Chapter 1

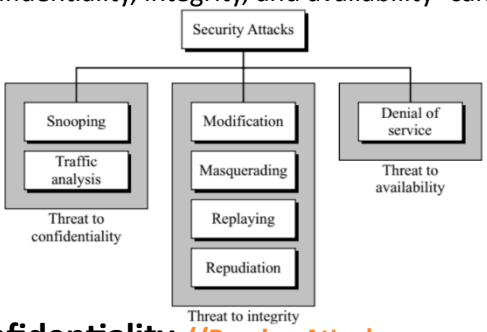
Security Goals

- **Availability**
  is the characteristic of something being accessible and usable during a specified time period.
- **Confidentiality**
  is the characteristic of something being made accessible only to authorized parties.
- **Integrity**
  is the characteristic of something not having been changed by an unauthorized party.

Note// To be secured, information needs to be hidden from unauthorized access (confidentiality), protected from unauthorized change (integrity), and available to an authorized entity when it is needed (availability).

Security Attacks

Our three goals of security- confidentiality, integrity, and availability- can be threatened by security attacks.



Attacks Threatening Confidentiality //Passive Attacks

- **Snooping**
  Snooping refers to unauthorized access to or interception of data.
- **Traffic Analysis**
  Although encipherment of data may make it non-intelligible for the interceptor, she can obtain some other type of information by monitoring online traffic.

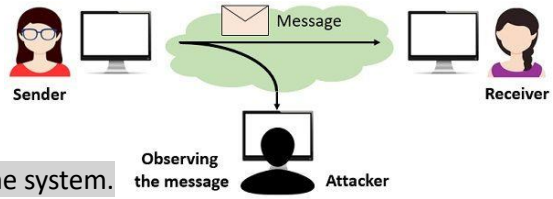
Attacks Threatening Integrity //Active Attacks

- **Modification**
  After intercepting or accessing information, the attacker modifies the information to make it beneficial to herself.
- **Masquerading**
  Masquerading, or spoofing, happens when the attacker impersonates somebody else.
- **Replaying**
  Replaying is another attack. The attacker obtains a copy of a message sent by a user and later tries to replay it.
- **Repudiation**
  This type of attack is different from others because it is performed by one of the two parties in the communication: the sender or the receiver.

Attacks Threatening Availability //Active Attacks

- **Denial of Service**
  Denial of service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system.

Passive versus Active Attacks



Passive Attacks

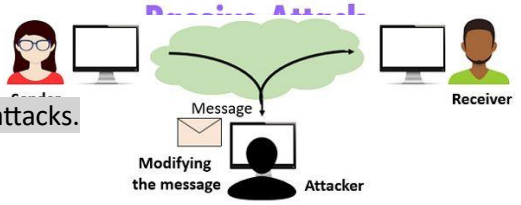
In a passive attack, the attacker's goal is just to obtain information.

Note// This means that the attack does not modify data or harm the system.

Active Attacks

An active attack may change the data or harm the system.

Note// Attacks that threaten the integrity and availability are active attacks.



Active Attack

Security Services

1- **Data confidentiality**
is designed to protect data from closure attack.

2- **Data Integrity**
is designed to protect data from unauthorized parties' modification, insertion, deletion, and replaying.

3- **Nonrepudiation**
Nonrepudiation service protects against repudiation by either the data's sender or receiver.

4- **Access Control**
Access control provides protection against unauthorized access to data.

5- **Authentication**
This service provides the party's authentication at the other end of the line.

Security Mechanisms

1- **Encipherment**
hiding or covering data, can provide confidentiality.

2- **Data integrity**
appends to the data a check valve that has been created from the data itself.

3- **Digital signature**
a means by which the sender can electronically sign the data and the receiver can electronically verify the signature.

4- **Authentication exchange**
two entities exchange messages to prove their identity to each other.

5- **Traffic padding**
inserting some bogus data into the data traffic to thwart the adversary's attempt to use the traffic analysis.

6- **Routing control**
changing different available routes between the sender and the receiver to prevent the opponent from eavesdropping on a route.

7- **Notarization**
selecting a third trusted party to control the communication between two entities.

8- **Access control**
uses methods to prove that a user has access right to the data or resources owned by a system.

Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

Chapter 2

Types of Encryptions

- **Symmetric Key (Secret Key, Private Key) Encryption**
  the message is encrypted by using a key and the same key is used to decrypt the message which makes it easy to use but less secure.
- **Asymmetric Key (Public Key) Encryption**
  is based on public and private key encryption techniques. It uses two different keys to encrypt and decrypt the message.

Modes of Network Encryption

- **End-to-end encryption**
  covers a communication from origin to destination.
- **link encryption**
  covers a communication from one node to the next on the path to the destination.

