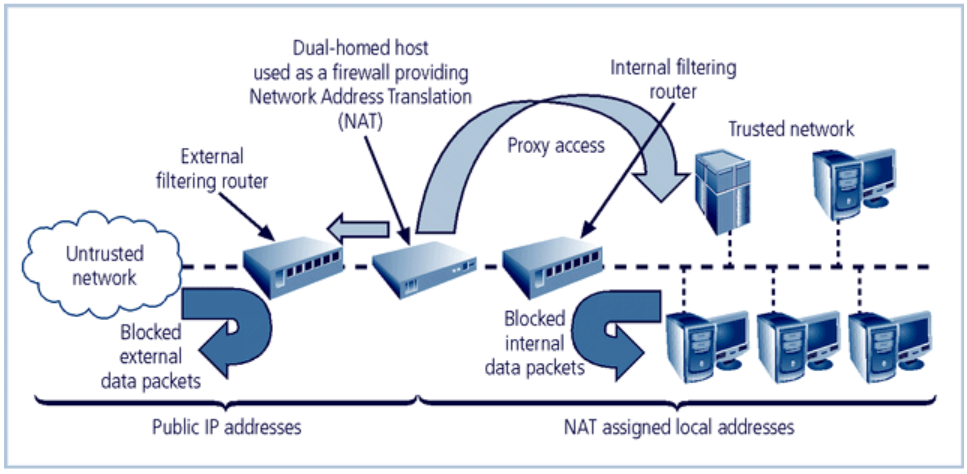


FIGURE 8-4 Dual-homed Host Firewall

7) What are Screened-Subnet Firewalls?

Screened-Subnet Firewalls (with DMZ)

- Consists of two or more internal bastion-hosts, behind a packet-filtering router, with each host protecting the trusted network
- The first general model consists of two filtering routers, with one or more dual-homed bastion-host between them
- The second general model involves the connection from the outside or untrusted network going through this path:
  - Through an external filtering router
  - 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

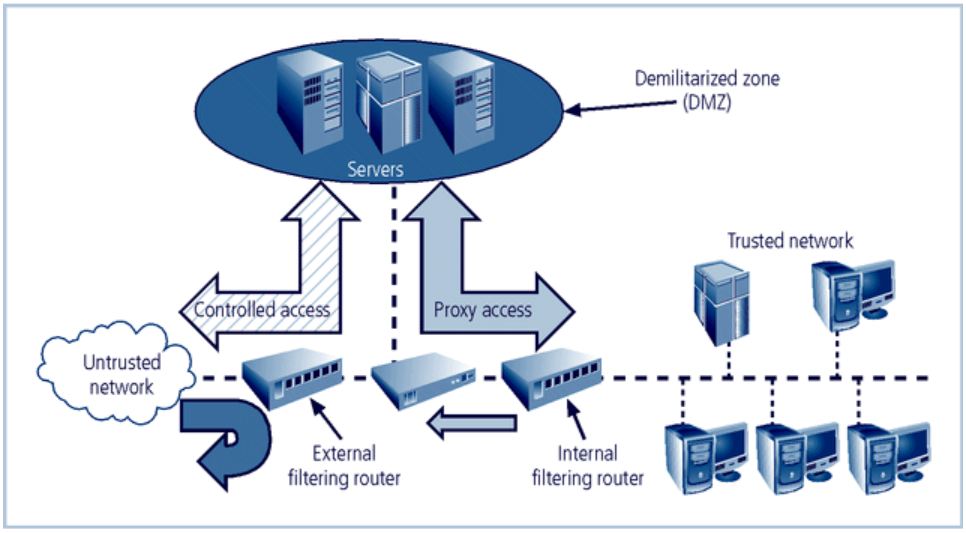


FIGURE 8-5 Screened Subnet (DMZ)

8) **What are the factors to be considered while selecting a right firewall?**

Selecting the Right Firewall

- What type of firewall technology offers the right balance of protection features and cost for the needs of the organization?
- What features are included in the base price? What features are available at extra cost? Are all cost factors known?
- How easy is it to set up and configure the firewall? How accessible are staff technicians with the mastery to do it well?
- Can the candidate firewall adapt to the growing network in the target organization?

