# Chapter 5

# Web Security

# 5.1 Intruders

- **An Intruder (Hacker or Cracker) is a person who attempts to gain unauthorized access to a system, to damage that system, or to disturb data on that system.**

- **Three Classes Of Intruders:**

1. **Masquerader:**
2. **Misfeasor:**
3. **Clandestine user:**

# IDS (Intusion Detection System)

- **An IDS is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.**
- **Intrusion**
  - A set of actions aimed to compromise the security goals, namely Integrity, confidentiality, or availability, of a computing and networking resource.
- **Intrusion detection**
  - The process of identifying and responding to intrusion activities.

# IDS (Intusion Detection System)

- **Functions of IDS:**

1. Monitoring and analyzing both user and system activities.
2. Analyzing system configuration and weaknesses.
3. Assessing system and file integrity.
4. Ability to recognize patterns typical of attacks.
5. Analysis of abnormal activity patterns.
6. Tracking user policy violations.

# IDS Types

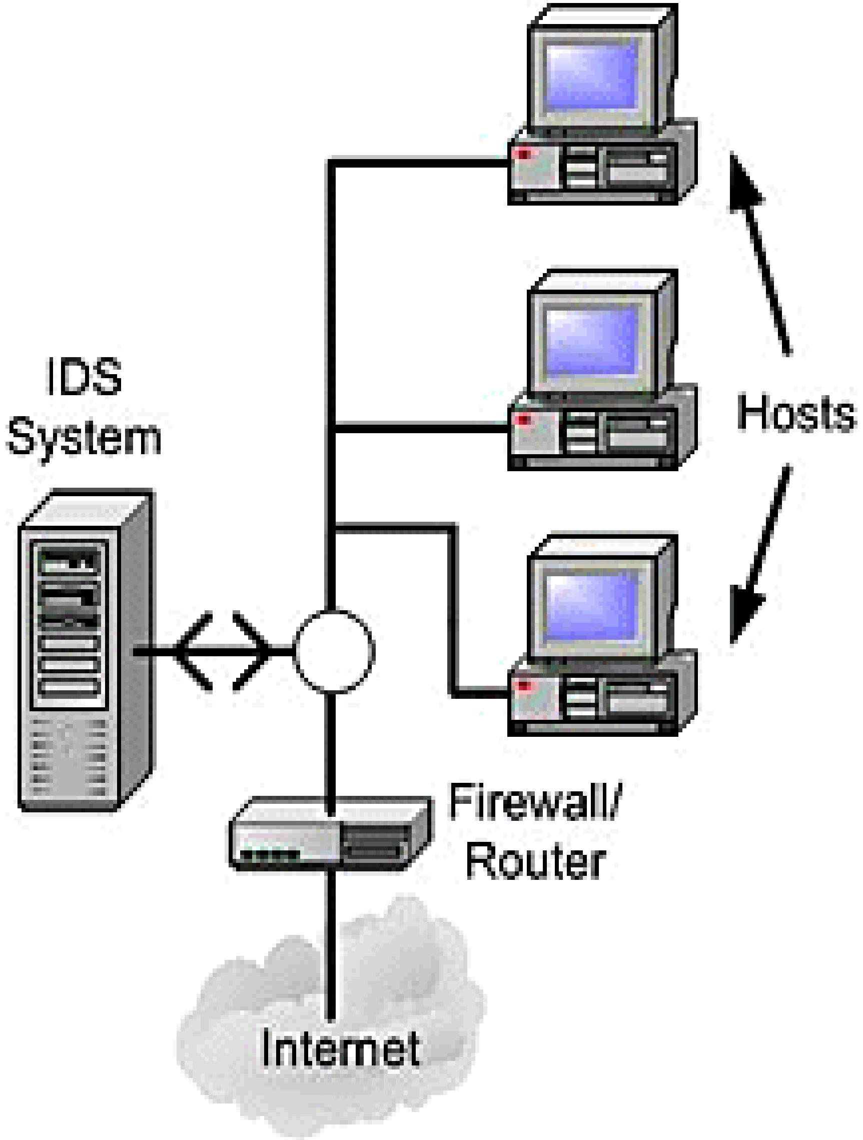
- Different Ways to classify the IDS are shown below,

1. **Network based (NIDS)**
2. **Host based (HIDS)**
3. **Anomaly based IDS**
4. **Signature based IDS**
5. **Rule based IDS**

# 1. NIDS

- **NIDS is used to monitor and analyze network traffic to protect the system from network based threats.**
- NIDS are **placed at a point within the network to monitor traffic to and from all devices** on the network.
- A NIDS **reads all inbound packets and searches for any suspicious patterns.**
- **When threats are discovered, based on some strict rules, the system can take action such as notifying administrators, or stopping the source IP address from accessing the network.**
- Example of the NIDS would be installing it on the subnet where firewalls are located in ordered to see if someone is trying to break into the firewall.

- The basic figure is,



**Advantages:**

- A few well-placed NIDS can monitor a large network.
- It detects network threats without interfering the normal network operations.
- NIDS can be made very secure against attack and even made invisible to many attackers.
- It is operating system independent.
- Deployment, maintenance and upgrade costs are generally lower.

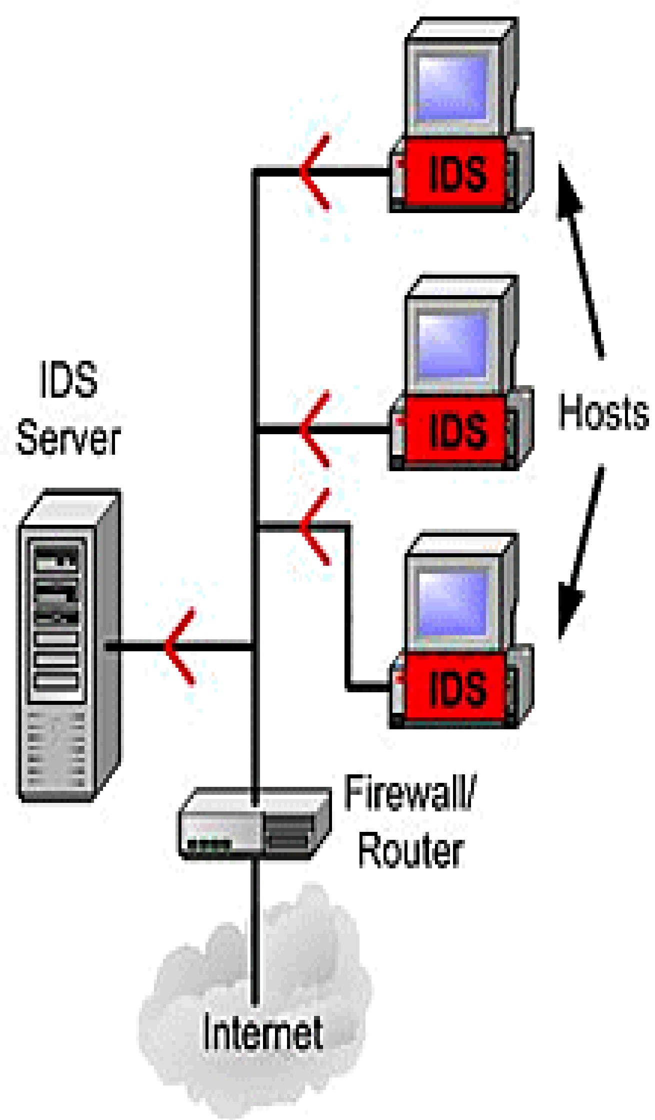
**Disadvantages:**

- Sometimes it fails to recognize an attack when there is a heavy network traffic.
- Not so secure against modern switch based network.
- Most NIDS can not tell whether or not an attack was successful; they can only find that an attack was initiated.

# 2. HIDS

- **HIDS run on individual hosts or devices on the network.**
- **HIDS detects the abnormal behavior of the system.**
- HIDS is an intrusion detection system that **monitors a computer system on which it is installed to detect intrusion.**
- A HIDS **monitors the inbound and outbound packets from the device only** and will alert the user or administrator if suspicious activity is detected.
- It takes a snapshot of existing system files and matches it to the previous snapshot.
- If the critical system files were modified or deleted, the alert is sent to the administrator.
- An example of HIDS usage can be seen on mission critical machines, which are not expected to change their configurations.

- The basic figure is,



Advantages:

- Verifies success or failure of an attack .
- Monitors system activities.
- Detects attacks that a network based IDS fail to detect.
- Near real time detection and response .
- Lower cost.