Link Encryption	End-to-End Encryption
Security within hosts	
Data partially exposed in sending host	Data protected in sending host
Data partially exposed in intermediate nodes	Data protected through intermediate nodes
Role of user	
Applied by sending host	Applied by user application
Invisible to user	User application encrypts
Host administrators select encryption	User selects algorithm
One facility for all users	Each user selects
Can be done in software or hardware	Usually software implementation; occasionally performed by user add-on hardware
All or no data encrypted	User can selectively encrypt individual data items
Implementation considerations	
Requires one key per pair of hosts	Requires one key per pair of users
Provides node authentication	Provides user authentication

SSH Encryption

SSH (secure shell) provides an authenticated and encrypted path to the shell or operating system command interpreter.

Note// SSH replaces Unix utilities such as Telnet, rlogin, and rsh for remote access.
SSH protects against spoofing attacks and modification of data in communication.
The SSH protocol involves negotiation between local and remote sites for encryption algorithm (for example, DES or AES) and authentication (including public key and Kerberos).

SSL and TLS Encryption

- **Secure Sockets Layer (SSL)**
  covers communication between a browser and the remote web host.
  Note// protects only from the browser to the destination decryption point. Vulnerabilities before encryption or after decryption are unaffected.
- **Transport Layer Security (TLS)**
  In 1999, the Internet Engineering Task Force upgraded to SSL 3.0 and named the upgrade **TLS**.

Note// The SSL protocol is simple but effective, and it is the most widely used secure communication protocol on the Internet.

Cipher Suite

Client and server negotiate encryption algorithms, called the **cipher suite**, for authentication, session encryption, and hashing.

Note// SSL supports use of popular cryptographic algorithms such as RSA, triple DES, and AES.

SSL Session

To use SSL, the client requests an SSL session. The server responds with its public key certificate so that the client can determine the authenticity of the server.

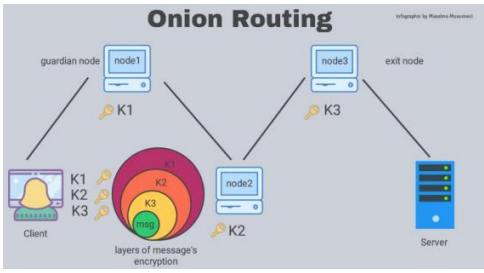
SSL & Keyloggers

Data is exposed from the user's keyboard to the browser and throughout the recipient's environment.

There are vulnerabilities of a keystroke logger and man in the browser.

Blue Gem Security has developed a product called **LocalSSL** that encrypts data from the time it has been typed until the operating system delivers it to the client's browser, thus thwarting any keylogging Trojan horse that has become implanted in the user's computer to reveal everything the user types.

Onion Routing



It uses a collection of **forwarding hosts**, each of whom knows only from where a communication was received and to where to send it next.

Note// onion routing prevents an eavesdropper from learning source, destination, or content of data in transit in a network.

IPsec

IPsec implements encryption and authentication in the Internet protocols.

Designed to address fundamental shortcomings such as spoofing, eavesdropping, and session hijacking, the IPsec protocol defines a standard means for handling encrypted data.

Note// IPsec is implemented at the IP layer (3), so it protects data produced in all layers above it, in particular, TCP and UDP control information, as well as the application data.

Q: Does IPsec require changes to TCP or UDP protocols?

A: IPsec requires no change to the existing large number of TCP and UDP protocols or applications.

Q: Compare between IPsec & SSL

A:

- Like SSL, IPsec supports **authentication** and **confidentiality** in a way that does not necessitate significant change either above it (in applications) or below it (in the TCP protocols).
- Like SSL, IPsec was designed to be independent of specific cryptographic algorithms and to allow the two communicating parties to agree on a mutually supported set of protocols.
- SSL is implemented at the application layer
- IPsec is implemented at the network layer

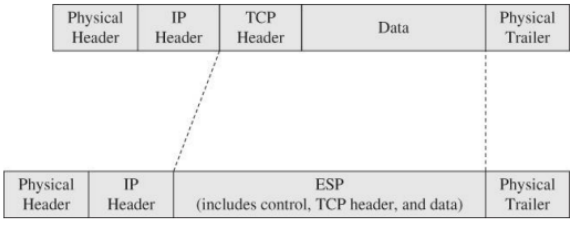
Security Association is the set of security parameters for a secured communication channel.

Q: How is a security association selected?

- A security association is selected by a security parameter index (SPI), a data element that is essentially a pointer into a table of security associations.

HEADERS AND DATA

The fundamental data structures of IPsec are the **authentication header (AH)** and the **encapsulated security payload (ESP)**.

