Module-4
NETWORK SECURITY

OVERVIEW OF NETWORK SECURITY

• Network security is required by the users to communicate on the network.

• If medium is insecure then an intruder may intercept, read and modify the transmitted-data from sender to receiver.

ELEMENTS OF NETWORK SECURITY

1) Confidentiality: Information should be available only to those who have rightful access to it

2) Authenticity and integrity: The sender of a message and the message itself should be verified at the receiving-point (Figure 4.1).

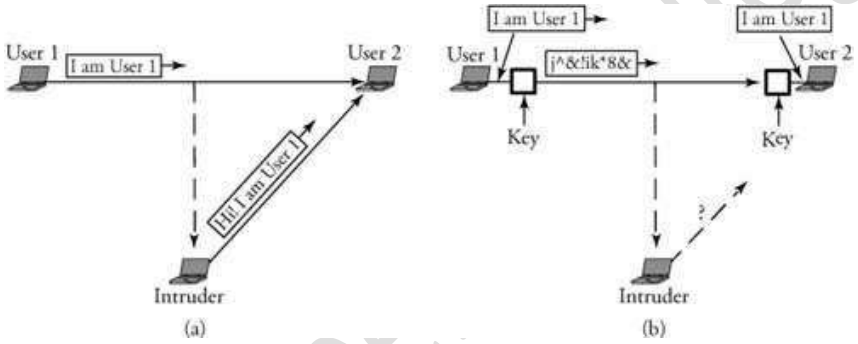

Figure 4.1. (a) Message content and sender identity falsified by intruder; (b) a method of applied security

• In figure 4.1a, user 1 sends a message ("i am user 1") to user 2.

Since the network lacks any security system, an intruder can receive the message and change its content to a different message ("hi i am user 1") and send it to user 2.

User 2 may not know that this falsified message is really from user 1(authentication).

• In figure 10.1b, a security block is added to each side of the communication, and a secret key that only users 1 and 2 would know about is included.

Therefore, the message is changed to a form that cannot be altered by the intruder.

THREATS TO NETWORK SECURITY

• Internet infrastructure attacks are broadly classified into 4 categories:

1. **DNS hacking**
2. **Routing table poisoning**
3. **Packet mistreatment**
4. **Denial of Service (DOS)**

DNS HACKING ATTACKS

• DNS server is a distributed hierarchical and global directory that translates domain names into numerical IP address.

• DNS is a critical infrastructure, and all hosts contact DNS to access servers and start connections.

• Name-resolution services in the modern Internet environment are essential for email transmission, navigation to web sites, or data transfer. Thus, an attack on DNS can potentially

affect a large portion of the Internet.

• A DNS hacking attack can appear in any of the following forms

Masquerading Attack

• The attacker poses as a trusted entity and obtains all the secret information.

• The attacker

→can stop any message from being transmitted further or

→can change the content or redirect the packet to bogus servers. This action is also known as a middle-man attack.

Domain Highjacking Attack

• Whenever a user enters a domain address, he is forced to enter into the attacker's Web site.

Information Leakage Attack

• The attacker

→sends a query to all hosts

→identifies which IP addresses are not used

→uses those IP address to make other types of attacks

Information-Level Attack(Cache Poisoning)

• This forces a server to correspond with other than the correct answer.

• The hacker

→tricks a remote name-servers into caching the answer for a third-party domain by providing malicious information.and

→ redirects traffic to a preselected site.

ROUTING TABLE POISONING

• This is the undesired modification of routing tables.

• This results in a lower throughput of the network.

• Two types of attacks are: i)link attack and ii)router attack.

Link Attack

• This occurs when a hacker gets access to a link and thereby intercepts, interrupts or modifies routing messages.

• This act similarly on both the link-state and the distance-vector protocols.

• If an attacker succeeds in placing an attack in a link-state routing protocol, a router may

→ send incorrect updates about its neighbors or

→ remain silent even if the link state of its neighbor has changed

Router Attack

• This may affect the link-state protocol or even the distance-vector protocol.

• In link-state protocol, if routers are attacked, they become malicious. As a result, routers may

→ add a nonexisting link to a routing table

→ delete an existing link or

→ change the cost of a link.

• In the distance-vector protocol, an attacker may cause routers to send wrong updates about any node in the network, thereby misleading a router and resulting in network problems.

