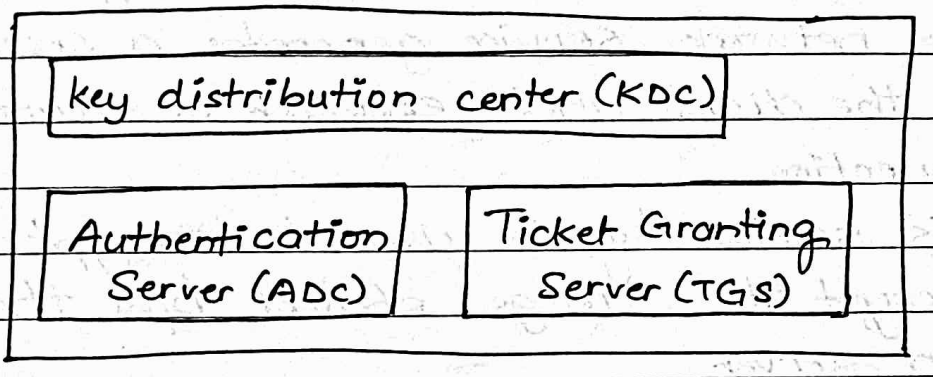
Unit - 3

Kerberos

- It is a network authentication protocol
- Follows client server architechture
- Symmetric key → same key for enc and dec
- Requires a third party for key (KDC) → db of server



Process:-

* Client sends a request to AS, providing its identificatio
* AS verifies client's identify and issues a Ticket Granting Ticket and a session key.
* TGT is encrypted using client's password or secret key and includes client's identity and session key.
* Client decrypts TGT using its secret key.
* The client provides the decrypted TGT to the Ticket Granting Server inorder to gain access to the network.
* Client also includes time stamp in the request.
* TGS verifies the decrypted TGT (which is basically a hash code) and issues a "service ticket" if client is authenticated and authorised to access the requested service.

* The service ticket is encrypted using service's secret key and include client's identity, a timestamp and session key for the client and service to communicate securely.
* Client sends service ticket to the network service, requesting access.
* The network service decrypts the service ticket to validate client's identity.
* The network service generates a session key for the client and establish a secure connection.
* This session key is used to encrypt and decrypt the msgs shared b/w the client and server.

=> Limitations of Kerberos
* Each network service must be modified individually for use with Kerberos.
* Stores all passwords are encrypted with a single key.
* Assumes workstations are secure.
* Doesn't work well with timeshare environment.
* Scalability.

Date: / / 2022

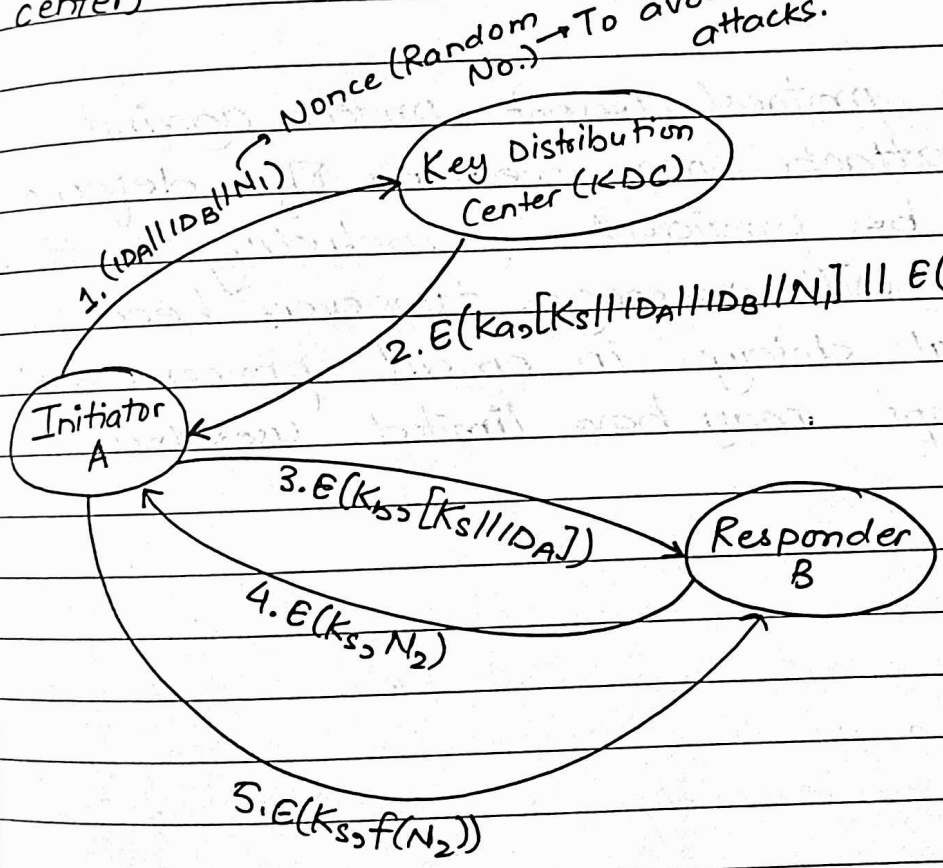
Page No.