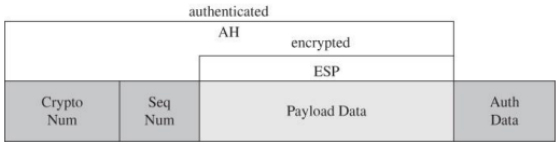


IPsec Encapsulated Security Payload

Encapsulated Security Payload (ESP).

The ESP contains both an authenticated portion and an encrypted portion.

The sequence number is incremented by 1 for each packet transmitted to the same address using the same security association, to prevent packet replay attacks.



Protection of the ESP in IPsec

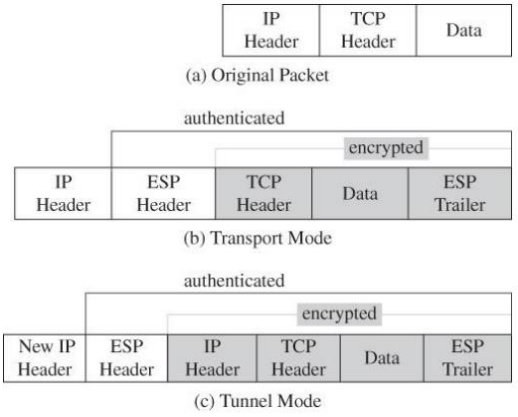
Note// The payload data are the actual data of the packet.
The authentication field is used for authentication of the entire object.

Key Management

- IPsec addresses this need with the **Internet Security Association Key Management Protocol (ISAKMP)**.
- **ISAKMP**
  is simple, flexible, and scalable. In IPsec, ISAKMP is implemented through the ISAKMP key exchange, or IKE, which provides a way to **agree** on and **manage protocols**, **algorithms**, and **keys**.
- For key exchange between unrelated parties, IKE uses the **Diffie-Hellman** scheme to generate a mutually shared secret that will then be used as an encryption key. With their shared secret, the two parties exchange identities, and certificates to authenticate those identities. Finally, they derive a shared cryptographic key and enter a security association.

IPsec modes of operation

- **Tunnel Mode**
  the recipient 's address is concealed by encryption, and IPsec substitutes the address of a remote device, such as a firewall, that will receive the transmission and remove the IPsec encryption.
- **Transport Mode**
  the IP address header is unencrypted.



Virtual Private Network (VPN)

A VPN carries private traffic over a public infrastructure (such as the Internet) and protect data that is transmitted over a public or shared infrastructure such as the Internet from threats such as man-in-the-middle attacks by tunneling links.

2 TYPES OF PRIVATE NETWORKS

Private Network

- A company has two physically separated offices, and the employees want to work as a single unit, exchanging sensitive data as if they were in one protected office.
- Each office maintains its own network. The two offices could implement a private network by acquiring, managing, and maintaining their own network equipment to provide a private link between the two sites.
- This solution is often costly, and the company assumes full responsibility for maintaining the connection. Often such companies are not in the networking business but maintaining that one link requires them to become or hire network administrators.

Virtual Private Network

- The alternative is a **virtual private network** between the offices.
- With link encryption, all communications between the sites are encrypted.
- Most of the cost of this solution is in acquiring and setting up the network.
- Some employee communications will involve sensitive plans and confidential data; other communications will be non-sensitive data.
- There is almost no harm in encrypting the non-sensitive data as well as the important traffic because the added time to encrypt and decrypt all traffic is usually insignificant relative to the network transmission time.

Chapter 3

Denial-of-Service

A **Denial-of-Service (DoS)** attack is an attempt to defeat availability, the third of the three basic properties to be preserved in computer security.
Note// Denial of service means that a user is denied access to authorized services or data.

Confidentiality and integrity are concerned with **preventing unauthorized access**; availability is concerned with **preserving authorized access**.

Confidentiality – Integrity – Availability

Confidentiality and integrity tend to be binary: Data or objects either are or are not kept private and unmodified. However, availability has is not binary.
Denial of service ranges from **complete loss** of access to **noticeable** and **unacceptable slowing** to inconvenience.
For example, a web page takes a few seconds to load, but as time passes you become more frustrated or suspicious that it will never display; then, suddenly it appears and you wonder why it took so long.

How service is denied?

