15 m

Page No. :
Date : / /

Chapter - 6.

Intrusion Detection System.

Defn - Intrusion :-

It is defined as any set of actions that attempts to compromise the integrity, confidentiality or availability of resource.

Defn -> Intrusion Detection :-

It is a process of monitoring the events occuring in a computer system or n/w and analyzing for signs of intrusions.

IDS [Intrusion Detection System] are H/w or S/w products that automate the monitoring & analysis process.

Imp

Functions of IDS are :-

1) Monitoring users & system activity
2) Auditing system configuration for vulnerabilities (weakness) & misconfiguration
3) Recognizing knocon attack patterns in system activity.
4) Identifying abnormal activity through statistical analysis.

Page No.
Date : / /

What is Not an IDS?

The following security devices are not IDS's:

1) Antivirus Products such as Avg, Quick heal, NetProtect. etc.
2) Firewalls.
3) Vulnerability assement tools. Eg- Cyber Cop Scanner
4) Security/Cryptographic systems Eg- VPN

Attack can be classified into two

1) Passive Attack
2) Active Attack

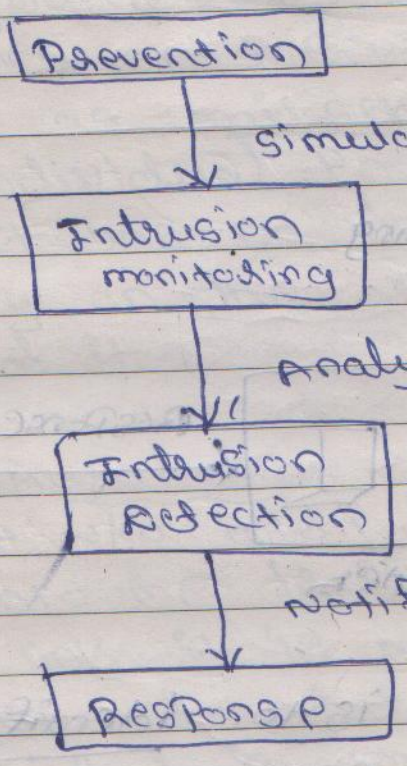
Passive Attack :- It is aimed to gain access to Penetrate the system without modifying (only read no write/modify/delete).

Active Attack :- It is aimed to gain access to penetrate the system by modifying content.

Page No. :
Date : / /

Infrastructure of IDS.

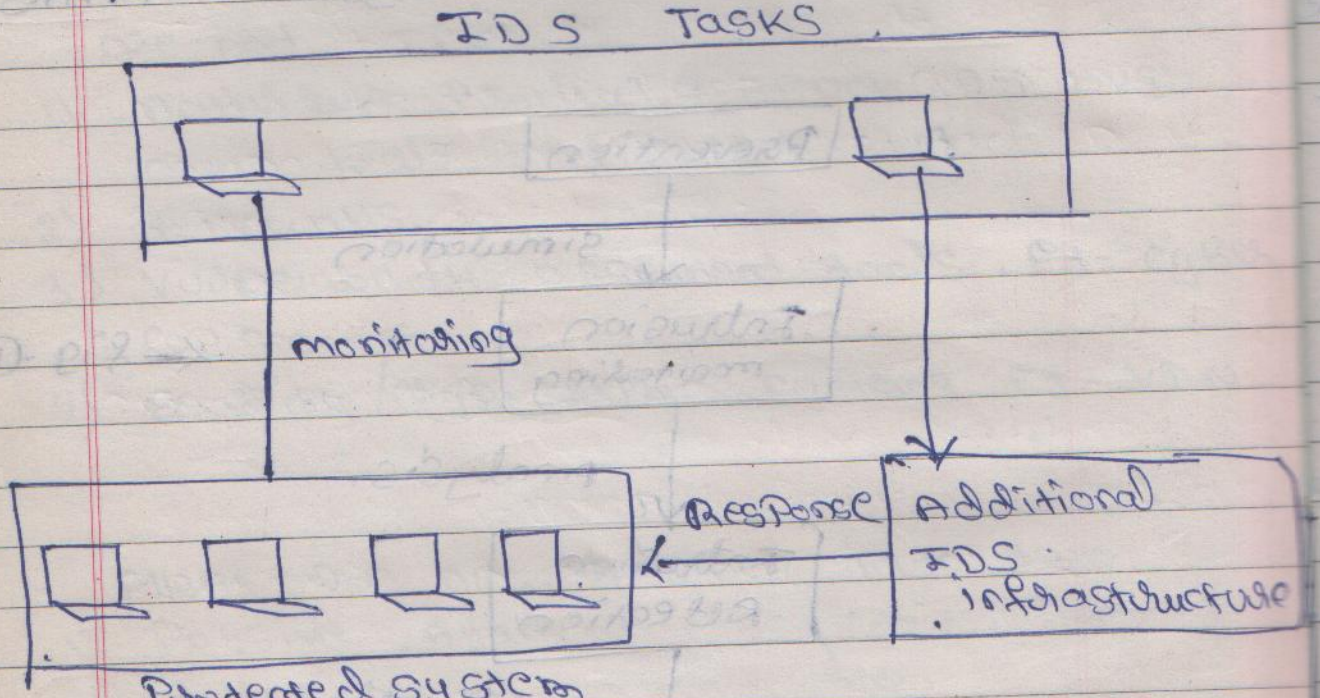
The following Fig-① shows the Intrusion detection system activities.



← fig-①

→ Intrusion Prevention requires investigation of threats.
→ All the Protected system are continously monitored by IDS.
→ Intrusion Detection system examines/Analyse Data generated for detecting possible attacks.
→ once intrusion has been detected, IDS issues alert notification to admin

The following fig ② shows Infrastructure of IDS.



IDS task is to identify intruder.

Classification of IDS.

Intrusion Detection Systems are typically classified in to two main categories, based on how they monitor activity:-

1) Host Based IDS
2) Network Based IDS.

Host-Based IDS → examines activities on the Individual system such as mail server, web server or individual Pc.

It has no visibility into the activity on the n/w or system around it.

N/w Based IDS → Examines activities on the n/w itself. It has visibility only into the traffic crossing the n/w link it is monitoring & has no idea of what is happening on individual systems.

Components of IDS are as follows: (common for Host Based IDS & n/w Based IDS)

1) Traffic collector :-

This component collects activity or events for the IDS to examine For Host-Based IDS this could be log file, or Audit logs or

traffic comming to or traffic sent to

Analysis Engine:- This component examines the collected n/w traffic & compares it to known Patterns of suspicious or malicious activity stored in the signature database.

Signature database:-
The signature Database is a collection of Patterns & definitions of known suspicious or malicious activity.

User Interface & reporting:-
This is the component that interfaces with human elements providing alerts, when appropriate & giving the user means to interact & operate the IDS.

Host-based IDS.

Host-based IDS checks the logfiles audit trails & n/w traffic as they enter into and go out from a particular host computer

* Host based IDS is a system of sensors that are loaded or installed on various m/c like servers, Laptops, workstations and centrally controlled by manager.

So Host-based IDS sensors can be found in 5 basic types & are as follows:

1) log Analyzers
2) Signature-based sensors
3) System call Analyzers
4) Application Behaviour Analyzers
5) File Integrity checkers.

Log Analyzers :- are used to keep track the activity of authorised user on internal system. Accordingly a Process runs on the Server & watches the log files of the user on the system

SR

Page No. :

Date : / /

Signature-based sensors :- are capable of locating attacks as they come into the systems for which it consists of a set of builtin security event signatures that are compared for a match with incoming data traffic

System call Analyzers :- are used to analyse calls between the application & the O.S to identify security events by comparing with Database of signatures.

