TY BTech Semester-V (AY 2022-23)

Computer Science and Engineering

Disclaimer:

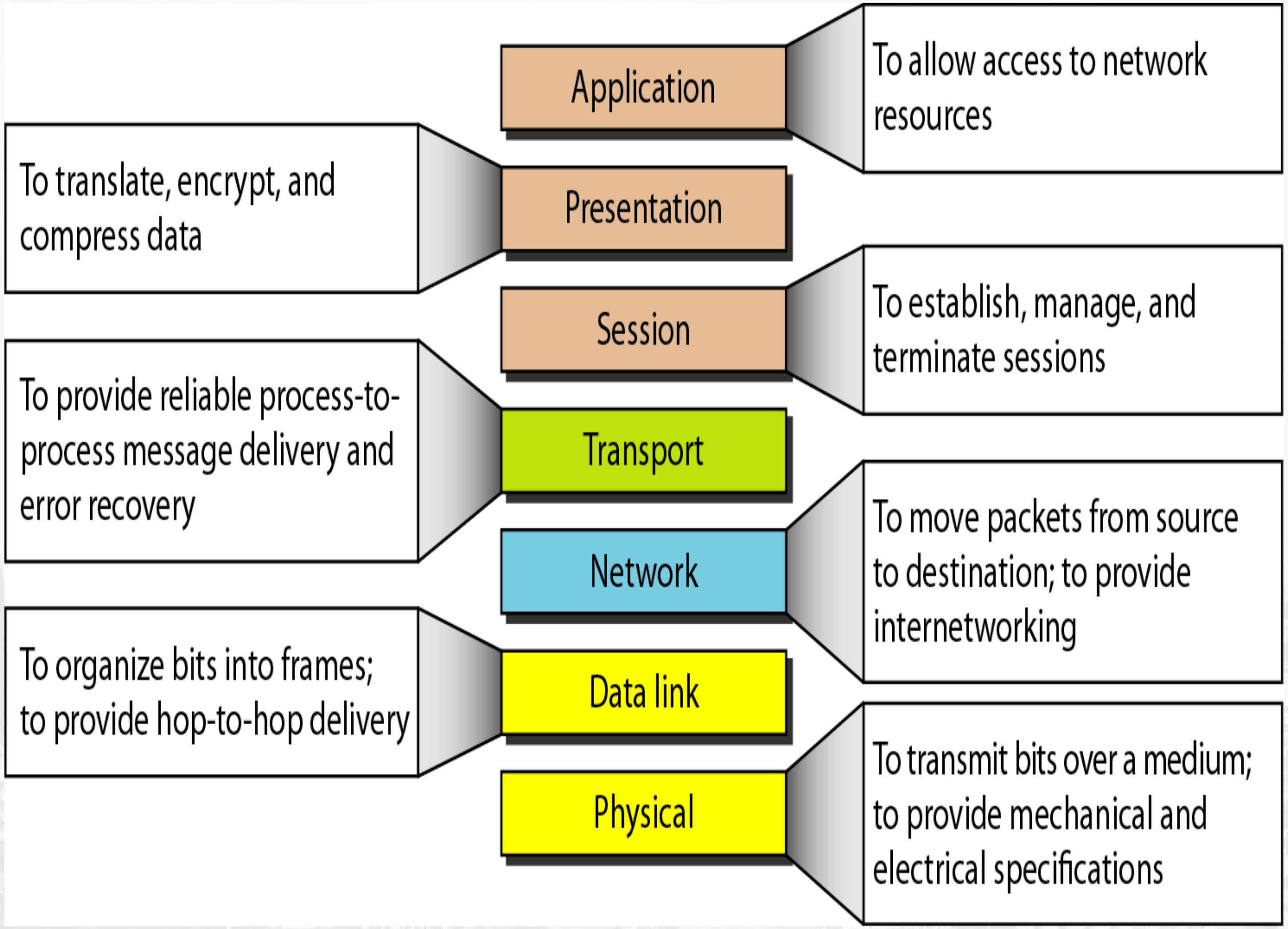
a. Information included in these slides came from multiple sources. We have tried our best to cite the sources. Please refer to the references to learn about the sources, when applicable.

b. The slides should be used only for preparing notes, academic purposes (e.g. in teaching a class), and should not be used for commercial purposes.

Syllabus

Unit: IV	**Network and Cyber Security:** Networks Security Fundamentals, Layer-wise Security concerns, Firewalls: Packet filtering, Stateless and Stateful, Intrusion detection systems: host based, network based IDS, Secured Socket Layer Security, IP level IPSEC security, Email Security: PGP, S/MIME. Cyber Security: Definition and origin, Cyber Crime and information security, Types of Cyber Crime, Classification of Cyber Criminals, Tools used in Cyber Crime, Challenges, Strategies, The Legal Perspective-Indian/Global Perspective, Types of Attack, Social Engineering, Cyber stalking, Ransomware.	**9 Hrs**

Summary of Layers



Application

To allow access to network resources

Presentation

To translate, encrypt, and compress data

Session

To establish, manage, and terminate sessions

Transport

To provide reliable process-to-process message delivery and error recovery

Network

To move packets from source to destination; to provide internetworking

Data link

To organize bits into frames; to provide hop-to-hop delivery

Physical

To transmit bits over a medium; to provide mechanical and electrical specifications

Layer wise Security concerns

- Each layer can be exploited and has inherent vulnerabilities.

Layer	Security issues
Application layer	Detecting and preventing viruses, worms, malicious codes, and application abuses
Presentation Layer	Cryptographic flaws may be exploited to circumvent privacy protections
Session Layer	Session identification may be subject to spoofing and hijack
Transport layer	Authenticating and securing end-to-end communications through data encryption
Network layer	Protecting the ad hoc routing and forwarding protocols
Data Link layer	Protecting the wireless MAC protocol and providing link-layer security support
Physical layer	Preventing signal jamming, denial-of-service attacks

FireWalls

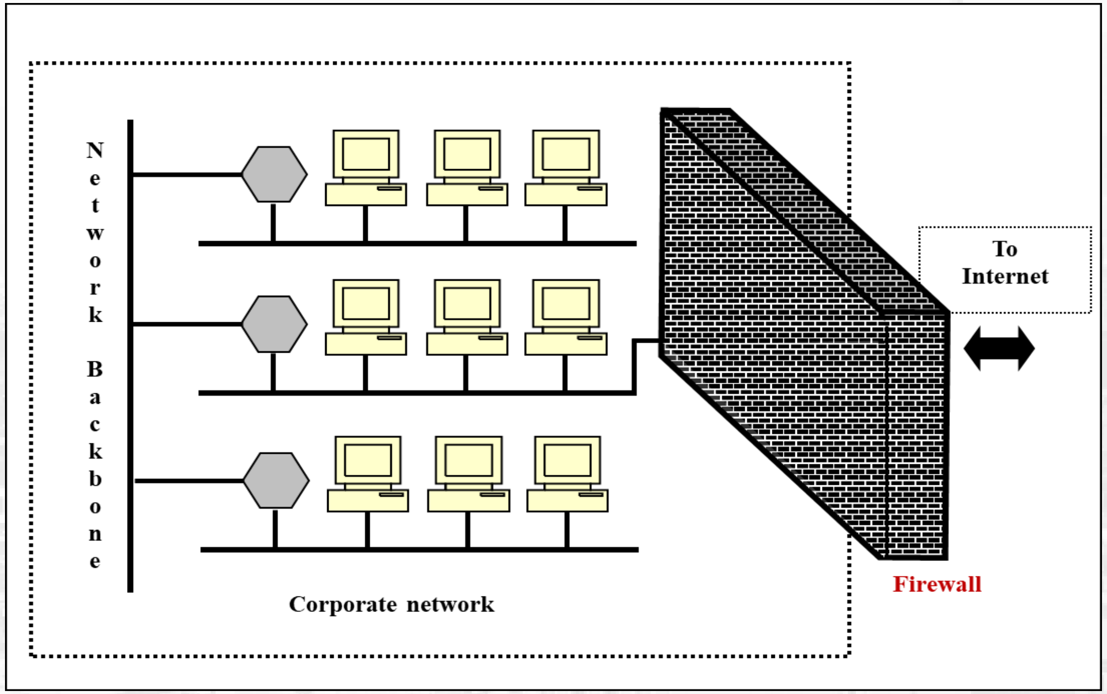
- ❖ Similar to a Security Guard
- ❖ Protects an organization’s network
- ❖ Stands between internet and Intranet

Aims:

- ❖ Establish a controlled link
- ❖ Protect the premises network from Internet-based attacks
- ❖ Provide a single choke point

❖ Unauthorized access to computer system by malicious user is detected as intrusion.

- A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks.



Need of Firewall

- Theft or disclosure of internal data
- Unauthorized access to internal hosts
- Interception or alteration of data
- Damage & denial of service
- Wasted employee time

Limitations of Firewall

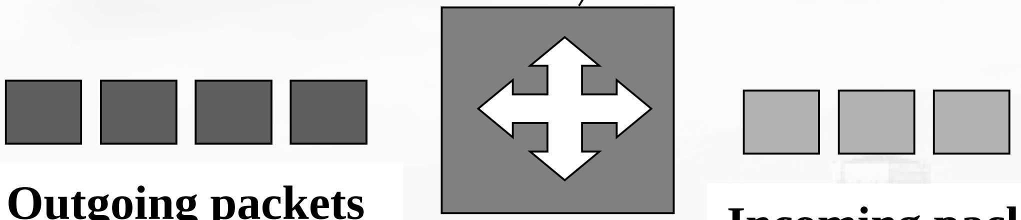
- The firewall cannot protect against attacks that bypass the firewall.
- The firewall may not protect fully against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.
- An improperly secured wireless LAN may be accessed from outside the organization.
- A laptop, PDA, or portable storage device may be used and infected outside the corporate network, and then attached and used internally.

Types of Firewall: Packet Filtering

- ❖ Also called screening router or screening filter

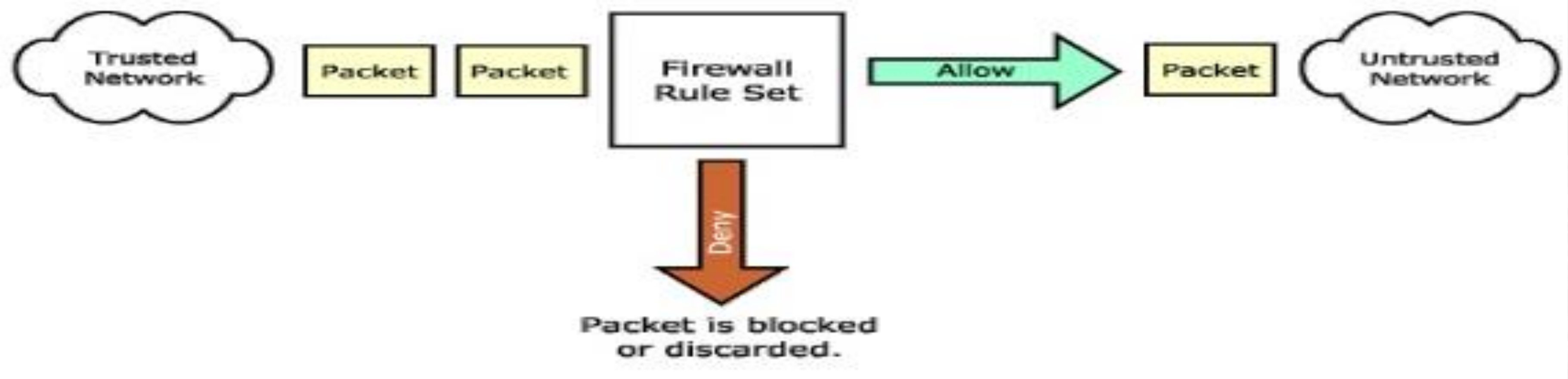
Filtering rules are based on number of fields in the IP and TCP/UDP headers.

Receive each packet. Apply rules.
If no rules, apply default rules.

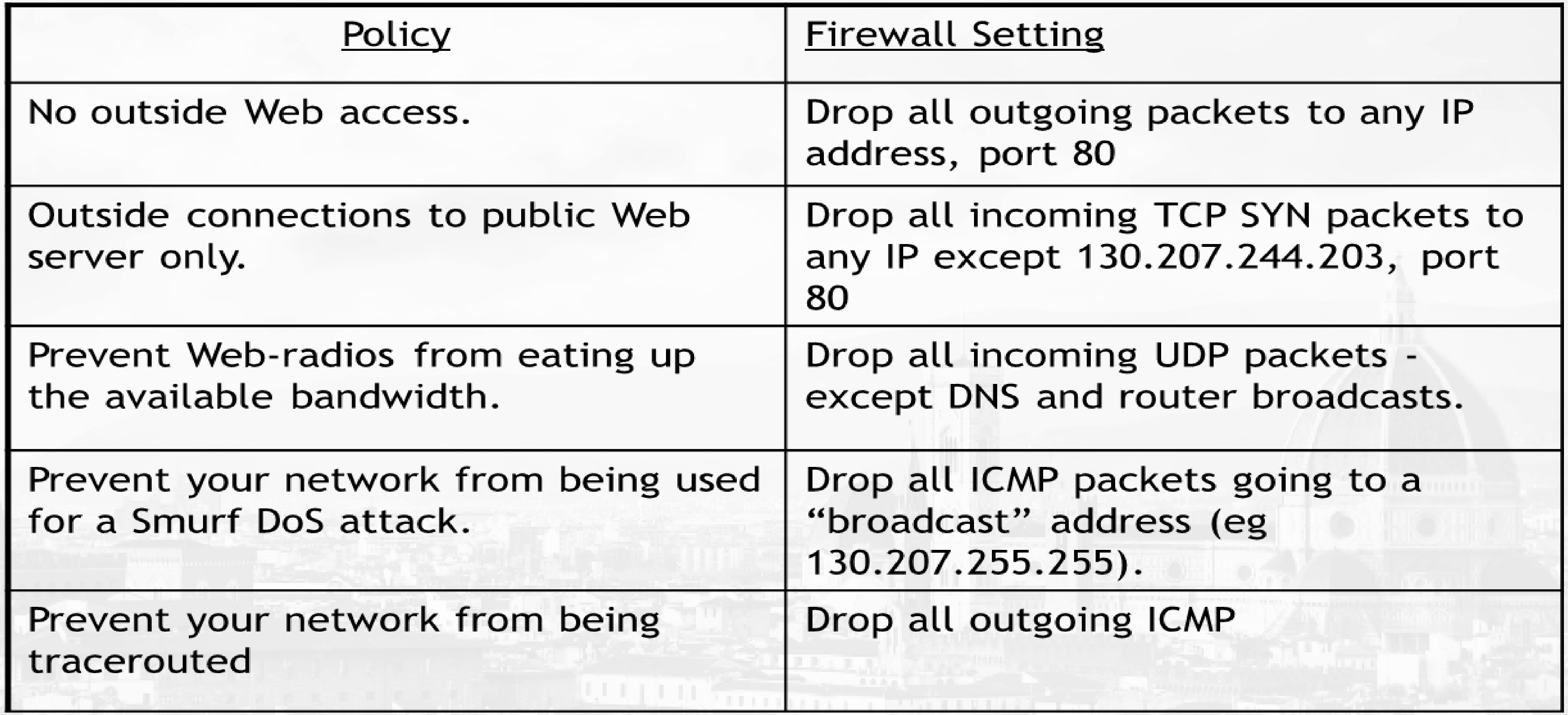


Outgoing packets

Incoming packets



Filtering rule examples



Policy	Firewall Setting
No outside Web access.	Drop all outgoing packets to any IP address, port 80
Outside connections to public Web server only.	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80
Prevent Web-radios from eating up the available bandwidth.	Drop all incoming UDP packets - except DNS and router broadcasts.
Prevent your network from being used for a Smurf DoS attack.	Drop all ICMP packets going to a “broadcast” address (eg 130.207.255.255).
Prevent your network from being tracerouted	Drop all outgoing ICMP

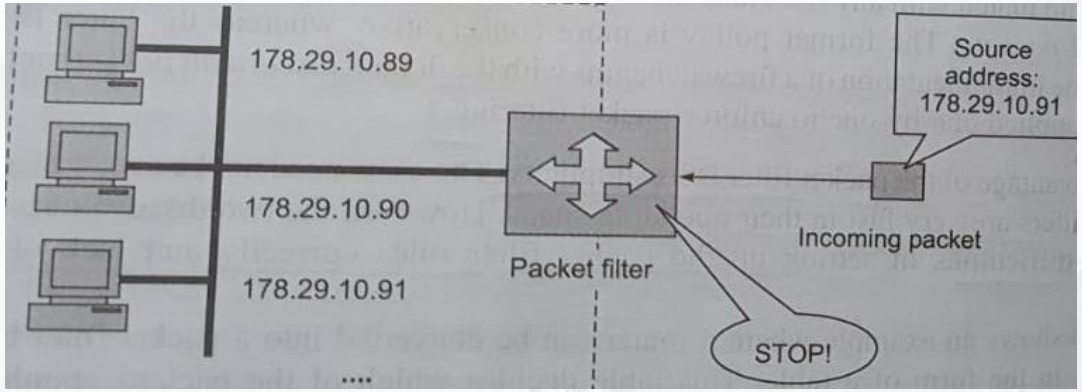
- ❖ Advantages:
  - Simplicity
  - Transparency to users
  - High speed

- ❖ Disadvantages:
  - Difficulty of setting up packet filter rules correctly
  - Lack of Authentication

- Packet filter firewalls do not examine upper-layer data, they cannot prevent attacks that employ application-specific vulnerabilities or functions.
- Because of the limited information available to the firewall, the logging functionality present in packet filter firewalls is limited.
- Most packet filter firewalls do not support advanced user authentication schemes.
- Packet filter firewalls are generally vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack, such as network layer address spoofing.
- Due to the small number of variables used in access control decisions, packet filter firewalls are susceptible to security breaches caused by improper configurations.