1. **Insufficient capacity (overload)**
   - **Flooding**
     A flooding attack occurs from demand in excess of capacity, from malicious or natural causes.
     // An attacker sends commands more quickly than a server can handle them → servers often queue unmet commands during moments of overload for service when the peak subsides, but if the commands continue to come too quickly, the server eventually runs out of space to store the demand. Such an attack is called an overload or flood.
     Targets of flooding attacks:
     - An application
       - Database management system
       - An operating system or one of its components like a file or print server
       - A network appliance like a router.
     - A resource
       - A memory allocation table
       - Web page
2. **Blocked access**
   The attacker may simply prevent a service from functioning. How?
   - The attacker could exploit a software vulnerability in an application and cause the application to crash.
   - The attacker could interfere with the network routing mechanisms, preventing access requests from getting to the server.
   - The attacker manipulates access control data, deleting access permissions for the resource, or to disable the access control mechanism so that nobody could be approved for access.
3. **Access Failure (unresponsive component)**
   Either maliciously or not, hardware and software fail from time to time; of course, it always seems that such nonmalicious failures occur only at critical times.
   // Software stops working due to a flaw, or a hardware device wears out or inexplicably stops. The failure can be sporadic, meaning that it goes away or corrects itself spontaneously, or the failure can be permanent, as from a faulty component.

Flooding Attack in details

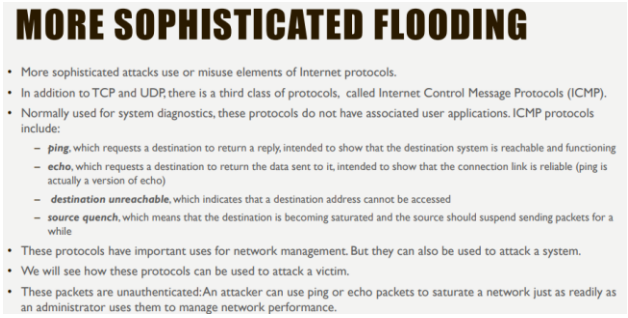
Flooding occurs because the incoming bandwidth is insufficient or resources—hardware devices, computing power, or software—are inadequate.

1. **Insufficient Resources**
   - An attacker can try to consume a critical amount of a limited resource.
   - Flooding a victim is basically an unsophisticated attack.
2. **Insufficient Capacity**
   - If the attacker's bandwidth is greater than that of the victim, the attacker can overwhelm the victim.
   - A victim is always potentially vulnerable to an attacker with more resources.

Basic Flooding

If an attacker sends you as much data as your communications system can handle, you are prevented from receiving any other data. Even if an occasional packet reaches you from someone else, communication to you will be seriously degraded.

Note// The most basic denial-of-service attack is flooding a connection.



1. **Ping of Death**

   A **ping of death** is a simple attack, using the ping command that is ordinarily used to test response time from a host.

   Since ping requires the recipient to respond to the packet, all the attacker needs to do is send a flood of pings to the intended victim.

2. **Smurf Attacks**

   The **Smurf** attack is a variation of a ping attack.

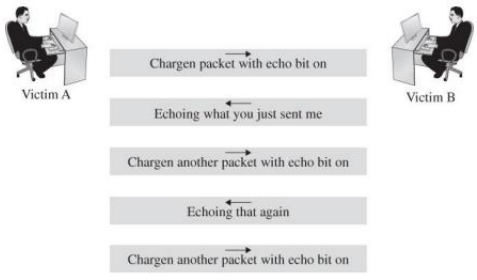
   It uses the same vehicle, a ping packet, with two extra twists.

   - First, the attacker chooses a network of unaware victims that become accomplices. The attacker spoofs the source address in the ping packet so that it appears to come from the victim, which means a recipient will respond to the victim.
   - Then, the attacker sends this request to the network in broadcast mode by setting the last byte of the address to all 1s; broadcast mode packets are distributed to all hosts on the subnetwork.

3. **Echo-Chargen Attack**

   The **echo–chargen** attack works between two hosts.

   - **Chargen** is an ICMP protocol that generates a stream of packets to test the network's capacity.
   - **Echo** is another ICMP protocol used for testing; a host receiving an echo returns everything it receives to the sender.



4. **SYN Flood**

   SYN flood is a popular denial-of-service attack.

   This attack uses the TCP protocol suite, making the session-oriented nature of these protocols work against the victim.

   Note// A session is established with a **three-way TCP handshake**.

   The attacker can deny service to the target by sending many SYN requests, to which the target properly responds with SYN-ACK. However, the attacker never replies with ACKs to complete the connections, thereby filling the victim's SYN_RECV queue.