Application behaviour Analyzers :- are used to examine the application's call to see whether that application is allowed to Perform such calls.

therefore a list of allowed calls for each application must be Prepared before analysing the application's ~~bee~~ behaviour.

File Integrity Checkers :- are used to verify changes if any, in files. For which MAC code / Hash code / Digital signatures ~~are~~ used of file will be verified.

SR
Page No. :
Date : / /

Network - Based IDS :-

It examines the data traffic that passes on - along the N/w cables / wires of the networked system.

It monitors the ~~traffic~~ in-coming & out-going traffic of the organization's internal system

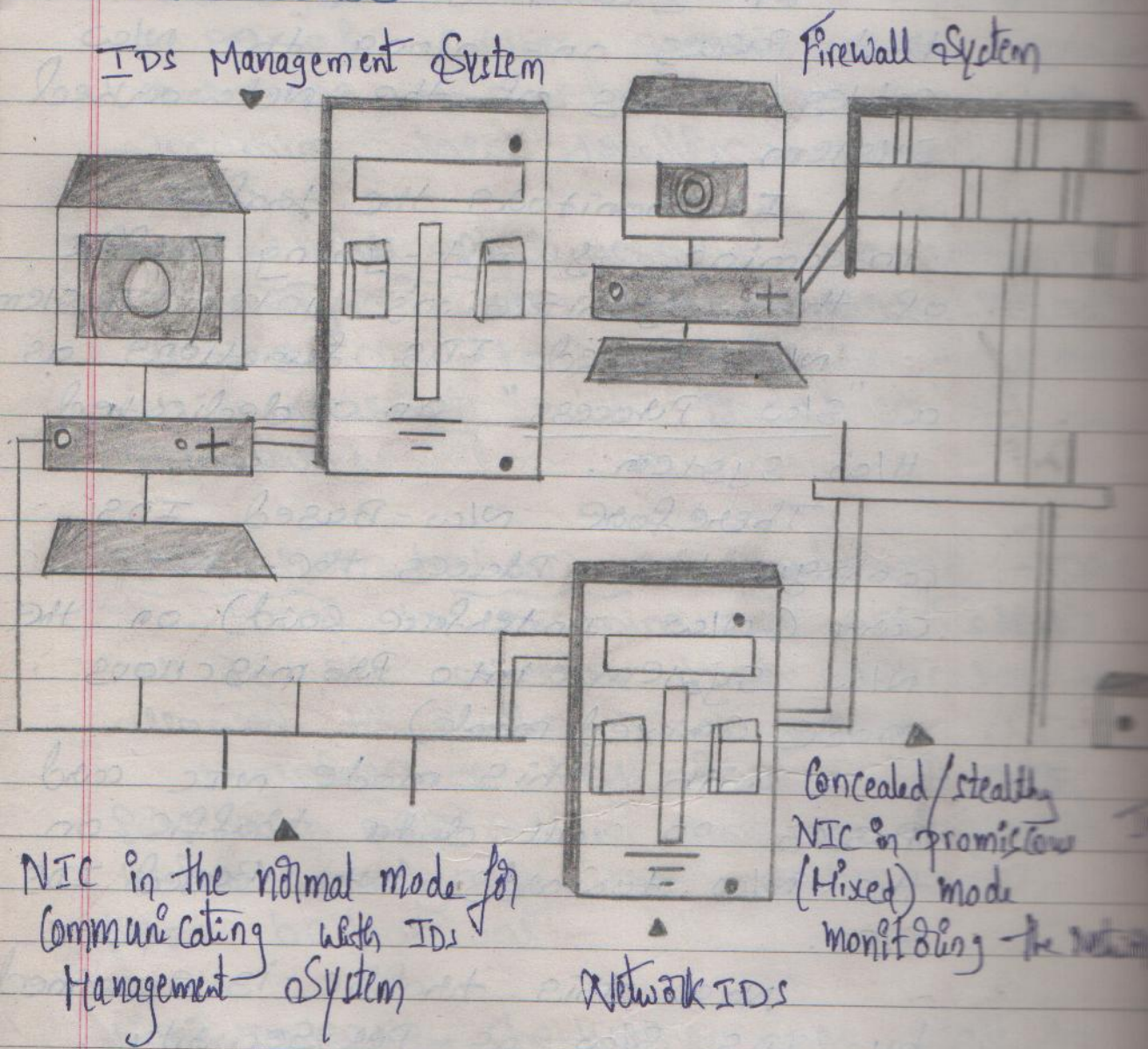
* N/w - Based IDS functions as a "S/w Process" on a dedicated H/w system.

Therefore N/w - Based IDS configuration places the NIC card (N/w Interface Card) on the N/w System into Promiscuous mode (mixed mode).

With this mode NIC card passes on all data traffic on the N/w towards N/w Based IDS S/w.

Now this traffic is examined by IDS S/w as Per Security rules & set of attack signature Patterns to determine whether the traffic of the data is desired & free from Attacks. or not.

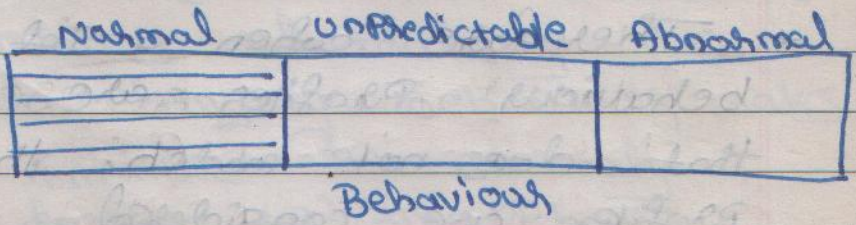
The following fig illustrates the N/w Based IDS configuration with two NIC cards.



Page No. :
Date : / /

Anomaly Vs Signature Detection:

IDS must be capable of distinguishing between normal & abnormal user activities, to detect malicious attacks well in time.



The above diagram shows the behaviour of the user in the system. For this IDS should be capable of distinguishing between normal (secure) & abnormal (anamalous) activities of user

Normal Behaviour Patterns - [Anamaly Detection]

Here in this case- anomaly detectors create well in advance the user profiles that represent normal usage of the system. The intial user profiles are called normal

behaviour Pattern, and are useful in Predicting both user & System behaviour

* Further they use current behaviours data called "event Profiles" to detect a possible mismatch between current user Profiles
* Therefore when a set of normal user behaviour Profiles are given, everything that does not match the stored Profile are considered to be a suspicious action / malicious attack
* Hence these anomaly detector system are known for very high detection efficiency.

Advantages of Anomaly Detection

1) Ability to detect large number of attacks on intrusions
2) Less dependency of IDS on O.S
3) Ability to detect violation of user Privileges (access rights).

Page No. :
Date : / /

Disadvantages of Anomaly Detection Methods :-

1) chances of generating false alarms rate is high.
2) Regular updation of initial user's profile in the Database is required
3) The necessity of training the system for changing behaviour makes a system immune to anomaly detection during training phase.

Misbehaviour Signatures - Signature Detection :-

Signature based (IDS) systems process intrusion information on abnormal / unsafe behaviours called misbehaviour signatures.

The misbehaviour signature are of two types :-

1) Attack signature.
2) Selected - Text strings.

Page No. SR
Date : / /

Attack Signatures – Exhibit action Pattern that can Present a security threat.

Selected Text Strings :- give rise to suspicious / malicious actions for selected Signature text.

The approaches used for signature detection include :

1) verification of Pathology of lower layer Packets.
2) verification of Application layer Protocols.

Advantages :-

1) very low false alarm rate
2) Attack signature Data base construction is simple & easy.
3) Ease of implementation
4) System resource usage is ~~maximum~~ minimum
5) Detection Algorithms are simple.