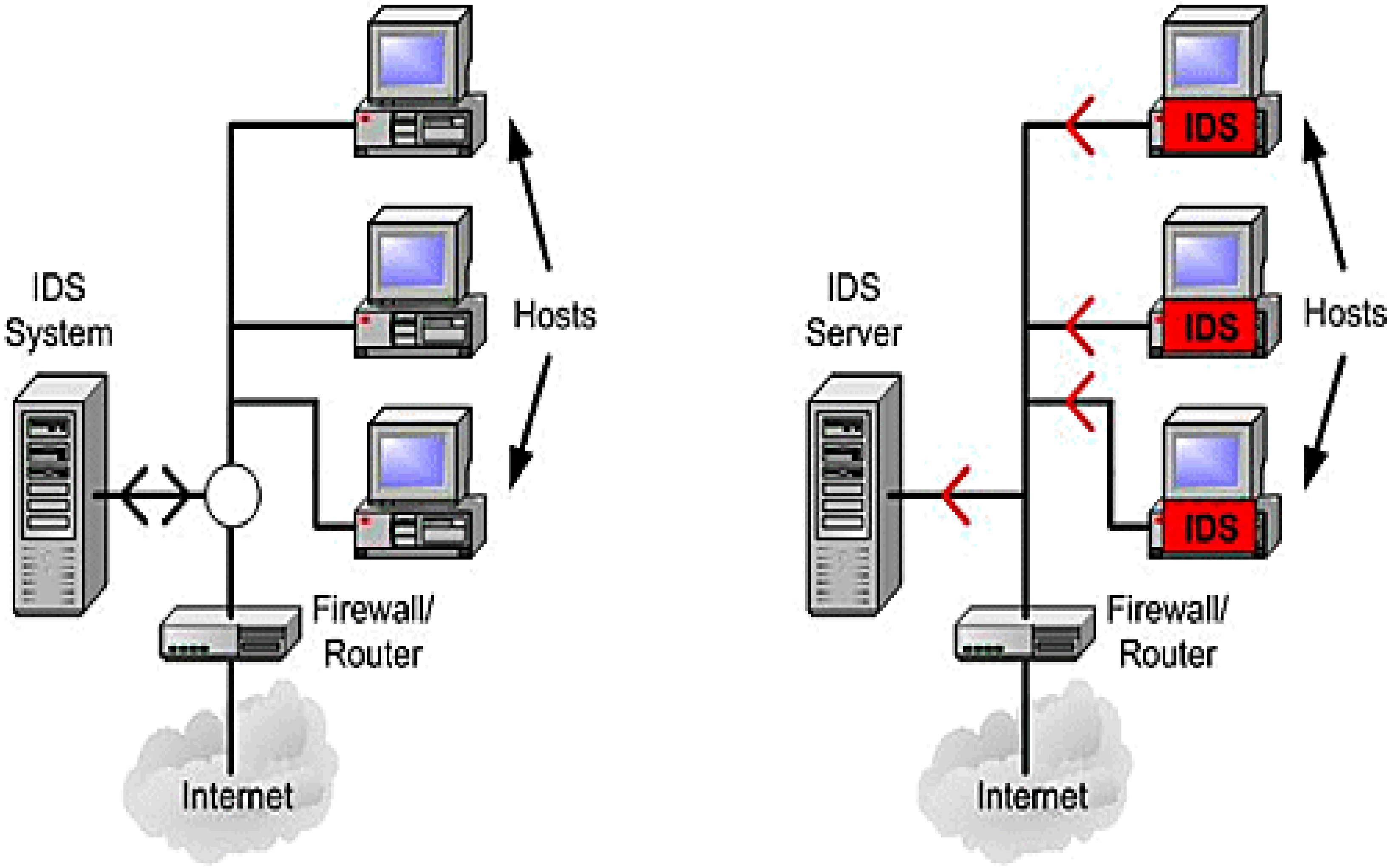
Disadvantages:

- HIDS are harder to manage.
- HIDS are not well suited for detecting network scans or other such surveillance that targets an entire network.
- HIDS can be disabled by certain DOS attacks.

# NIDS v/s HIDS

| HIDS | NIDS |
|---|---|
| It is installed in a single host and it can monitor traffics that are originating and coming to particular host only. | It is positioned in a network to detect any attack on the hosts of that network. |
| It is capable of verifying if an attack was successful or not. | It only gives an alert of attack. |
| It can monitor all user activities. | It cannot monitor user activities. |
| Deployment cost is high. | Deployment cost is low. |
| It is more accurate and useful than NIDS. | It is less accurate than HIDS. |
| It can analyze the decrypted traffic. | It cannot analyze network traffic. |

# NIDS v/s HIDS


IDS
System
Hosts
Firewall/
Router
Internet
IDS
Server
IDS
IDS
IDS
Hosts
Firewall/
Router
Internet

# 3. Signature Based IDS

- A signature based IDS will monitor packets on the network and compare them with the predefined rules or signatures defined in the database.
- Alerts are generated on the basis of the result of the comparison.
- This is similar to the way most antivirus software detects malware.
- Until you didn't update your signature, your IDS would be unable to detect the new threat.

Advantages:

- Signature are easy to develop and understand if you are know what network behavior you’re trying to identify.
- The event generated by signature based IDS generate a alarm.
- Pattern matching can be performed very quickly.

Disadvantages:

- They are unable to detect new attacks.
- Suffer from false alarms.
- Have to programmed again for every new pattern to be detected.

# 4. Anomaly Based IDS

- An IDS which is anomaly based will **monitor network traffic** and **compare it against an defined baseline.**
- The baseline will **identify what is “normal” for that network.**
- It will alert the administrator or user when traffic is detected which is abnormal, or different, than the baseline.
- Rules are applied to test whether the user behavior is legal or not.
- This is  as opposed to signature based system which can only detect attacks for which a signature has previously been created.
- In order to determine what is attack traffic, the system must be taught to recognize normal system activity.

- This can be accomplished in several ways, most often with artificial intelligence type techniques.

**Advantages:**

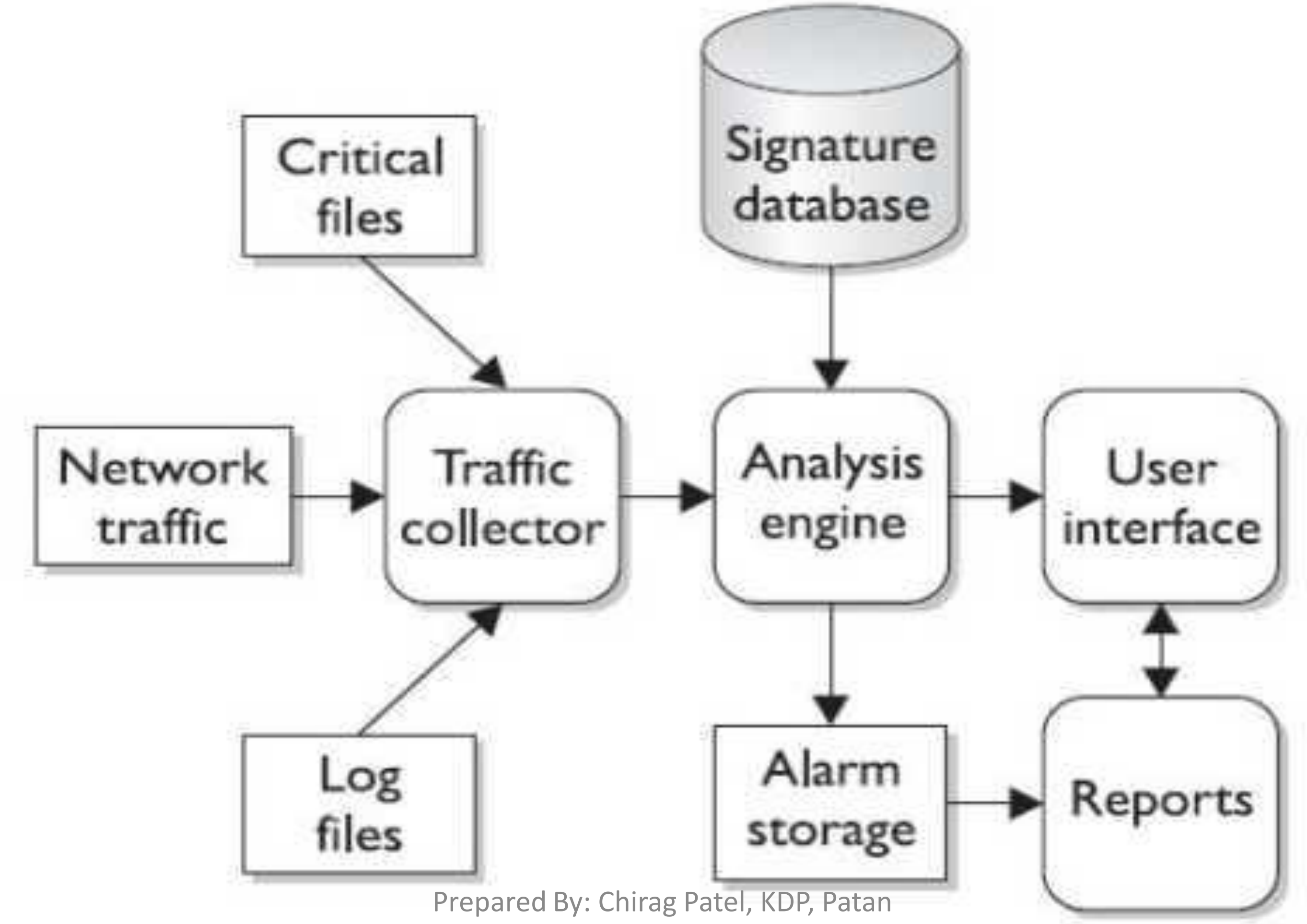
- It can detect new attacks.

**Disadvantages:**

- Difficultly of defining rules.
- Malicious activity that comes within normal usage patterns is not detected.

# Logical components of IDS

- Whether it is NIDS or HIDS, an IDS typically consists several specialized components working together shown below,



# Logical components of IDS

- These components are often logical and software based rather than physical.
- It will very from product to product and vendor to vendor.
- **Traffic Collector:**
- It collects activity/events for the IDS to examine.
- In HIDS, this could be log file, audit logs or traffic to or from specific system.
- In NIDS, this can work as sniffer.
- **Analysis Engine:**
- It examines the collected network traffic and compares it to known patterns of suspicious or malicious activity stored in the signature database.
- This analysis engine is brain of IDS system.