9) What are Sock Servers?

SOCKS Servers

- The SOCKS system is a proprietary circuit-level proxy server that places special SOCKS client-side agents on each workstation
- Places 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 of filtering responsibilities, but then requires each workstation to be managed as a firewall detection and protection device
- A SOCKS system can require additional support and management resources to configure and manage possibly hundreds of individual clients, versus a single device or set of devices

10) What are the recommended practices in designing firewalls?

Firewall Recommended Practices

- All traffic from the trusted network is allowed out
- The firewall device is always inaccessible directly from the public network
- Allow Simple Mail Transport Protocol (SMTP) data to pass through your firewall, but insure it is all routed to a well-configured SMTP gateway to filter and route messaging traffic securely
- All Internet Control Message Protocol (ICMP) data should be denied
- Block telnet (terminal emulation) access to all internal servers from the public networks
- When Web services are offered outside the firewall, deny HTTP traffic from reaching your internal networks by using some form of proxy access or DMZ architecture

11) What are intrusion detection systems(IDS)?

Intrusion Detection Systems (IDSs)

- IDSs work like burglar alarms
- IDSs require complex configurations to provide the level of detection and response desired
- An IDS operates as either network-based, when the technology is focused on protecting network information assets, or host-based, when the technology is focused on protecting server or host information assets
- IDSs use one of two detection methods, signature-based or statistical anomaly-based

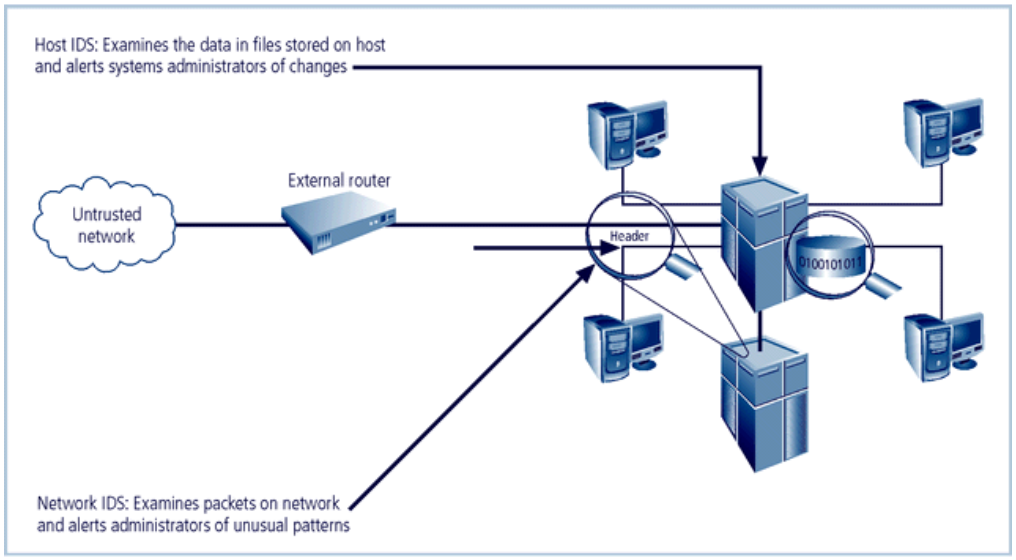


FIGURE 8-7 Intrusion Detection Systems

12) What are different types of IDSs?

a) Network-based IDS

A network-based IDS(NIDS) resides on a computer or an appliance connected to a segment of an organization's network and monitors traffic on that network segment,looking for indications of ongoing or successful attacks.

b) Host-based IDS

A Host-based IDS(HIDS) works differently from a network-based version of IDS. While a netwerok-based-IDS resides on a network segment and monitors activities across that segment,a host-based IDS resides on a particular computer or server,known as the host and monitors activity only on that system. HIDs are also known as **System Integrity Verifiers**
as they benchmark and monitorthe status of key system files and detect when an intruder creates ,modifies or deletes monitored files. A HIDs is also capable of monitoring system configuration databases,such as windows registries,in addition to stored configuration files like .ini,.cfg,and .dat files.

c) Application-based IDS

A refinement of Host-based IDs is the application-based IDS(AppIDS). Whereas the HIDs examinesa sigle system for file modification,the application based IDs examines an application for abnormal incidents. It looks for anomalous occurrences such as users exceeding their authorization,invalid file executions etc.

d) Signature-based IDS

It is based on detection methods. A signature-based IDS(also called Knowledge-based IDs) examines data traffic in search of patterns that match known signatures – that is,preconfigured ,predetermined attack patterns.