Page No. :
Date : / /

Disadvantages :-

1) Maintenance & updation of information on new attack type's signatures is difficult.
2) Maintenance of IDS is Time-consuming
3) unable to detect unknown, sever attacks.
4) Regular & continuous updation of attack signature Data Base is necessary.
5) ~~Attack Knowledge~~
   It is more dependent on O.S

20 marks.

Page No. : SR
Date : / /

CO-4 Wireless Security.

Advantages of wireless Network.

1) They allow multiple devices to use the same internet connection remotely as well as shares file and other resources.
2. Using wireless networks is cost-saving when compared to wired network.
3. It is Scaleable - being able to add new user is no more difficult than having to issue a new password and update the server accordingly
4. Portability and Mobility - They also allow mobile device such as laptops, tablets and ipods to move around within N/w area freely

Wireless Application Protocol (WAP).

There are certain limitation with wireless devices such as
→ Small display
→ limited Processing capabilities
→ Low bandwidth

SR

Page No. :

Date : / /

WAP specification adopts the layering concept. Layering is the concept of breaking up the entire communication into discrete pieces. Each piece handles a specific function. The following fig illustrates the WAP Protocol architecture.

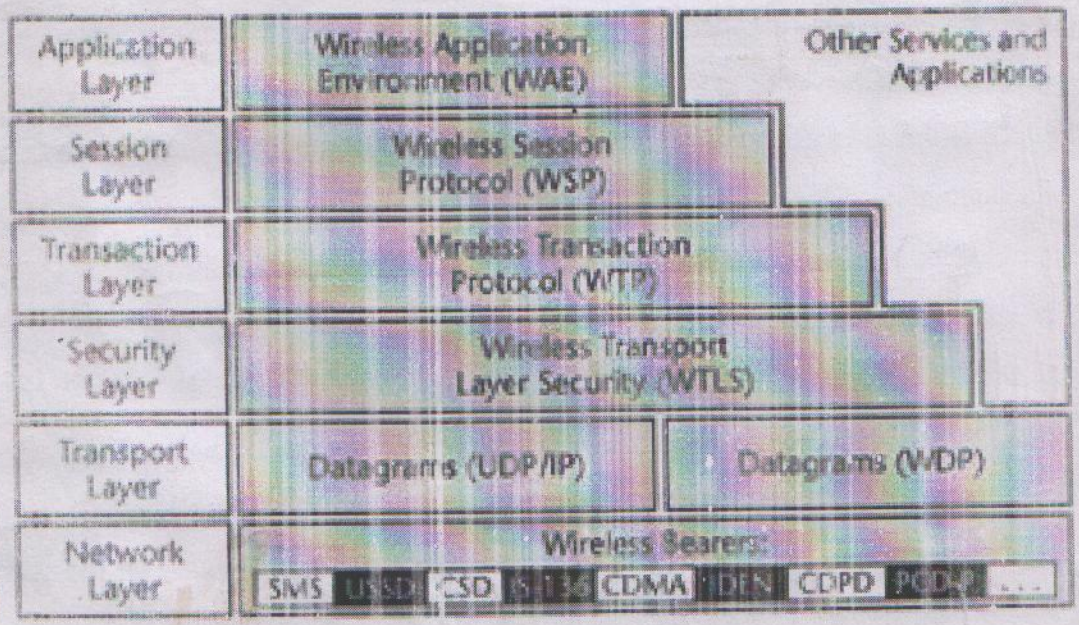


Fig-1 WAP architecture and its relat onship to the OSI model.

WAE (wide less application environment) is to provide interoperable environment to build services. WAE provides

→ user agent : The browser or client program.

Page No. :
Date : / /

→ WML (wireless markup language) :
a lightweight mark up language. Similar to HTML but optimized for use in wireless device.

→ wireless telephony application :- Telephony Services and Programming I/F.

→ content formats :- set of well defined data formats - images, Phone book records, and calendar information.

* WSP (wireless session Protocol) :-

It Provides consistent I/F between two session (client and server)
→ Establish a reliable session from client to server and close it in orderly manner.
→ Exchange content between client and server using compact encoding.
→ Suspend and resume the session.

102

* Note: Bearer service allows the transmission of signals between N/w & H/F

* WTP (Wireless Transaction Protocol)

It runs on top of a datagram service and provides a light weight transaction-oriented protocol that is suitable for implementation in thin clients. WTP allows for interactive browsing applications & supports 3 transaction
(1) unreliable with no result message
(2) reliable with no result message
(3) reliable with one reliable message.

* WTLS (Wireless Transport layer Security)
It is based on TLS Protocol
WTLS provides data integrity, Privacy, authentication, denial-of-service protection. Security is optional.

* WDP (Wireless Datagram Protocol):-
It provides interface to upper layers Protocols from many bearers' service.

SR

Page No.:

Date: / /

Imp

WAP Security :-

In the WAP Specification Security is Provided through the WTLS layer which operates on transport layer.

WTLS Provides ① authentication
② Integrity
③ confidentiality

⇒ Authentication –

In WTLS authentication is Provided with Digital certificates.

However the authentication in WTLS Protocol is optional.

client and Server exchange the Digital certificates and once the certificates are accepted by each other, then the authentication Process is said to be completed.

⇒ Integrity :-

It is a kind of assurance that is required that the data being sent and received is not altered during it transmission.

To ensure the integrity WTLS makes use of MAC.

SR

Page No. :

Date : / /

⇒ Confidentiality :-

It suggests both secrecy and Privacy of data being transmitted.

In wireless technology it is not possible to stop the third Party's listening of data as it has no Physical access control over the medium (air).

To ensure the confidentiality confidentiality - WAP makes use of encryption algorithms such as DES, 3DES, ... etc.

Imp

Wireless LAN:

⇒ wireless LAN consists of computers, workstation, Laptops, N/w components such as bridges, wireless Network Interface cards (NIC), wireless accesspoint.

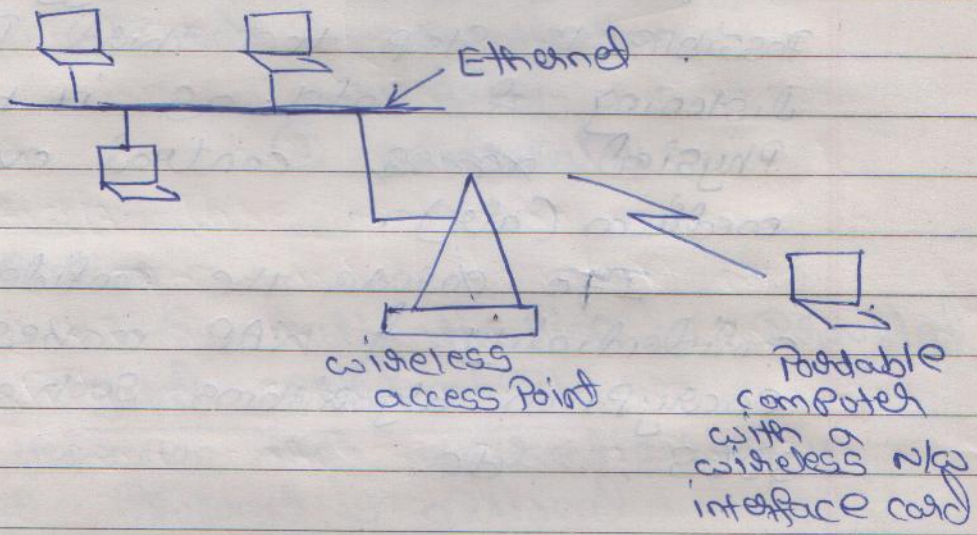
⇒ In wireless LAN the packets will be sent over the air using electromagnetic waves / high frequency radio waves.