Countermeasures to attacks of Packet Filter firewall

❖ **IP address spoofing:** The countermeasure is to discard packets with an inside source address if the packet arrives on an external interface.

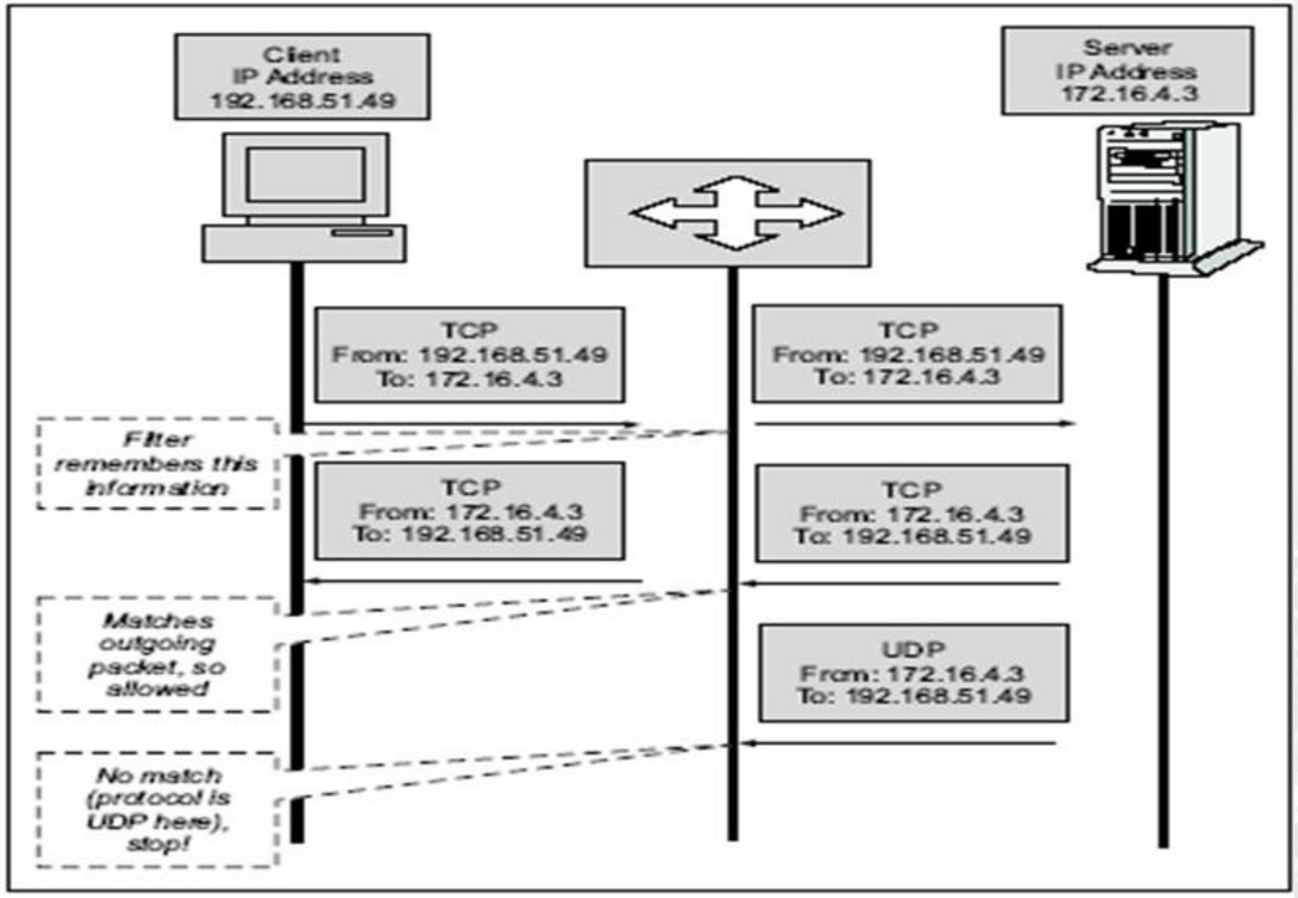


❖ **Source routing attacks:** The countermeasure is to discard all packets that do not analyze the source routing information.

❖ **Tiny fragment attacks:** The countermeasure to inspect all fragment and setting restriction on minimum size of packet.

❖ Dynamic packet filter or Stateful packet filter or Stateful firewall

- keeps track of the state of network connections (such as TCP streams) traveling across it.
- Stateful firewall is able to hold in memory significant attributes of each connection, from start to finish. These attributes, which are collectively known as the state of the connection, may include such details as the IP addresses and ports involved in the connection and the sequence numbers of the packets traversing the connection.


Client IP Address 192.168.51.49
Server IP Address 172.16.4.3
TCP From: 192.168.51.49 To: 172.16.4.3
TCP From: 192.168.51.49 To: 172.16.4.3
Filter remembers this information
TCP From: 172.16.4.3 To: 192.168.51.49
TCP From: 172.16.4.3 To: 192.168.51.49
Matches outgoing packet, so allowed
UDP From: 172.16.4.3 To: 192.168.51.49
No match (protocol is UDP here), stop!

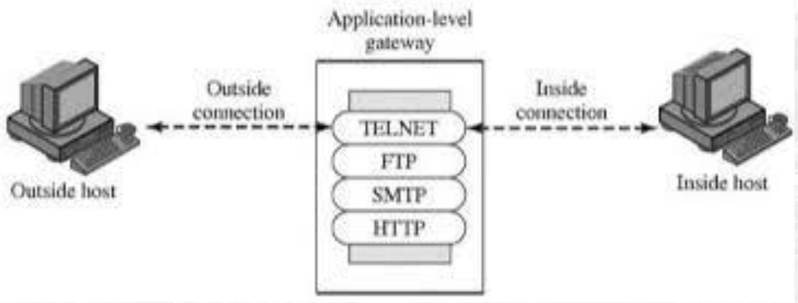
❖ Stateless firewall

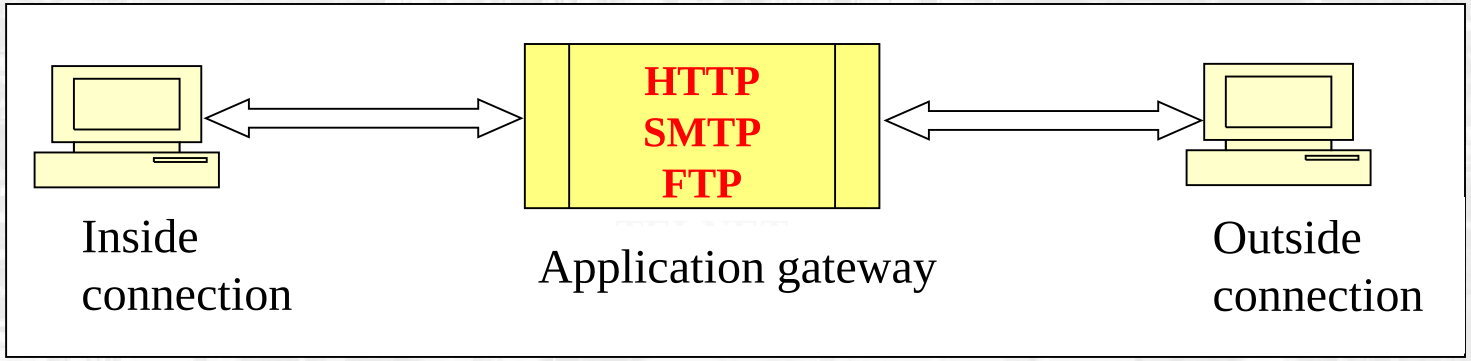
- Treats each network frame (Packet) in isolation. Such a firewall has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is just a rogue packet.

- The classic example is the File Transfer Protocol, because by design it opens new connections to random ports.

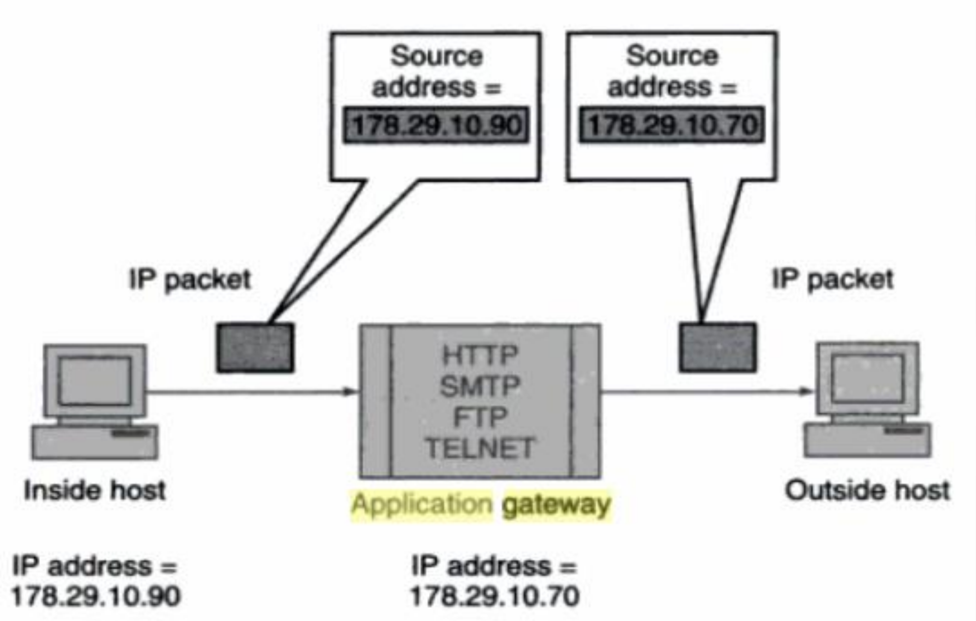
Application-Level Gateway

- An application-level gateway, also called an application proxy, acts as a relay of application-level traffic.
- The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed.
- When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints.
- If the gateway does not implement the proxy code for a specific application, the service is not supported and cannot be forwarded across the firewall.





Circuit Gateway



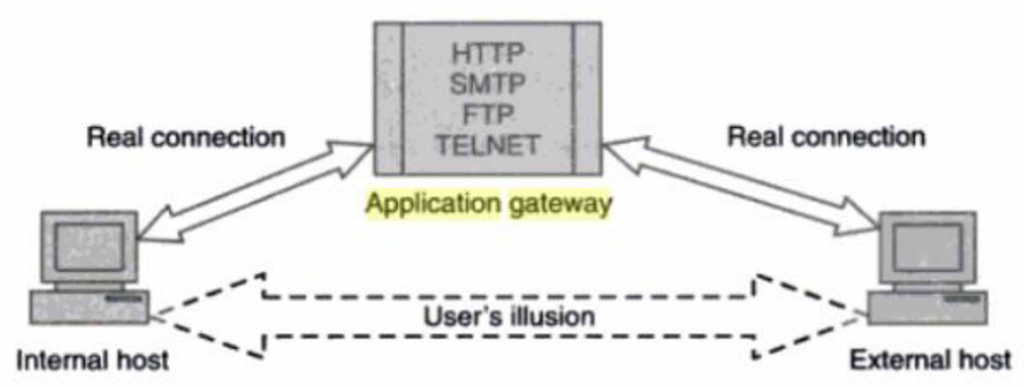


Figure: Application gateway creates an illusion

Figure: Circuit gateway operation

- Application-level gateways tend to be more secure than packet filters.
- The application-level gateway only scrutinize a few allowable applications.
- The application level gateways logs and audit all incoming traffic at the application level.

Drawback: Additional processing overhead on each connection.

Intrusion Detection Systems (IDS)

- **Intrusion:** A set of actions aimed to compromise the security goals
- **Intrusion detection:** The process of identifying and responding to intrusion activities.
- **Intrusion prevention:** Extension of ID with exercises of access control to protect computers from misuse.

- Intruders may be from outside the network or legitimate users of the network.

- Three types of intruders:
  - **Masquerader:** an unauthorized user who penetrates a system's access control to exploit other's account; most likely an outsider
  - **Misfeasor:** a legitimate user but accesses data, program or resources for which he/she is not authorized; generally an insider
  - **Clandestine user:** an individual those have supervision/administrative control over the system and misuse the authoritative power given to them

IDS functions:

- ❖ It monitors and analyzes the user and system activities
- ❖ It performs auditing of the system files and other configurations and the operating system
- ❖ It assesses the integrity of system and data files
- ❖ It conducts an analysis of patterns based on known attacks
- ❖ It detects errors in system configuration
- ❖ It detects and cautions if the system is in danger

Firewall	IDS
A firewall is a hardware and/or software which functions in a networked environment to block unauthorized access while permitting authorized communications.	An Intrusion Detection System (IDS) is a software or hardware device installed on the network (NIDS) or host (HIDS) to detect and report intrusion attempts to the network.
A firewall can block an unauthorized access to network (E.g. A **watchman** standing at gate can block a thief)	An IDS can only report an intrusion; it cannot block it (E.g. A **CCTV camera** which can alert about a thief but cannot stop it)
A firewall **cannot detect security breaches** for traffic that does not pass through it (E.g. a gateman can watch only at front gate. He is not aware of wall-jumpers)	IDS is fully **capable of internal security** by collecting information from a variety of system and network resources and analyzing the symptoms of security problems
Firewall doesn’t inspect content of permitted traffic. (A gateman will never suspect an employee of the company)	IDS keeps a check of overall network
No man-power is required to manage a firewall.	An administrator (man-power) is required to respond to threats issued by IDS
Firewalls are most visible part of a network to an outsider. Hence, more vulnerable to be attacked first. (A gateman will be the first person attacked by a thief!!)	IDS are very difficult to be spotted in a network (especially stealth mode of IDS).

Intrusion Detection Method

Detection Method:

Analysis approach: piecing the evidences together

- ❖ Misuse detection (signature-based)
- ❖ Anomaly detection (statistical-based/behavior-based)

Deployment/Location :

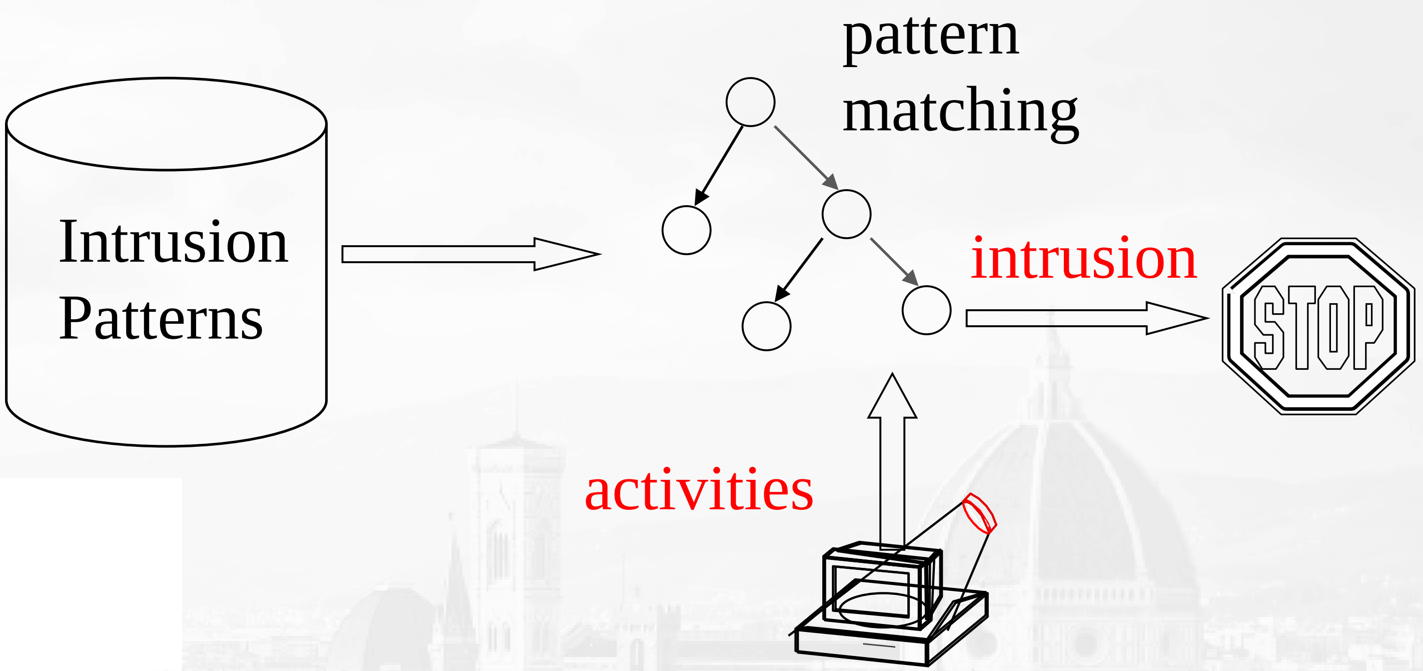
- ❖ Network-based
- ❖ Host-based

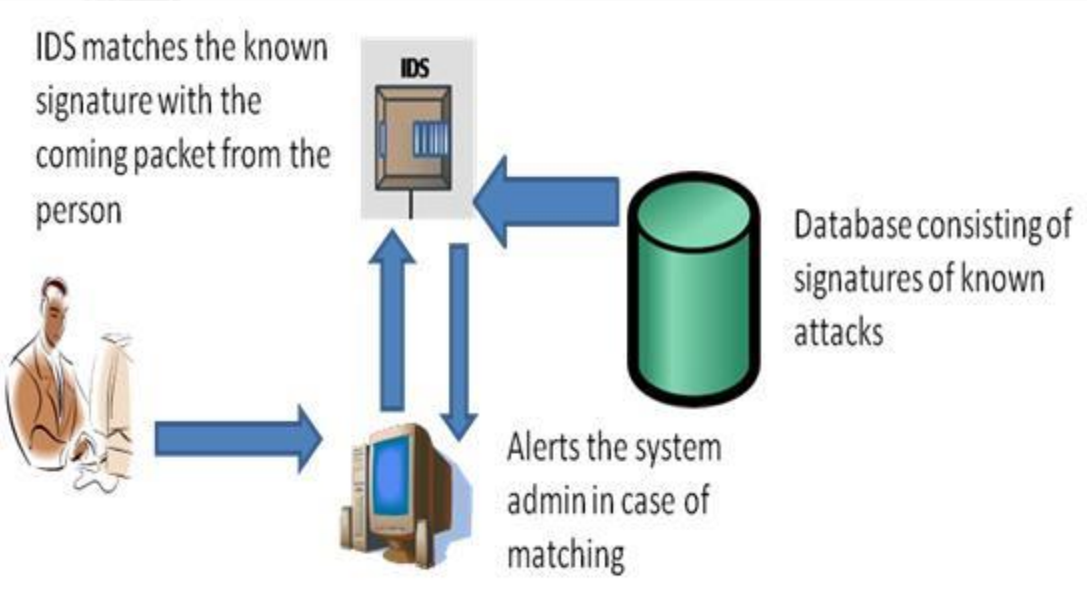
❖ Misuse Detection (signature-based)