# Logical components of IDS

- **Signature database:**
- It is collection of patterns and definitions of known suspicious or malicious activities.
- User interface and report:
- These are the interfaces with the human elements,

# 5.2 Web Security Threats

- **Web security is the protection given to the data on the internet preventing from the detecting & corrupting the data.**
- It is the process of securing confidential data stored online from unauthorized access and modification.
- A web Security threat is any threat that uses the World Wide Web to facilitate cybercrime.
- Web security is security standard that addresses security concerns when data is exchanged using web.
- **There are mainly four types of threats which founds in web services: Integrity, Confidentiality, Denial of Service and Authentication.**

# 1.INTEGRITY

| Threats | Effect | Solution (remedy) |
|---|---|---|
| • Modification of user data<br>• Trojan horse browser<br>• Modification of memory<br>• Modification of message traffic in transit | • Loss of information<br>• Compromise of data<br>• Vulnerability to all other threats | • Cryptographic checksums |

# 2.CONFIDENTIALITY

| **Threats** | **Effect** | **Solution (remedy)** |
|---|---|---|
| • Eavesdropping on the net<br>• Theft of info from server<br>• Theft of data from client<br>• Info about network configuration<br>• Info about which client talks to server | • Loss of information<br>• Loss of privacy | • Encryption<br>• Web proxies |

# 3.DENIAL OF SERVICES

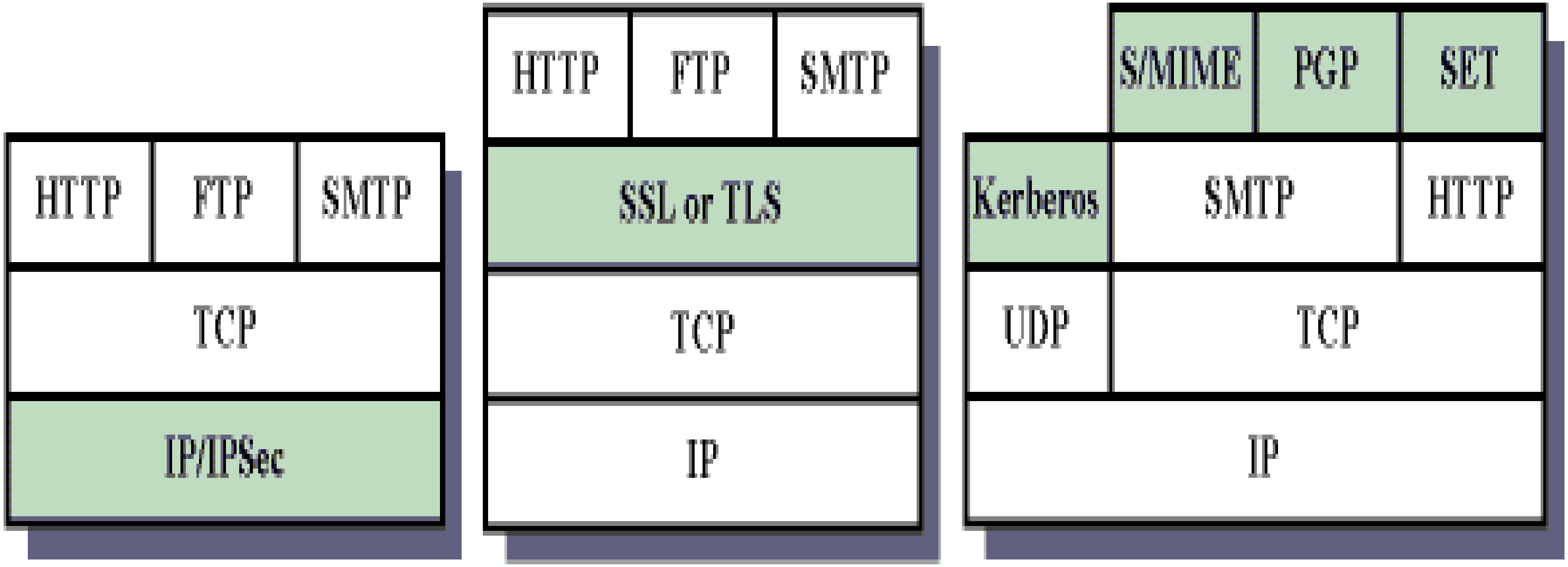
| **Threats** | **Effect** | **Solution (remedy)** |
|---|---|---|
| • Killing of user threads<br>• Flooding machine with fake requests<br>• Filling up disk or memory | • Disruptive<br>• Annoying<br>• Prevent user from getting work done | • Difficult to prevent |

# 4.AUTHENTICATION

| Threats | Effect | Solution (remedy) |
|---|---|---|
| - Impersonation of legitimate users<br>- Data forgery | - Misrepresentation of user information is valid | - Cryptographic techniques |

# Web Traffic Security Approaches

- A number of approaches to providing Web security are possible.
- Solutions for web security are shown below.


HTTP | FTP | SMTP
TCP
IP/IPSec

HTTP | FTP | SMTP
SSL or TLS
TCP
IP

S/MIME | PGP | SET
Kerberos | SMTP | HTTP
UDP | TCP
IP

(a) Network Level

(b) Transport Level

(c) Application Level

**1. One solution is to provide security at network layer using IPSec.**

- The main advantage of IPSec is that it is transparent to the end users and applications and provide general purpose solution.
- IPSec also provides filtering capability, so only selected traffic id allowed.

**2. Another solution is to implement security just above TCP.**

The security implemented above TCP called as Secure Socket Layer (SSL).

# Secure Electronic Transaction (SET)

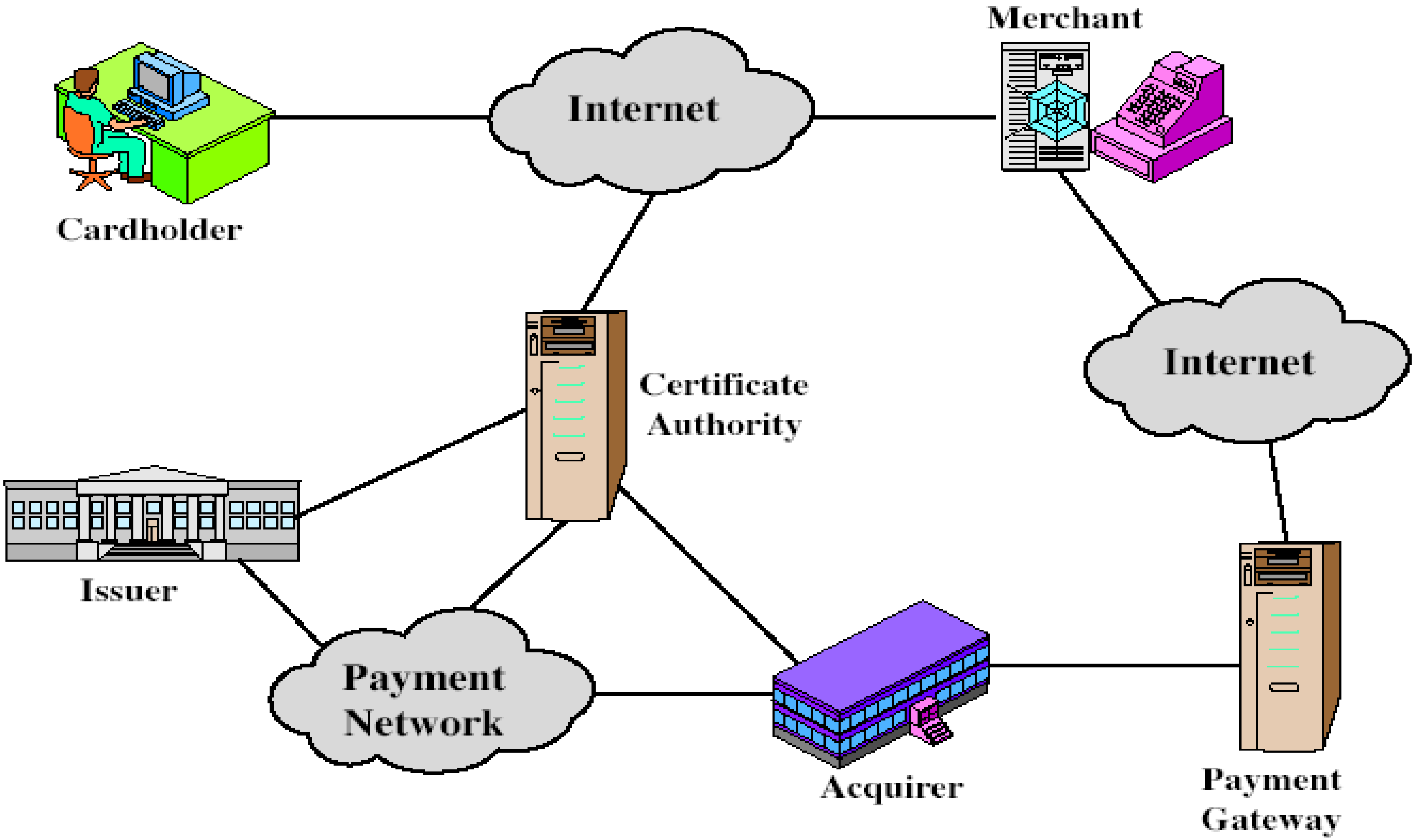
- SET is set of protocols and formats designed to protect credit card transactions through Internet.

OR

- SET is a system for ensuring the security of financial transactions on the Internet, It was supported initially by MasterCard, Visa, Microsoft, Netscape, and others.
- With SET, a user is given an electronic wallet (digital certificate) and a transaction is conducted and verified using a combination of digital certificates and digital signatures among the purchaser, a merchant, and the purchaser's bank in a way that ensures privacy and confidentiality.
- SET makes use of Netscape's Secure Sockets Layer (SSL), Microsoft's Secure Transaction Technology (STT), and Teresa System's Secure Hypertext Transfer Protocol (S-HTTP).SET uses some but not all aspects of a PKI.