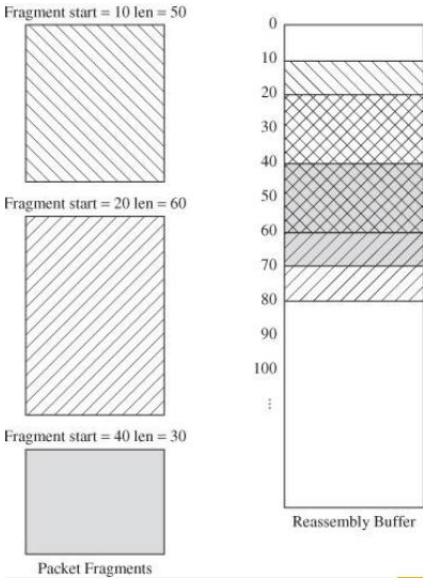
Types of Flooding Attacks

1. Flooding by Malicious Code
   - Ping of Death
   - Smurf
   - Echo-Chargen
   - SYN Flood
2. Flooding by Resource Exhaustion
   - Teardrop

Teardrop Attack

The teardrop attack misuses a feature intended to improve network communication.

A network IP datagram is a variable -length object. To support different applications and conditions, the datagram protocol permits a single data unit to be fragmented (broken into pieces and transmitted separately).
Each fragment indicates its length and relative position within the data unit. The receiving end reassembles the fragments into a single data unit.

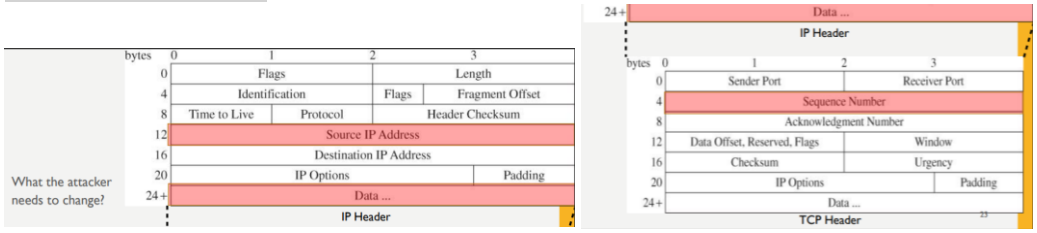


The **attacker** sends a series of datagrams that cannot fit together properly.

One datagram might say it is position 0 for length 60 bytes, another position 30 for 90 bytes, and another position 41 for 173 bytes. These three pieces overlap, so they cannot be reassembled properly. In an extreme case, the operating system locks up with these partial data units it cannot reassemble, thus leading to **denial of service**.

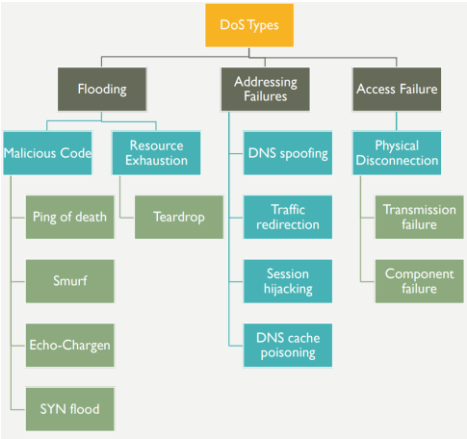
DOS by addressing failures

1. **DNS Spoofing**
   Note// Domain Name System (DNS) is an Internet addressing protocol.
   DNS is the database of translations of Internet names to addresses, and the DNS protocol resolves the **name** to an **address**.// **microsoft.com** to **207.46.197.32**
   DNS service is implemented on a remote server, so a man-in-the-middle attack involves the attacker's intercepting and replying to a query before the real DNS server can respond.
2. **Rerouting Traffic**
3. **Session Hijack**
   In a session hijacking attack, the attacker allows an interchange to begin between two parties but then diverts the communication, much as would a man in the middle.
   for example, of logging in to a financial site, completing the authentication, and then losing the session to an attacker.



4. **DNS Cache Poisoning**
   The DNS cache poisoning attack causes a DNS server to redirect clients to a specified address. A simple DNS poisoning attack is to forge a message to a DNS server, requesting that a particular domain name be changed from one address to another.
   // An attacker poisons the IP address DNS entries for a target website on a given DNS server, replacing them with the IP address of the server the attacker controls.

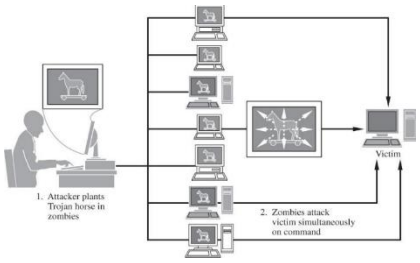
DOS attacks summary



Distributed DOS (DDOS)

To make a **distributed denial-of-service** (DDoS) attack, an attacker does two things:

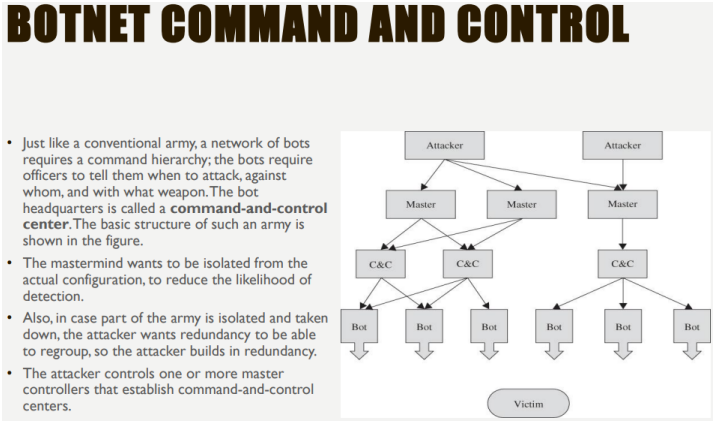
1. Plant a trojan horse in zombies.
2. Zombies attack the victim simultaneously on the attacker's command.



شرح الخطوتين في الشابتر 3 السلايد 29

Bots and Botnets

- **Zombies (or bots)** are machines running pieces of malicious code under remote control.
- **Botnets**, networks of bots, are used for massive denial-of-service attacks, implemented from many sites working in parallel against a victim.
  // They are also used for spam and other bulk email attacks, in which an extremely large volume of email from any one point might be blocked by the sending service provider.



Bots for Rent!

People who infect machines to turn them into bots are called **botmasters**.
// A **botmaster** may own (in the sense of control) hundreds or thousands of bots.
Botnet operators make money by renting compromised hosts for DDoS or other activity. The rent is mostly profit.

DDOS Prevention

- DDoS attacks are not hard to prevent, at least in theory.
- Most bots infect computers using well-known **vulnerabilities**.
- The **patches** for these vulnerabilities have been distributed for some time.
- if the entire world would just install patches in a timely manner, DDoS threat would **disappear**.
- Some computer users do not have legal copies of their operating systems and other software, so they cannot subscribe for and obtain patches through the manufacturers' chains.
- Computer software is one of a small number of commodities, including illegal firearms and illicit drugs, in which the black market also affects legitimate consumers.

Chapter 4

Firewall.

A firewall is a device that filters all traffic between a protected or “inside” network and a less trustworthy or “outside” network.
Note// Usually a firewall runs on a dedicated device.
In practice, a firewall is a computer with memory, storage devices, interface cards for network access, and other devices.

Purpose of Firewall

The purpose of a firewall is to keep “bad” things outside a protected environment.
To accomplish that, firewalls implement a security policy that is specifically designed to address what bad things might happen.
For example, the policy might be to prevent any access from outside (while still allowing traffic to pass from the inside to the outside).

Design of Firewalls

Firewalls are simple devices that rigorously and effectively control the flow of data to and from a network.
Two qualities lead to that effectiveness:

- A well-understood traffic flow policy
- A trustworthy design and implementation

Firewall Policy

security policy is a set of rules that determine what traffic can or cannot pass through the firewall.

Rule	Type	Source Address	Destination Address	Destination Port	Action
1	TCP	*	192.168.1.*	25	Permit
2	UDP	*	192.168.1.*	69	Permit
3	TCP	192.168.1.*	*	80	Permit
4	TCP	*	192.168.1.18	80	Permit
5	TCP	*	192.168.1.*	*	Deny
6	UDP	*	192.168.1.*	*	Deny

Example Firewall Configuration

An example of a simple firewall configuration is shown in table above.
The table is processed from the top down, and the first matching rule determines the firewall’s action.
// The * character matches any value in that field.

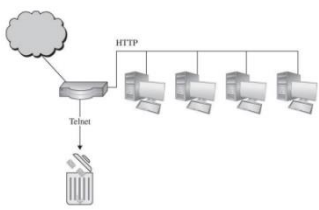
Firewall Properties

- Reference monitor: access control that is always invoked, tamperproof, and verifiable.
- A firewall is a reference monitor, positioned to monitor all traffic, not accessible to outside attacks, and implementing only access control.

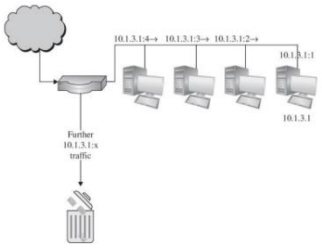
Types of Firewalls

1. **Packet Filtering Gateway**

   A **packet filtering gateway** or **screening router** is the simplest, and in some situations, the most effective type of firewall.
   A **packet filtering gateway** controls access on the basis of **packet address** (source or destination) or **specific transport protocol** type (such as HTTP web traffic), that is, by examining the control information of each single packet.
   Note// Packet filters operate at OSI level 3.