DOS ATTACKS (DENIAL OF SERVICE)

- This is a type of security breach that prohibits a user from accessing normally provided services.
- This can cost the target person a large amount of time and money.
- This affects the destination rather than a data-packet or router.
- They take important servers out of action for few hours, thereby denying service to all users.
- Two types of attacks are:

1) *Single-source:* An attacker sends a large number of packets to a target system to overwhelm & disable it

2) *Distributed:* A large number of hosts are used to flood unwanted traffic to a single target. The target cannot then be accessible to other users in the network.

PACKET MISTREATMENT ATTACKS

- This can occur during any data transmission.
- A hacker may capture certain data packets and mistreat them.
- The attack may result in

→congestion
→lowering throughput &
→DOS attacks

- Link-attack causes interruption, modification or replication of data packets.

Whereas, a router-attack can misroute all packets and may result in congestion or DOS

- Following are some examples:

Interruption

- If an attacker intercepts packets, they may not be allowed to be propagated to their destinations.

Modification

- Attackers may succeed in accessing the content of a packet. They can then
  →change the address of the packet or
  →change the data of the packet
- This kind of attack can be detected by digital signature mechanism.

Replication

- An attacker may trap a packet and replay it.
- This kind of attack can be detected by using the sequence number for each packet.

Malicious Misrouting of Packets

- A hacker may attack a router and change its routing table, resulting in misrouting of data packets.

Ping of death

- An attacker may send a ping message, which is large and therefore must be fragmented for transport.
- The receiver then starts to reassemble the fragments as the ping fragments arrive.
- The total packet length becomes too large and might cause a system crash.

OVERVIEW OF SECURITY METHODS

- Common solutions that can protect computer communication networks from attacks are classified are cryptographic techniques or authentication techniques(verification).

CRYPTOGRAPHIC TECHNIQUES

- Cryptography is the process of transforming a piece of information or message shared by two parties into some sort of code.
- The message is scrambled before transmission so that it is undetectable by outside watchers.

- The scrambled-message needs to be decoded at the receiving-end before any further processing.
- The main tool used to encrypt a message M is a secret-key K.

  The fundamental operation used to encrypt a message is the exclusive-OR(⊕).
- Assume that we have one-bit M and a secret-bit K. A simple encryption is carried out using:

  M ⊕ K.
- To decrypt this message, the second party can detect M by performing the following operation:

  (M ⊕ K)⊕ K = M
- In *end-to-end encryption*, secret coding is carried out at both end systems (Figure 4.2).

  In *link encryption*, all the traffic passing over that link is secured.
- Two types of encryption techniques are secret-key & public-key encryption

  1) In *secret-key model*, both sender & receiver conventionally use same key for an encryption process. In *public-key model*, a sender and a receiver each use a different key.

  2) The public-key system

  →is more powerful than the secret key system &

  →provides better security and message privacy.

  3) Drawbacks of public-key system:

  →slow speed

  →more complex computationally

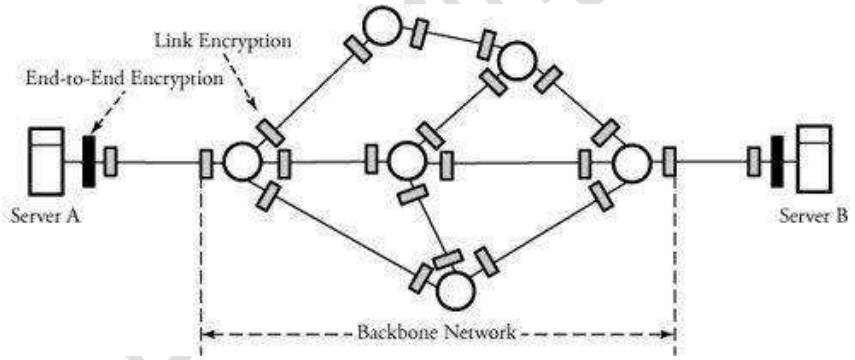

Figure 4.2. Overview of encryption points in a communication network

AUTHENTICATION TECHNIQUES

- Encryption methods offer the assurance of message confidentiality.
- A networking-system must be able to verify the authenticity of the message and the sender of the message. These forms of security techniques are known as authentication techniques.
- Authentication techniques are categorized as i) authentication with message digest and ii) authentication with digital signature.