# SET Participants

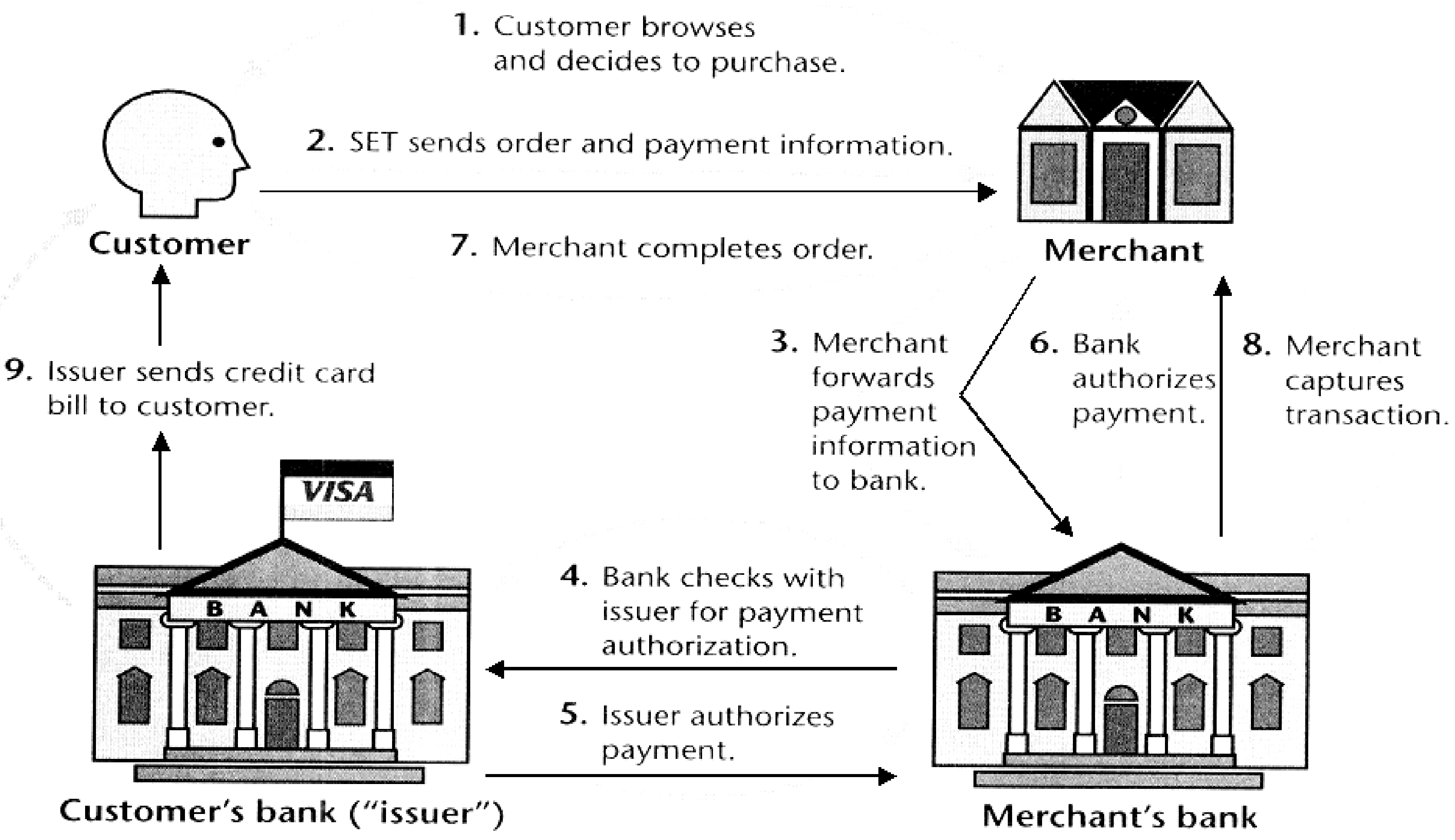
- The basic figure is,



1. Cardholder (Customer)
   - This is an authorized holder of a payment card (e.g., MasterCard, Visa) that has been issued by an issuer.
2. Merchant (Web Server)
   - This is a person or organization who has things to sell to the cardholder.
3. Issuer (Issuers bank)
   - This is a financial institution such as a bank that provides the card holder with the payment card.
4. Acquirer
   - This is a financial institution that establishes an account with the merchant and processes credit card authorizations and payments
5. CA
   - This is an entity that is entrusted to issue X.509v3 public-key certificates for cardholders, merchants, and payment gateways.
6. Payment Gateway
   - This is a function that can be undertaken by the acquirer or some third party that processes merchant payment messages and Performs Authentication Function

# SET Transaction

- The basic figure is,


1. Customer browses and decides to purchase.
2. SET sends order and payment information.
Customer
Merchant
7. Merchant completes order.
9. Issuer sends credit card bill to customer.
3. Merchant forwards payment information to bank.
6. Bank authorizes payment.
8. Merchant captures transaction.
VISA
B A N K
4. Bank checks with issuer for payment authorization.
5. Issuer authorizes payment.
B A N K
Customer's bank ("issuer")
Merchant's bank

1. Customer Opens an account – customer gets a credit card account from, such as a Visa or MasterCard, with a bank that supports SET.
2. The customer places an order and Payment Information together with the customers certificate so the merchant can verify that he is dealing with a valid customer. The PI is encrypted in such a way that the merchant cannot read it.
3. Merchant Requests PI authorization – The merchant forwards the PI to the payment gateway, to determine whether the customer has sufficient funds/credit for the purchase.
4. Merchant’s bank checks with Issuer for Payment Authorization.
5. Issuer Authorizes Payment.
6. Merchant’s Bank Sends Payment Authorization to Merchant.
7. Merchant Confirms the order –Merchant sends confirmation of the order to the customer. Merchant ships goods and services.
8. Merchant capture all transaction detail from merchant’s bank.
9. Issuer sends Credit Card Bill

# SSL & TLS

- SSL(Secure Socket Layer) & TLS (Transport Layer Security) Both provide a secure transport connection between applications (e.g., web server and a browser).
- SSL was developed by Netscape, SSL version 3.0 has been implemented in many web browsers (e.g., Netscape Navigator and MS Internet Explorer) and web servers and widely used on the Internet
- SSL v3.0 was specified in an Internet Draft (1996)
- TLS can be viewed as SSL v3.1
- Transport Layer Security (TLS) is an email security tool based on the Secure Sockets Layer (SSL) 3.0 protocol. It secures the transmission of email over the internet using standard encryption technology.
- TLS provides transport layer security for Internet applications.

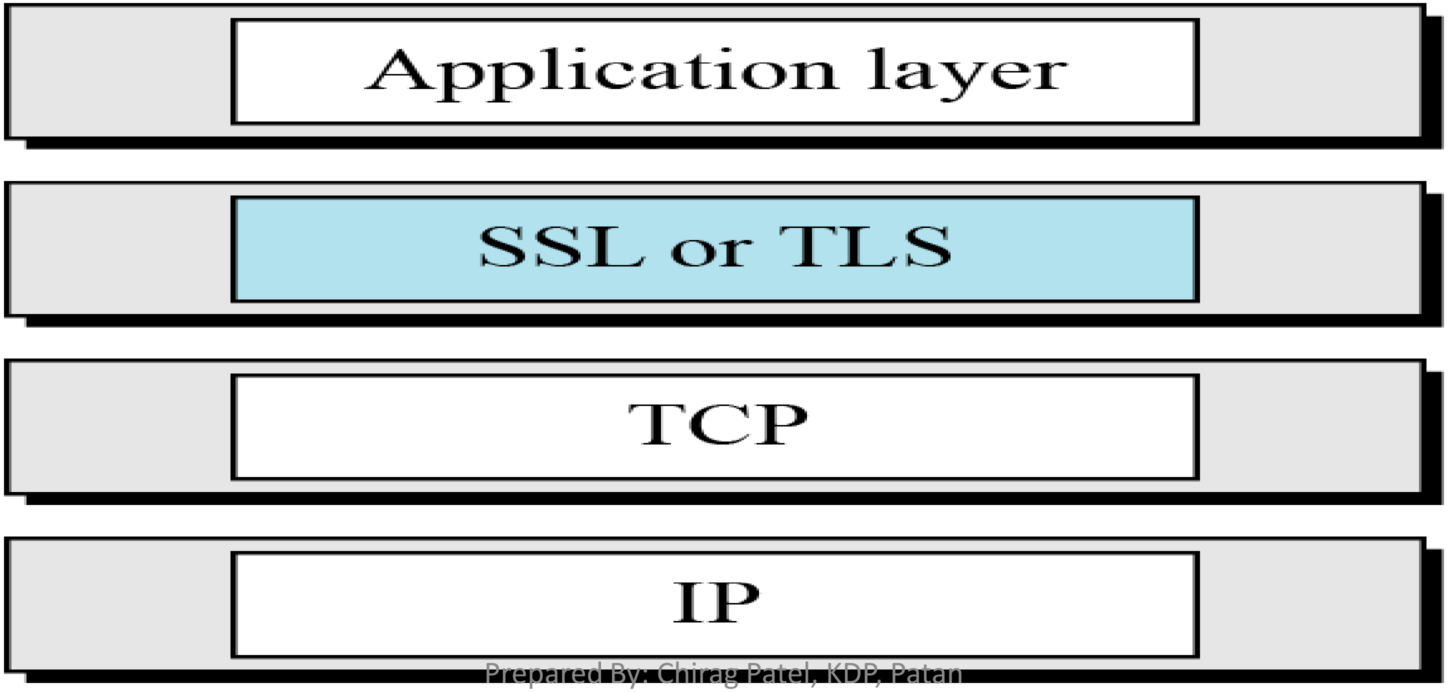
# How TLS Works????

- To work, TLS needs to be enabled on the mail servers of both the sender and the receiver of the email.
- Any information exchanged between the servers is encrypted, including the subject line, text and any attachments.
- When sending encrypted messages, the mail exchange works as follows:

1. When the sender connects to the recipient, the system automatically checks whether TLS is enabled on the client’s mail server.
2. If TLS is enabled at both ends, a secure TLS connection is established by using a ‘handshake’ procedure.
3. During the handshake, TLS certificates are exchanged. If the sender’s server trusts the certificate from the client mail server, the TLS session starts, and the email sent via a secure internet connection.