SR

Page No. :

Date : / /

The following fig- illustrates the simple wireless LAN :



wireless LAN consists of two Primary components

1) wireless NIC
2) wireless Access Point.

V.V
MP

Page No. :
Date : / /

WLAN Configuration

There are various WLAN configurations

1) Ad hoc network or mesh configuration
2) Infrastructure network.
3) Hot spots
4) Point-to-Point Bridge
5) Point-to-multipoint Bridge
6) Ethernet to wireless Bridge.

⇒ Ad hoc Network.

It's a Peer-to-Peer network, any two stations can communicate each other directly with in the need for wireless access Point.

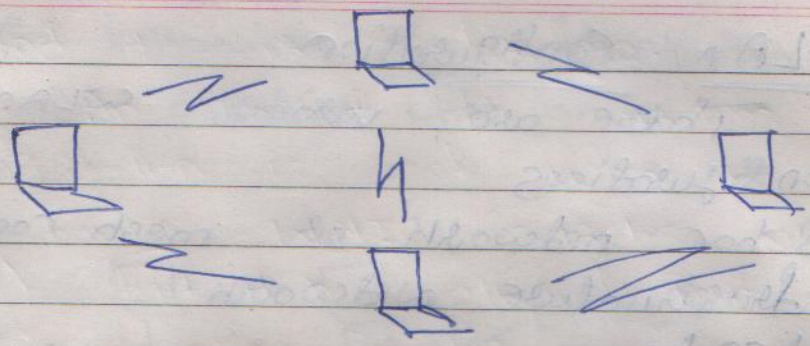
Every node in wireless network must Play the role of a router and Pass-on the messages to peers.

If several nodes try to communi-cate with one another at a same instance the data will be lost.

To overcome this Problem master-slave approach is used by adopting Spokesman election algorithm.

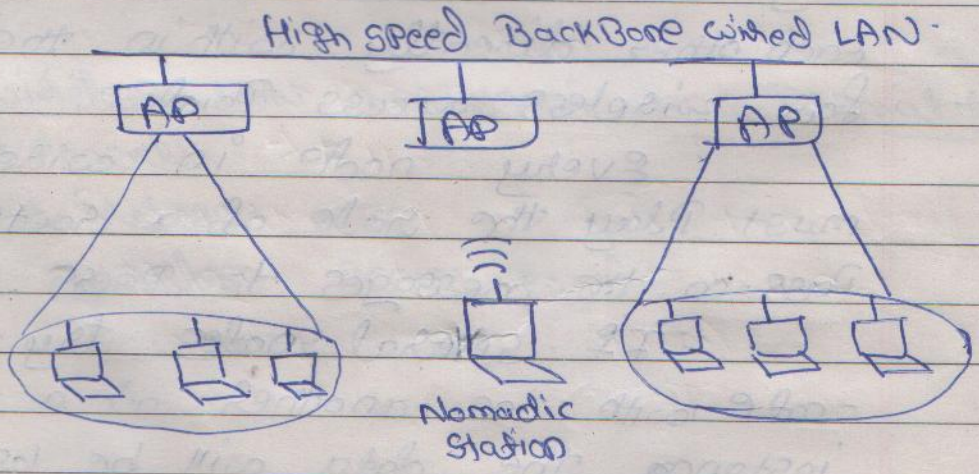
Page No. :
Date : / /

Ad-hoc WAN configuration



=> Infrastructure network.

In infrastructure n/w configuration the wireless LAN establish a connection to the wired LAN via wireless access points.



⇒ Hot SPots :

To use hotSPots. the users Laptop / mobiles / notebook should be configured with wi-Fi (wireless Fidelity) and can send and recieve data anywhere within the range of wireless LAN. ✎.

⇒ Point - to - Point - Bridge :-

A Point-to-Point bridge configuration suggests that a wireless LAN bridge can connect to an wired ethernet LAN directly through a particular access point.

It would interconnect two buildings having their own Ethernet networks.

⇒ Point-to- multiPoint bridge:

when connecting three or more LANs that may be located on different floors in a building or across buildings, the Point - to - multiPoint bridge is used.

Page No. :
Date : / /

=> Ethernet to wireless bridge.

An ethernet to wireless bridge configuration is used when the device is not having WNIC (wireless N/w interface card) but it has ethernet port.

ex:- N/w printer can be accessed over the air using ethernet to wireless bridge configuration.

WLAN Technology consideration :-

The different WLAN technologies are
1. spread spectrum technology
   - DSSS
   - FHSS
2. Narrow band radio technology.
3. orthogonal frequency division multiplexing (OFDM)

SR

Page No. :

Date : / /

WLAN Technology consideration :=

i) spread - spectrum:

Most wireless LAN system use spread - spectrum technology, which is wideband radio frequency technique in which a transmitted signal occupies a bandwidth which is kept much larger than that which is required by a baseband information signal spread - spectrum trads transmission bandwidth for enhanced detectability interfare rejection and security.

(a) := Direct - sequence spread - spectrum technology :=

Direct - sequence spread - spectrum (DSSS) is a spread spectrum modulation scheme that generates a redundant bit pattern for each transmitted bit. The bit pattern, called a chip or chipping code, enables recivers

to filter out signals that do not use the same bit pattern, including noise or interference.

(b) :- Frequency - hopping spread - spectrum technology :-

In the frequency - hopping spread - spectrum scheme (FHSS), the frequency of the data transmission is continously changing (hopping) in time among the 79 frequencies specified in IEEE standard 802.11, fixed time interval over which data are transmited on a given frequency say is called dwell time.

FHSS technology uses bandwidth inefficiently in order to assure high security; therefore FHSS system typically have lower throughput speeds than direct - sequence spread - spectrum (DSSS) system. Slower performing WLAN devices 1 mbps use FHSS.

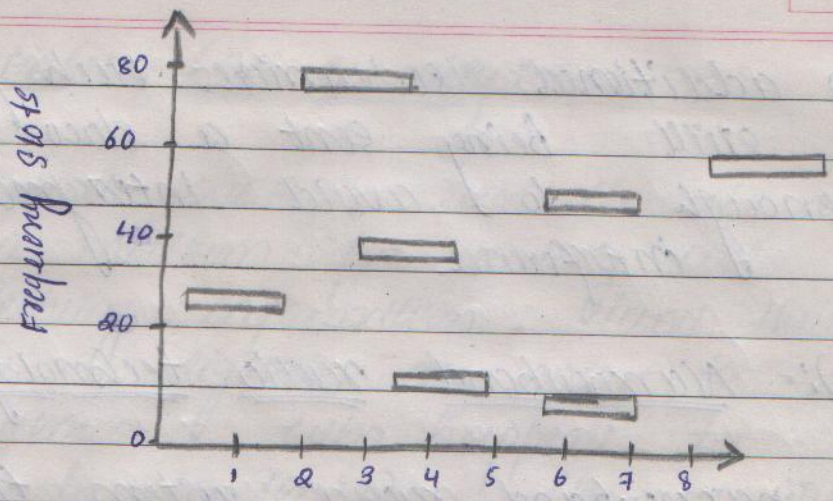


Fig 11.9 : Frequency - hopping spread - spectrum

(ii) :- Orthogonal frequency division multiplexing :- (OFDM) :-

Breaking the signal into parts and transmitting each of the parts on different subcarrier at a different centere frequency. Thus a fast data rate transmission seems to consist of many low data rate transmission rate, ~~without sending the actual data transmission~~ simultaneously on different frequencies.

If higher data rates are required then the signal can be broken up into more part and transmitted

on additional subcarriers, each part still being sent a slow enough to avoid intersymbol interference.