SECRET KEY ENCRYPTION PROTOCOLS

- This is also called as symmetric encryption or single-key encryption.
- Sender and receiver conventionally use the same key for an encryption process.
- This consist of

  →an encryption-algorithm

  →a key and

  →a decryption-algorithm
- The encrypted-message is called ciphertext.
- Two popular protocols are: 1) DES (Data Encryption Standard)

  2) AES (Advanced Encryption Standard)

- A shared secret-key between a transmitter and a receiver is assigned at the transmitter and receiver points.
- At the receiving end, the encrypted information can be transformed back to the original data by using
  →decryption algorithm and
  →secret key

DES

- Plaintext messages are converted into 64-bit blocks & each block is encrypted using a key.
- The key length is 56 bits.
- This consists of 16 identical rounds of an operation (Figure 4.3).

Begin DES Algorithm

1) Initialize. Before round 1 begins, all 64 bits of the message and all 56 bits of the secret key
` are separately permuted(shuffled).
2) Each incoming 64-bit message is broken into two 32-bit halves denoted by L_i and R_i respectively.
3) The 56 bits of the key are also broken into two 28-halves, and each half is rotated one or two bit positions, depending on the round.
4) All 56 bits of the key are permuted, producing version k_i of the key on round i.
5) L_i and R_i are determined by

$$L_i = R_{i-1}$$

and

$$R_i = L_{i-1} \oplus F(R_{i-1}, k_i)$$

6) All 64 bits of a message are permuted.

Operation of function F()

- Out of 56 bits of k_i, function F( ) chooses 48 bits.
- The 32-bit R_{i-1} is expanded from 32 bits to 48 bits so that it can be combined with 48 bit k_i.
- F( ) also partitions the 48 bits of k_i into eight 6-bit chunks.
- The corresponding eight chunks of R_{i-1} and eight chunks of k_i are combined as follows

$$R_i = R_{i-1} \oplus k_i$$

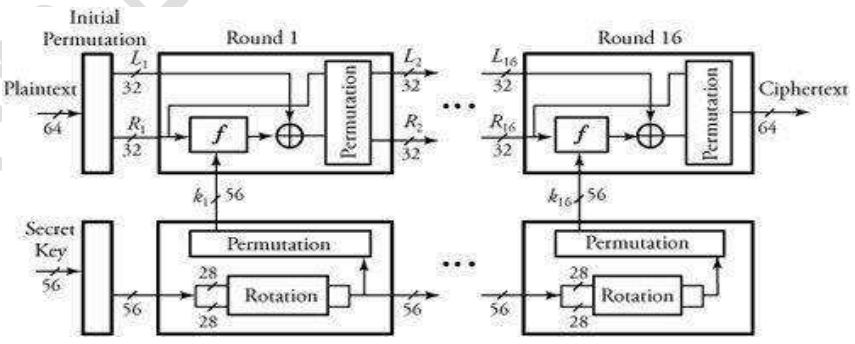

Figure 4.3. The Data Encryption Standard (DES)

AES (Advanced Encryption Standard)

- This has a better security strength than DES (Figure 4.4).
- Message size=128-bit block
  Key size=128,192 or 256 bit
  Number of rounds= 10,12 OR 14
- The plaintext is formed as 16 bytes m_0 through m_{15} and is fed into round 1 after an

initialization stage.
• In this round, substitute-units(S) perform a byte-by-byte substitution of blocks.
• The ciphers move through a permutation-stage to shift rows to mix-columns.
• At the end of this round, all 16 blocks of ciphers are Exclusive-ORed with the 16 bytes of round 1 key $k_0(1)$ through $k_{15}(1)$.