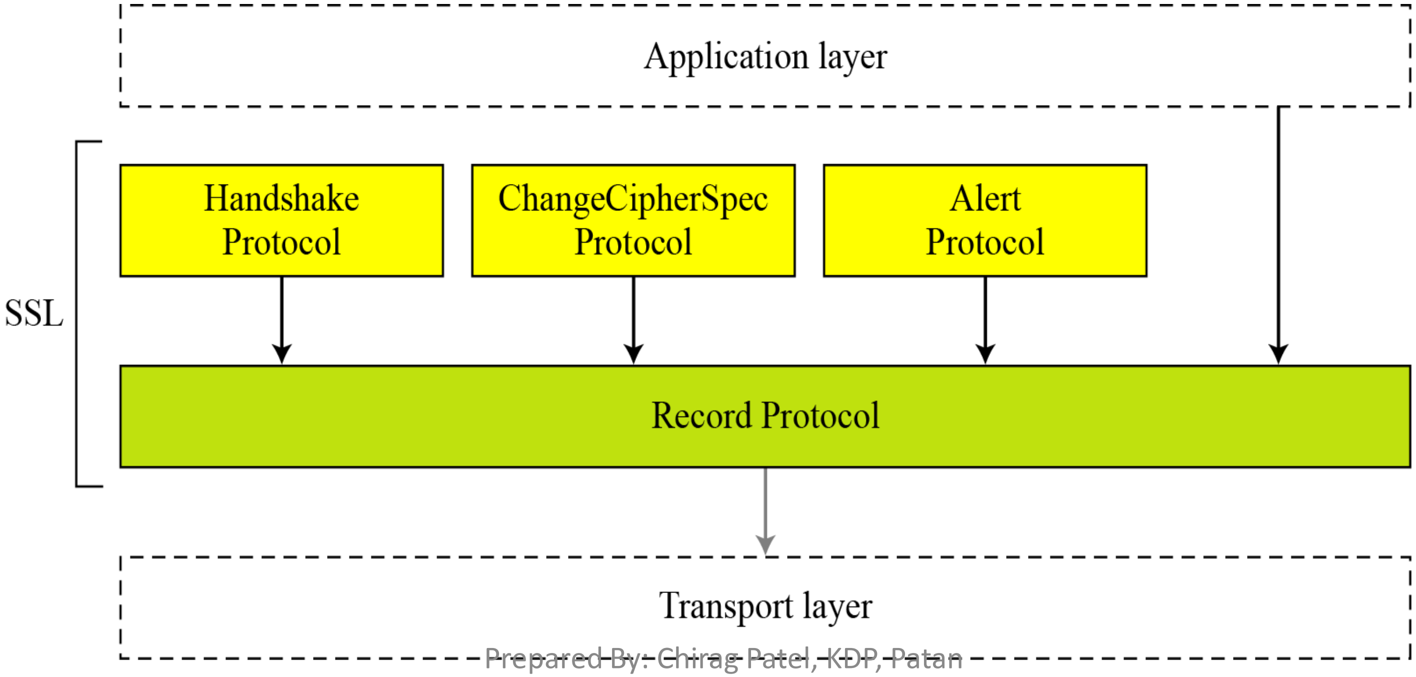
# SSL & TLS Architecture

- SSL is designed to provide security and compression services to data generated from the application layer.
- SSL protocol is implemented just above the TCP to provide web security.
- SSL is designed to make use of TCP to provide a reliable end-to-end secure service.
- The Location of SSL & TLS in internet model are depicted below,



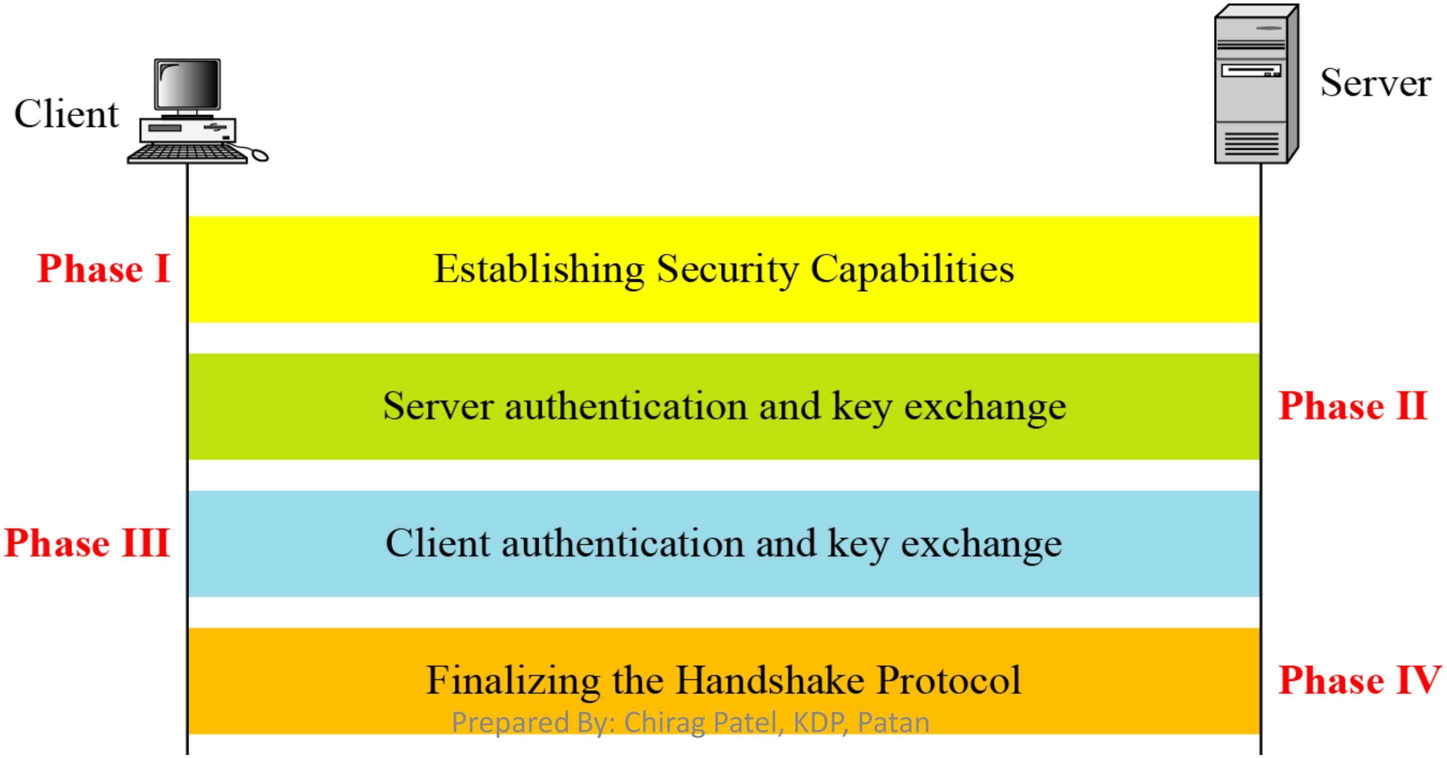
# SSL & TLS Protocol Stack

- Four Protocols defined by SSL.
  1. Handshake Protocol
  2. Record Protocol
  3. Alert Protocol
  4. Change Chiper Spec Protocol

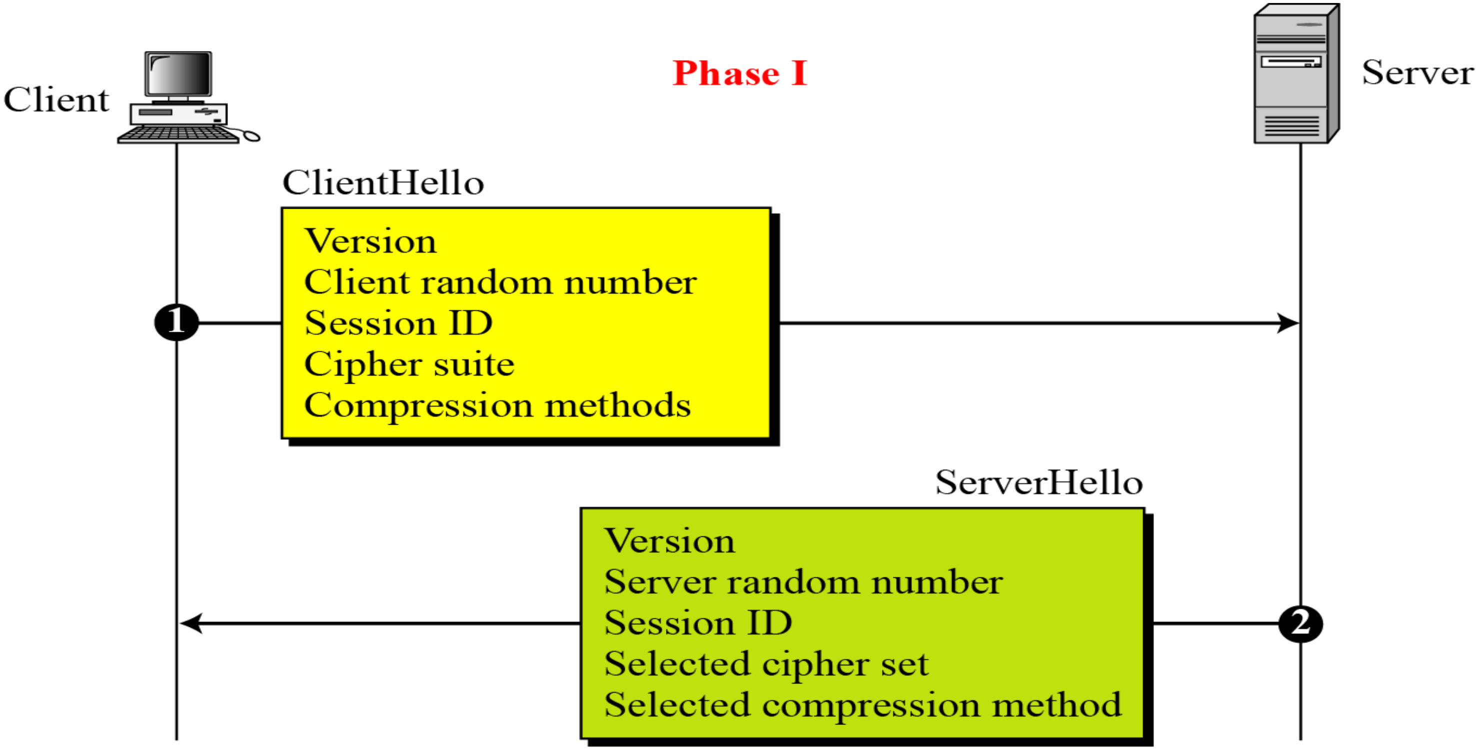


# 1. Handshake Protocol

- TLS Handshake Protocol is layered on top of the TLS Record Protocol and basically it is used to
  - Authenticate the client and the server
  - Exchange cryptographic keys
- SSL Handshake performs in four phases as describe in below figure,


Client
Server
Phase I
Establishing Security Capabilities
Server authentication and key exchange
Phase II
Phase III
Client authentication and key exchange
Finalizing the Handshake Protocol
Phase IV

