Digicoders technologies (P) Ltd.

LECTURE NOTES

ON

INTERNET AND WEB TECHNOLOGY

Unite-3

Compiled by

Team Digicoders
B-36, Sector O, Near Ram Ram Bank Chauraha, Aliganj,
Lucknow Uttar Pradesh 226021

CONTENTS

UNIT-3

Internet Security

INTERNET SECURITY

Internet security is a branch of computer security which comprises various security measures exercisedfor ensuring the security of transactions done online

In the process, the internet security prevents attacks targeted at browsers, network, operating systems,and other applications.

Types of security

Network layer security

• TCP/IP can be made secure with the help of cryptographic methods and protocols.

• These protocols include Secure Sockets Layer (SSL), succeeded by Transport Layer Security (TLS) for webtraffic, Pretty Good Privacy (PGP) for email, and IPsec for the network layer security.

Internet

Protocol Security (IPsec)

• This protocol is designed to protect communication in a secure manner using TCP/IP.

• It is a set of security extensions developed by the Internet Task force IETF, and it provides securityand authentication at the IP layer by transforming data using encryption.

• Two main types of transformation that form the basis of IPsec : the Authentication Header (AH) andEncapsulating Security Payload (ESP).

• These two protocols provide data integrity, data origin authentication, and anti replay service.

Electronic mail security (E mail)

• Email messages are composed, delivered, and stored in a multiple step process, which starts with themessage s composition. When the user finishes composing the message and sends it, the message is transformed into a standard format: an RFC 2822 formatted message

• Afterwards, the message can be transmitted. Using a network connection, the mail client, referred to asa mail user agent (MUA), connects to a mail transfer agent (MTA) operating on the mail server.

• he mail client then provides the sender s identity to the server. Next, using the mail server commands,the client sends the recipient list to the mail server.

• The client then supplies the message. Once the mail server receives and processes the message, severalevents occur: recipient server identification, connection establishment, and message transmission.

• Using (DNS) services, the sender s mail server determines the mail server(s) for the recipient(s). Then,the server opens up a connection(s) to the recipient mail server(s) and sends the message employing a process similar to that used by the originating client, delivering the message to the recipient(s).

Pretty Good Privacy (PGP)

• Pretty Good Privacy provides confidentiality by encrypting messages to be

transmitted ordata files to be stored using an encryption algorithm such Triple

DES or CAST 128

• Email messages can be protected by using cryptography in various ways, such as the following:
  - Signing an email message to ensure its integrity and confirm the identity of its sender.
  - Encrypting the body of an email message to ensure its confidentiality.
  - Encrypting the communications between mail servers to protect the confidentiality of bothmessage body and message header.

Multipurpose Internet Mail Extensions (MIME)

•MIME transforms non ASCII data at the sender s site to Network Virtual Terminal (NVT) ASCII data anddelivers it to client s Simple Mail Transfer Protocol (SMTP) to be sent through the Internet

• The server SMTP at the receiver s side receives the NVT ASCII data and delivers it to MIME to betransformed back to the original non ASCII data.

Message Authentication Code

• A Message authentication code (MAC) is a cryptography method that uses a secret key to encrypt amessage.

• This method outputs a MAC value that can be decrypted by the receiver, using the same secret keyused by the sender.

• The Message Authentication Code protects both a message s data integrity as well as its authenticity.

Authentication & Authorization

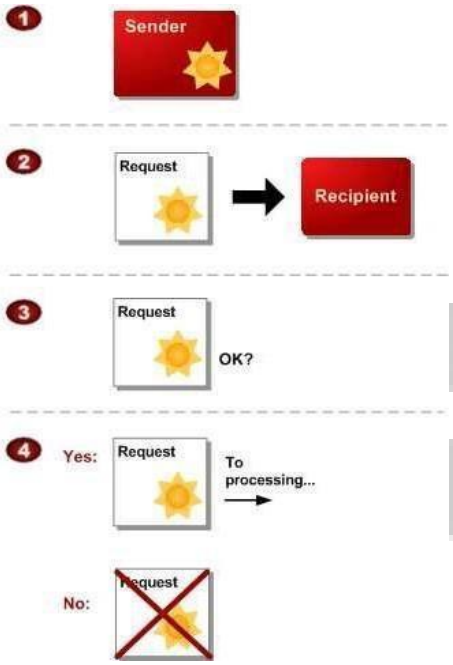
Authentication: It is a process of identifying and verifying who is sending request

Authorization : It is a process to provide access rights to the individuals.