Many attacks have clear and distinct signatures such as (i) footprinting and fingerprinting activities,have an attack pattern that includes the use of ICMP,DNS querying,and e-mail routing analysis (ii) Exploits involve a specific attack sequence designed to take advantage of a vulnerability to gain access to a system (iii) Denial of Service(DoS) and Distributed Denial of Service(DDoS) attacks.

e) Statistical Anomaly-Based IDS(Also called Behaviour-based IDS)

This approach is used for detecting intrusions based on the frequency with which certain network activities takes place. **Statistical Anomaly-Based IDS** collects statistical summaries by observing traffic that is known to be normal. A baseline is established based on normal period. The Stats IDs periodically sample network activity,and using statistical methods ,compares the sampled network activity to the baseline. When the measured activities are outside the baseline parameters,it is said to be exceeding the **clipping level**;at this point,the IDS will trigger an alert to notify the administrator.

f) Log File Monitors(LFM)

Log File Monitor(LFM) is an approach to IDS that is similar to NIDS. Using LFm the system reviews the log files generated by servers,network devices,and wven other IDSs. These systems look for patterns and signatures in the log files that may indicate an attack or intrusion is in process or has already succeeded.

13) What are Honey Pots,Honey Nets,and Padded Cell Systems?

A class of powerful security tools that go beyond routine intrusion detection is known variously as **honey pots,honey nets,and padded cell systems.**
Oney pots are decoy systems designed to lure potential attackers away from critical systems and encourage attacks against the themselves. These systems are created for the sole purpose of deceiving potential attackers. In Industry they are known as decoys,lures,and fly-traps.
When a collection of honey pots connects several honey pot systems on a subnet,it may be called a **honey net**.
In sum,honey pots are designed to

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

A Padded Cell is a honey pot that has been protected so that it cannot be easily compromised. In otherwords,a padded cell is a hardened honey spot..

14) What are the advantages and disadvantages of using honey pot or padded cell approach?

Advantages:

- Attackers can be diverted to targets that they cannot damage.
- Administrators have time to decide how to respond to an attacker.
- Attackers action can be easily and extensively monitored
- Honey pots may be effective at catching insiders who are snooping around a network.

Disadvantages:

- The legal implication of using such devices are not well defined.
- Honey pots and Padded cells have not yet been shown to be generally useful security technologies.
- An exper attacker,once diverted into a decoy system,may become angry and launch a hostile attack againt an organization's systems
- Admins and security managers will need a high level of expertise to use these systems.

15) How Scanning and Analysis tools are useful in enforcing Information Security?

Scanning and Analysis Tools

- Scanners, sniffers, and other analysis tools are useful to security administrators in enabling them to see what the attacker sees
- Scanner and analysis tools can find vulnerabilities in systems
- One of the preparatory parts of an attack is known as footprinting – collecting IP addresses and other useful data
- The next phase of pre-attack data gathering process is called fingerprinting – scanning all known addresses to make a network map of the target

16) What are foot printing and finger printing?

The attack protocol is a series of steps or processes used by an attacker ,in a logical sequence ,to launch an attack against a target system or netweok. One of the

preparatory part of the attack protocol is the collection of publicly available information about a potential target,a process known **as footprinting**.

Footprinting is the organized research of the Internet addresses owned or controlled by the target organization. The attacker uses public Internet data sources to perform keyword searches to identify the network addresses of the organization. This research ios augmented by browsing the organization's web pages.

The next phase of the attack protocol is a second intelligence or data-gathering process called **fingerprinting.** This is systematic survey of all of the target organization's

Internet addresses(which are collected during the footprinting phase); the survey is conducted to ascertain the network services offered by the hostsin that range. Fingerprinting reveals useful information about the internal structure and operational nature of the target system or network for the anticipated attack.