classfellow

Needham and Schroeder Protocol

* User KDC → third party authentication
* Symmetric key encryption
* KDC shares a symmetric key b/w all users
* Used for authentication also
* Purpose is to share session key.

* Needham and schroeder propose a protocol for secret key distribution using KDC (key distribution center)



* Secrect keys K_a and K_b are shared b/w A and KDC and B and KDC respectively.
* The purpose of the protocol is to distribute securely a session key K_s to A and B.
* A securely acquires a new session key is Step 2.
* The message in Step 3 can be decrypted and hence understood only by B.
* Step 4 reflects B's knowledge of K_s.

* The purpose of step 4 and 5 is to prevent a certain type of replay attack.
* In particular if opponent is able to capture the message in step 3 and replay it, this might in some fashion disrupt operations at B.

This approach guarantees that only the intended recipient of message will be able to read it. It also provides a level of authentication that the sender is A.

But the protocol doesnot protect against replay attacks. Some measures of defence could be provided by including a time stamp with message. However, because of potential delays in email process, such timestamps may have limited usefulness.

Firewall

A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security ~~ee~~ rules. Its primar purpose is to act as a barrier b/w a trusted internal network and an untrusted external network, to protect the internal network from unauthorised access, malicious activities and potential threats.

Firewalls operate by examining each network packet that passes through them and applying rules to determine whether the packet should be allowed or blocked. These rules can be based on various criteria and by enforcing these rules firewalls can prevent unauthorised access attempts and protect against network based attacks.

Need of Firewalls

1. Acts as a biarrier b/w internal network and external untrusted network, hence protecting the internal network from unauthorized access and malicious activities.
2. Prevents unauthorised access to a network by enforcing access control policies. They can allow or block certain ports or IP addresses based on the predefined rules.
3. Detect and blocks malvares, viruses and other malicious activities. They inspect incoming and outgoing traffic and prevent infected files from entering the network.

4. Firewalls can provide application level control allowing or blocking specific applications or services based on security policies.
5. Firewalls can encrypt data transmitted over data networks, ensures data privacy and data integrity.

⇒ Types of Firewall
* Hardware
* Software

⇒ Hardware Firewall
* Physical device
* Installed b/w modem and computer
* Can be incorporated into a broadband router.
* Protects entire network
* More expensive

Example:- Netscreen, Cisco pix

Advantages:-
* More secure
* Uses very little resources
* Enhanced security
* Easy to disable or remove
* Works independtly
* More reliable

Disadvantages:-
* Installation is complex
* Takes up physical space
* Expensive
* Harder to upgrade and repair.

classfollow

⇒ Software Firewall
* Software Application
* Installed on the computer system.
* Protects a single computer
* Easy to configure, less expensive
Example: Norton Internet Security
MacAfree Internet Security