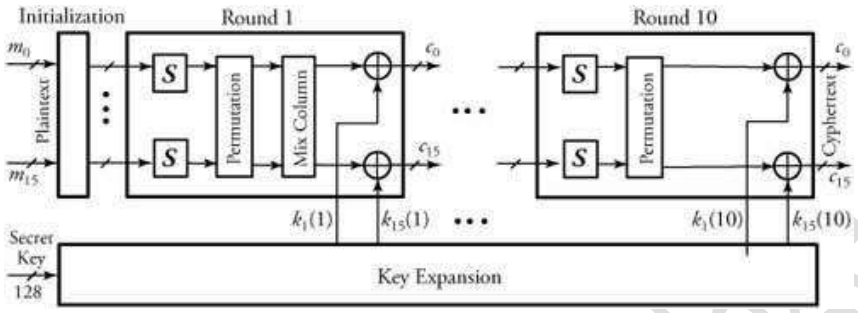

Figure 4.4. Overview of Advanced Encryption Standard (AES) protocol

PUBLIC KEY ENCRYPTION PROTOCOLS

• This is also called as asymmetric or two key encryption.
• A sender/receiver pair use different keys.
• This is based on mathematical functions rather than on substitution or permutation.
• Two popular protocols are: i)RSA protocol ii)Diffie-Hillman key-exchange protocol.
• Either of the two related keys can be used for encryption; the other one for decryption.
• Each system publishes its encryption key by placing it in a public-register & sorts out key as public one. The companion key is kept private.
• If A wishes to send a message to B, A encrypts the message by using B's public key.
At receiving end, B decrypts the message by using its private key.
No other recipients can decrypt the message, since only B knows its private key.
• The public-key system
→is more powerful than the secret key system &
→provides better security and message privacy.
• Drawbacks of public-key system:
→slow speed
→more complex computationally

RSA(Rivest Shamir Adleman) ALGORITHM

• Assume that a plaintext m must be encrypted to a ciphertext c.
• This has three phases: key generation, encryption and decryption.

Key Generation Algorithm

1) Choose two prime numbers a and b and compute n=a.b
2) *Find x*. Select encryption-key x such that x and (a-1)(b-1) are relatively prime.
3) *Find y*. Calculate decryption-key y.

$$x\,y \bmod (a-1)(b-1) = 1$$

4) At this point, a and b can be discarded.
5) The public key = {x, n}
6) The private key = {y, n}

Encryption

1) Both sender and receiver must know the value of n.
2) The sender knows the value of x and only the receiver knows the value of y.
3) Ciphertext c is constructed by

$c=m^x \bmod n$

Decryption

1) Given the ciphertext c, the plaintext m
is extracted by $m=c^y \bmod n$.

DIFFIE-HILLMAN KEY-EXCHANGE PROTOCOL

- Two end users can agree on a shared secret-code without any information shared in advance.
- This protocol is normally used for VPN(virtual private network).
- Assume that user-1 wishes to communicate with user-2.

Key Generation Algorithm

1) User-1
→ selects a prime number 'a', random integer number 'x_1',and a generator 'g'
→ creates 'y1' such that
$y_1 = g^{x1} \bmod a$
2) User-2
→ performs the same function and
→ creates y2 such that
$y_2 = g^{x2} \bmod a$
3) User-1 then sends y1 to user-2. Now, user-1 forms its key k_1 using the information its
partner sent as
$k_1 = y_2^{x1} \bmod a$
4) User-2 forms its key ka using the information its partner send it as
$k_2 = y_1^{x2} \bmod a$
5) The two keys k_1 and k_2 are equal. The two users can now encrypt their messages, each using its own key

AUTHENTICATION

- Message-authentication verifies the authenticity of both the message-sender and the message-content.
- Message-sender is authenticated through implementation of a digital signature.
- Message-content is authenticated through implementation of a hash function and encryption of the resulting message-digest.
- Hash-function is used to produce a "fingerprint" of a message.

Cryptographic Hash function

- A hash function is a mathematical function that converts a numerical input value into another compressed numerical value.
- The input to the hash function is of arbitrary length but output is always of fixed length.
- Values returned by a hash function are called message digest or simply hash values.
- The hash-value is added at the end of message before transmission.
- The receiver re-computes the hash-value from the received message and compares it to the received hash-value.
- If the two hash-values are the same, the message was not altered during transmission.
- Once a hash-function is applied on a message m, the result is known as a message-digest h(m).