17) Explain different types of the Scanning and Analyis tools available.

Port Scanners

- Port scanners fingerprint networks to find ports and services and other useful information
- Why secure open ports?
  - An open port can be used to send commands to a computer, gain access to a server, and exert control over a networking device
  - The general rule of thumb is to remove from service or secure any port not absolutely necessary for the conduct of business

Vulnerability Scanners

- Vulnerability scanners are capable of scanning networks for very detailed information
- As a class, they identify exposed usernames and groups, show open network shares, expose configuration problems, and other vulnerabilities in servers

Packet Sniffers

- A network tool that collects copies of packets from the network and analyzes them
- Can be used to eavesdrop on the network traffic
- To use a packet sniffer legally, you must be:
  - on a network that the organization owns
  - under direct authorization of the owners of the network
  - have knowledge and consent of the content creators (users**)**

Content Filters

- Although technically not a firewall, a content filter is a software filter that allows administrators to restrict accessible content from within a network
- The content filtering restricts Web sites with inappropriate content

Trap and Trace

- Trace: determine the identity of someone using unauthorized access
- Better known as honey pots, they distract the attacker while notifying the administrator

18) What is Cryptography? Explain the key terms associated with cryptography.

Cryptography ,which comes from the Greek work kryptos,meaning "hidden",and graphein,meaning "to write",is aprocess of making and using codes to secure the transmission of information.
Cryptoanalysis is the process of obtaining the original message(called **plaintext**) from an encrypted message(called the **ciphertext**) without knowing the algorithms and keys used to perform the encryption.
Encryption is the process of converting an original message into a form that is unreadable to unauthorized individuals-that is,to anyone without the tools to convert the encrypted message back to its original format.
Decryption is the process of converting the cipher text into a message that conveys readily understood meaning.

19) Explain briefly the basic Encryption Definitions.

Encryption Definitions

- **Algorithm:** the mathematical formula used to convert an unencrypted message into an encrypted message**.**
- **Cipher:** the transformation of the individual components (characters, bytes, or bits) of an unencrypted message into encrypted components**.**
- **Ciphertext or cryptogram:** the unintelligible encrypted or encoded message resulting from an encryption.
- **Code:** the transformation of the larger components (words or phrases) of an unencrypted message into encrypted components**.**
- **Cryptosystem:** the set of transformations necessary to convert an unencrypted message into an encrypted message**.**
- **Decipher**: to decrypt or convert ciphertext to plaintext**.**
- **Encipher**: to encrypt or convert plaintext to ciph**ertext.**
- **Key or cryptovariable: the information used in conjunction with the algorithm to create ciphertext from plaintext.**
- **Keyspace:** the entire range of values that can possibly be used to construct an individual key.
- **Link encryption:** a series of encryptions and decryptions between a number of systems, whereby each node decrypts the message sent to it and then re-encrypts it using different keys and sends it to the next neighbor, until it reaches the final destination.
- **Plaintext:** the original unencrypted message that is encrypted and results from successful decryption**.**
- **Steganography:** the process of hiding messages in a picture or graphic**.**
- **Work factor:** the amount of effort (usually in hours) required to perform cryptanalysis on an encoded message**.**

20) What is Data Encryption Standard(DES)?

Data Encryption Standard (DES)

- Developed in 1977 by IBM
- Based on the Data Encryption Algorithm (DEA)
- Uses a 64-bit block size and a 56-bit key

- With a 56-bit key, the algorithm has 256 possible keys to choose from (over 72 quadrillion)
- DES is a federally approved standard for non classified data
- DES was cracked in 1997 when RSA put a bounty on the algorithm offering $10,000 to the team to crack the algorithm - fourteen thousand users collaborated over the Internet to finally break the encryption

21) What is Triple DES?

Triple DES (3DES)

- Developed as an improvement to DES
- Uses up to three keys in succession and also performs three different encryption operations:
  - 3DES encrypts the message three times with three different keys, the most secure level of encryption possible with 3DES
- In 1998, it took a dedicated computer designed by the Electronic Freedom Frontier (www.eff.org) over 56 hours to crack DES
- The successor to 3DES is Advanced Encryption Standard (AES), based on the Rijndael Block Cipher, a block cipher with a variable block length and a key length of either128, 192, or 256 bits
- It would take the same computer approximately 4,698,864 quintillion years to crack AES

22) What are Digital signatures?