Advantages:-
* Cheaper or even free
* Easy to install
* Ideal for home/family use
* Takes up no physical space
* Requires no physical change to hardware

Disadvantages:-
* May & sometimes crash
* May be incompatible with system
* Difficult to completely disable
* Incompatible with OS
* Software bugs can be there

Types of Firewall Techniques:-

1. Packet Filter
2. Application Gateway
3. Circuit level gateway
4. Bastion Host

Packet Filter

Inspects individual packets of data based on predetermined rules. They make packet filtering decisions based on the packet header information, allowing or blocking packets accordingly.

It is a basic and efficient technique but does inspect packet content beyond the header.

Drawbacks of packet filter:-

* Rules can be complex
* Logging facility is not provided
* If filtering is not done fully, it may lead to a security loop hole.
* Cannot handle remote procedure calls.

Application Gateway

Operates at the application layer of the network stack. Acts as an intermediate b/w clients and server, analyzing and filtering traffic at the application layer.

Offer enhanced security.

Uses TCP/IP application

Considered to be one of the most secure firewalls.

Advantages:-
* Less complex rules
* Cost effective
* Robust authentication
* Authenticates only those services for which it is configured.

Circuit Level Gateway
Operates at the transport layer.
Instead of inspecting packet content they monitor network connections to ensure they are valid and trusted.
Primarily focused on validating and controlling network connections.

Advantages:-
* Inexpensive than other firewalls
* Provide anonymity to private network
* Monitor TCP's three way handshake.

Bastion Host
Also known as jump host
Highly secured computer or server located in a network's demilitarized zone.
Designed to withstand attacks.
Act as entry point for all external connections.
Have strict security measures in place.
Example: DNS, FTP server, Proxy server

Advantages:-
* Controlled access
* Enhanced security
* Application Proxy

Attacks possible on Packet Filtering:-
1. IP Address Spoofing
Intruder may send an external packet with source IP address as an address of an internal host.

2. Source routing attack
Attacker manipulates the routing information in network packets to bypass normal network security measures.

3. Tiny Fragment Attack
The intruder uses the IP Fragmentation option to creat extremely small fragment and force TCP header information into a seperate packet fragment.

⇒ Four general techniques that firewalls use to control access:-
1. Service Control
Determine the type of Internet service that can be accessed, inbound or outbound. Firewall may filter traffic on the basis of IP address, or port number.

2. Direction Control
Determine the direction in which particular

service requests may be initiated and allowed to flow through the firewall.

3. User Control
Controls access to a service according to which user is attempting to access it.

4. Behaviour Control
Controls how particular services are used
Eg Email Spam Filtering.

Intruder
↳ Hacker or a cracker that tries to get an unauthorised access to a system using various methods.
Three classes of intruders:-
1. Masquerader → An individual who is not authorized to use the computer and who penetrates a system's access control to exploit a users account. This person is an outsider (not a part of the organization)

2. Misfeasor → A legitimate user who accesses data, programs or resources for which access is not authorised or who is an authorised person but misuses the privileges. He/she is an insider.

3. Clandestine User → An individual who seizes supervisory controls of the system and uses this control to steal data or audit the collection. This person can either be an insider or an outsider

Intrusion Detection System

1. Statiscal Anomaly Detection → Involves the collection of data relating to the behaviour of legitimate users over a period of time, then statistical tests are applied on the data to determine whether the behaviour is legitimate or not.
   a) Threshold detection → Involves defining of threshold for frequency of occurence of events.
   b) Profile based → Observing the changes to each user profile.

2. Rule based detection → Defining a set of rules to determine the behaviour is that of an intruder.
   a) Anomaly Detection → Rules are developed to detect changes from previous usage pattern.
   b) Penetration Identification → An expert system approach that searches for suspicious behaviour.

Malicious Software

Softwares that exploit vulnerabilities in a computer system.