General Process of authentication

1. The sender obtains the necessary credential.
2. The sender sends a request with the credential to the recipient.
3. The recipient uses the credential to verify the sender truly sent the request.
4. If yes, the recipient processes the request. If no, the recipient rejects the request and respondsaccordingly.

The following diagram shows a simplified version of an authentication process.



Types of Authentication

Cybercriminals always improve their attacks. As a result, security teams are facing plenty of authentication-related challenges. The list below reviews some common authentication methodsused to secure modern systems.

1. Password-based authentication

Passwords are the most common methods of authentication. Passwords can be in the form of astring of letters, numbers, or special characters. To protect yourself you need to create strong passwords that include a combination of all possible options.

2. Multi-factor authentication

Multi-Factor Authentication (MFA) is an authentication method that requires two or more independent ways to identify a user. Examples include codes generated from the user's smartphone,Captcha tests, fingerprints, or facial recognition.

3. Certificate-based authentication

Certificate-based authentication technologies identify users, machines or devices by using digital certificates. A digital certificate is an electronic document based on the idea of a driver's license or apassport.

4. Biometric authentication

Biometrics authentication is a security process that relies on the unique biological characteristics ofan individual. Here are key advantages of using biometric authentication technologies:

- Biological characteristics can be easily compared to authorized features saved in a database.
- Biometric authentication can control physical access when installed on gates and doors.
- You can add biometrics into your multi-factor authentication process.

5. Token-based authentication

Token-based authentication technologies enable users to enter their credentials once and receive aunique encrypted string of random characters in exchange. You can then use the token to access protected systems instead of entering your credentials all over again. The digital token proves that you already have access permission.

Firewall

A Firewall is simply a program or hardware device that filters the information coming through theinternet connection into your private network or computer system

The Role of Firewalls

A firewall is a term used for a ``barrier'' between a network of machines and users that operateunder a common security policy and generally trust each other, and the outside world.

There are two basic reasons for using a firewall at present: to save money in concentrating your security on a small number of components, and to simplify the architecture of a system by restrictingaccess only to machines that trust each other.

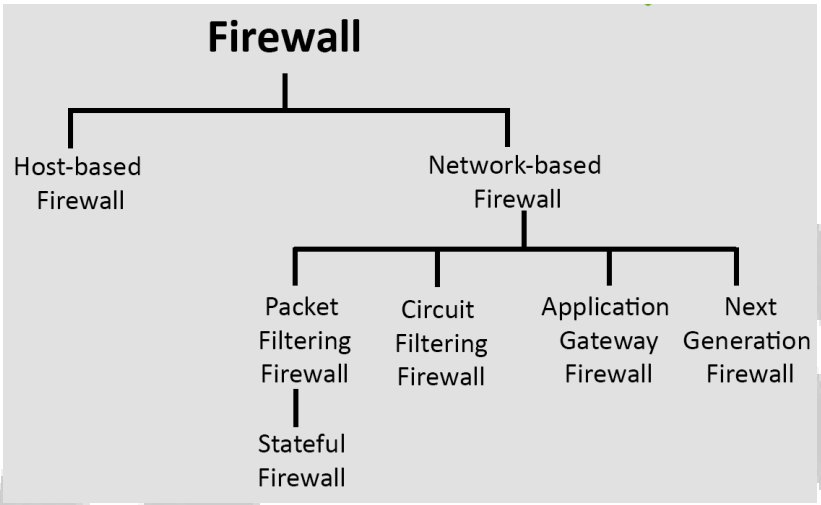
Firewall components

A firewall is a collection of hardware and software that, when used together, prevent unauthorizedaccess to a portion of a network. A firewall consists of the following components:

- **Hardware:** Firewall hardware typically consists of a separate computer or device dedicated torunning the firewall software functions.
- **Software:** Firewall software provides a variety of applications. In terms of network security, a firewallprovides these security controls through a variety of technologies:
    - Internet Protocol (IP) packet filtering
    - Network address translation (NAT) services
    - SOCKS server
    - Proxy servers for a variety of services such as HTTP, Telnet, FTP, and so forth
    - Mail relay services
    - Split Domain Name System (DNS)
    - Logging
    - Real-time monitoring

Types of Firewalls

Firewalls can be divided into two types: host-based and network-based firewalls



1. Host-based Firewalls

A host-based firewall is installed on each network node, which controls each incoming and outgoing packet. It is a software application or suite of applications that come as a part of theoperating system. Host firewall protects each host from attacks and unauthorized access.