- data packets e.g. logs
- model of attack pattern

known attacks report to admin
Eg. SNORT IDS

- Can’t detect new attacks



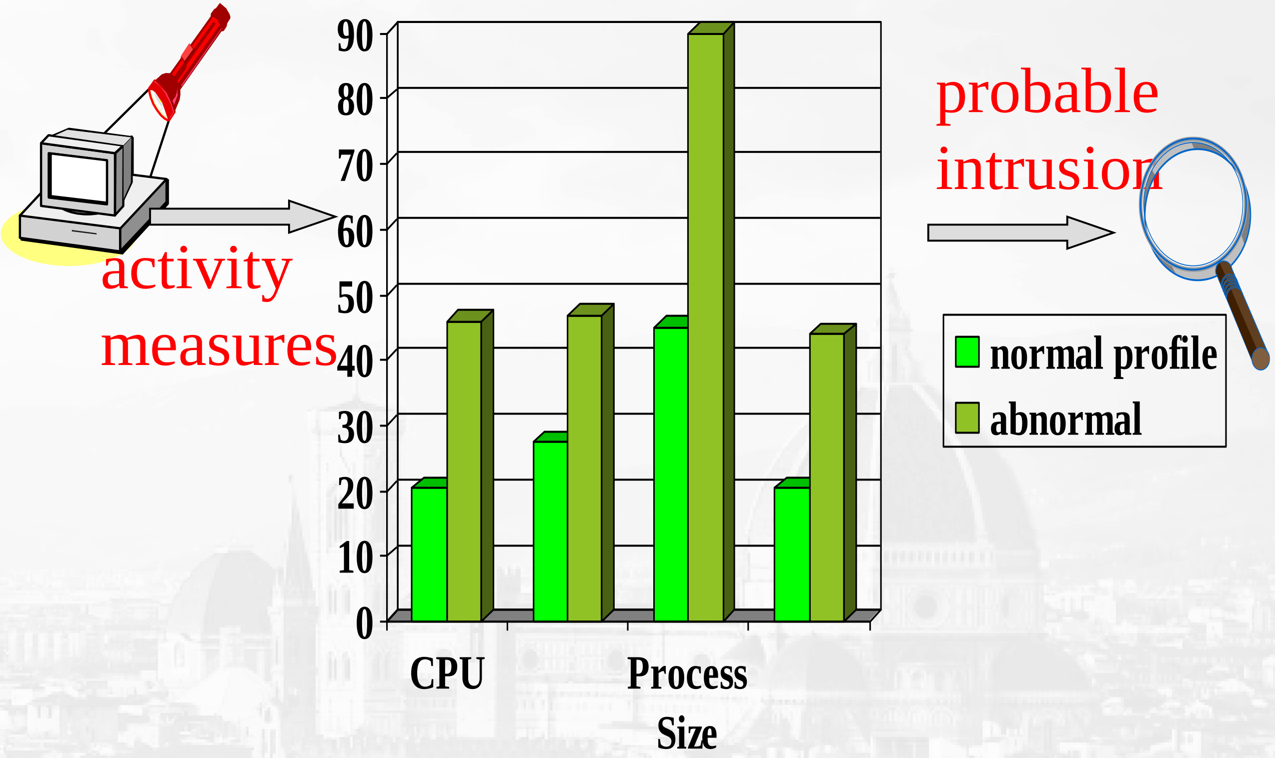

IDS matches the known signature with the coming packet from the person

Database consisting of signatures of known attacks

Alerts the system admin in case of matching

❖ Anomaly detection (Statistical)

- This IDS models the normal usage of the network as a noise characterization.
- Anything distinct from the noise is assumed to be an intrusion activity.
  - E.g flooding a host with lots of packet.
- The primary strength is its ability to recognize novel attacks.
- **Threshold**
- **Mean and standard deviation**



Host Based IDS

- Installed on individual host or device on network.
- Makes use of the resources of a host server – disk space, RAM and CPU time
- It monitor data packets from the device only and will alert the admin if suspicious activity is detected.
- Monitoring user activities & system programs executions
- Works on snapshots.
- Tracks behavior changes associated with misuse.
- Using OS auditing mechanisms
- Audit information includes events like the use of identification and authentication mechanisms (logins etc.), file opens and program executions, admin activities etc.
- This audit is then analyzed to detect trails of intrusion

- Strengths Of The Host Based IDS
  - Attack verification
  - System specific activity
  - Monitoring key components
  - Near Real-Time detection and response
  - No additional hardware

- Drawback Of The Host Based IDS
  - The kind of information needed to be logged in is a matter of experience.
  - Unselective logging of messages may greatly increase the audit and analysis burdens.
  - Selective logging runs the risk that attack manifestations could be missed.

Network Based IDS

- This IDS looks for attack signatures in network traffic
- Filter is applied to determine which traffic will be discarded or passed on to an attack recognition module.
- Monitor, Capture and Analyze.
- Detect malicious data present into packet.
- Analysis: Matches traffic to the library of known attack.

Strengths Of The Network Based IDS

- Packet analysis
- Real time detection and response
- Malicious intent detection
- Operating system independence

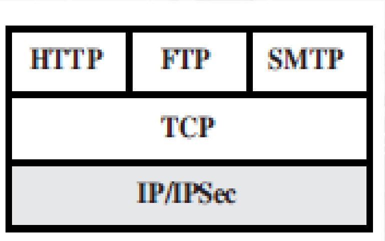
- **Limitations:** NIDS Analysis very difficult in busy n/w.

Web Security

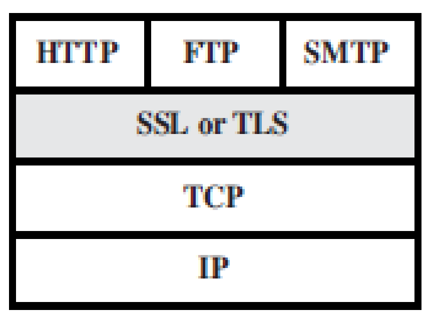
- Web now widely used by business, government, individuals
- But internet & web are vulnerable
- Have a variety of threats
  - Integrity
  - Confidentiality
  - Denial of service
  - Authentication
- Need added security mechanisms

Web Traffic Security Approaches

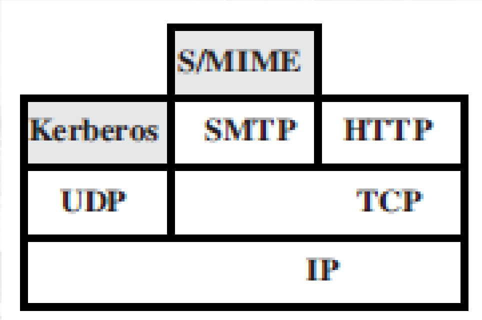
- One way to provide Web security is to use IP security.
- IPsec is transparent to end users and applications and provides a general-purpose solution.
- IPsec includes a filtering capability so that only selected traffic need incur the overhead of IPsec processing.
- Foremost example of Ipsec is Secure Sockets Layer (SSL) and Transport Layer Security (TLS).


HTTP FTP SMTP
TCP
IP/IPSec

(a) Network level


HTTP FTP SMTP
SSL or TLS
TCP
IP

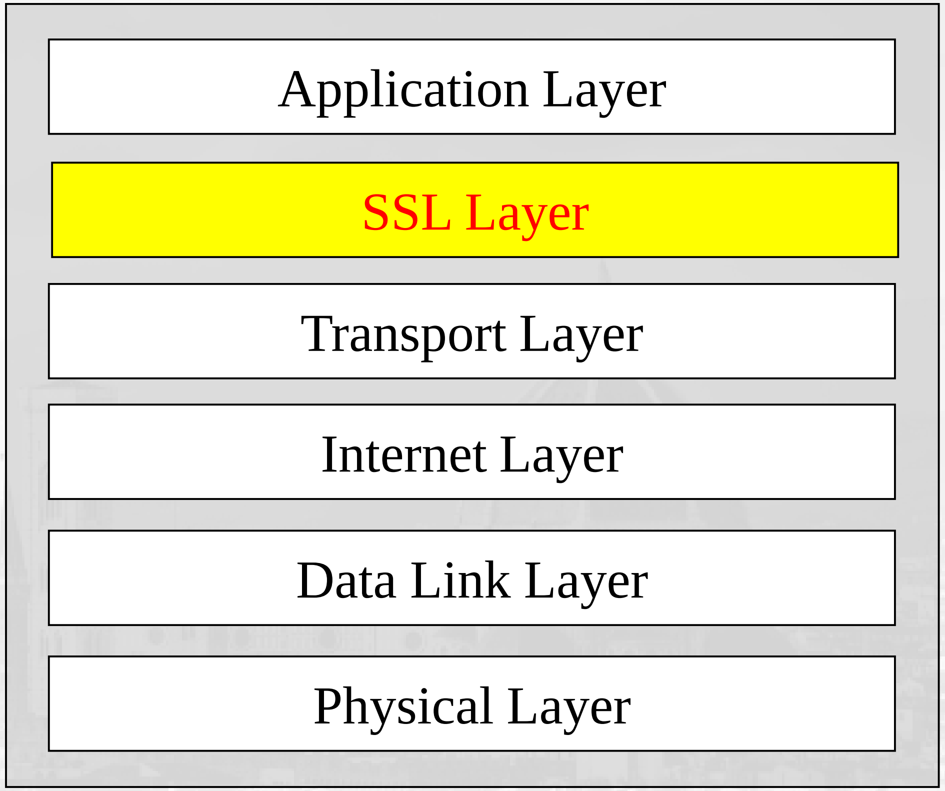
(b) Transport level


S/MIME
Kerberos SMTP HTTP
UDP TCP
IP

(c) Application level

Secured Socket Layer (SSL) Security

- Security service provides: authentication and confidentiality
- World’s most widely used security mechanism on the Internet
- Secures communication between a client and a server
- Located between the Application and Transport Layers of TCP/IP protocol suite
- Version 2, 3 and 3.1



Application Layer

SSL Layer

Transport Layer

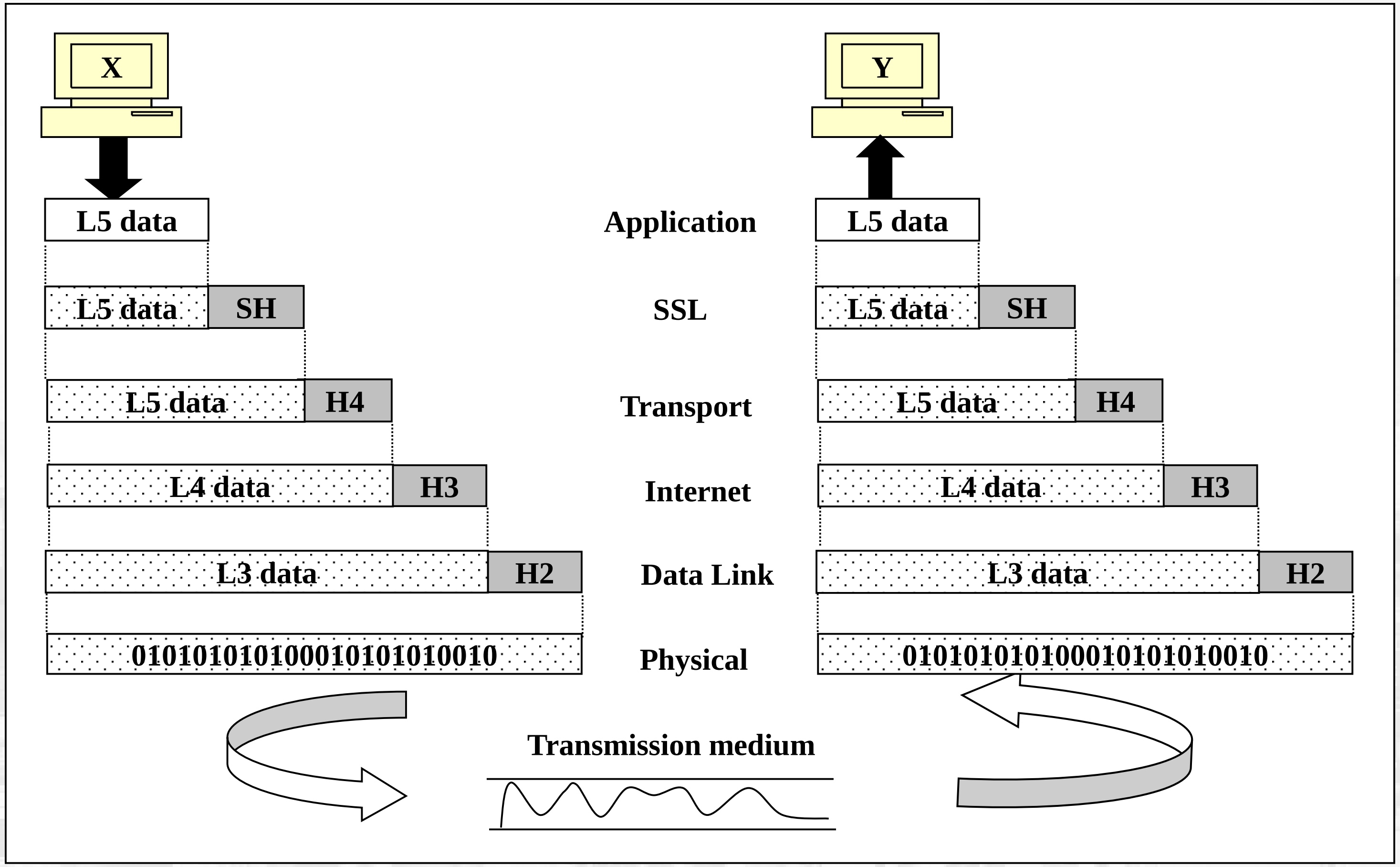
Internet Layer

Data Link Layer

Physical Layer

Data Exchange including SSL

- SSL perform encryption on data and add encryption information header



How SSL Works?