Malicious software can be divided into two categories:-

* Dependent → That need a hostprogram
  Eg. Virus, Logic Bombs

* Independent → Self contained programs, can be run by OS.
  Eg. Worms, Bot programs

Date: / / 2022
Page No.

Computer Virus has three parts!-

* Infection Mechanism → The means by which virus replicates and spreads.
* Trigger → Event that determine payload is activated.
* Payload → Involves damage to the system.

Phases of virus :-

1. Dormant Phase → Virus is idle. Not all viruses have this stage.
2. Propogation Stage → Virus places a copy of itself on the program or the system disk.
3. Triggering Phase → Virus is activated to perform the activity or function for which it was intended.
4. Execution Phase → Function is performed.

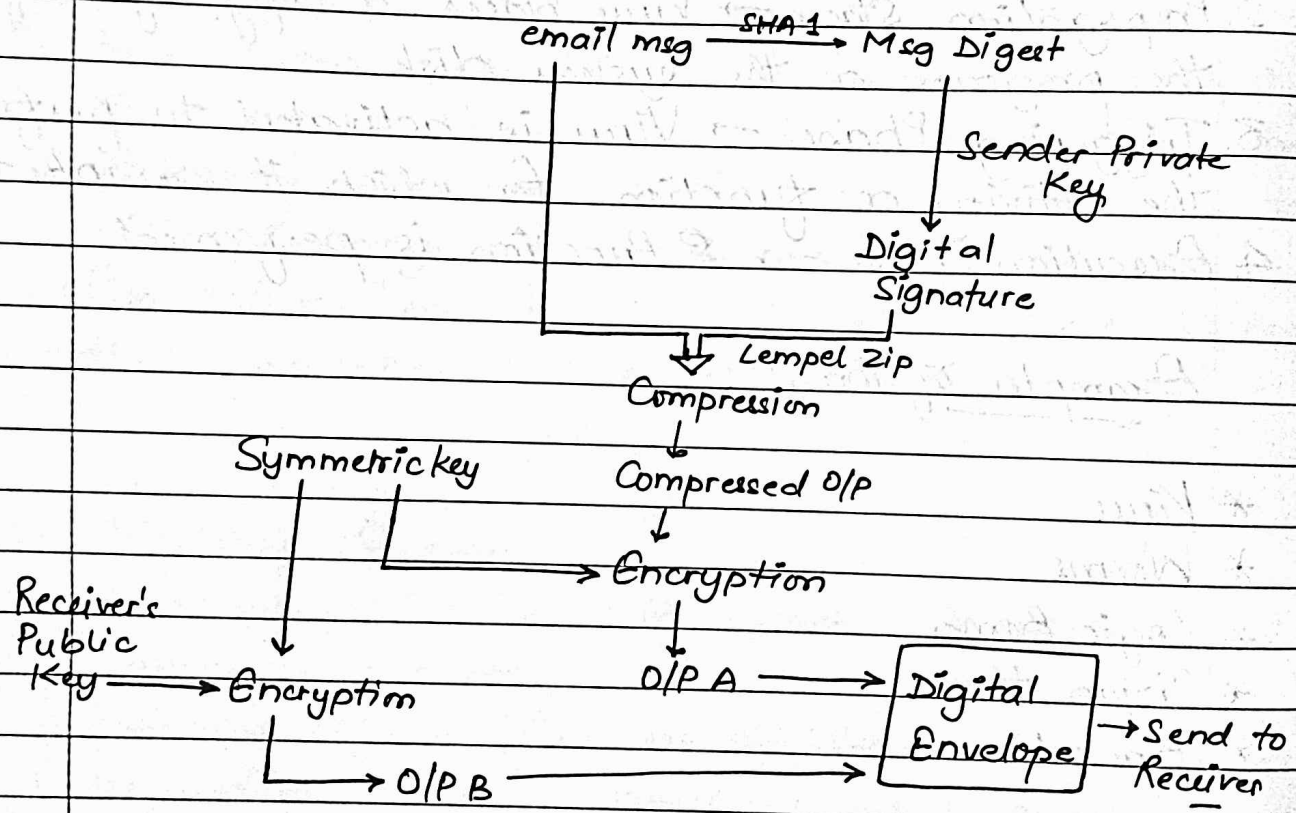
Examples of Threats :-

* Virus
* Worms
* Logic Bomb
* Trojan Horse
* Backdoor.