2. Network-based Firewalls

Network firewall functions on the network level by employing two or more network interface cards (NICs). In other words, these firewalls filter all incoming and outgoing traffic across the network byusing firewall rules. A network-based firewall is typically a dedicated system with proprietary software installed.

Firewall categories have evolved over the years. In addition to the above broad classifications,here are the five distinct types of firewalls that continue to play a significant role in network security.

A)Packet filtering firewall

Packet filtering firewalls operate in line at junction points where devices such as routers and switches do their work. These firewalls don't route packets but compare each packet to a set ofestablished criteria — such as the allowed IP addresses, packet type, port number, and other aspects of the packet protocol headers. Packets that are flagged as troublesome are dropped.

B)Circuit-level gateway

Circuit-level gateways monitor TCP handshakes and other network protocol session initiation messages across the network as they are established between the local and remote hosts to determine whether the session being initiated is legitimate, whether the remote system is considered trusted. They don't inspect the packets themselves. However, they provide a quickway to identify malicious content

C)Stateful inspection firewall

State-aware devices examine each packet and keep track of whether that packet is part of anestablished TCP or other network sessions. Such provision offers more security than packet filtering or circuit monitoring alone but takes a greater toll on network performance.

Another variant of stateful inspection is the multilayer inspection firewall, which considers the flowof transactions in process across multiple protocol layers of the seven-layer open systems interconnection (OSI) model.

D)Application-level gateway

Application-level gateway, also known as a proxy or a proxy firewall, combines some of the attributes of packet filtering firewalls with those of circuit-level gateways. They filter packets according to the service they are intended for (specified by the destination port) and certain othercharacteristics, such as the HTTP request string.

E)Next-generation firewall (NGFW)

NGFW combines packet inspection with stateful inspection, including a variety of deep packet inspection, along with other network security systems, such as intrusion detection/prevention,malware filtering, and antivirus.

Advantages of firewall:

- Concentration of security all modified software and logging is located on the firewall system asopposed to being distributed on many hosts;
- Protocol filtering, where the firewall filters protocols and services that are either not necessary or thatcannot be adequately secured from exploitation;
- Information hiding, in which a firewall can ``hide'' names of internal systems or electronic mailaddresses, thereby revealing less information to outside hosts;
- Application gateways, where the firewall requires inside or outside users to connect first to the firewallbefore connecting further, thereby filtering the protocol;

Disadvantages of firewall

- The most obvious being that certain types of network access may be hampered or even blocked forsome hosts, including telnet, ftp, X Windows, NFS, NIS, etc.
- A second disadvantage with a firewall system is that it concentrates security in one spot as opposed todistributing it among systems, thus a compromise of the firewall could be disastrous to other less protected systems on the subnet.

Encryption and Decryption

Encryption: Encryption is a process of encoding a message so that its meaning is

not obviousplaintext to ciphertext:encryption

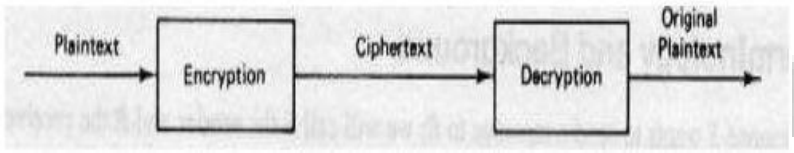
$$C = E(P)$$

Decryption : The conversion of encrypted data into its original form is called Decryption. It isgenerally a reverse process of encryption.

ciphertext to plaintext:decryption:

$$P = D(C)$$

requirement: $P = D(E(P))$



- Encoding : It is the process of translating entire words or phrases to other words or phrases
- Enciphering : It is the process of translating letters or symbols individually
- Encryption : it is the group term that covers both encoding and enciphering

The Elements of Encryption

There are many different ways that you can use a computer to encrypt or decrypt information.Nevertheless, each of these so-called encryption systems share common elements:

Encryption algorithm: The encryption algorithm is the function, usually with some mathematicalfoundations, which performs the task of encrypting and decrypting your data.

Encryption keys: Encryption keys are used by the encryption algorithm to determine how data is encrypted or decrypted. Keys are similar to computer passwords: when a piece of information isencrypted, you need to specify the correct key to access it again.

Plaintext: The information which you wish to encrypt.

Ciphertext: The information after it is encrypted.

Encryption Techniques:

1. Symmetric key encryption
2. Asymmetric key encryption

Symmetric key encryption

- In this encryption techniques, Sender and recipient share a common key
- All traditional schemes are symmetric / single key / private key encryption

algorithms, witha single key , used for both encryption and decryption, since both sender and receiver are equivalent, either can encrypt or decrypt messages using that common key.