(iii):- Narrowband radio technology:-

A narrowband radio system transmits and receives information on a specific radio frequency.

Narrowband radio keeps the radio signal frequency as narrow as possible just to transmit the information.

The listener is required to tune his receiver to that frequency to receive the transmission.

Undesirable crosstalk between communication channels is avoided by carefully coordinating different users on different channel frequencies.

=> Wireless LAN security :-

Because WLANs use the air as a medium for sending and Reciving information (and thus, the signals are open to anyone who happens to be in range), the security of the transmission is very important to the security of the entire system.

without proper protection for the confidentiality and integrity of information as it travel between workstation and access points, there can be little confidence that the information has not been compromised or that the workstation and access point have not been replaced by an intruder.

=> Access point security :-

configuring the AP for security

is an important starting is an starting point. Ideally, the AP will allow you set a WEP key. make sure this key cannot be easily guessed.

while this will not prevent the cracking of the key, it will make it a little more difficult. If possible, use MAC addresses to limit the workstation that are allowed to connect.

=> workstation security :-

protection for workstation on a WLAN is no different than desktops anywhere else.

Appropriate antivirus software should be used. If the risk is high, personal firewalls should also be deployed on the workstations.

SR

Page No. :

Date : / /

⇒ Safeguarding wireless LANs:-

Several levels of security can be implemented to safeguard the wireless LAN.

The two primary security safeguards that should be considered when implementing wireless LANs are the degree of control that is required in identifying the remote users and the degree to which the N/W traffic must be safeguarded.

Unit - V.

Web Security.

Page No. : SR
Date : / /

⊛ Introduction.

As business enterprises and government agencies's transactions are growing, the individual companies, government departments would like to have more websites and there by Intenet Access is expanding very rapidly by individual end-users, customers and stake-holders.

Defⁿ - web Security is a set of Procedures, Practices and technologies for Protecting web servers, web users and their surrounding organizations against unexpected behaviour.

⊛ client / server Architecture :-

The WWW or web is basically an infrastructure of information. This information is stored on web server and it uses the Intenet to transmit data around the world. These servers are special Programs that allow information to be transmitted to remote computers which are running a web ~~servers~~ browser. as shown in fig

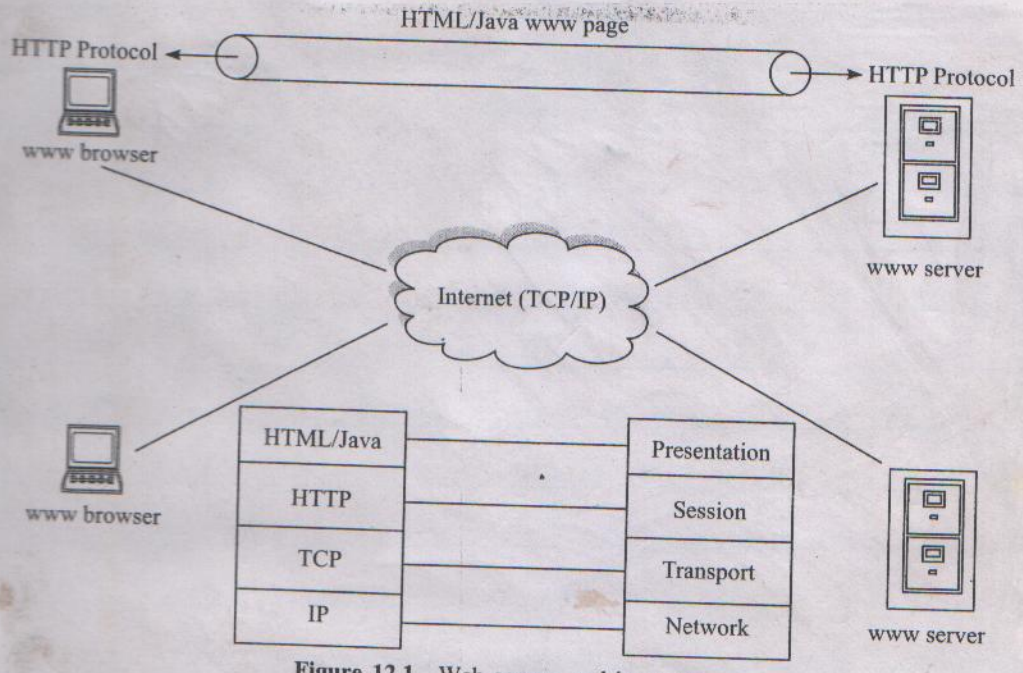


Figure 12.1 Web servers and browsers.

The client access services from the server. These servers can be either local or available through a global N/w connection. The Local connection requires LAN, but global connection requires connection to an Internet service Provider (ISP)

Page No. : SR
Date : / /

✱ Security considerations and Threads.

The WWW is a client-server application running over the Internet.

⇒ This web is prone to attacks on the web server over the Internet.

⇒ web security threads is in terms of
(1) web browser
(2) web server
(3) N/w traffic between browser and server.

web security Threads :-

The table shows the types of security threads faced in using the web

Page No. :
Date : / /

Table : Comparison of Threats on the web

Category	Threats (ಬೆದರಿಕೆಗಳು)	Consequences (ದುಷ್ಪರಿಣಾಮಗಳು)	Counter measures (ಪ್ರತಿಬಂಧಕೋಪಾಯಗಳು)
1. Integrity	• Modification of user data. • Trojan horse browser. • Modification of memory. • Modification of message traffic in transit.	• Loss of information. • Compromise of machine. • Vulnerability to all other threats.	Cryptographic checksums. Eg: MAC, one-way hash etc
2. Confidentiality	• Eavesdropping on the net. • Theft of info from server. • Theft of data from client. • Info about network configuration. • Info about which client talks to server.	• Loss of information. • Loss of privacy.	Encryption, Web proxies.
3. Denial of Service	• Killing of user threads. • Flooding machine with bogus requests. • Filling up disk / memory. • Isolating machine by DN attacks.	• Disruptive. • Annoying. • Prevent user from getting work done.	Difficult to prevent.
4. Authentication	• Impersonation of legitimate users. • Data forgery.	• Misrepresentation of user. • Belief that false information is valid.	Cryptographic techniques.

Page No. : SR
Date : / /

(*) Web traffic security Approaches.

There are number of approaches to Provide web security. These security Providing approaches differ with respect to their scope of applicability and their relative location within the TCP/IP Protocal Stack.

(1) At N/w layer with IPSec.
(2) At Transport layer with SSL / TLS.
(3) At Application layer with S/MIME.

The following fig illustrate this difference.

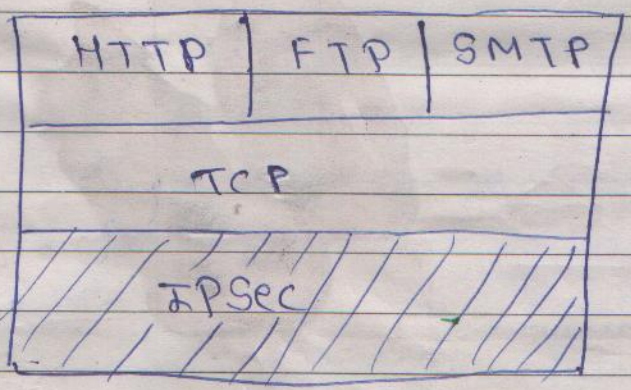


fig (a) At n/w layer.