PGP → Pretty Good Privacy

* Network security concept which provides email security.
* It is an encryption program that provides cryptographic privacy, authentication and integrity for data communication.
* Used for signing, encrypting and decrypting texts, emails, files, directories and to increase the security of email communication.

Working :- uses public and private key cryptography.



CPPL
Date: / / 2022
Page No.

MIME Protocol
↳ Multipurpose Internet Mail Extension

Previously emails could be sent only in NVT 7bit ASCII format.
(i.e. audio/video/images could not be sent)
So, MIME was introduced.
↓
It is basically an add on that allows us to transfer non ASCII data over mail.
↓
other types of data

S/MIME Protocol
↳ Secure MIME

* Encrypts emails and provides security
* Allows us to digitally sign on our email
* Uses assymetric key cryptography.

Functions of S/MIME:-
1. Authentication
2. Message Integrity
3. Non Repudiation
4. Privacy
5. Data Security.

Services of S/MIME:-
1. Digital Signature
2. Message Encryption

classfellow

CPPL
Date: / / 2022
Page No.

Difference b/w PGP and S/MIME:-

	PGP	S/MIME
1.	Designed for procesing the plain texts.	Designed to process emails as wells as multimedia files.
2.	Less costly	Expensive
3.	Good for personal and office use.	Good for industrial use.
4.	Less efficient	More efficient
5.	Less convinient	More convinient
6.	Can be used in VPNs	Can't be used in VPNs.
7.	Doesnot provide authenticaon.	Provides authentication.
8.	Less use of PGP in industry	Widely used in industry.

classfellow

IP Address

Stands for Internet Protocol Address
A unique set of numbers that identifies a device connected to a computer network.
It is like a digital address that helps computers and other devices communicate with each other.
It is made up of four sets of numbers seperated by dots such as 192.168.0.1
There are two types of IP Address → Private and Public
Public IP is assigned by ISP whereas Private IP is assigned by your router.

IPv4

↳ Internet Protocol version 4
IPv4 address consists of two things → Network address and Host Address.
IPv4 addresses are 32 bit integers that have to be expressed in Decimal Notation.
It is represented by 4 numbers seperated by dots each ranges from 0 to 255.

IPv6

↳ Internet Protocol version 6
↳ New version of Internet Protocol
↳ Better than IPv4 interms of complexity and efficiency.
↳ 128-bit IP Address
↳ written as a group of 8 hexadecimal numbers seperated by colon.

Benefits of IPv6:-

1. Larger address space
2. Improved security

3. Simple and more effective header
4. Helps in increasing more traffic on websites
5. Improved and better support for mobile devices.

Difference b/w IPv4 and IPv6:-

	IPv4	IPv6
1.	32-bit	128-bit
2.	End-to-end connection integrity is unachievable.	End-to-end connection integrity is achievable
3.	Security feature dependent on application.	Inbuilt security feature
4.	Address representation in decimal.	Address representation in hexadecimal.
5.	Checksum is available	Checksum not available
6.	Encryption and Authentication facility is not there.	Encryption and Authentication is there.
7.	Header is of 20-40 bytes	Header is of 60 bytes
8.	Can be converted to IPv6	Not all IPv6 can be converted to IPv4.

ESP → Encapsulating Security Payload.

* Involves the encryption of the content and then authenticating the same in an IP Network. Encryption and authentication make the payload extremely secure and safe from any kind of third party. Encryption is performed by authenticated user, similarly decryption is done by the authenticated user.

Working of ESP:-

1. Supports both Transport layer protocols: IPV4 and IPV6
2. Performs the function of encryption in headers of Internet Protocols.