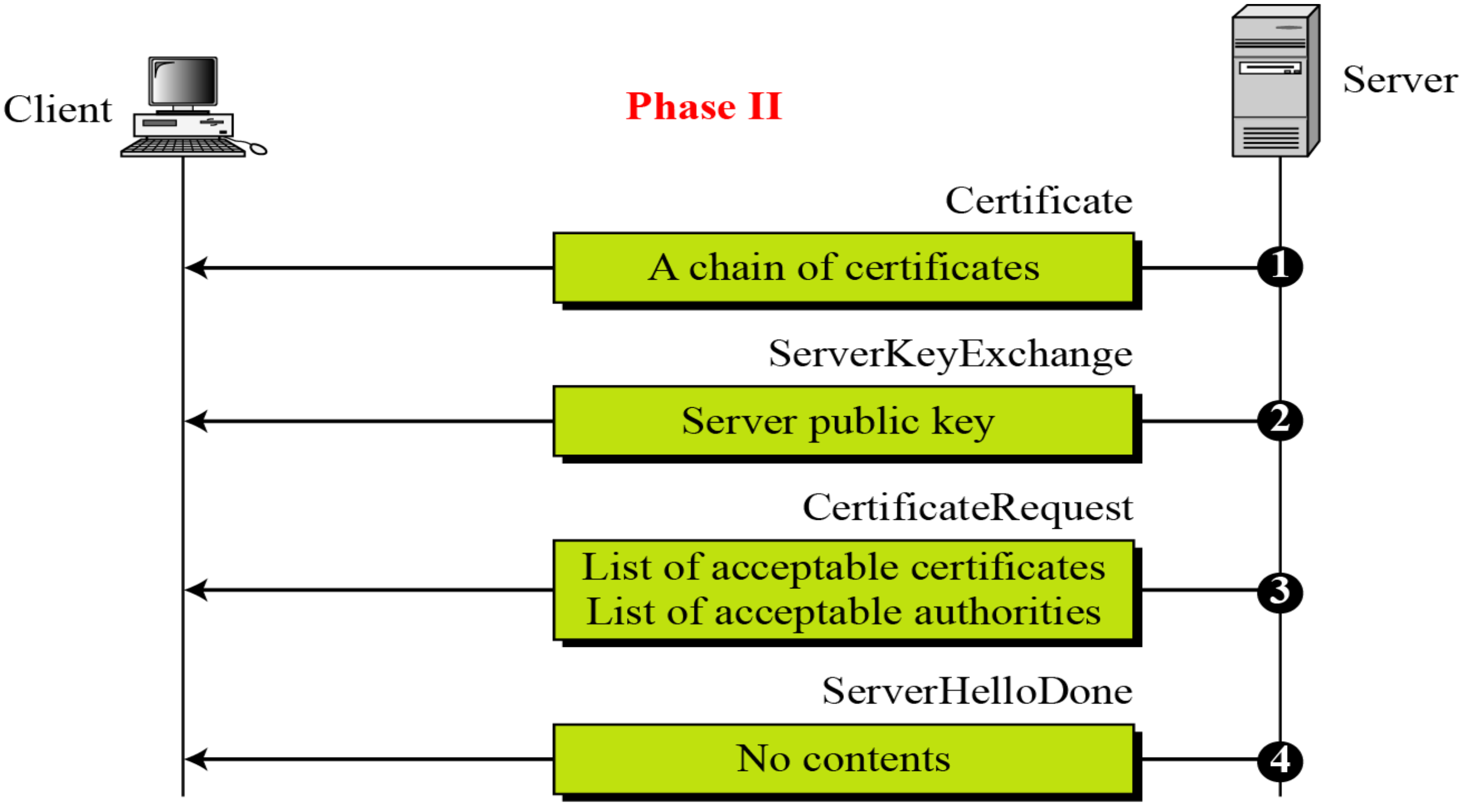
# Phase I



- After Phase I, the client and server know the following:

1. The version of SSL
2. The algorithms for key exchange, message authentication, and encryption.
3. The compression method.
4. The two random numbers for key generation

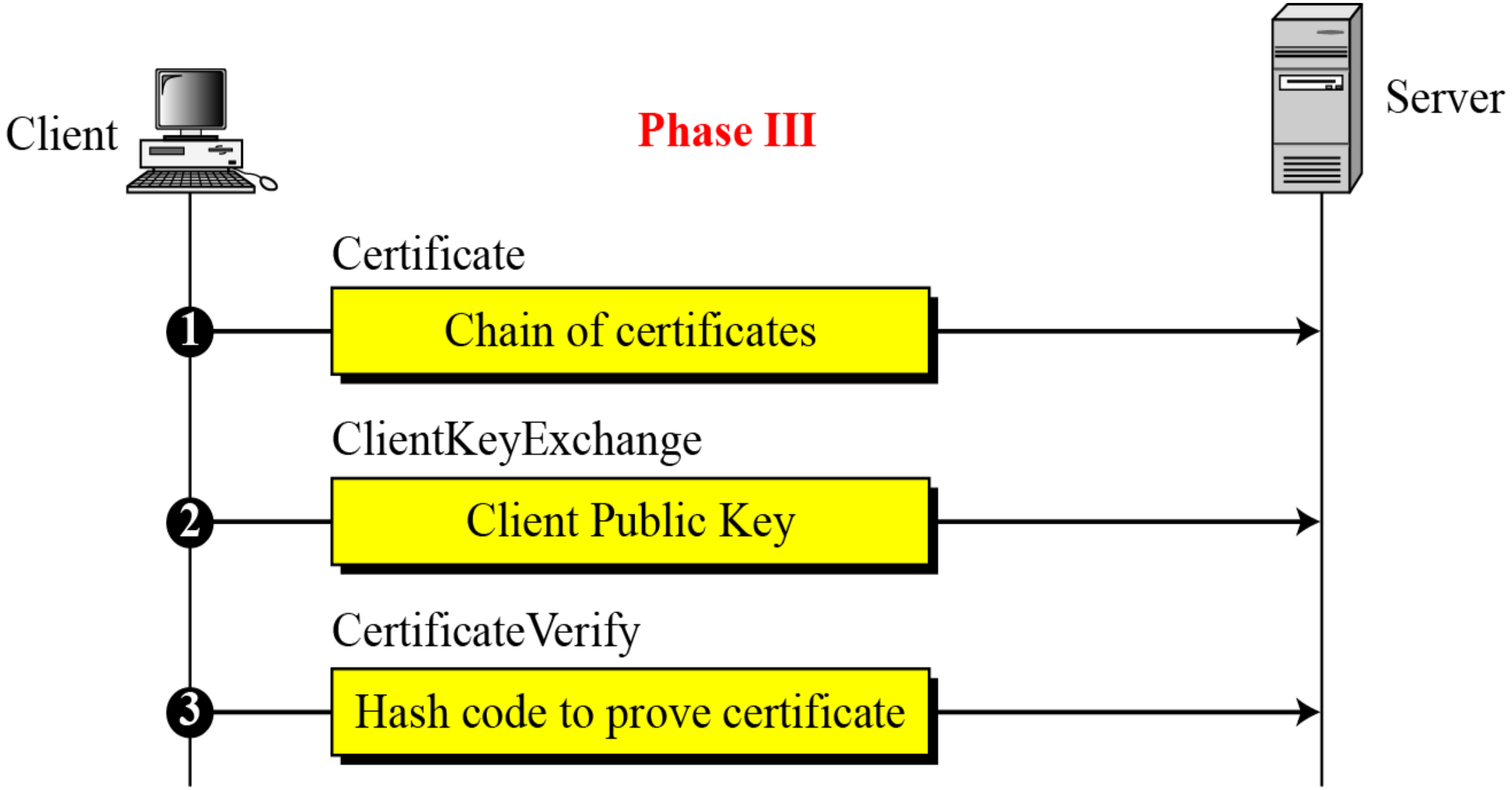
# Phase II



- After Phase II,

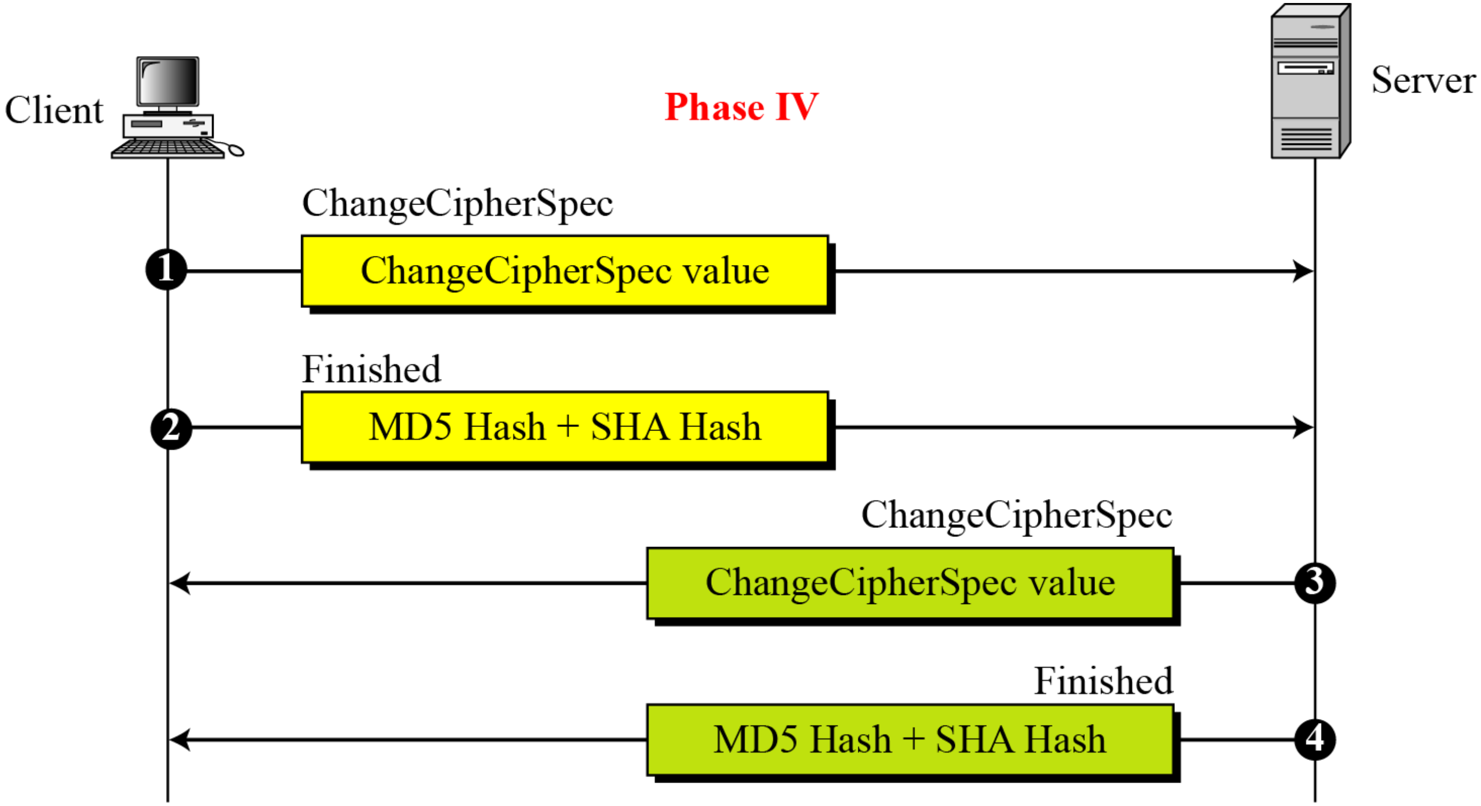
1. The server is authenticated to the client.
2. The client knows the public key of the server if required.