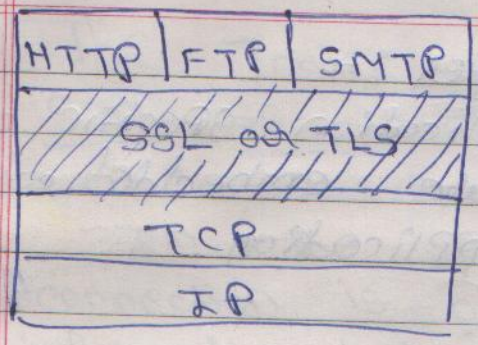


fig (b) At Transport layer.

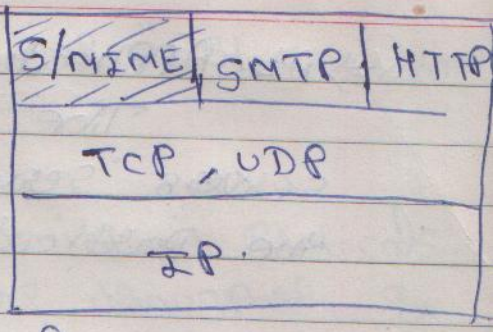


fig (c) At Application layer

⇒ At n/w layer :- The advantage of using IPSec is that it is transparent to end users. Further IPSec includes filtering capability so that only selected traffic need incur the overhead of IPSec processing.

⇒ At Transport Layer :-
The SSL/TLS can be implement above the TCP. SSL can be embedded in specific application packages itself. Ex :- Netscape and Microsoft Explorer browsers come equipped with SSL, Also web servers have implemented this protocol.

Page No.: SR
Date: / /

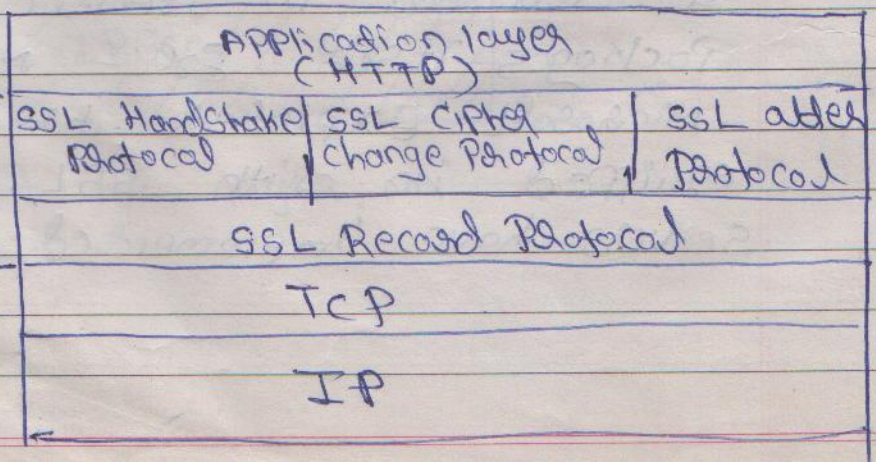
⇒ At Application layer :-
The application specific web ~~servers~~ services are embedded within the particular application.

(*) SSL / TLS for Secure web services.

⇒ SSL (Secure Socket layer) was developed by Netscape in 1995 to Provide secure and authendicated connections between browser & server

⇒ SSL Provide transport layer security as show in fig (b)

⇒ SSL is not a single Protocal, or even a single layer, SSL is composed of four Protocals in two layer as shown below.



The SSL Protocal stack.

fig-(b)

Imp.

Page No.:
Date: / /

⊛ The Twin concepts of "SSL connection" and "SSL session" :—

In the SSL family of Protocols, a connection is one-time transport of information between two nodes in a communication N/w.

* A connection constitutes a Peer-to-Peer relationship between the two nodes.
* Being one-time, connections are transient.
* Every connection is associated with a session.
* A session is an association between client and a server.
* A session is created by the SSL handshaking Protocol.
* A session can consist of multiple connection.

Page No. :
Date :

(*) SSL Session State :-

An SSL session state is characterized by the following Parameters.

1) Session identifier : An arbitary byte sequence choosen by the server to identify an active or resumable session state.

2) Peer certificate : An X509.V3 certificate of the peer. This

3) Compression method : The algorithm used to compress the data prior to encryption

4) Cipher spec : Specifics of the bulk data encryption algorithm and the hash used for MAC calculation

5) Master secret : A 48-byte secret shared between the client and the server.

6) Is resumable : A flag indicating whether the session is allowed to initiate new connections.

Imp V.V.V.

Page No. :
Date : / /

(*) SSL connection State:

An SSL connection state is characterized by the following parameters:

1. Server write MAC secret :- The secret key used in calculating the MAC value for the data sent by the server.
2. Client write MAC secret : The secret key used in calculating the MAC value for the data sent by client.
3. Server write key :- The symmetric-key encryption key for data encrypted by the server and decrypted by the client.
4. Client write key :- The symmetric-key encryption key for data encrypted by client and decrypted by server.
5. Initialization vectors: An initialization vector for each key used by a block cipher operating in the CBC Mode is maintained. The IV are initialized by

SSL Handshake Protocol.

6) Sequence numbers:- Each party maintains seperate sequence numbers for the transmitted and received message through each connection. Sequence nor may not exceed $2^{64} - 1$.

(*) SSL Record Protocol:-

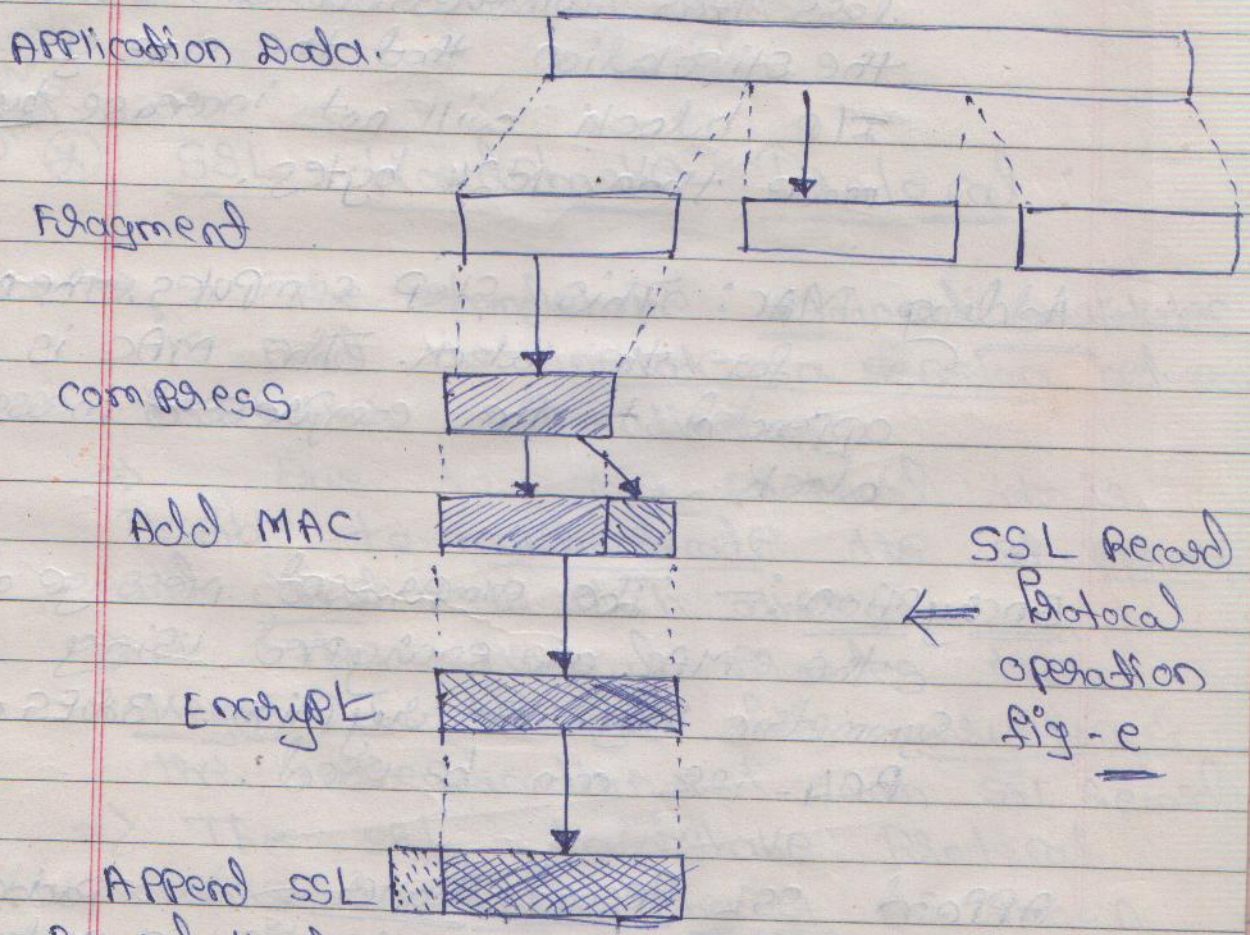
The SSL record Protocol sits directly above the TCP Protocol as shown in fig (d) (previous page). This Protocol provides two services:

1) confidentiality
2) Message Integrity.

This Protocol is incharge of taking the data from server to client and from client to the server. , fragmenting the data into blocks, applying authentication and encryption primitives to each block and handling the block to TCP for transmission over N/w. On the recieved side the blocks are decrypted, verified for message integrity, reassembled and

delivered to the higher-level Protocol.

The operation of the SSL Record Protocol is shown in fig-e. It consists of following five steps:



SSL Record Protocol operation
fig-e

Page No. :
Date : / /

Fragmentation :- The message is fragmented into block whose length does not 2^{14} (16384) bytes.

Compression :- This optional step requires loss less compression and carries the stipulation that the size of I/P block will not increase by more than 1024 bytes.

Adding MAC : This step computes the MAC for the block. The MAC is appended to the compressed message block.

Encryption :- The compressed message and the MAC are encrypted using Symmetric key encryption. 3DES or RC4-128 can be used.

Append SSL Record Header :- Finally, an SSL header is ~~prepended~~ added to the encrypted. The header consists of ① 8-bit for declaring the content type
② 8-bits for declaring the major

version used for SSL.

③ 8-bits for declaring the minor version used.

④ 16-bits for declaring the length of compressed Plaintext.

The length of Record is not to exceed 32767 bytes.

⑧ SSL Handshake Protocol :-

⇒ The handshake Protocol ~~constitutes~~ is used to initiate a session between the server and client.

⇒ Due to this Protocol, it is possible to authenticate the server and client to each other.

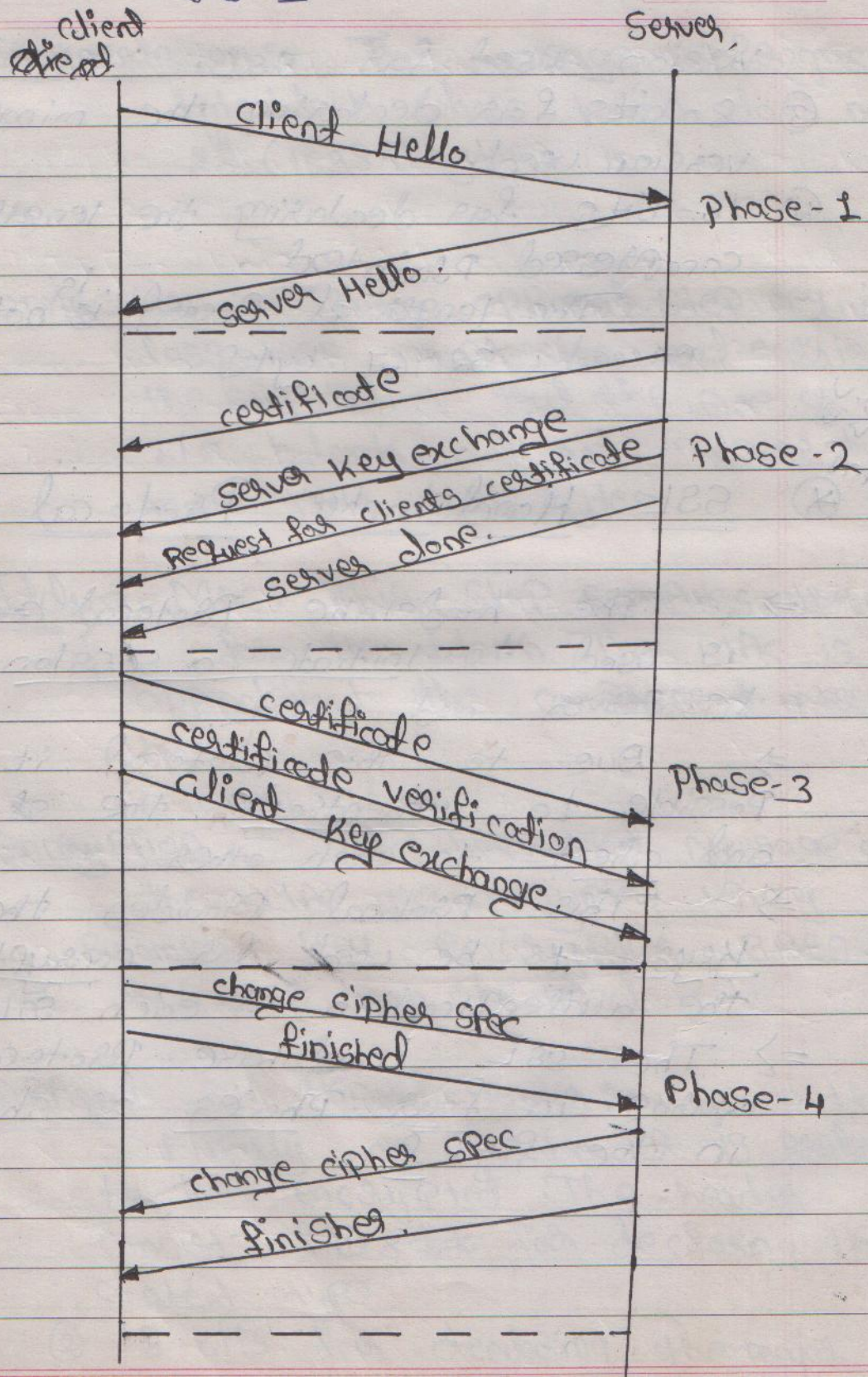
⇒ This Protocol Provides the keys to be used for encryption & the authentication of each SSL Record

⇒ The SSL handshake Protocol works in four Phases as shown in the fig-1

SSL HandShake Protocol action.

Page No. :
Date : / /

fig - 1



The hand shake Protocol consists of a series of messages exchanged by client and server, which can be viewed in 4- Phases: -

Phase-1: Establish security capabilities - this Phase is used by client to initiate a logical connection and to establish the security capabilities that will be associated with it such as - Protocol version, session ID, cipher suit, compression method, and initial random numbers.

Phase-2: Server may send certificate, s. key exchange, and request certificate. server signal end of hello message Phase.

Phase-3: client sends certificate if requested client send key exchange. client may send certificate verification.

Phase-4: Finish - this Phase completes the setting up of a secure connection. The client sends change cipher suit.

Page No. SR
Date : / /

(*) Secure HyperText Transfer Protocal (S-HTTP).