Advantages:-

1. Encrypts data to provide security
2. Maintains secure gateway for data transmission.
3. Maintaining data confidentiality
4. Maintains data integrity
5. Authenticates origin of data.

Disadvantages:-

1. There is a restriction on the encryption method

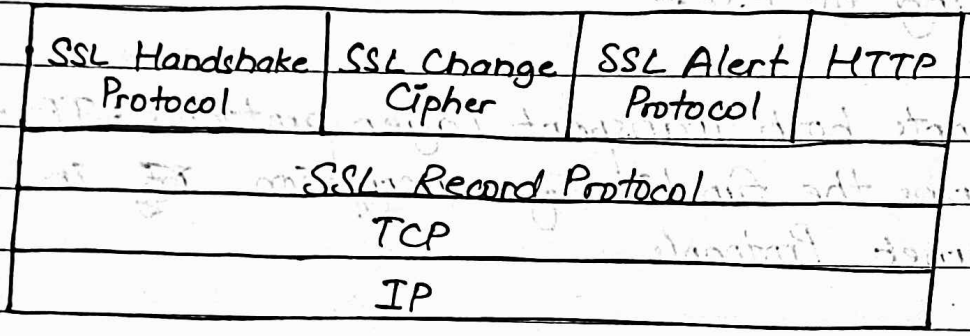
Compiments of ESP:-

Security Parameter	→ size of 32 bits
Sequence Number	→ works as increment calculator / 32 bits
Pay Load Data	→ variable in size
Padding	→ size of 0-255 bytes
Padding Length / Next Header	→ 8 bits each
Authentication Data	→ optional field. / provides integrity

SSL → Secure Socket Layer

* To provide security for communication b/w 2 users
* ensures Integrity, Authentication and Confidentiality
* lies b/w application layer and transport layer of TCP/IP