Digital Signatures

- An interesting thing happens when the asymmetric process is reversed, that is the private key is used to encrypt a short message
- The public key can be used to decrypt it, and the fact that the message was sent by the organization that owns the private key cannot be refuted
- This is known as **nonrepudiation**, which is the foundation of digital signatures
- **Digital Signatures** are encrypted messages that are independently verified by a central facility (registry) as authentic

23) What is Public Key Infrastructure(PKI)? What are its benefits?

PKI or Public Key Infrastructure

- Public Key Infrastructure is the entire set of hardware, software, and cryptosystems necessary to implement public key encryption
- PKI systems are based on public-key cryptosystems and include digital certificates and certificate authorities (CAs) and can:
  - Issue digital certificates
  - Issue crypto keys
  - Provide tools to use crypto to secure information
  - Provide verification and return of certificates

PKI Benefits

- PKI protects information assets in several ways:
  - Authentication

- Integrity
- Privacy
- Authorization
- Nonrepudiation

24) How E-mail systems are secured?

Securing E-mail

- Encryption cryptosystems have been adapted to inject some degree of security into e-mail:
  - S/MIME builds on the Multipurpose Internet Mail Extensions (MIME) encoding format by adding encryption and authentication
  - Privacy Enhanced Mail (PEM) was proposed by the Internet Engineering Task Force (IETF) as a standard to function with the public key cryptosystems
  - PEM uses 3DES symmetric key encryption and RSA for key exchanges and digital signatures
  - Pretty Good Privacy (PGP) was developed by Phil Zimmerman and uses the IDEA Cipher along with RSA for key exchange

25) What are the seven major sources of physical loss?

Seven Major Sources of Physical Loss

- Temperature extremes
- Gases
- Liquids
- Living organisms
- Projectiles
- Movement
- Energy anomalies

26) What is a Secure Facility?

- A secure facility is a physical location that has been engineered with controls designed to minimize the risk of attacks from physical threats
- A secure facility can use the natural terrain; traffic flow, urban development, and can complement these features with protection mechanisms such as fences, gates, walls, guards, and alarms

27) What are the controls used in a Secure Facility?

Controls for Protecting the Secure Facility

- Walls, Fencing, and Gates
- Guards
- Dogs, ID Cards, and Badges
- Locks and Keys
- Mantraps
- Electronic Monitoring
- Alarms and Alarm Systems
- Computer Rooms
- Walls and Doors

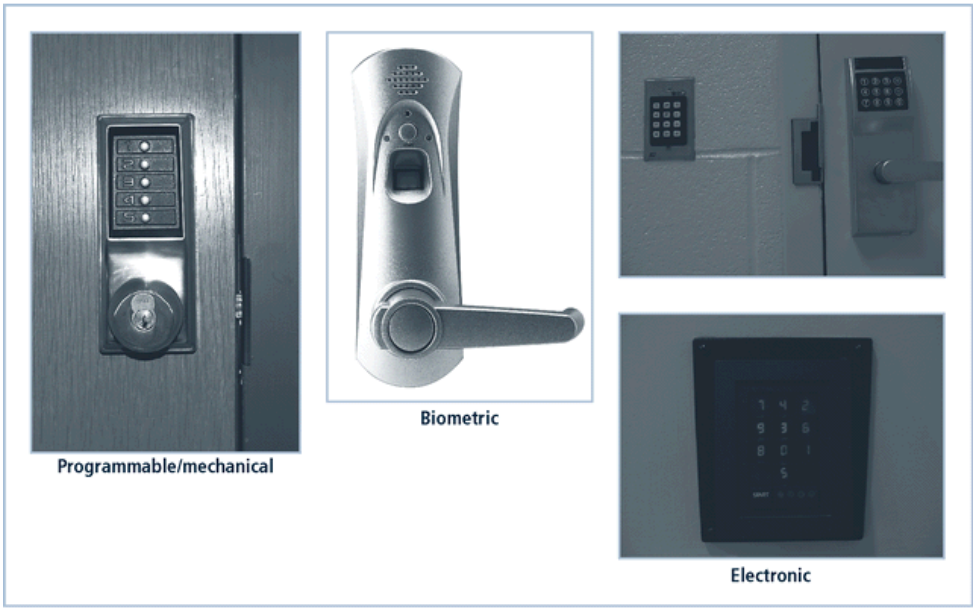
28) Explain in detail the controls used in a Secure Facility?