The native Protocal that web clients and servers use to communicate is HTTP. This Protocal is ideal for open communication. S-HTTP works in conjuction with HTTP to Provide Private and secure transactions between clients and servers.

(*) Secure Electronic Transaction (SET)

SET is an open encryption and security specification designed to Protect credit card transactions on the Internet.

SET Provides three services:

1) Provides a secure communications channel among all parties invalved in a transaction.
2) Provides the trust by the use of X.509 V3 digital certificates
3) Ensures Privacy.

Page No. : SKT
Date : / /

Business Requirements :-

i) Provide authentication that a cardholder is legitimate user of a credit card account.
ii) Provide authentication that a merchant can accept credit card transactions through its relationship with a financial institution.
iii) Provide confidentiality of Payment and ordering information.
iv) Ensures the integrity of all transmitted data.
v) Ensures the use of best security & system design techniques to protect all legitimate parties in an E-commerce transaction.
vi) Create a protocal that neither depends on transport security mechanism
vii) Facilitate interoperability among S/w and N/w Providers.

SR

Page No. :

Date : / /

Key Features :-

To meet the business requirements SET incorporates the following features.-

1) cardholder account authentication
2) merchant authentication

uses X.509v3 digital certificates with RSA signatures.

3) Integrity of data - uses RSA digital signature with SHA-1

4) confidentiality of information:
uses conventional encryption AES.

(*) SET Participants :-

12.6.2 SET Participants

Figure 12.7 indicates the participants in the SET system, which include the cardholder and the merchant, in addition to the issuer, acquirer, payment gateway, and a certification authority.

Cardholder: In the electronic environment, consumers and corporate purchasers interact with merchants from personal computers over Internet. A cardholder is an authorized holder of a payment card (e-g. Master card, Visa) that has been issued by an issuer.

Merchant: A merchant is a person or organization that has goods or services (offered by web site or by electronic mail) to the cardholder.

Issuer: This is the financial institution, such as a bank that provides the cardholder with the payment card.

Acquirer: This is also financial institution that establishes an account with a merchant and processes payment card authorizations and payments.

Payment gateway: This is the function operated by the acquirer or designed third party that processes merchant payment messages. The payment gateway interfaces between SET and the existing bankcard payment networks for authorization & payment functions.

Certification Authority (CA): This is an entity that is trusted to issue X.509 V3 public-key certificates for cardholders, merchants and payment gateways.

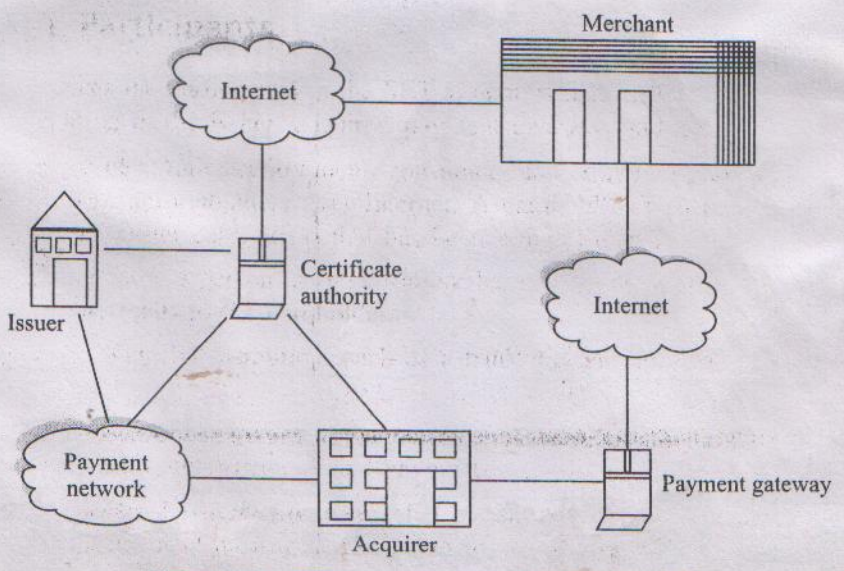


Figure 12.7 SET components and their relationships.

V.V. V.V. Imp

Page No.: SR
Date: / /

SET Transactions :-

1. The customer opens an account and obtains a credit card account with a bank that supports electronic payment and SET.
2. These customers receive a certificate after suitable verification of identity. It establishes a relationship between the customer's key pair and the credit card.
3. Merchants have certificates consisting of one key for signing messages and one for key exchange. They also need a copy of the payment gateway's public key certificate.
4. The customer places an order, which is accepted by the merchant. The order form returned from the merchant includes the items, the cost, and an order number.
5. The customer receives the merchant certificate.
6. The customer sends the order, payment, and this certificate to the merchant.
7. The merchant requests payment authorization through the payment gateway.
8. The merchant provides the customer with order confirmation.
9. The merchant ships the product or service.
10. The merchant request payment gateway, which handles all payment processing.

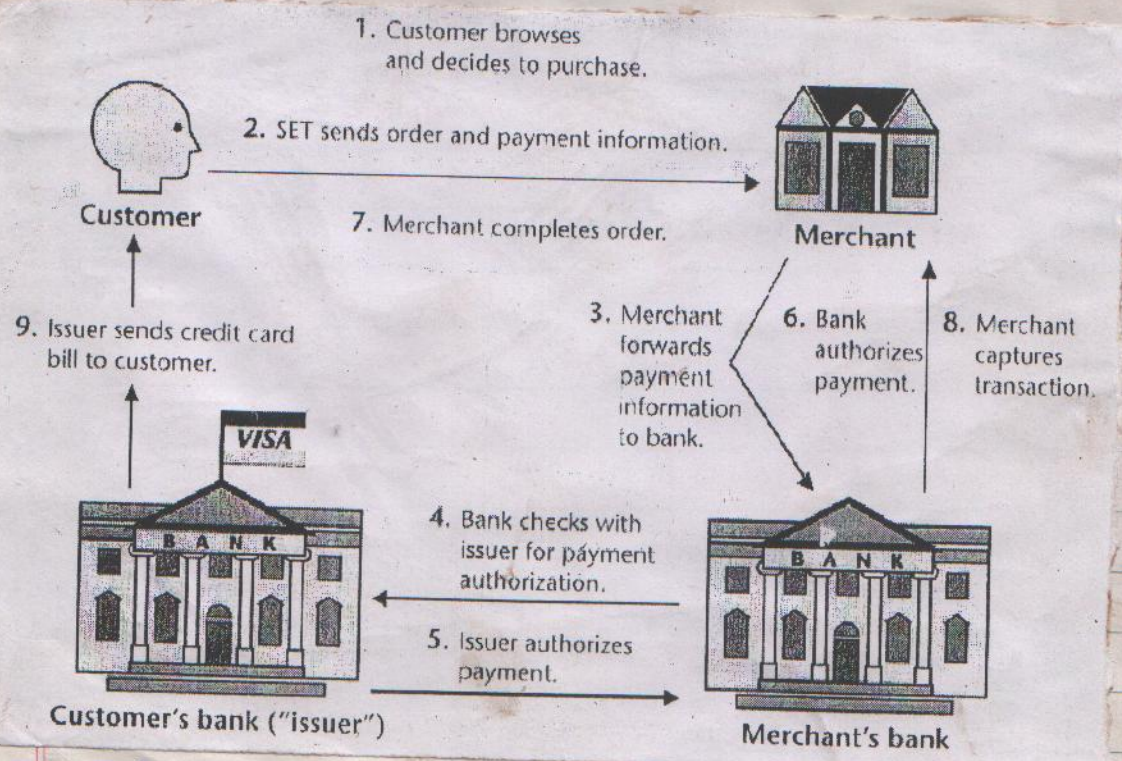


fig : SET Transactions flow.