Protocol Stack of SSL :-

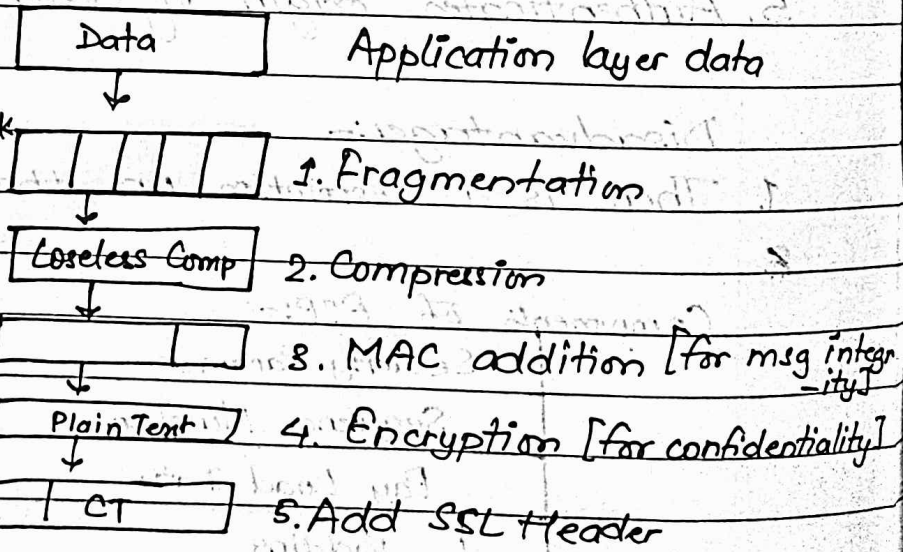


SSL Record Protocol

It has 2 services

1. Confidentiality
2. Message Integrity

Working :-



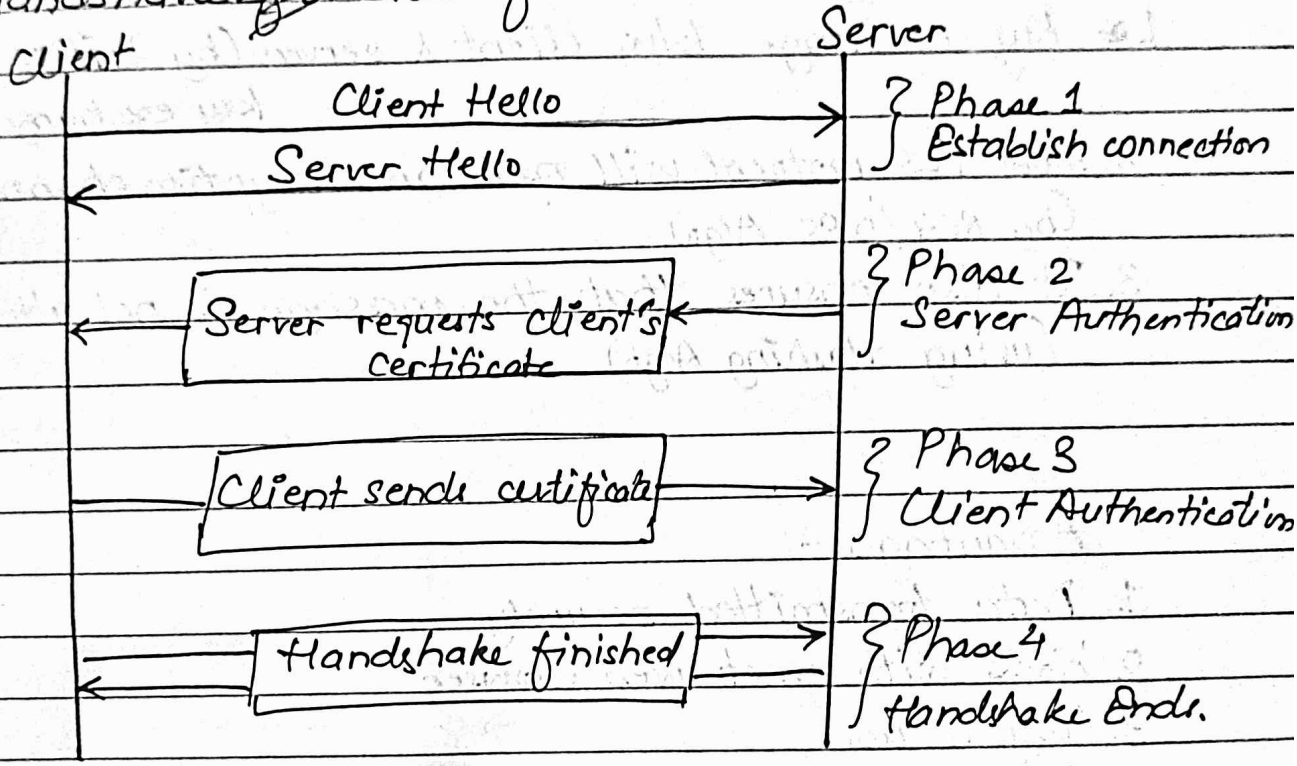
Date: / / 2022
Page No.

SSL Handshake Protocol

* Ensures Authentication
* Key exchange b/w client and server

Working:-

1. Client establishes connection with server
2. Key exchange from server to client } authentication
3. Key exchange from client to server
4. Handshake done from server.



SSL Alert Protocol

* Alerts related to SSL are sent to the clients
* has 2 bytes

byte 1 can have two values → 1 or 2

1 → means warning 2 → means fatal error

byte 2 Specifies the type of error.

TLS → Transport Layer Security
* for providing security in transport layer
* derived from SSL.
* provides a secure connection b/w client and server (No third parties)
* Used by HTTP, SMTP.

Working :-
* Uses client server handshake method
1. Key exchange b/w client & server (by Diffie Hellman key exchange Algo)
2. Now TLS protocol will open an encryption channel (by RC4/DES Algo)
3. It also ensures that the message is not altered (using Hashing Algo)

Advantages :-
1. Data transmitted securely
2. Works with most web browser
3. Easy to use
4. Ease of deployment.

classfollow

Date: / / 2022

Page No.