SSL has 3 Sub-protocols:

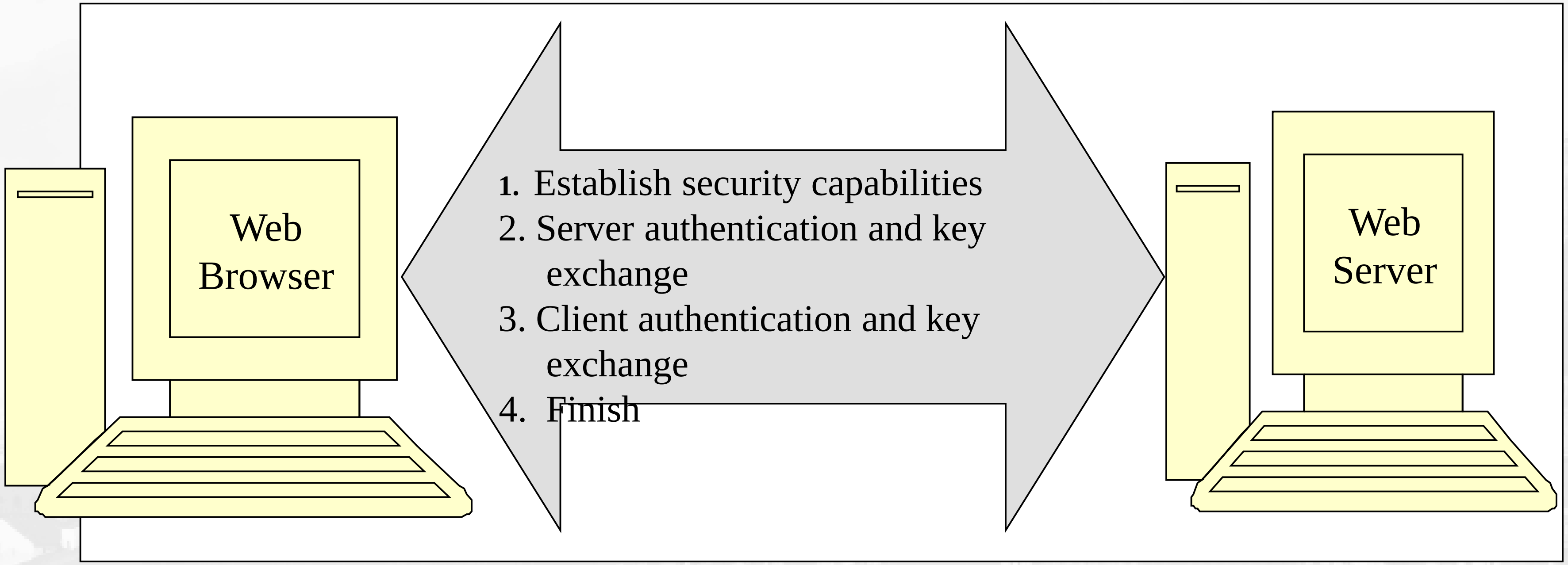
- Handshake Protocol
- Record Protocol
- Alert Protocol

SSL Handshake Protocol and Message Format

Type	Length	Content
1 byte	3 bytes	1 or more bytes

Message Type	Parameters
Hello request	None
Client hello	Version, Random number, Session id, Cipher suite, Compression method
Server hello	Version, Random number, Session id, Cipher suite, Compression method
Certificate	Chain of X.509V3 certificates
Server key exchange	Parameters, signature
Certificate request	Type, authorities
Server hello done	None
Certificate verify	Signature
Client key exchange	Parameters, signature
Finished	Hash value

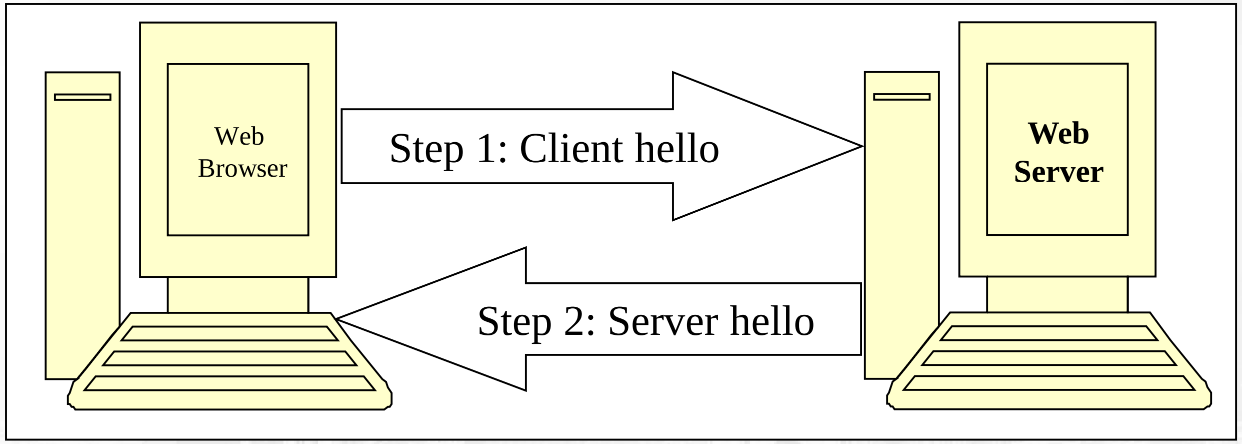
SSL Handshake Process



1. Establish security capabilities
2. Server authentication and key exchange
3. Client authentication and key exchange
4. Finish

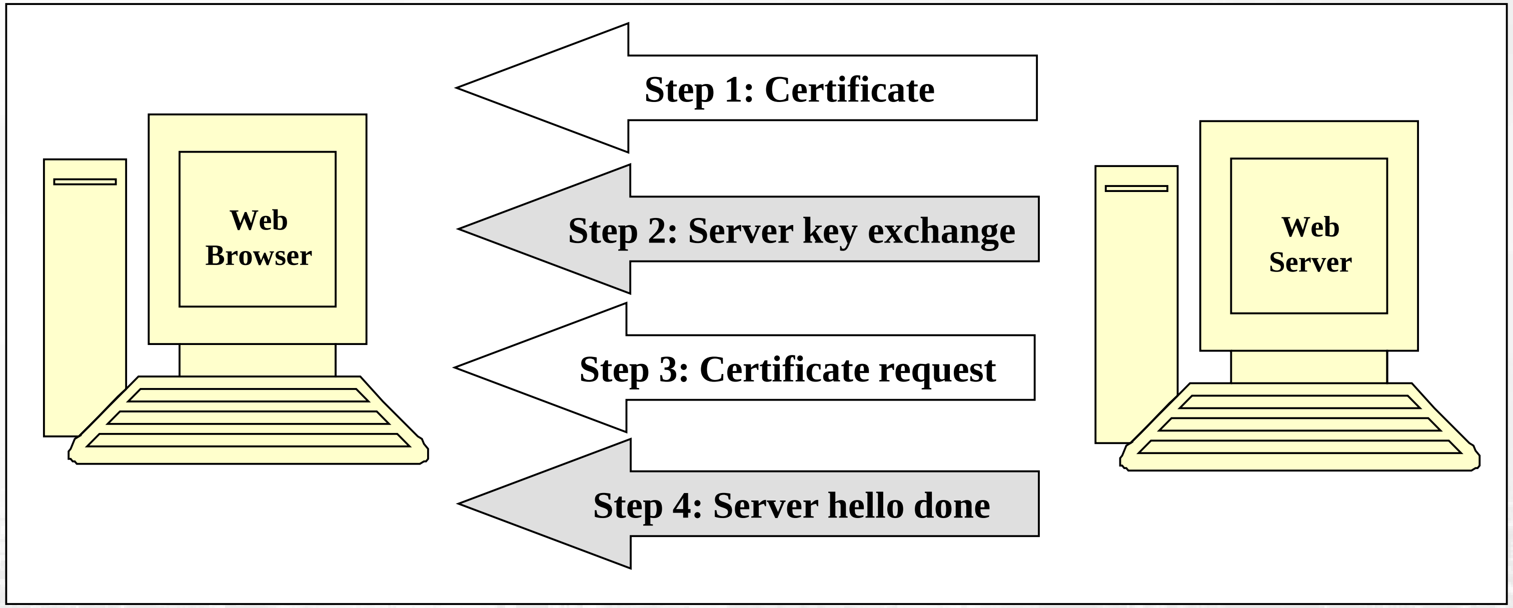
SSL Handshake – Phase 1: Establish security capabilities

- Version: 2, 3 or 3.1
- Random Number: actual communication, two sub-field:
  - 32-bit date time field
  - 28-byte random number
- Session id: 0 – new connection and nonzero – already a connection
- Cipher suite: list of cryptographic algorithm
- Compression method: list of compression algorithms



SSL Handshake – Phase 2: Server authentication and key exchange

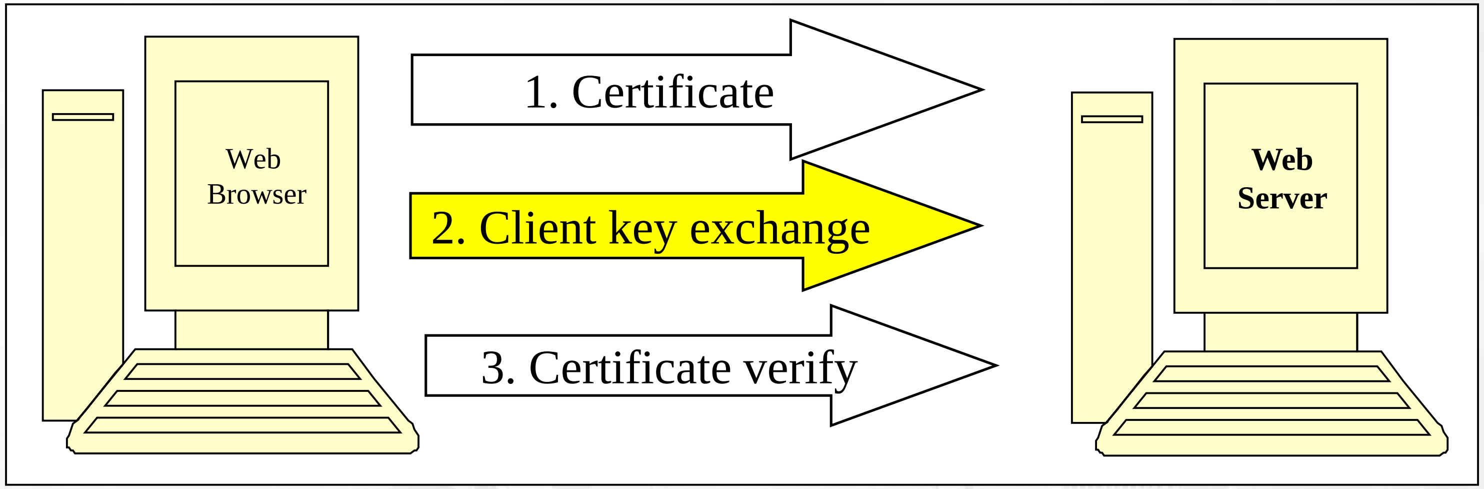
- Server sends digital certificate and it is mandatory
- Server key exchange is optional. The server send its public key as the certificate is not available
- Client verify certificate sent by the server and insure that all parameters send by server are acceptable


Web Browser
Step 1: Certificate
Step 2: Server key exchange
Step 3: Certificate request
Step 4: Server hello done
Web Server

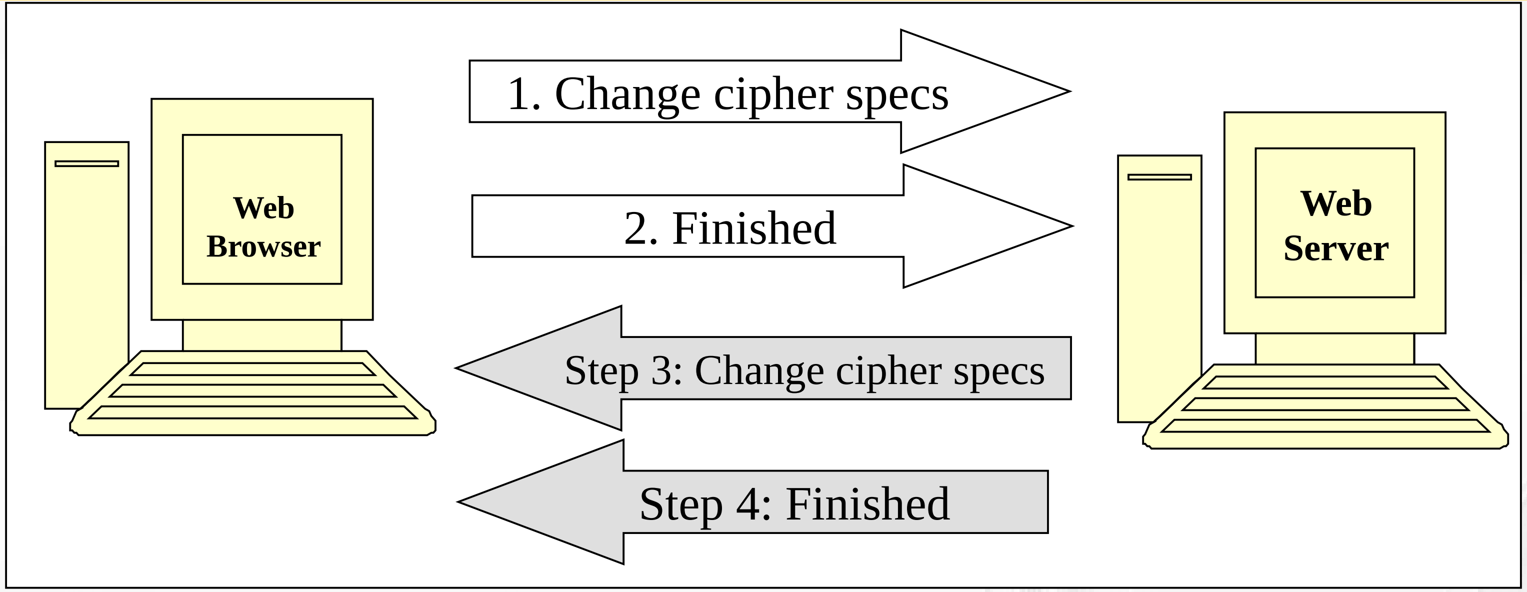
SSL Handshake – Phase 3: Client authentication and key exchange

- Client creates a 48-byte **pre-master secret** and encrypts it with the server's public key and sends this encrypted pre-master secret it to the server

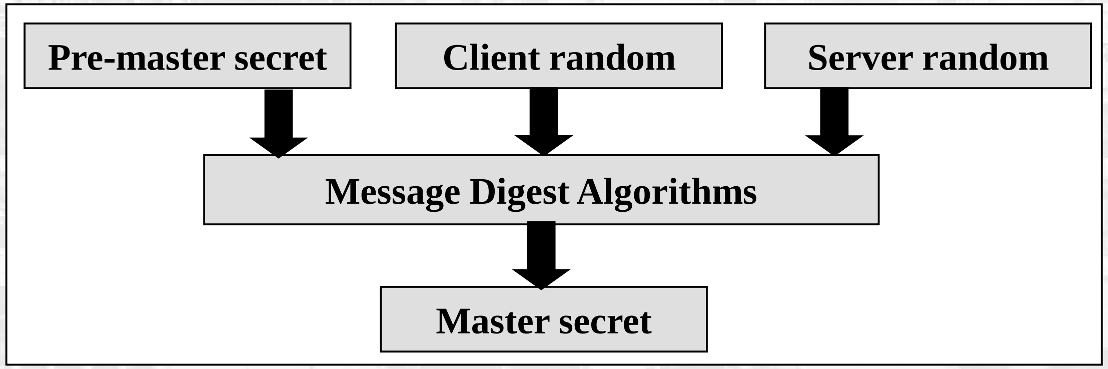
- Certificate verify is necessary only if server had demanded client authentication



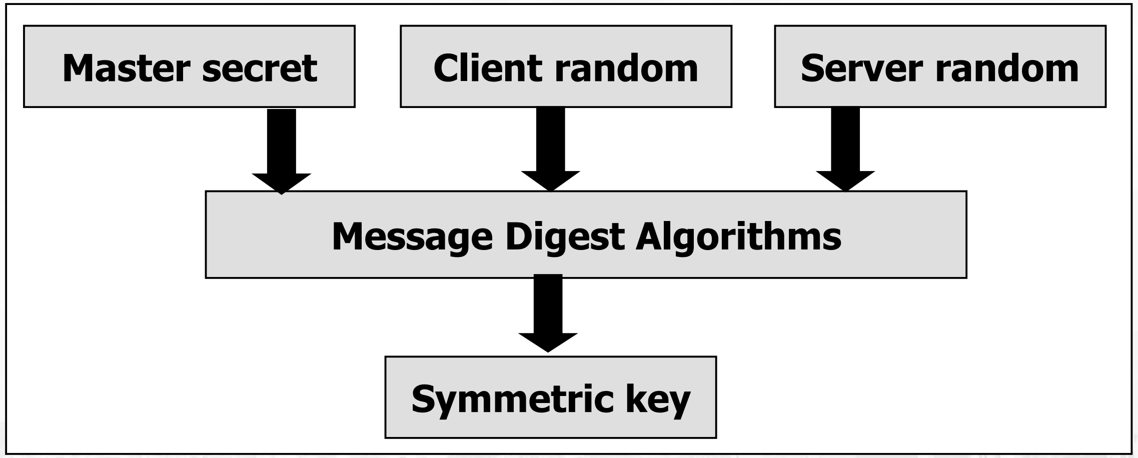
SSL Handshake – Phase 4: Finish



- The master secrete is used to generate keys and secrets for encryption and MAC computations

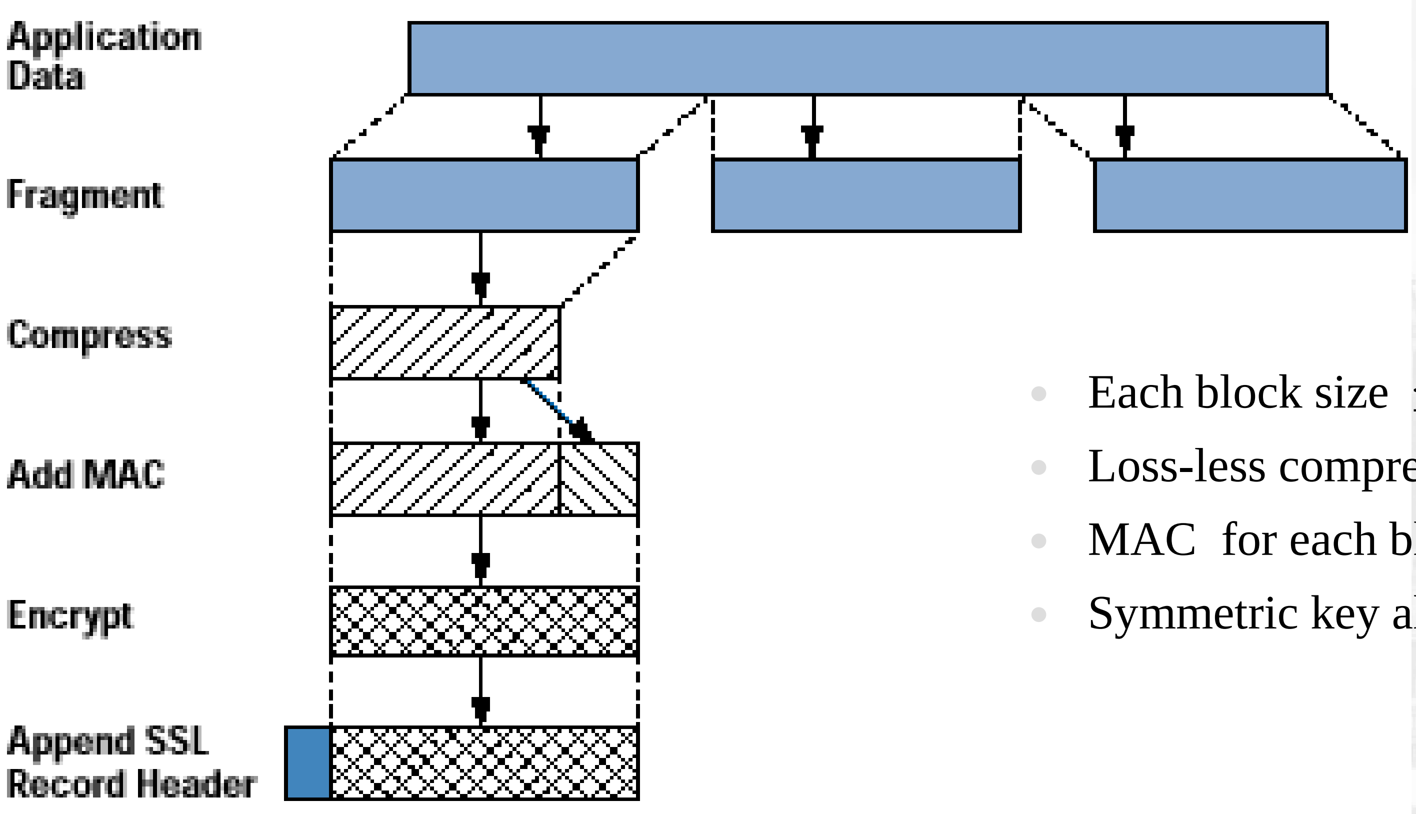


- Finally, the symmetric keys to be used by the client and the server are generated.