Requirements

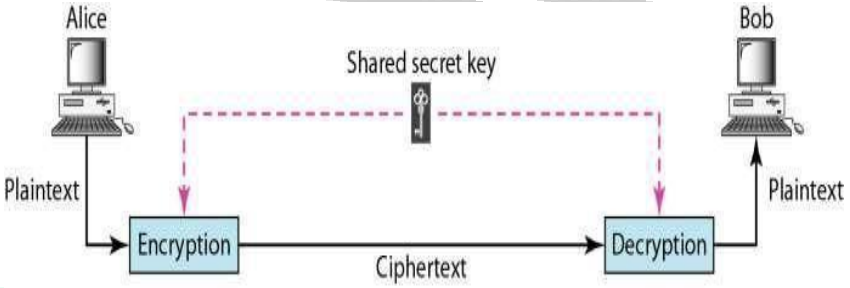
•Two requirements for secure use of symmetric encryption:

–a strong encryption algorithm

–a secret key known only to sender /receiver

$$Y = EK(X)$$

$$X = DK(Y)$$



Here, plaintext X, cipher text Y, key K,encryption algorithm Ek, decryption algorithmDk.

•Assume encryption algorithm is known

•Implies a secure channel to distribute key

- Symmetric encryption is generally more efficient than asymmetric encryption and therefore preferredwhen large amounts of data need to be exchanged.

Advantages:

- It is Simple to implement
- It is Faster

Disadvantages:

- Key must exchanges in secure way
- Easy for hacker to get a key as it is passed in unsecure way.

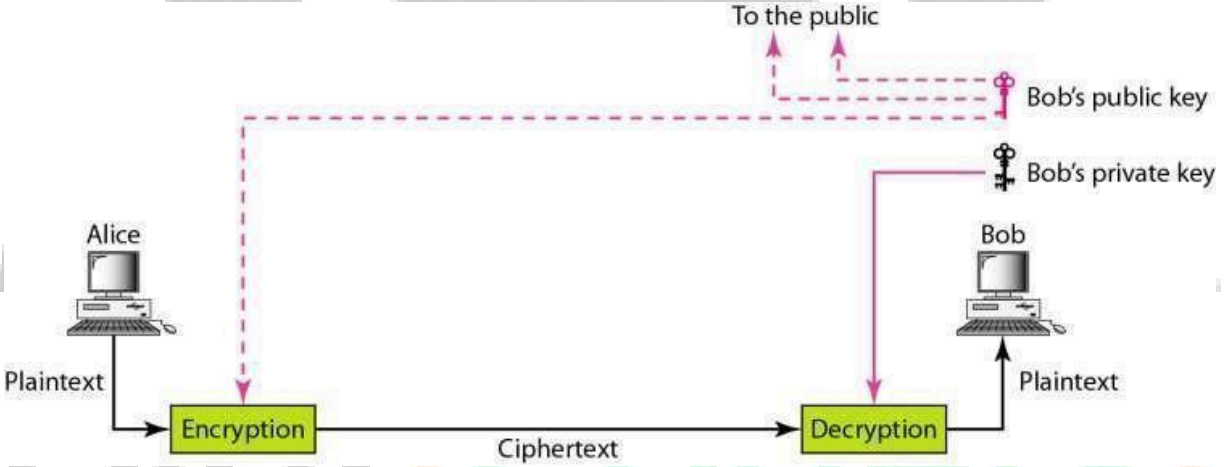
Asymmetric encryption

•Asymmetric encryption use two keys, one to encrypt the data, and another key to decrypt the data.

•These keys are generated together

•.One is named as Public key and is distributed freely. The other is named as Private Key and it iskept hidden.

•Both Sender & Recipient has to share their Public Keys for Encryption and has to use their PrivateKeys for Decryption.



Advantages

1. It is More Secured
2. It is provides more Authentication

Disadvantages

It is Relatively Complex to implement.

Characteristic	Symmetric Cryptography	Asymmetric Cryptography
Key used for encryption/decryption	Same key is used	One key is used for encryption and another for decryption
Speed of encryption/decryption	Very fast	Slower
Size of resulting encrypted text	Usually same as or less than the original plaintext size	More than the original plaintext size
Known keys	Both parties should know the key in symmetric key encryption	One of the keys is known by the two parties in public key encryption
Usage	Confidentiality	Confidentiality, Digital signature

Difference between Symmetric key encryption and Asymmetric keyencryptio

Digi{Coders}