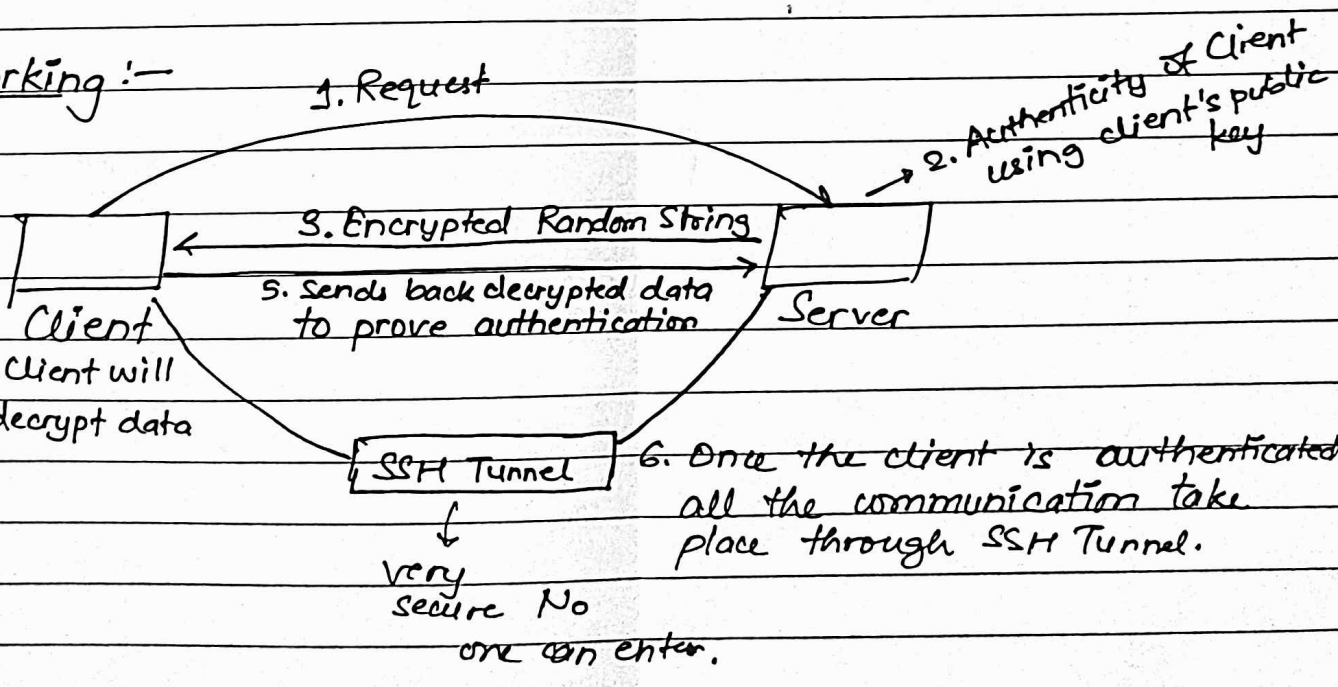
Difference b/w SSL and TLS

	SSL	TLS
1.	Secure Socket Layer	Transport Layer Security
2.	More complex	Simple
3.	Less reliable	More reliable
4.	Slower	Faster
5.	Has been depreciated	Still widely used
6.	Sets up explicit connection.	Sets up implicit connection.

SSH → Secure Shell Protocol

* Protocol for operating network services over an unsecured network.
* Alternative to FTP
* Follows client server Architechture
* Follows Assymmetric key cryptography
* Provides confidentiality and integrity

Working :-



Date: / / 2022

Page No.

Difference b/w HTTP and HTTPS

	HTTP	HTTPS
1.	Data sent as plain text.	Data sent as plain text and cipher text
2.	Uses port 80	Uses port 443
3.	Works at Application layer.	Works at Transport layer
4.	Faster	Slower
5.	Less secure	More secure
6.		