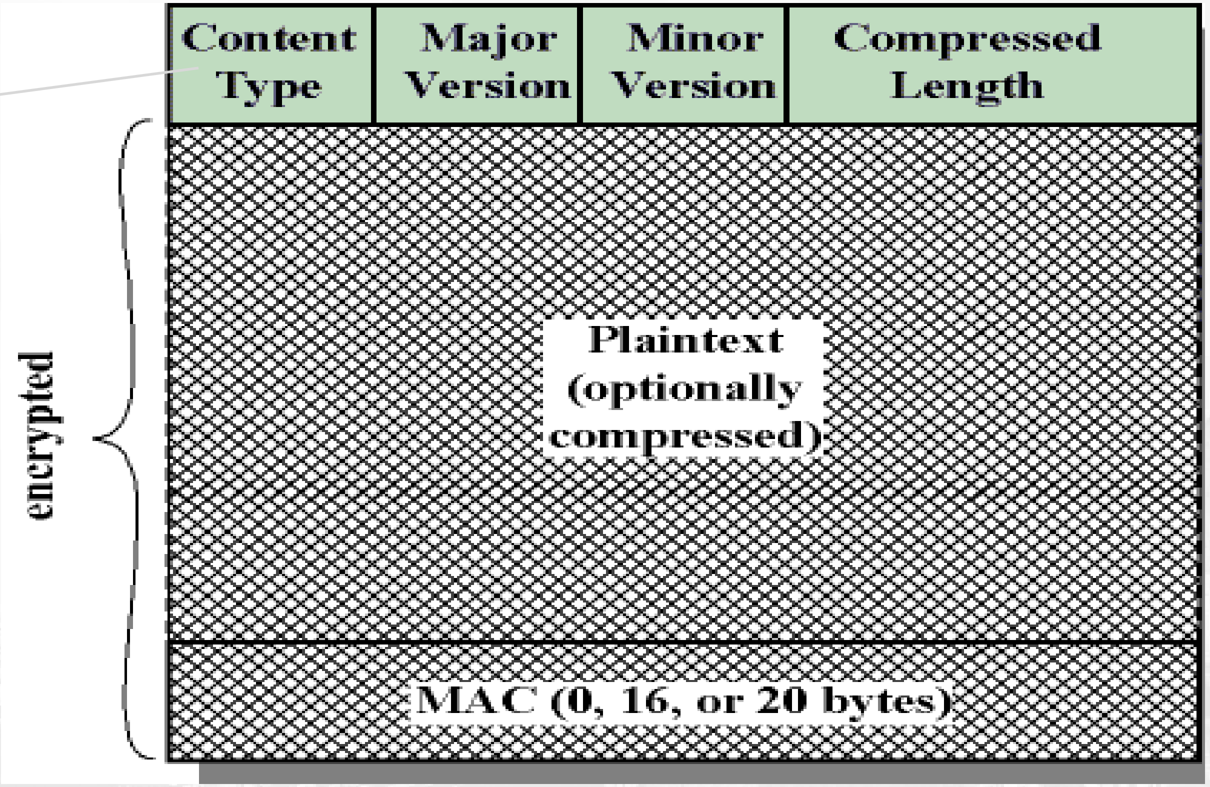
The Record Protocol

- Two service:
  - Confidentiality
  - Integrity



- Each block size $\leq 2^{14}$
- Loss-less compression mechanism
- MAC for each block
- Symmetric key algorithm

- Append header

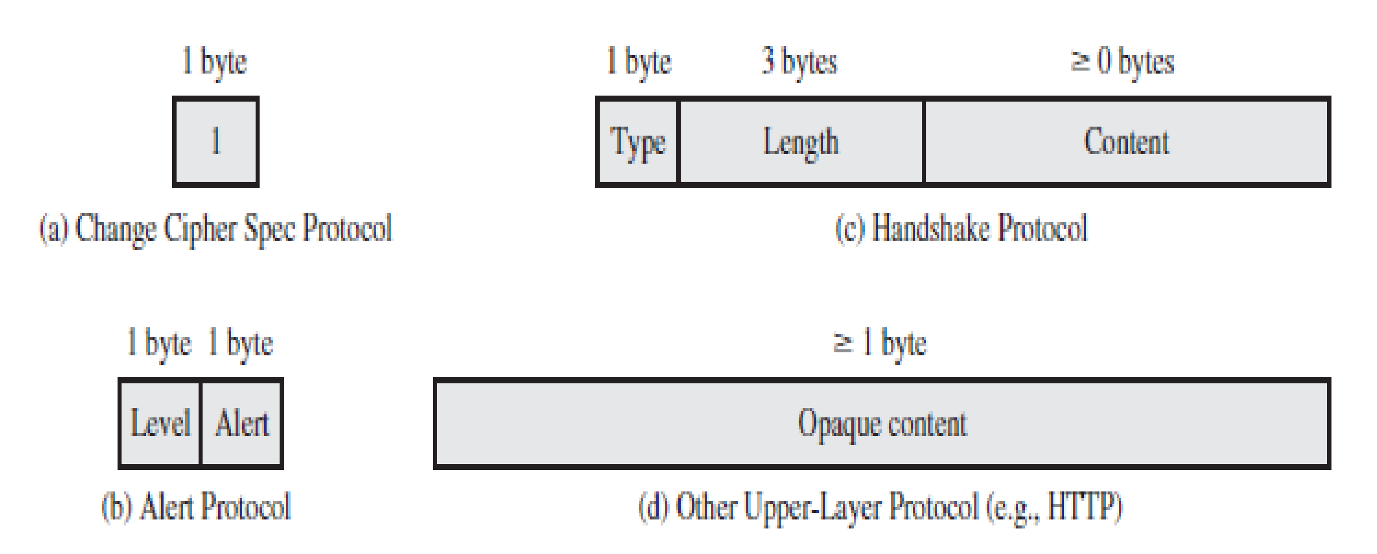


- Handshake, alert, cipher change

Change Cipher Spec Protocol

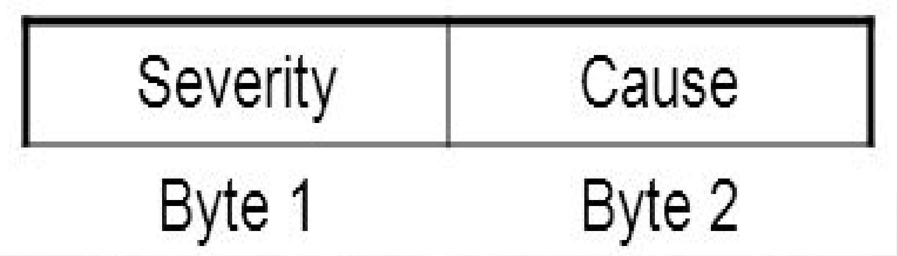
- This protocol uses the SSL Record protocol and consists of a single message (single byte with the value 1)

- The only purpose of this message is to cause the pending state to be copied into the current state, which updates the cipher suite to be used on this connection.



Alert Protocol

- When client or server detects an error, the detecting party sends an alert message to the other party.
  - If an **error is fatal**, both the parties immediately close SSL connection
  - Other error, which are not severe, do not result in the termination of the connection

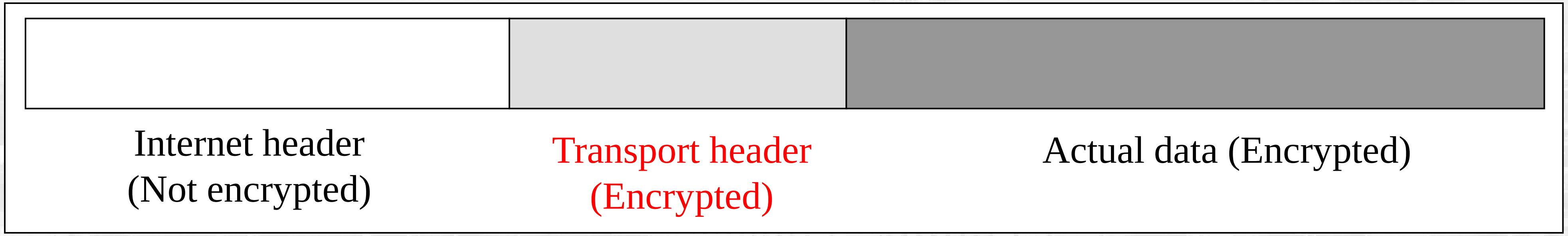


Severity	Cause
Byte 1	Byte 2

Fatal Alert	Description
Unexpected message	An inappropriate message was received.
Bad record MAC	A message is received without a correct MAC.
Decompression failure	The decompression function received an improper input.
Handshake failure	Sender was unable to negotiate an acceptable set of security parameters from the available options.
Illegal parameters	A field in the handshake message was out of range or was inconsistent with the other fields.

IP Security (IPsec)

- **Idea:** to encrypt and seal the transport and application layers data during transmission
- Internet Protocol Security (IPsec) provides for various security services on the IP layer, in IPv4 as well as IPv6, thus offering protection for protocols in the upper layers
- IPsec is typically used to secure communications between hosts and security gateways
- IPsec encompasses three functional areas: authentication, confidentiality, and key management.



❖ Applications

- Secure remote Internet access
- Secure branch office connectivity
- Set up communication with other organizations

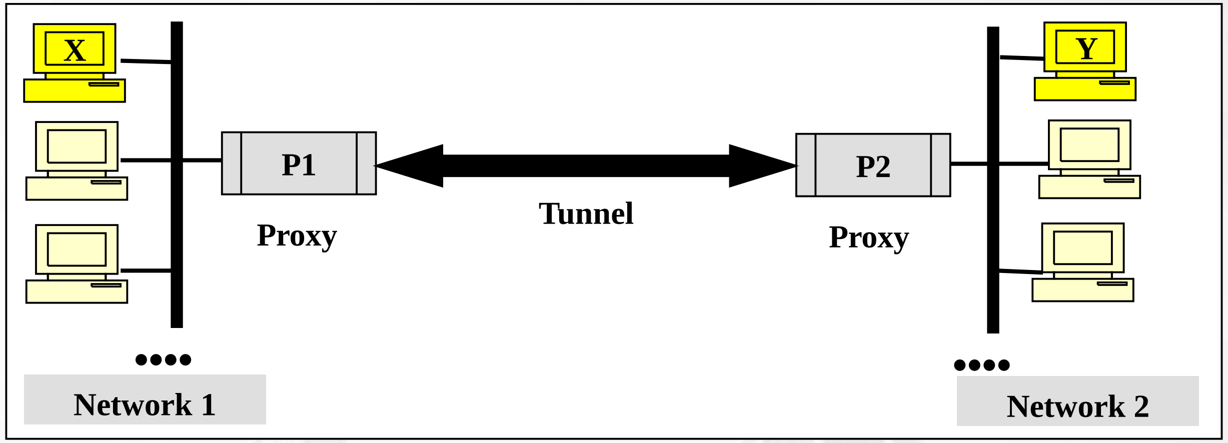
❖ Advantages

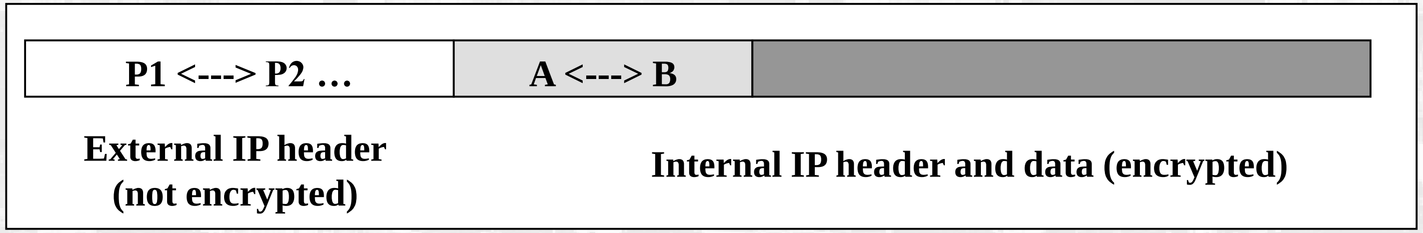
- IPSec is transparent to the end users
- When IPSec is configured to work with a firewall, it becomes the only entry - exit point for all traffic
- IPSec works at the network layer

- IPsec can operate in two modes:

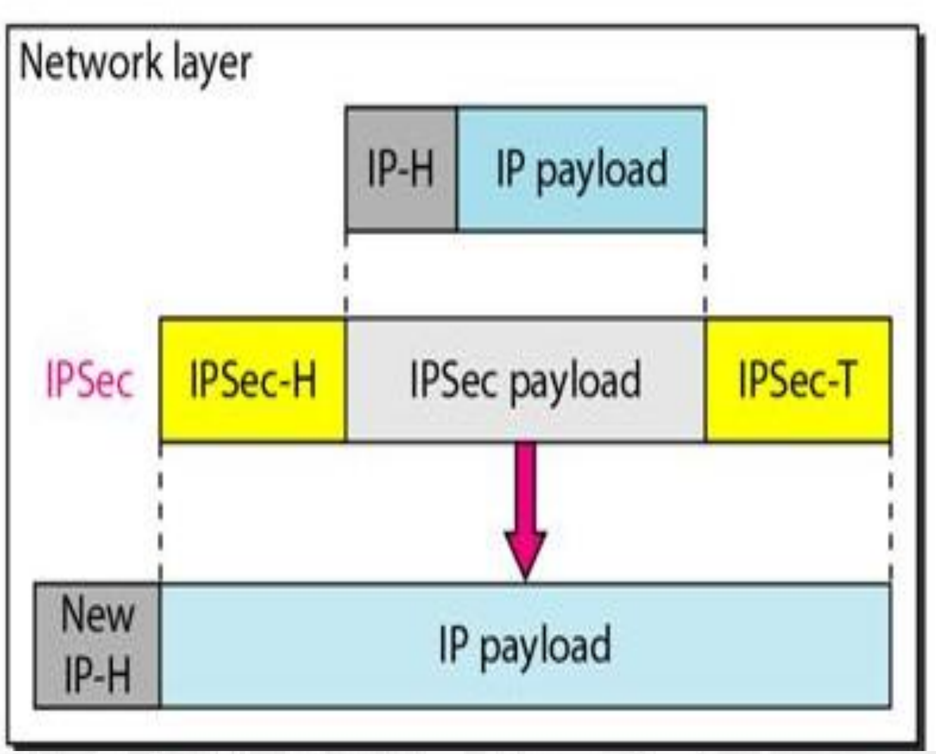
❖ **Tunnel mode**

  - typically used to tunnel IP traffic between two security gateways



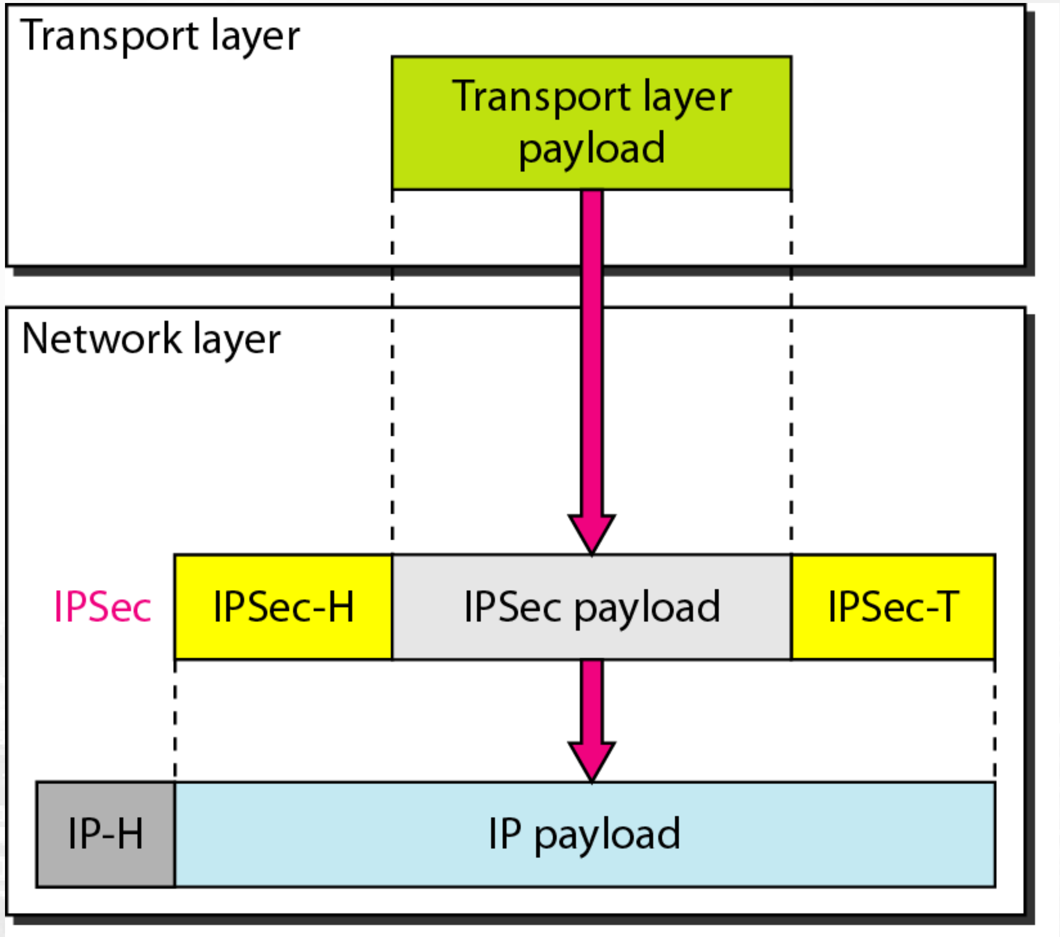


- IPsec protects the full IP datagram
- The tunnel mode is normally used between two routers, a host and a router



❖ Transport mode

- It does not hide source and destination addresses
- IPSec in the transport mode **does not protect the IP header**; it only **protects** the **information** coming from the transport layer.
- The transport mode is normally used when we need **host-to-host protection (end-to-end encryption)** of data.



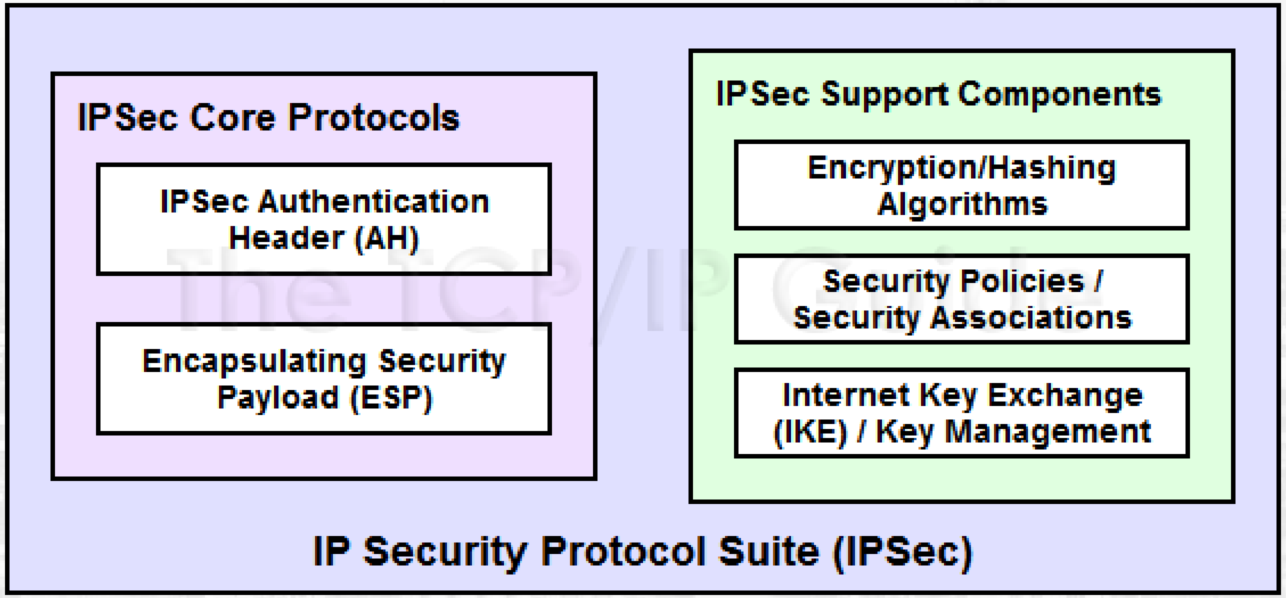
- IPsec provide two protocols:

- IPsec offers two services: authentication and confidentiality. Also, provides key management

❖ **Authentification header (AH):** allows to verify that the intermediate devices have not changed any of the data in the datagram

❖ **Encapsulated security payload (ESP):** AH ensures the integrity of the data in a datagram, but not its privacy.

- AH provides authentication, integrity
- ESP allows encryption to ensure privacy of a message



IPSec Core Protocols

IPSec Authentication Header (AH)

Encapsulating Security Payload (ESP)

IPSec Support Components

Encryption/Hashing Algorithms

Security Policies / Security Associations

Internet Key Exchange (IKE) / Key Management

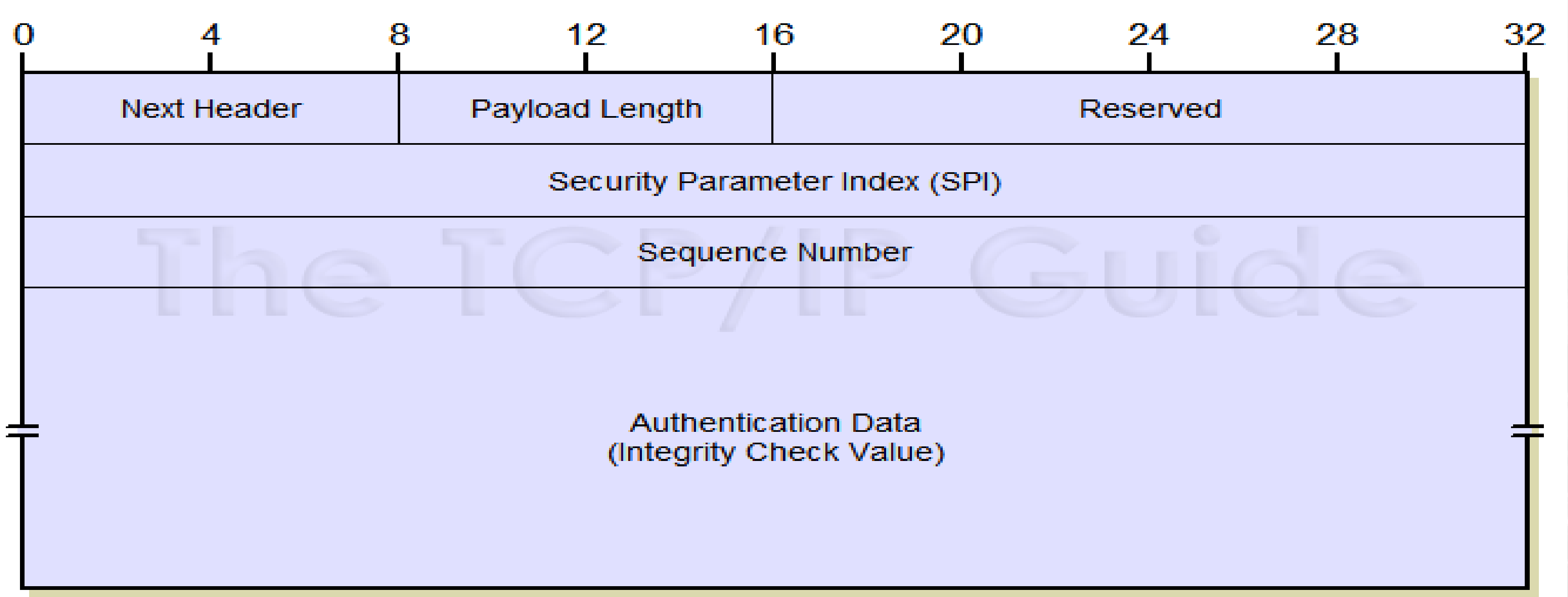
IP Security Protocol Suite (IPSec)

Internet Key Exchange (IKE) and Security Associations (SA)

- IPsec Security Association (SA) established using IKE
- Payload packets are encapsulated with ESP and/or AH
- IPsec Security Association could be configured manually (at least in theory) or using some other protocol
  - a one-way relationship between sender & receiver
    - specifies IPSec related parameters
  - Identified by 3 parameters:
    - Destination IP Address
    - Security Protocol: AH or ESP
    - Security Parameters Index (SPI)
      - A local 32-bit identifier (to be carried later to endpoints within AH and ESP)
  - There are several other parameters associated with an SA
    - stored locally in **Security Association Databases** (SAD)

Authentication Header (AH)

- AH deals with and prevents the replay attacks
- AH is based on MAC
- SPI used to identify SA for the traffic to which a datagram belongs



Next Header

Payload Length

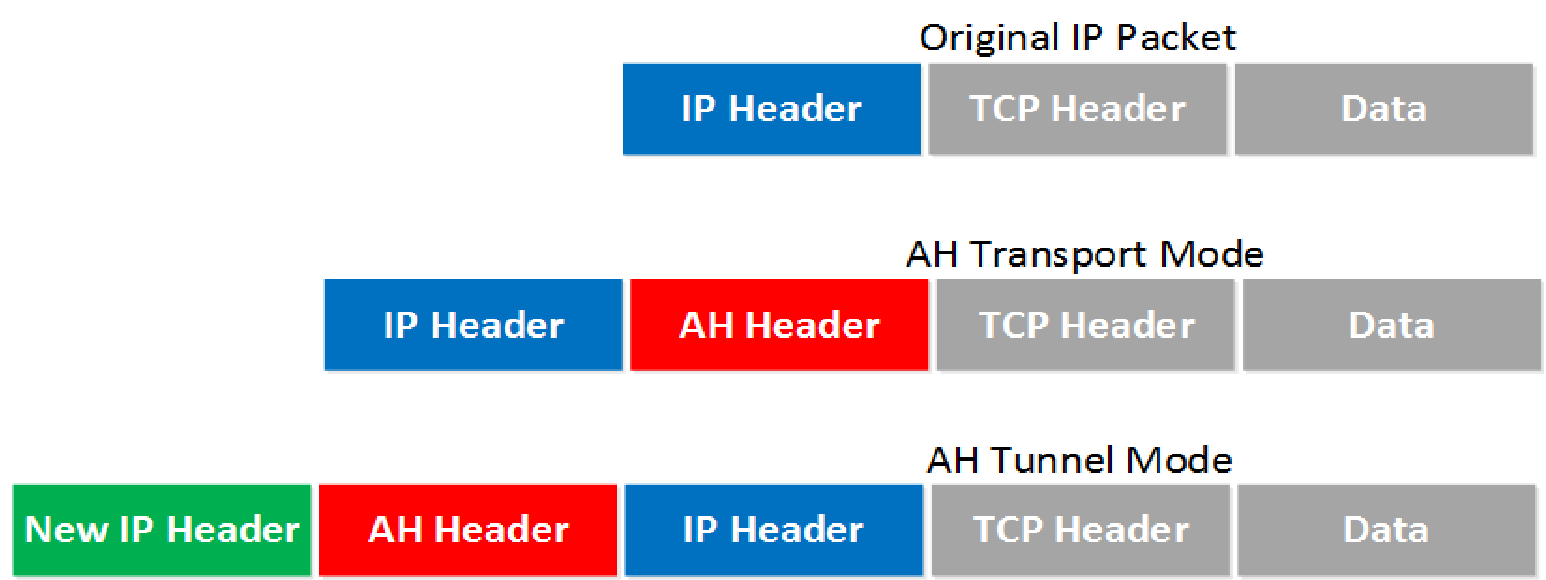
Reserved

Security Parameter Index (SPI)

Sequence Number

Authentication Data
(Integrity Check Value)