ID Cards and Badges

- Ties physical security to information access with identification cards (ID) and/or name badges
  - ID card is typically concealed
  - Name badge is visible
- These devices are actually biometrics (facial recognition)
- Should not be the only control as they can be easily duplicated, stolen, and modified
- Tailgating occurs when unauthorized individuals follow authorized users through the control

Locks and Keys

- There are two types of locks
  - mechanical and electro-mechanical
- Locks can also be divided into four categories
  - manual, programmable, electronic, and biometric
- Locks fail and facilities need alternative procedures for access
- Locks fail in one of two ways:
  - when the lock of a door fails and the door becomes unlocked, that is a fail-safe lock
  - when the lock of a door fails and the door remains locked, this is a fail-secure lock



Biometric image courtesy of the BioThentica Corporation

FIGURE 9-1 Locks

Mantraps

- An enclosure that has an entry point and a different exit point
- The individual enters the mantrap, requests access, and if verified, is allowed to exit the mantrap into the facility

- If the individual is denied entry, they are not allowed to exit until a security official overrides the automatic locks of the enclosure

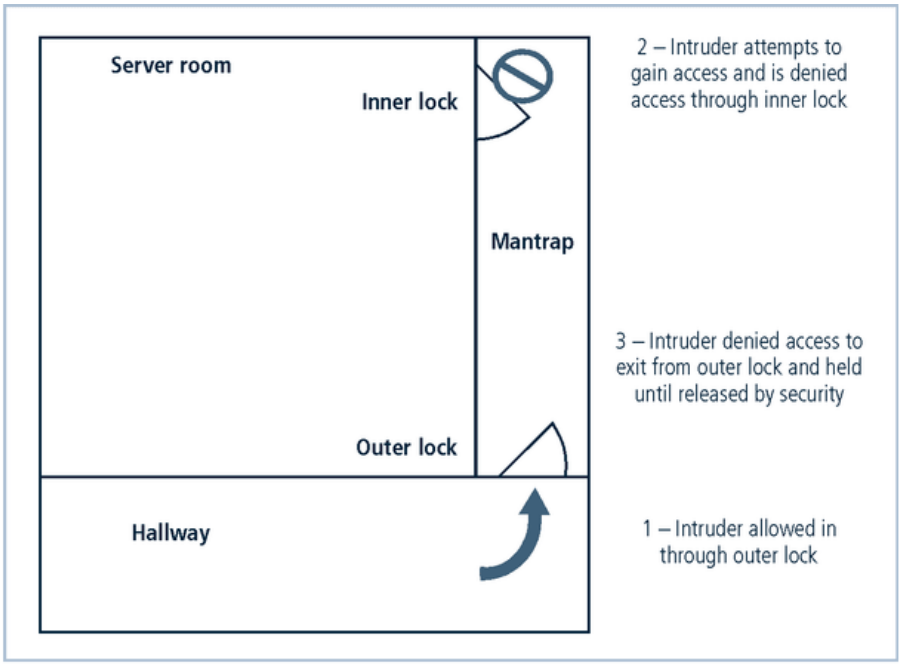


FIGURE 9-2 Mantraps

Electronic Monitoring

- Records events where other types of physical controls are not practical
- May use cameras with video recorders
- Drawbacks:
  - reactive and do not prevent access or prohibited activity
  - recordings often not monitored in real time and must be reviewed to have any value

Alarms and Alarm Systems

- Alarm systems notify when an event occurs
- Used for fire, intrusion, environmental disturbance, or an interruption in services
- These systems rely on sensors that detect the event: motion detectors, smoke detectors, thermal detectors, glass breakage detectors, weight sensors, and contact sensors