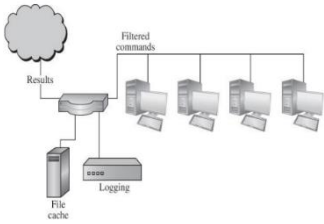
2. Stateful Inspection Firewall



A **stateful inspection firewall** maintains **state** information from one packet to another in the input stream.

//The name stateful inspection refers to accumulating threat evidence across multiple packets.

3. Application Proxy



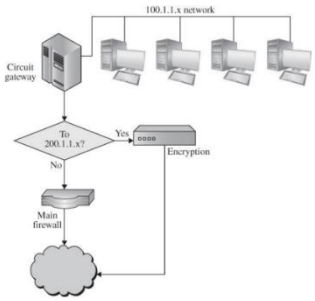
An **application proxy** simulates the behavior of a protected application on the inside network, allowing in only safe data.

// A proxy gateway is a two-headed device: From inside, the gateway appears to be the outside (destination) connection, while to outsiders the proxy host responds just as the insider would. In fact, it behaves like a man in the middle.

Typically, firewalls focus on protecting insider recipients from harmful **content** sent from outside.

Example: receiving emails, scanning emails from viruses, then forwarding them to the intended recipient.

4. Circuit-Level Gateway



A **circuit-level gateway** is a firewall that essentially allows one network to be an extension of another.

// It operates at OSI **level 5**, the **session level**, and it functions as a virtual gateway between two networks.

// A circuit is a logical connection that is maintained for a period of time, then torn down or disconnected.

The firewall verifies the circuit when it is first created. After the circuit has been verified, subsequent data transferred over the circuit are not checked.

// Circuit-level gateways can **limit** which connections can be made through the gateway.

5. Guard

A guard can implement any programmable set of conditions, even if the program conditions become highly sophisticated.

Example: A school wants its students to be able to access the World Wide Web but, because of the capacity of its connection to the web, it will allow only so many bytes per second (that is, allowing text mode and simple graphics but disallowing complex graphics, video, music, or the like).

6. Personal Firewalls

A personal firewall is a program that runs on a single host to monitor and control traffic to that host. It can only work in conjunction with support from the operating system.

// Just as a network firewall screens incoming and outgoing traffic for that network, a personal firewall screens traffic on a single workstation.

Commercial implementations of personal firewalls include **SaaS** Endpoint Protection from **McAfee**, **F-Secure Internet Security**, **Microsoft Windows Firewall**, and **Zone Alarm** from **CheckPoint**.

Packet Filter	Stateful Inspection	Application Proxy	Circuit Gateway	Guard	Personal Firewall
Simplest decision-making rules, packet by packet	Correlates data across packets	Simulates effect of an application program	Joins two subnetworks	Implements any conditions that can be programmed	Similar to packet filter, but getting more complex
Sees only addresses and service protocol type	Can see addresses and data	Sees and analyzes full data portion of pack	Sees addresses and data	Sees and analyzes full content of data	Can see full data portion
Auditing limited because of speed limitations	Auditing possible	Auditing likely	Auditing likely	Auditing likely	Auditing likely
Screens based on connection rules	Screens based on information across multiple packets—in either headers or data	Screens based on behavior of application	Screens based on address	Screens based on interpretation of content	Typically, screens based on content of each packet individually, based on address or content
Complex addressing rules can make configuration tricky	Usually preconfigured to detect certain attack signatures	Simple proxies can substitute for complex decision rules, but proxies must be aware of application's behavior	Relatively simple addressing rules; make configuration straightforward	Complex guard functionality; can be difficult to define and program accurately	Usually starts in mode to deny all inbound traffic; adds addresses and functions to trust as they arise

Chapter 5

Intruders.

Intruders are the attackers who attempt to breach the security of a network. They attack the network in order to get unauthorized access.

Intruders are of three types:

1. **Masquerader**
   Masquerader is an external user who is not authorized to use a computer, and yet tries to gain privileges to access a legitimate user's account.
2. **Misfeasor**
   a legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuse his or her privileges.
3. **Clandestine user**
   an individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

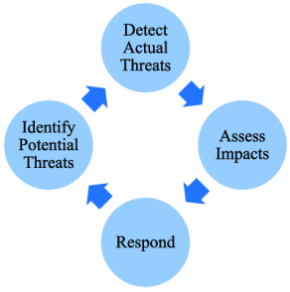
Intrusion Detection Systems (IDS)

// Intrusion detection systems complement preventive controls such as firewalls as the next line of defense.

An **Intrusion Detection System** (IDS) is a device, typically another separate computer, that monitors activity to identify malicious or suspicious events. An IDS is a sensor, like a smoke detector, that raises an alarm if specific things occur.