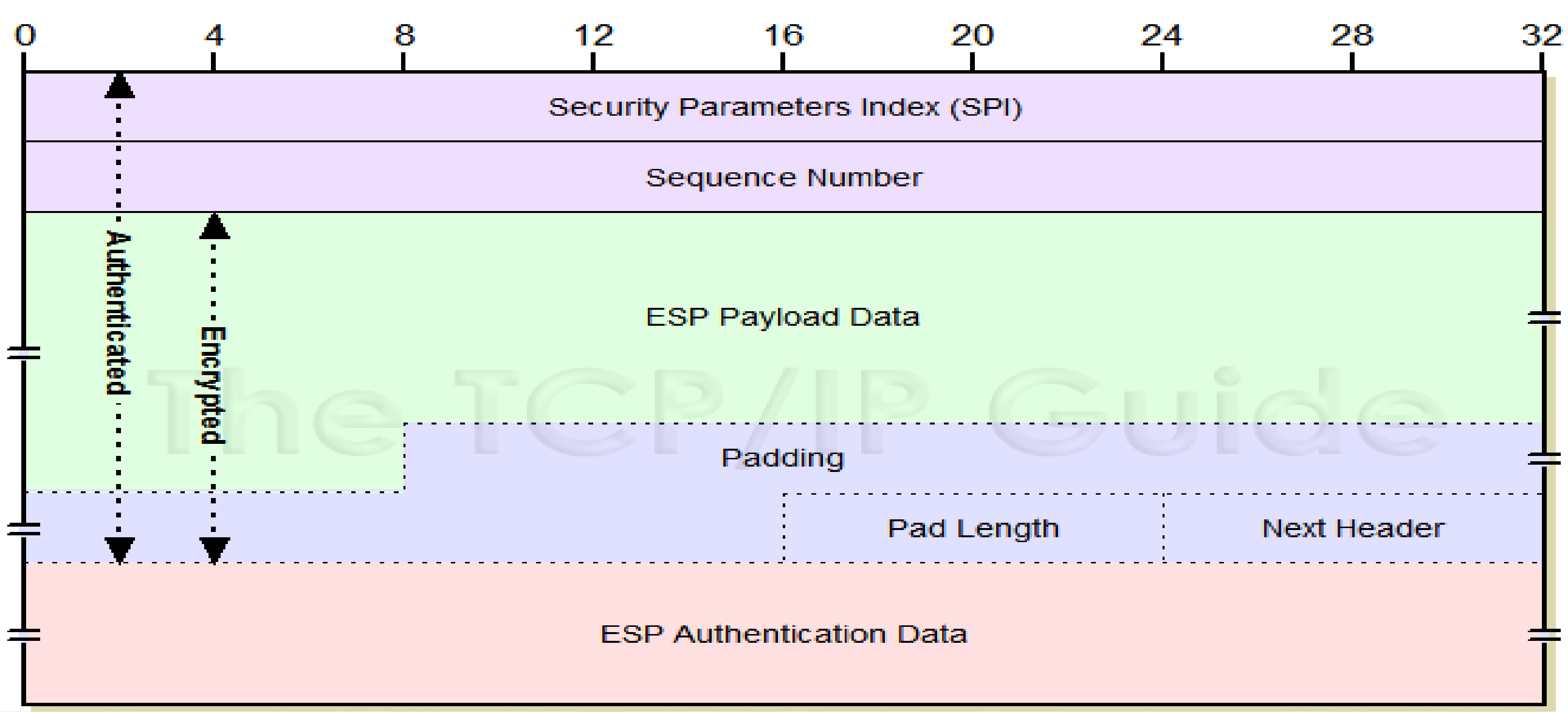
- AH transport mode and tunnel mode



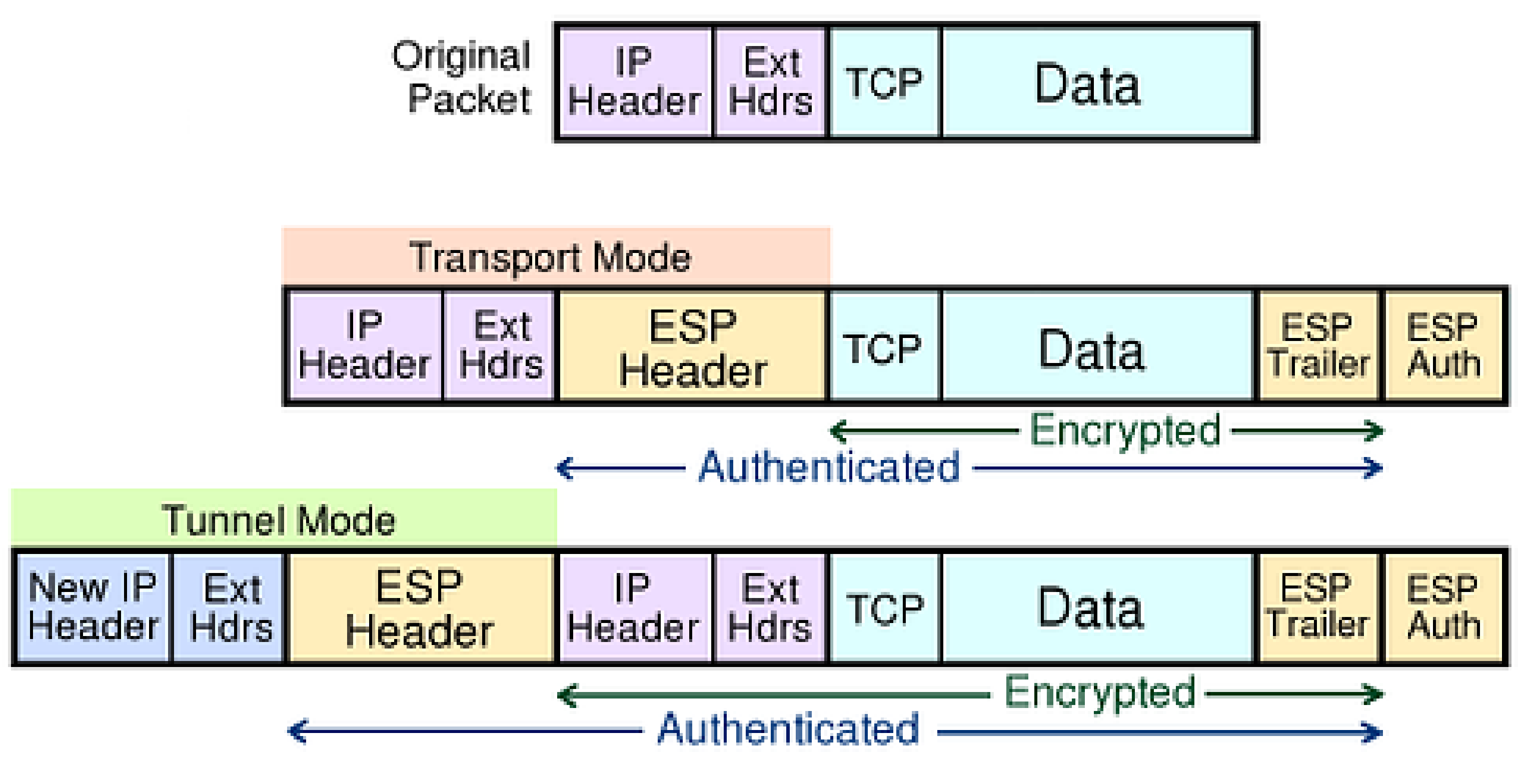
- In tunnel mode, entire IP packet is authenticated

Encapsulating Security Payload (ESP)

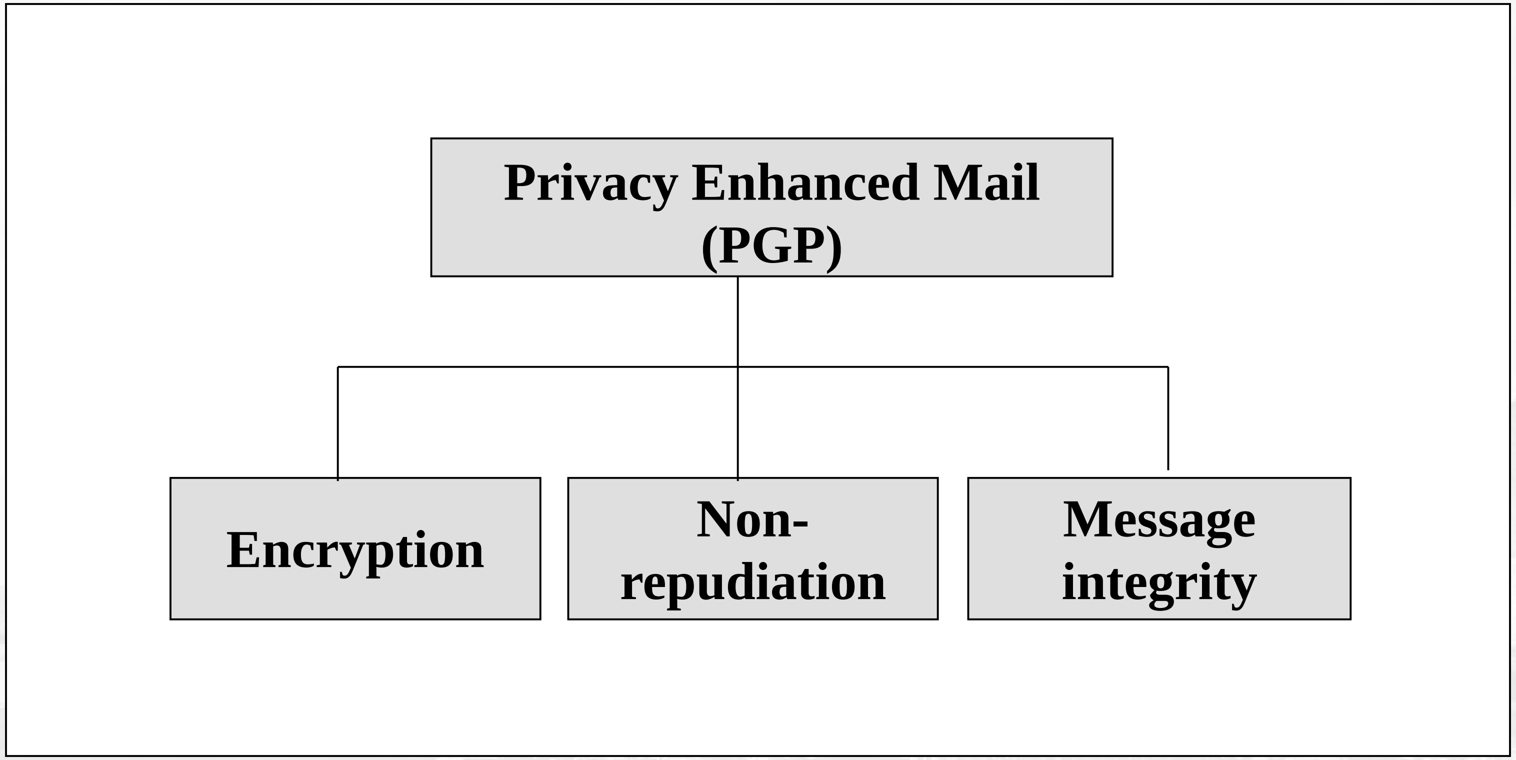
- Provides confidentiality and integrity of messages
- Based on symmetric key cryptography



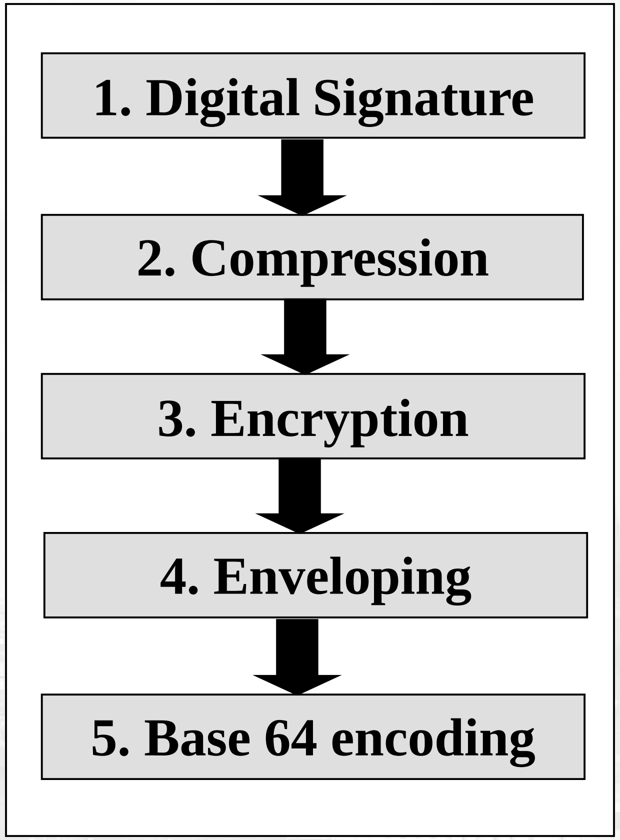
- ESP transport mode and tunnel mode



Web Security: PGP Security Features



PGP Operations



1. Digital Signature

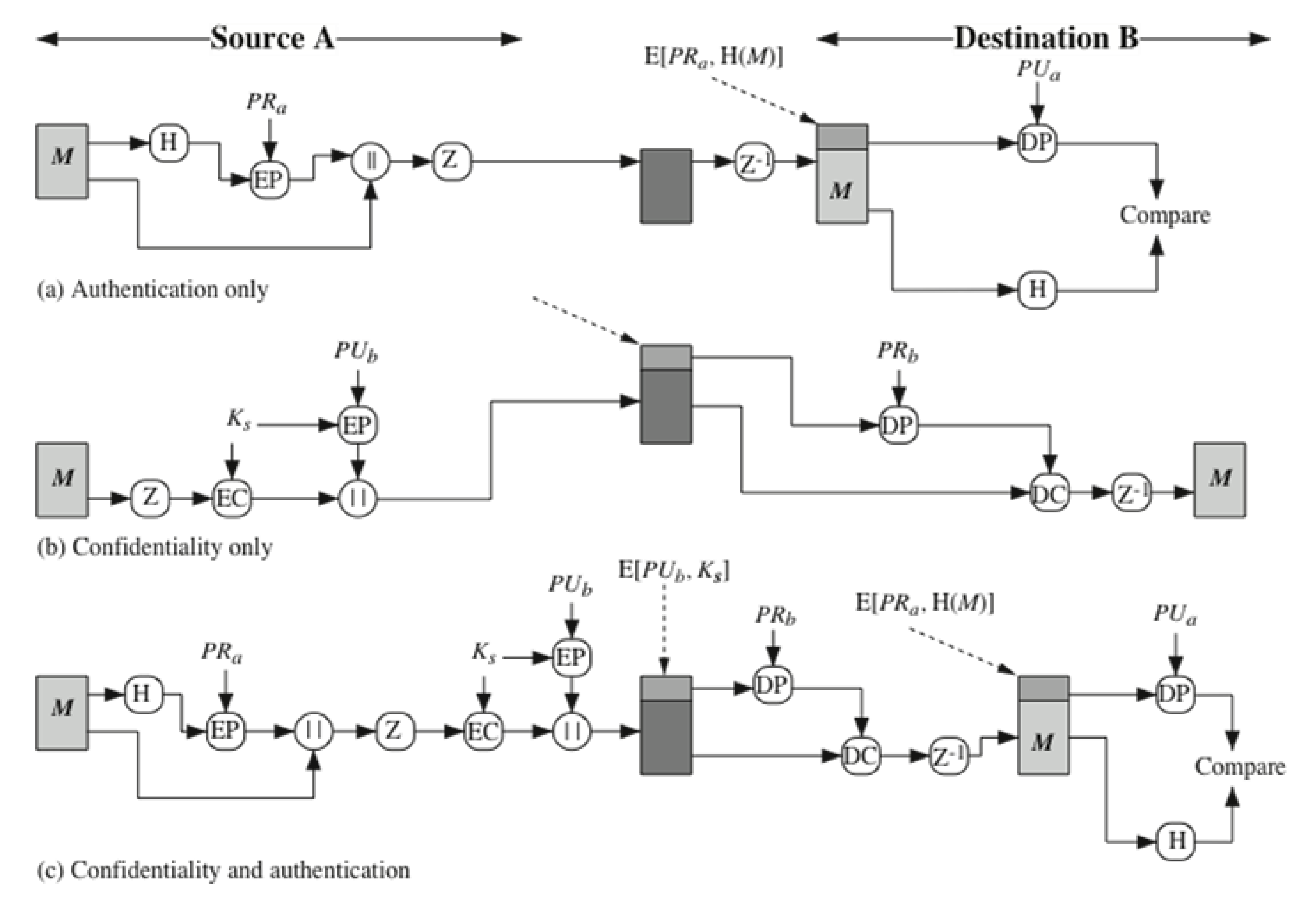
2. Compression

3. Encryption

4. Enveloping

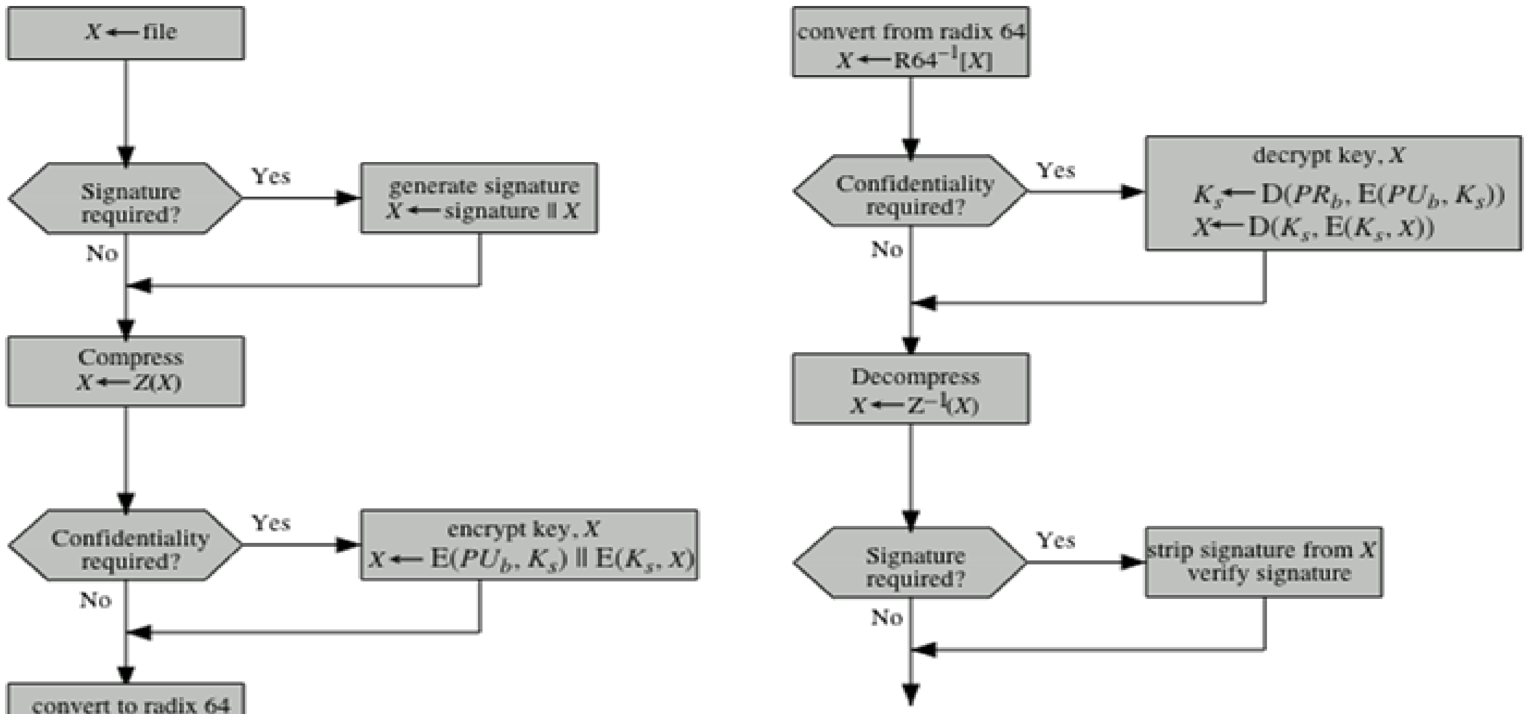
5. Base 64 encoding

PGP Cryptographic Functions



Transmission and reception of PGP messages

- Radix 64 bit conversion is used to convert raw 8 bit binary stream to a stream of printable ASCII characters.



(a) Generic Transmission Diagram (from A)

(b) Generic Reception Diagram (to B)

S/MIME

From: Giridhar Kale <giridhar@yahoo.com>
To: Amit Joshi <amit@rediffmail.com>
Subject: Cover image for the book
MIME-Version: 1.0
Content-Type: image/gif

<Actual image data in the binary form such as R019a0asdjas0 …>

Functionality	*Description*
Enveloped data	Consists of encrypted content of any type, and the encryption key encrypted with the receiver's public key.
Signed data	Consists of a message digest encrypted with the sender's private key. The content and the digital signature are both Base-64 encoded.
Clear-signed data	Similar to Signed data. However, only the digital signature is Base-64 encoded.
Signed and Enveloped data	Signed-only and Enveloped-only entities can be combined, so that the Enveloped data can be signed, or the Signed/Clear-signed data can be enveloped.

Thank You !!!!!!

ICS
Unit 4
Part-II

Cyber Security: Definition and origin, Cyber Crime and information security, Types of Cyber Crime, Classification of Cyber Criminals, Tools used in Cyber Crime, Challenges, Strategies, The Legal Perspective-Indian/Global Perspective, Types of Attack, Social Engineering, Cyber stalking, Ransomware.