# Phase III



- After Phase III,
  1. The client is authenticated for the server.
  2. Both the client and the server know the pre-master secret.

# Phase IV



- After Phase IV,

1. Client and server are ready to exchange data.

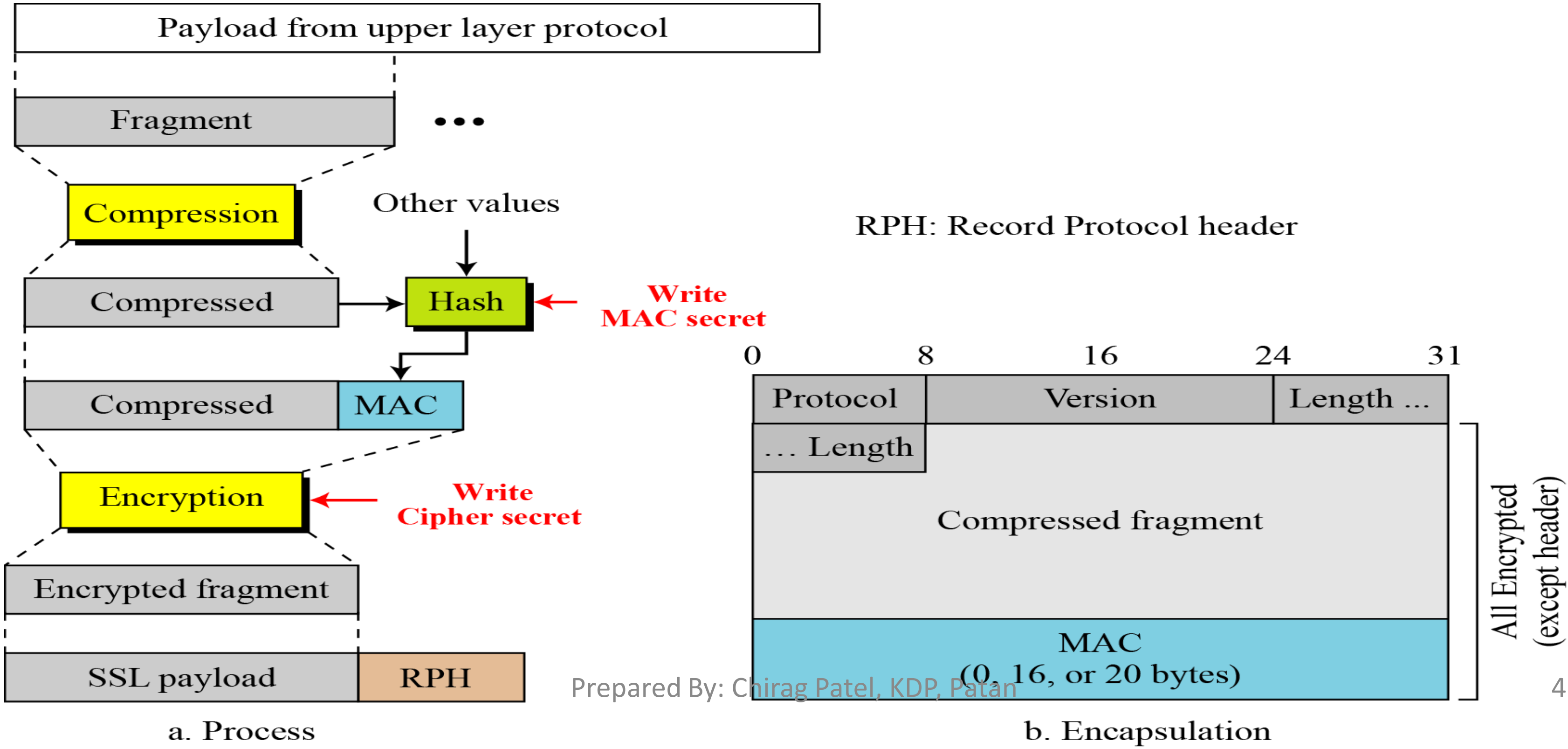
# 2. Record Protocol

- TLS Record Protocol layers on top of a reliable connection-oriented transport, such as TCP and basically it provides

1. data confidentiality using symmetric key cryptography
2. data integrity using a keyed message authentication checksum (MAC)

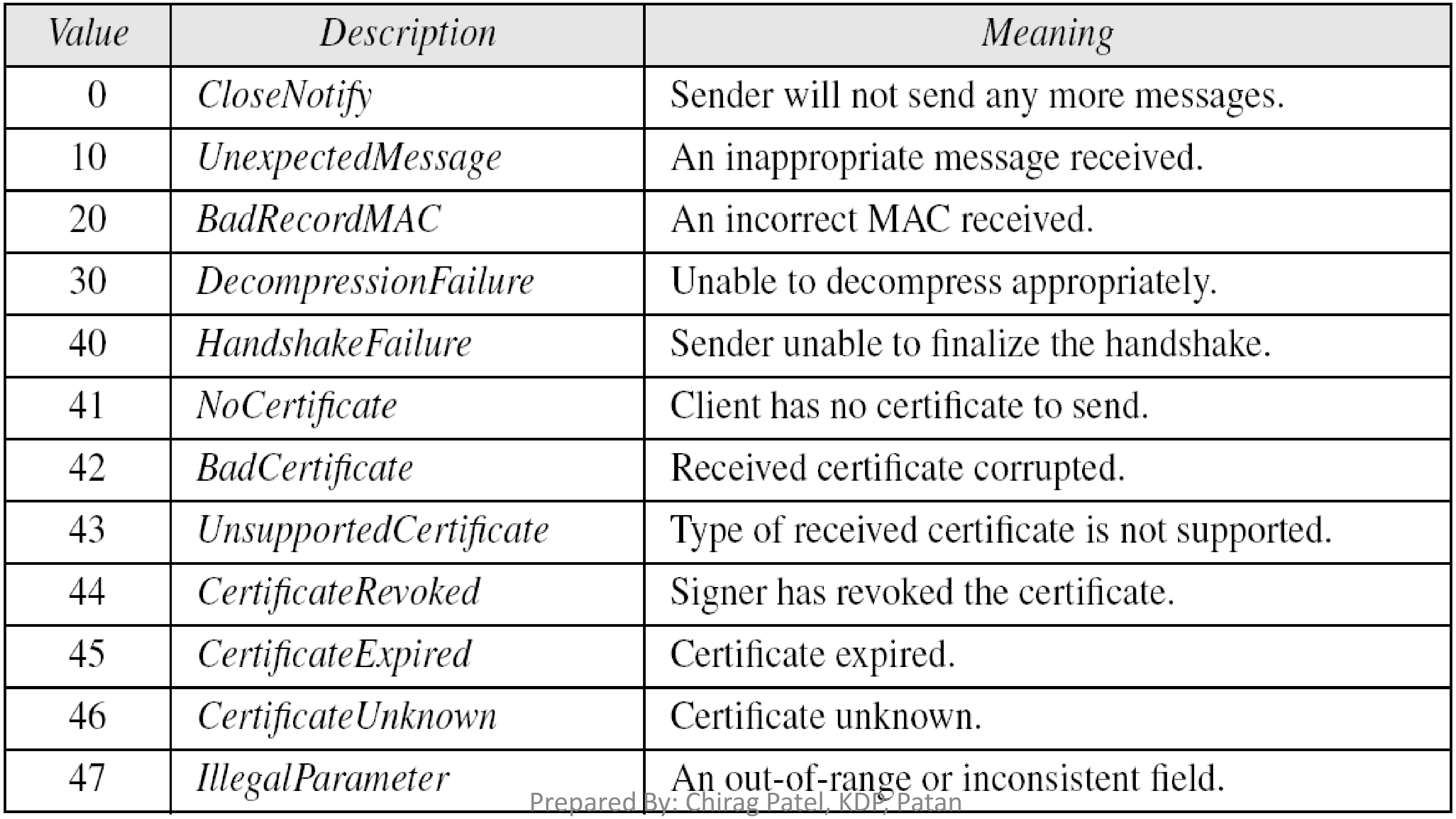
- Basic Operation of Record Protocol,
  1. Read messages for transmit
  2. Fragment messages into manageable chunks of data
  3. Compress the data, if compression is required and enabled
  4. Calculate a MAC
  5. Encrypt the data
  6. Transmit the resulting data to the peer

- At the opposite end of the TLS connection, the basic operation of the sender is replicated, but in the reverse order
  1. Read received data from the peer
  2. Decrypt the data
  3. Verify the MAC
  4. Decompress the data, if compression is required and enabled
  5. Reassemble the message fragments
  6. Deliver the message to upper protocol layers