Computer Rooms and Wiring Closets

- Computer rooms and wiring and communications closets require special attention
- Logical controls are easily defeated, if an attacker gains physical access to the computing equipment
- Custodial staff are often the least scrutinized of those who have access to offices and are given the greatest degree of unsupervised access

Interior Walls and Doors

- The walls in a facility are typically either:
  - standard interior

- firewall

- All high-security areas must have firewall grade walls to provide physical security from potential intruders and improves the facility's resistance to fires
- Doors that allow access into secured rooms should also be evaluated
- Computer rooms and wiring closets can have push or crash bars installed to meet building codes and provide much higher levels of security than the standard door pull handle

Fire Safety

- The most serious threat to the safety of the people who work in the organization is the possibility of fire
- Fires account for more property damage, personal injury, and death than any other threat
- 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 installed and maintained to detect and respond to a fire
- They work to deny an environment of one of the three requirements for a fire to burn: heat, fuel, and oxygen
  - Water and water mist systems reduce the temperature and saturate some fuels to prevent ignition
  - Carbon dioxide systems rob fire of its oxygen
  - Soda acid systems deny fire its fuel, preventing spreading
  - Gas-based systems disrupt the fire's chemical reaction but leave enough oxygen for people to survive for a short time

29) What are the functions of Chief Information Security officer?

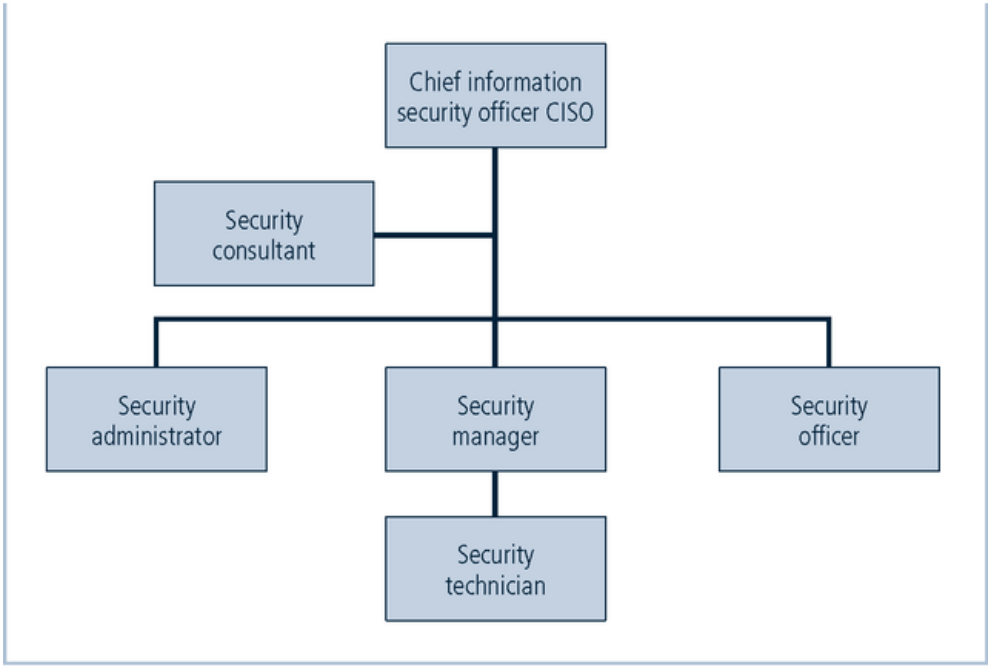


FIGURE 11-2 Positions in Information Security

Chief Information Security Officer

- The top information security position in the organization, not usually an executive and frequently reports to the Chief Information Officer
- The CISO performs the following functions:
  - Manages the overall InfoSec program
  - Drafts or approves information security policies
  - Works with the CIO on strategic plans, develops tactical plans, and works with security managers on operational plans
  - Develops InfoSec budgets based on funding
  - Sets priorities for InfoSec projects & technology
  - Makes decisions in recruiting, hiring, and firing of security staff
  - Acts as the spokesperson for the security team

Textbook

Principles of Information Security, by Michael Whitman and Herbert Mattord; ISBN: 0-619-06318-1, 2003