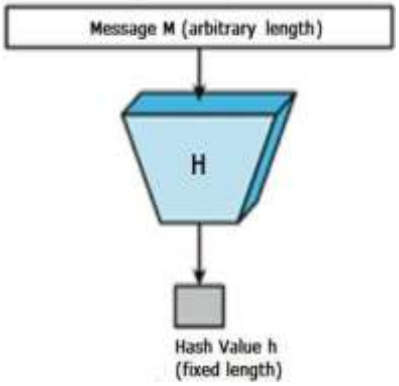

Figure 4.5: Cryptographic hash function

- The hash-function has the following properties :
  1) Unlike the encryption-algorithm, the authentication algorithm is not required to be reversible.
  2) Given a message-digest h(m),it is computationally infeasible to find m.
  3) This is computationally infeasible to find two different messages m_1 and m_2 such that $h(m_1)=h(m_2)$.
- Message-authentication can be implemented by two methods (Figure 4.6):
  1) In first method, a hash-function is applied on a message and then a process of encryption is implemented. At the receiver site, the received message-digest is decrypted and the comparison is made between the decrypted h(m) and the message-digest made locally from the received message. compare it with the one made locally at its site for any judgments on the integrity of the message.
  2) In second method, no encryption is involved. The two parties share a secret key. Hence, at the receiving site, the comparison is made between the received h(m) and the message-digest made locally from the received message.

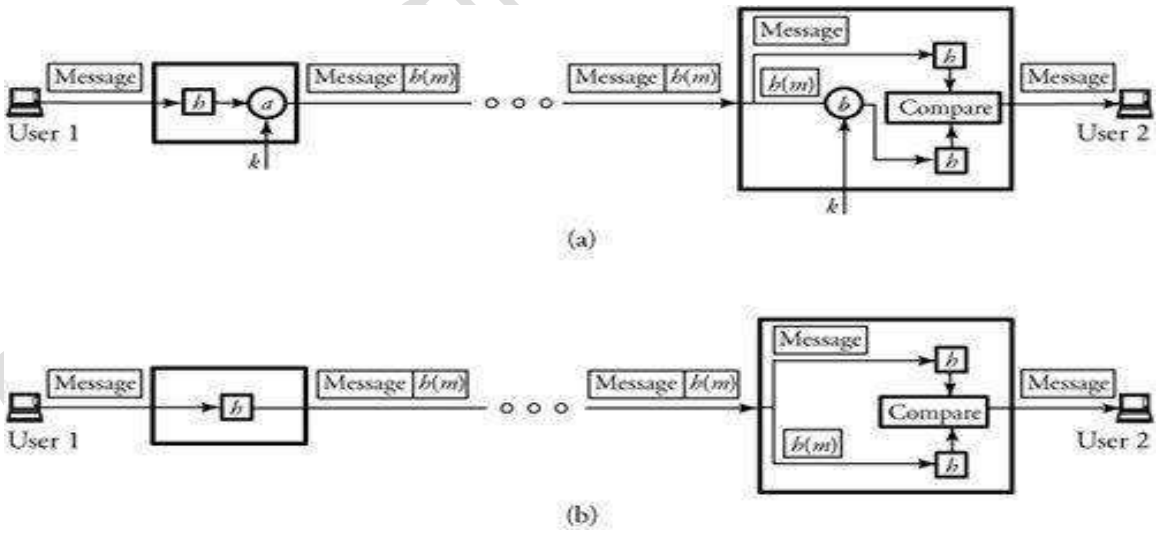

Figure 4.6. Message authentication: (a) combined with encryption; (b) use of the hash function

AUTHENTICATION AND DIGITAL SIGNATURE

- A digital signature on a message is required for the authentication and identification of the right sender.
- RSA algorithm can be used to implement digital signature.
- The message is encrypted with the sender's private key. Thus, the entire encrypted message

serves as a digital signature.

• At the receiving end, the receiver can decrypt the message using the public key. This authenticates that the packet comes from the right user.