# 3. Alert Protocol

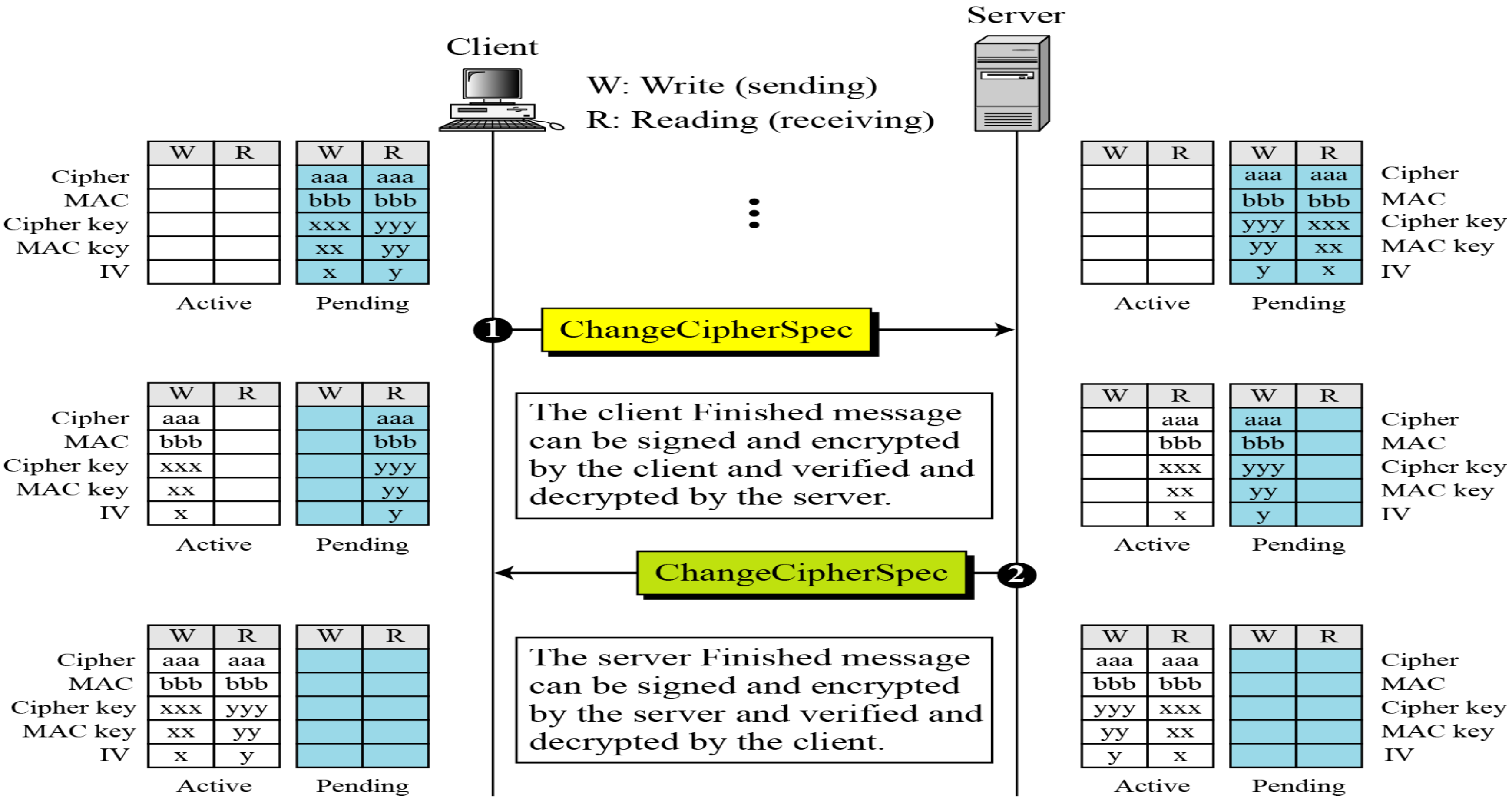
- SSL Alert Protocol
  - Error messages (fatal alerts and warnings)



| Value | Description | Meaning |
|---|---|---|
| 0 | *CloseNotify* | Sender will not send any more messages. |
| 10 | *UnexpectedMessage* | An inappropriate message received. |
| 20 | *BadRecordMAC* | An incorrect MAC received. |
| 30 | *DecompressionFailure* | Unable to decompress appropriately. |
| 40 | *HandshakeFailure* | Sender unable to finalize the handshake. |
| 41 | *NoCertificate* | Client has no certificate to send. |
| 42 | *BadCertificate* | Received certificate corrupted. |
| 43 | *UnsupportedCertificate* | Type of received certificate is not supported. |
| 44 | *CertificateRevoked* | Signer has revoked the certificate. |
| 45 | *CertificateExpired* | Certificate expired. |
| 46 | *CertificateUnknown* | Certificate unknown. |
| 47 | *IllegalParameter* | An out-of-range or inconsistent field. |

# 4. Change Cipher Spec Protocol

- A single message that indicates the end of the SSL handshake



| Client | Active W | Active R | Pending W | Pending R |
|---|---|---|---|---|
| Cipher | | | aaa | aaa |
| MAC | | | bbb | bbb |
| Cipher key | | | xxx | yyy |
| MAC key | | | xx | yy |
| IV | | | x | y |

| Server | Active W | Active R | Pending W | Pending R |
|---|---|---|---|---|
| Cipher | | | aaa | aaa |
| MAC | | | bbb | bbb |
| Cipher key | | | yyy | xxx |
| MAC key | | | yy | xx |
| IV | | | y | x |

| Client | Active W | Active R | Pending W | Pending R |
|---|---|---|---|---|
| Cipher | aaa | | | aaa |
| MAC | bbb | | | bbb |
| Cipher key | xxx | | | yyy |
| MAC key | xx | | | yy |
| IV | x | | | y |

The client Finished message can be signed and encrypted by the client and verified and decrypted by the server.

| Server | Active W | Active R | Pending W | Pending R |
|---|---|---|---|---|
| Cipher | | aaa | aaa | |
| MAC | | bbb | bbb | |
| Cipher key | | xxx | yyy | |
| MAC key | | xx | yy | |
| IV | | x | y | |

| Client | Active W | Active R | Pending W | Pending R |
|---|---|---|---|---|
| Cipher | aaa | aaa | | |
| MAC | bbb | bbb | | |
| Cipher key | xxx | yyy | | |
| MAC key | xx | yy | | |
| IV | x | y | | |

The server Finished message can be signed and encrypted by the server and verified and decrypted by the client.

| Server | Active W | Active R | Pending W | Pending R |
|---|---|---|---|---|
| Cipher | aaa | aaa | | |
| MAC | bbb | bbb | | |
| Cipher key | yyy | xxx | | |
| MAC key | yy | xx | | |
| IV | y | x | | |

# Intruders Patterns of Behavior.

- **Hacker**

1. Select the target using IP lookup tools such as NSLookup and others.
2. Map network for accessible services using tools such as NMAP.
3. Identify potentially vulnerable services (in this case, pc Anywhere).
4. Brute force (guess) pc Anywhere password.
5. Install remote administration tool called Dame Ware.
6. Wait for administrator to log on and capture his password.
7. Use that password to access remainder of network.

- **Criminal Enterprise**

1. Act quickly and precisely to make their activities harder to detect.
2. Exploit perimeter through vulnerable ports.
3. Use Trojan horses (hidden software) to leave back doors for reentry.
4. Use sniffers to capture passwords.
5. Do not stick around until noticed.
6. Make few or no mistakes.

- **Internal Threat**

1. Create network  accounts for themselves and their friends.
2. Access accounts and applications they wouldn’t normally use for their daily jobs.
3. E-mail former and prospective employers.
4. Conduct furtive instant-messaging chats.
5. Visit Web sites that cater to disgruntled employees, such as f’dcompany.com.
6. Perform large downloads and file copying.
7. Access the network during off hours.

# Web Security Threats

1. Virus
2. Worms
3. Trojan
4. Spyware
5. Spam
6. Phishing

- Top 5 Web Security Threats are listed below,

1. Cross site scripting
2. Injection flaws
3. Improper session management
4. Insecure direct object reference
5. Cross site request forgery

| NO. | QUESTIONS | MARKS | YEAR | | | | | |
|---|---|---|---|---|---|---|---|---|
| 1 | Write full form of SSL, TLS,IDS | 2 | | | 2016 | | | |
| 2 | Define intrusion detection system. | 2 | | | 2016 | | | |
| 3 | List any Two Advantages of Intrusion Detection System. | 2 | | 2015 | | | | |
| 4 | Explain Intrusion Detection System in brief. | 3 | | | | | 2018 | |
| 5 | Explain logical components of IDS. Or Explain Logical Component of IDS with Diagram. | 4 | | 2015 | 2016 | | | |
| | Explain Logical Components of IDS. | 3 | | 2015 | | | | |
| 6 | Write an advantages of NIDS. Or List advantages of NIDS. | 2 | 2014 | | 2016 | | | |
| 7 | Explain Network Based Intrusion Detection System. Or Explain network based IDS. Or Write a short note on network intrusion detection system. | 3 | | 2015 | 2016 | | | |
| 8 | List advantages and disadvantages of NIDS. | 4 | | | 2016 | | | |
| 9 | Explain host based IDS. | 3 | | 2015 | | | | |
| 10 | Write an advantages of HIDS. | 3 | 2014 | | | | | |

|  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|
| 11 | Distinguish host based IDS with network based IDS. | 4 |  |  |  | 2017 |  | 2019 |
| 12 | List the features of Secure electronic transaction. | 2 | 2014 |  |  |  |  | 2019 |
| 13 | Explain Secure Electronic Transaction(SET) Protocol . | 3 |  | 2015 |  |  |  |  |
|  | Explain Secure Electronic Transaction. | 4 |  | 2015 |  |  |  | 2019 |
| 14 | Describe the key participants in Secure Electronic Transaction. | 4 |  |  |  | 2017 |  |  |
| 15 | List security features supported by SSL/TLS. | 2 |  |  |  | 2017 |  |  |
| 16 | Explain SSL in brief. Or Explain SSL. Or What do you mean by SSL? Explain in brief. | 3 |  |  | 2016 | 2017 |  |  |
|  | Explain SSL/TLS. Or Explain SSL in detail. | 4 | 2014 | 2015 |  |  |  |  |
| 17 | Explain Transport Layer Security. | 4 |  | 2015 |  |  |  |  |
| 18 | Explain Web Security Threats. | 3 |  | 2015 |  |  |  |  |
| 19 | What do you mean by  web traffic? | 2 | 2014 |  |  |  |  |  |
| 20 | Explain web traffic security approaches. | 3 |  |  |  | 2017 |  |  |