Functions of IDS

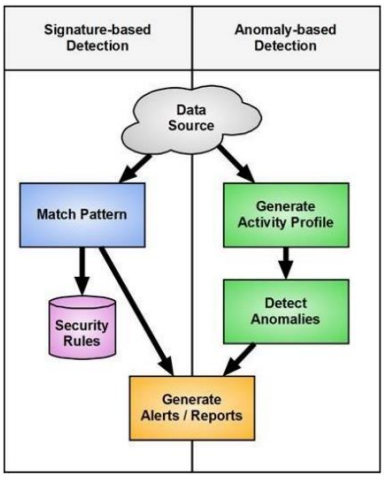
- Monitoring users and system activity
- Auditing system configuration for vulnerabilities and misconfigurations
- Assessing the integrity of critical system and data files
- Recognizing known attack patterns in system activity
- Identifying abnormal activity through statistical analysis
- Managing audit trails and highlighting user violation of policy or normal activity
- Correcting system configuration errors
- Installing and operating traps to record information about intruders



Main Function of IDS

Types of IDS

1. **Signature-based** intrusion detection systems perform simple pattern matching and report situations that match a pattern (signature) corresponding to a known attack type.
2. **Heuristic** intrusion detection systems, also known as anomaly based, build a model of acceptable behavior and flag exceptions to that model; for the future, the administrator can mark a flagged behavior as acceptable so that the heuristic IDS will now treat that previously unclassified behavior as acceptable.
   heuristic intrusion detection looks for behavior that is out of the ordinary. It focuses on the individual, trying to find characteristics of that person that might be helpful in understanding **normal** and **abnormal behavior**.



Signature-based IDSs look for patterns; heuristic ones learn characteristics of unacceptable behavior over time.

Advantages of Signature-Based Intrusion Detection

- Signature-based detection has high processing speed for known attacks and low false positive rates, which allows this detection method to quickly and accurately identify malicious events.
- Simple to implement
- Lightweight

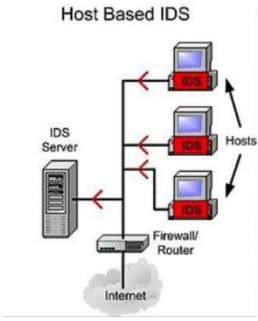
Disadvantage of Signature-Based Intrusion Detection

- Signature-based IDS cannot detect new attacks until it is updated with new signatures.
- Signature-based IDS are easy to evade since they are based on known attacks and are depended on new signatures to be applied before they can detect new attacks.
- Signature-based IDS can be easily bypassed by attackers who modify known attacks and target systems that have not been updated with new signatures that detect the modification.

Signature vs Anomaly-Based IDS

SN	Signature Based IDS	Anomaly-Based IDS
1.	It is used for threats we know.	It is used for changes in behavior.
2.	It relies on a preprogrammed list of known indicators of compromise (IOCs).	It is capable of alerting on unknown suspicious behavior.
3.	It may also include alerts on network traffic, including known malicious IP addresses that are attempting to access a system.	Alerts can be triggered by anything that does not align with the normalized baseline, including a user logging in during non-business hours, a flood of new IP addresses attempting to connect to the network, or new devices being added to a network without permission.

Host-Based IDS (HIDS)



Host-based intrusion detection (called HIDS) protects a single host against attacks.
The device either analyzes data itself or forwards the data to a separate machine for analysis and perhaps correlation with HIDSs on other hosts.

The goal of a host-based system is to protect one machine and its data. If an intruder disables that IDS, however, it can no longer protect its host.

Network-Based IDS (NIDS)

A network-based IDS or NIDS is generally a separate network appliance that monitors traffic on an entire network.
It receives data from firewalls, operating systems of the connected computers, other sensors such as traffic volume monitors and load balancers, and administrator actions on the network.

The goal of a NIDS is to protect the entire network or some set of specific sensitive resources, such as a collection of servers holding critical data.

A network IDS is better able to protect itself against detection or compromise than a host-based one because the network IDS can operate in **so-called stealth mode**, observing but never sending data onto the network.

Comparison Between NIDS & HIDS

NIDS	HIDS
Well for sensing attacks from outside	Well for sensing attacks from inside that NIDS cannot examine
Examines packet headers & entire packet	Does not understand packet headers
Host independent	Host dependent
Bandwidth in need of	Bandwidth free
Slow down the networks that have IDS clients installed	Slow down the hosts that have IDS clients installed
Senses network attacks, as payload is analyzed	Senses local attacks before they hit the network
Not reasonable for encoded and switches arrange	Well-suited for scrambled and switches organize
Does not perform ordinarily discovery of complex attacks	Powerful for examining a conceivable attack in view of pertinent data in database
High false positive rate	Low false positive rate