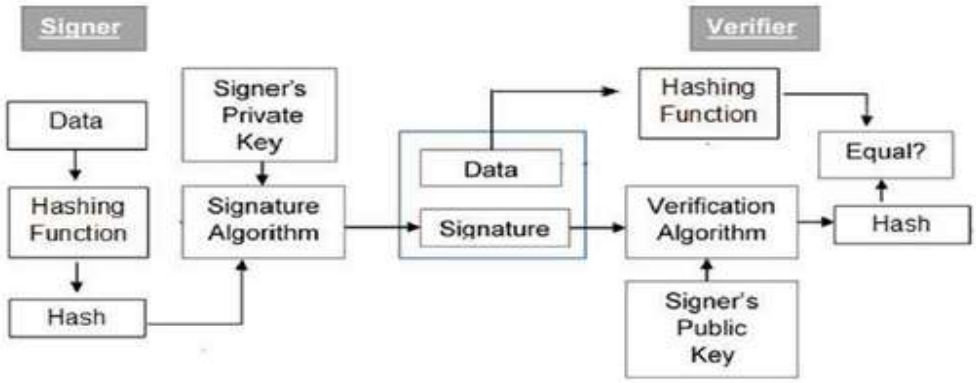

Figure 4.7: Authentication using Digital Signature

FIREWALLS

• This is placed between hosts of a certain network and the outside world (Figure 4.8).
• This is used to protect the network from unwanted web sites and potential hackers.
• The main objective is to monitor and filter packets coming from unknown sources.
• This can also be used to control data traffic.
• This can be a software program or a hardware device.

1) Software firewalls can be installed in home computers by using an Internet connection with gateways.
2) Hardware firewalls
→are more secure than software firewalls
→are not expensive.

• A firewall controls the flow of traffic by one of the following three methods:

1) Packet filtering: A firewall filters those packets that pass through.
If packets can get through the filter, they reach their destinations: otherwise, they are discarded
2) A firewall filters packets based on the source IP address. This filtering is helpful when a host has to be protected from any unwanted external packets.
3) Denial of Service (DOS). This method controls the number of packets entering a network.

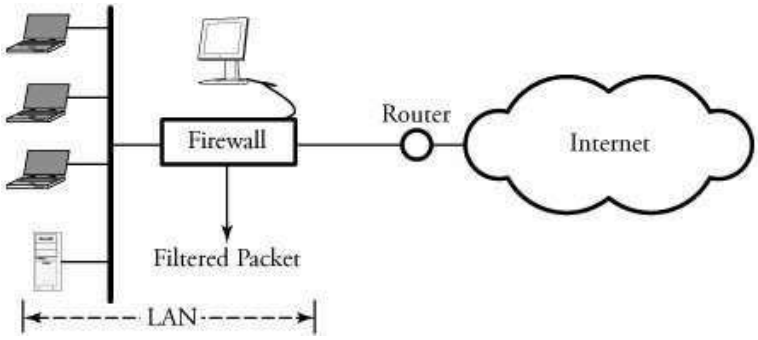

Figure 4.8. A simple configuration of a secured network using

Packet Filtering

Packet filtering is a network security mechanism that works by controlling what data can flow to and from a network.

Packet filtering lets you control (allow or disallow) data transfer based on:

- The address the data is (supposedly) coming from
- The address the data is going to
- The session and application protocols being used to transfer the data

The main advantage of packet filtering is leverage: it allows you to provide, in a single place, particular protections for an entire network.

Proxy server

- In computer networking, a proxy server is a server application or appliance that acts as an intermediary for requests from clients seeking resources from servers that provide those resources.
- The word **proxy** means "to act on behalf of another," and a **proxy server** acts on behalf of the user.
- A proxy server thus functions on behalf of the client when requesting service, potentially masking the true origin of the request to the resource server.

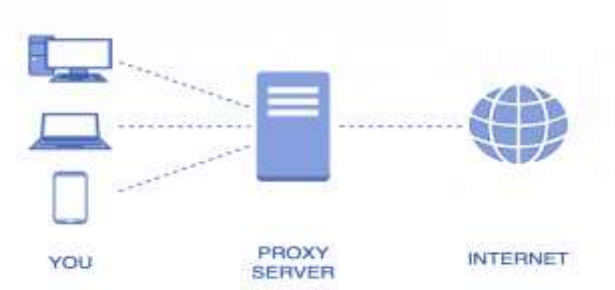

Figure 4.9: Proxy server

- Instead of connecting directly to a server that can fulfill a requested resource, such as a file or web page, the client directs the request to the proxy server, which evaluates the request and performs the required network transactions.
- This serves as a method to simplify or control the complexity of the request, or provide additional benefits such as load balancing, privacy, or security.
- It helps prevent an attacker from invading a private network and is one of several tools used to build a firewall.