Cybercrime

- Definition and origin:
- A crime in which a computer was directly and significantly instrumental
  - not universally accepted

- Other definitions:

- Any illegal act where special knowledge of computer technology is essential for its perpetration, investigation or prosecution

- Any traditional crime that has acquired a new dimension or order or magnitude through the aid of a computer, and abuses that have come into being because of computers

- Any threat to computer itself, such as theft of hardware or software, sabotage and demands for ransom

Cybercrime

- Cyber crime has evolved since adoption of internet connection on a global scale with millions of users

- Cybercrime refers to the act of performing a criminal act using cyberspace as the communication vehicle

Cybercrime

- **Cybercrimes** are any crimes that involve a computer and a network. In some cases, the computer may have been used in order to commit the crime, and in other cases, the computer may have been the target of the crime.

or

- **Cybercrime** is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes).

Cybercrime

- Any illegal/criminal activity done through internet or on the computer

- Computer used to commit a crime
  - Child porn, threatening email, assuming someone’s identity, sexual harassment, defamation, spam, phishing

- Computer as a target of a crime
  - Viruses, worms, industrial espionage(spying), software piracy, hacking

Cybercrime and Information Security

- Lack of information security gives rise to cybercrimes

- Indian Information Technology Act 2000
- From an Indian perspective, the new version of act (ITA 2008) provides a new focus on “Information Security in India”

- Cyber security means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

- The term incorporates both physical security of devices as well as information stored in them

Cybercrime and Information Security

- Typical network misuses are for internet radio/streaming audio, streaming video, file sharing, instant messaging and online gaming(such as online poker, online casinos, online betting, etc).

- Online gambling is illegal in India
- India has yet to pass laws that specifically deal with the issue, leaving sort of legal loophole

Who are Cybercriminals

- Cybercriminals are those who are involved in activities such as:
  1. Credit card fraud,
  2. Cyberstalking,
  3. Defaming another online,
  4. Gaining unauthorized access to computer,
  5. Ignoring copyright, software licensing and trademark protection,
  6. Overriding encryption to make illegal copies, software piracy,
  7. Identity theft to perform criminal act

Categories of Cybercriminals

- Categorized into 3 groups that reflect their motivation:

- **Type I: Cybercriminals-Hungry for recognition**
  - Hobby hackers
  - IT Professionals(social engineering is one of the biggest threat)
  - Politically motivated hackers
  - Terrorist organizations

Categories of Cybercriminals

- **Type II: Cybercriminals-not interested in recognition**
  - Psychological perverts (a person whose sexual behaviour is regarded as abnormal and unacceptable)
  - Financially motivated hackers (corporate espionage)
  - State-sponsored hacking (national espionage, sabotage)
  - Organized criminals

Categories of Cybercriminals

- **Type III: Cybercriminals-the insiders**
  - Disgruntled or former employees seeking revenge
  - Competing companies using employees to gain economic advantage through damage and/or theft

- Thus typical "motives" behind cybercrime seems to be:
  - greed, desire to gain power and/or publicity,
  - desire for revenge, a sense of adventure,
  - looking for thrill to access forbidden information,
  - destructive mindset

Classifying Cybercrimes-broad and narrow

	Cybercrime in Narrow Sense	Cybercrime in Broad Sense	
Role of computer	**Computer as an object:** The computer / information stored in it is the subject / target of crime	**Computer as a tool:** The computer / information stored in it constitutes an important tool for committing the crime	**Computer as the environment or context:** The computer/information stored in it plays a non-substantial role in the act of crime, but does not contain evidence of the crime
Examples	Hacking, Computer sabotage, DDoS Attacks	Computer fraud, forgery, distribution of child pornography	Murder using computer technique, bank robbery and drugs trade

Classification of Cybercrimes

1. Cybercrime against individual
2. Cybercrime against property
3. Cybercrime against organization
4. Cybercrime against society
5. Crimes emanating from Usenet newsgroup

Classification of Cybercrimes

1. Cybercrime against individual
   - E-mail spoofing and other online frauds
   - Phishing, Spear phishing, Vishing, Smishing
   - Spamming
   - Cyberdefamation
   - Cyberstalking and harassment
   - Computer sabotage
   - Pornographic offences
   - Password sniffing

2. Cybercrime against property
   - Credit card frauds
   - Intellectual property crimes
   - Internet time theft

Classification of Cybercrimes

3. Cybercrime against organization
   - Unauthorized accessing of computer
   - Password sniffing
   - Denial of Service attacks
   - Virus attack / dissemination of viruses
   - E-mail bombing / mail bombs
   - Salami attack / salami technique
   - Logic bomb
   - Trojan Horse
   - Data diddling
   - Industrial espionage / spying
   - Computer network intrusions
   - Software piracy

Classification of Cybercrimes

4. Cybercrime against society
    - Forgery
    - Cyberterrorism
    - Web jacking

5. Crimes emanating from Usenet newsgroup
    - **Usenet** is a worldwide distributed discussion system available on computers (an early non-centralized computer network for the discussion of particular topics and the sharing of files via newsgroups)

    - Usenet groups may carry very offensive, harmful, inaccurate or otherwise inappropriate material, or in some cases, postings that have been mislabeled or are deceptive(misleading) in another way

Cybercrime against individual: E-mail Spoofing

- E-mail spoofing is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source.

- **Email spoofing** is a tactic used in phishing and spam campaigns because people are more likely to open an **email** when they think it has been sent by a legitimate source.

- Basically in a spoofed email the **from:** field is modified to make it look like the email is coming from a person the recipient know.

- The result is that the email recipient sees the email as having come from the address in the ***From:*** field; but if they reply to the email it will go to ***Reply-to*** email address which is an email address the spammer might have setup to receive those replies.

Cybercrime against individual: E-mail Spoofing

- **Why is email spoofing possible?**
- The reason why email spoofing is possible and relatively easy for spammers to do is because of a vulnerability in the protocol used to transport emails through the Internet.
- **SMTP (Simple Mail Transport Protocol)** does not use any authentication mechanism for header fields like **from**, **Reply-to**, **Return-Path.**
- Spammers forge these headers using certain commands to make it appear that is coming from a different source than its original one.
- **Prevention:**
- Use cryptographic signatures (e.g., PGP "Pretty Good Privacy" or other encryption technologies) to exchange authenticated email messages.
- Authenticated email provides a mechanism for ensuring that messages are from whom they appear to be, as well as ensuring that the message has not been altered in transit.
- Similarly, sites may wish to consider enabling SSL/TLS in their mail transfer software.

Cybercrime against individual: Phishing

- Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication

- Communications purporting (Pretending) to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting victims.

- Phishing e-mails and websites have a similar/familiar appearance as original websites e.g. banking website

- Phishing emails may contain links to websites that are infected with malware

Cybercrime against individual: Phishing

- Methods of Phishing

1. **Dragnet method**
2. **Rod – and – Reel method**
3. **Lobsterpot method**
4. **Gillnet phishing**

Cybercrime against individual: Phishing

Methods of Phishing

1. Dragnet method

This method involves the use of spammed emails, bearing falsified corporate identification (e.g., trademarks, logos, and corporate names), that are addressed to a large class of people (e.g., customers of a particular financial institution or members of a particular auction site) to websites or pop-up windows with similarly falsified identification.

2. Rod – and – Reel method

In rod and reel method, phishers identify specific prospective victims in advance, and convey false information to them to prompt their disclosure of personal and financial data.

Cybercrime against individual: Phishing

Methods of Phishing

3. Lobsterpot method

- It focuses on the use of spoofed websites.
- It consists in the creation of spoofed websites, similar to legitimate corporate ones, that a narrowly defined class of victims is likely to seek out.

4. Gillnet phishing

- In gillnet phishing, phishers introduce malicious code into emails and websites. They can, for example misuse browser functionality by injecting hostile content into another site's pop – up window.
- Merely by opening a particular email, or browsing a particular website, Internet users may have a Trojan horse introduced into their systems.
- In some cases, the malicious code will change settings in user's systems, so that users who want to visit legitimate banking websites will be redirected to a lookalike phishing site.
- In other cases, the malicious code will record user's keystrokes and passwords when they visit legitimate banking sites, then transmit those data to phishers for later illegal access to users' financial accounts.

Cybercrime against individual: Spear phishing

- **Spear phishing** is an email that appears to be from an individual or business that you know. But it isn't.

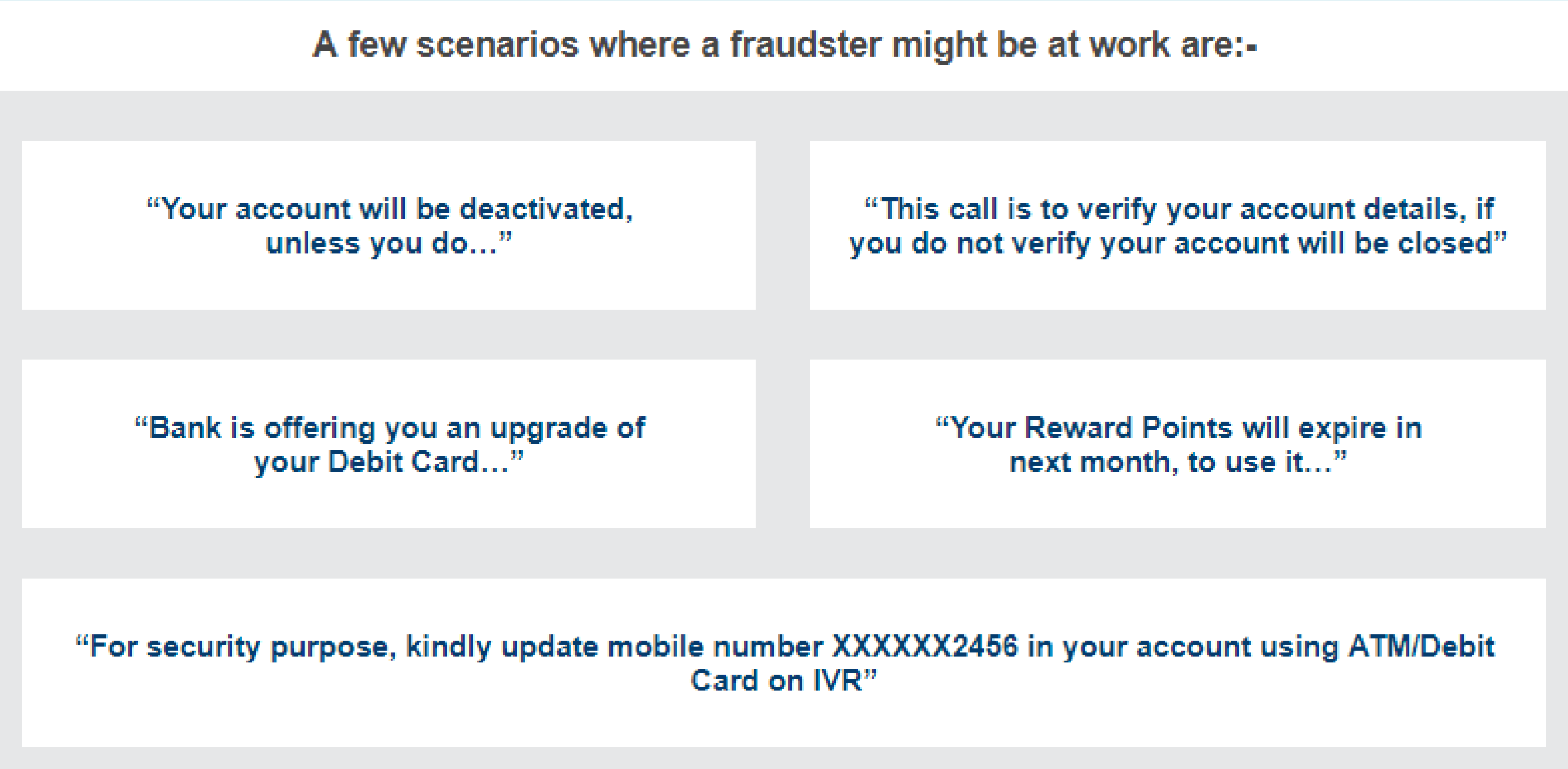
- It's from the same criminal hackers who want your credit card and bank account numbers, passwords, and the financial information on your PC.

Cybercrime against individual: Vishing

- **Vishing** is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft.

- The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.

Cybercrime against individual: Vishing



A few scenarios where a fraudster might be at work are:-

"Your account will be deactivated, unless you do..."

"This call is to verify your account details, if you do not verify your account will be closed"

"Bank is offering you an upgrade of your Debit Card..."

"Your Reward Points will expire in next month, to use it..."

"For security purpose, kindly update mobile number XXXXXX2456 in your account using ATM/Debit Card on IVR"

Cybercrime against individual: Smishing

- **SMiShing** is a security attack in which the user is tricked into downloading a Trojan horse, virus or other malware onto his cellular phone or other mobile device.
- **SMiShing** is short for “SMS phishing”

- A combination of phishing and Short Message Service (SMS) text messages is called SMISHING. These messages are usually crafted to provoke an immediate action from the user, requiring them to share their sensitive and confidential banking details.

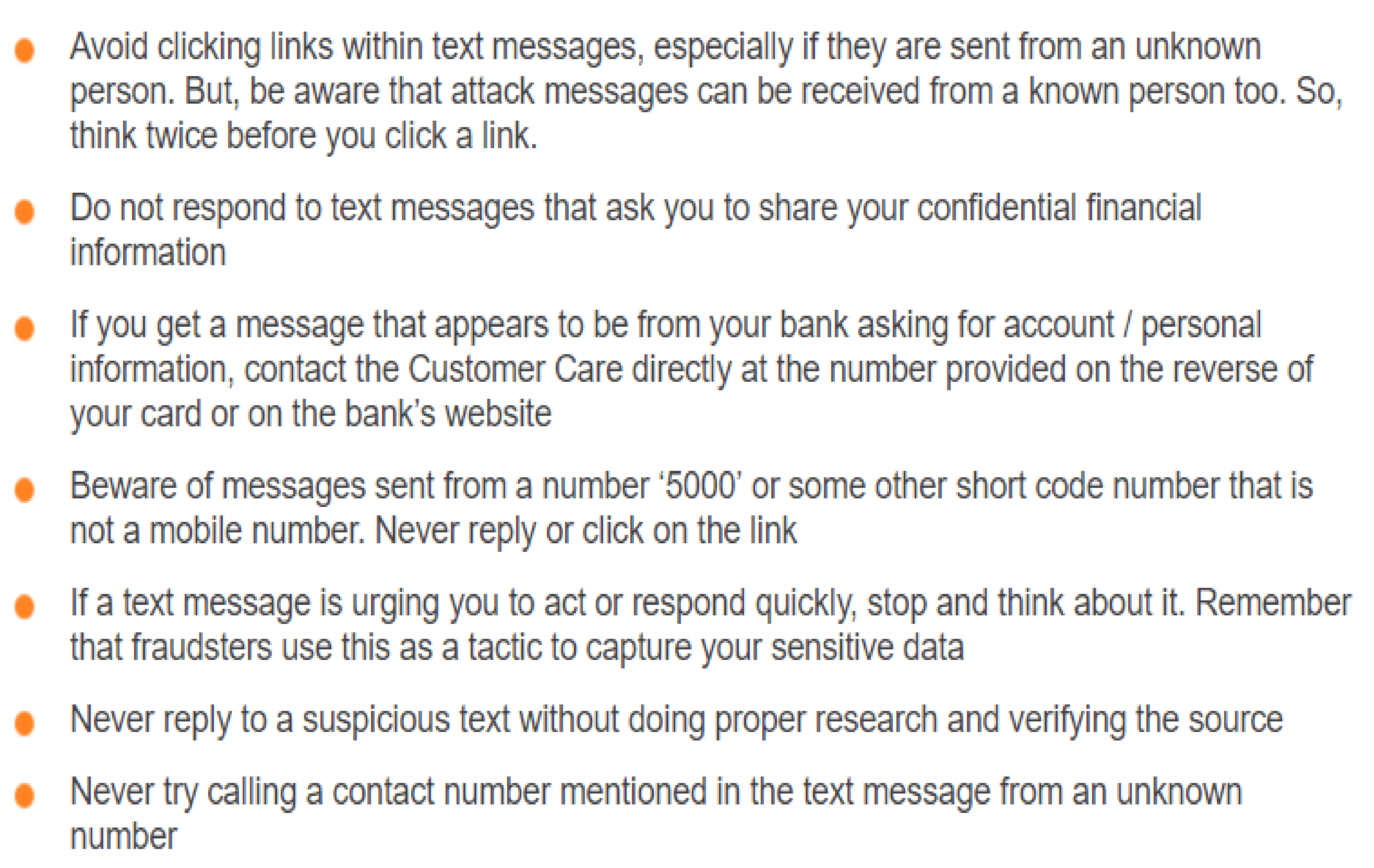
Smishing

- In ‘Smishing’, the message can also ask the users to click on a link or call on toll free numbers.

- If the user clicks on the link provided in the message, then a malicious software can get downloaded on their mobile or a single click on the link can take the user to a malicious website in pretext of an offer, discount or account credit.

- The text message can also create an urgency, by informing an account closure due to delinquency (negligence) or in need of an important information or even to register for a new programme.

Cybercrime against individual: Smishing: A Few Safety Tips



- Avoid clicking links within text messages, especially if they are sent from an unknown person. But, be aware that attack messages can be received from a known person too. So, think twice before you click a link.
- Do not respond to text messages that ask you to share your confidential financial information
- If you get a message that appears to be from your bank asking for account / personal information, contact the Customer Care directly at the number provided on the reverse of your card or on the bank's website
- Beware of messages sent from a number '5000' or some other short code number that is not a mobile number. Never reply or click on the link
- If a text message is urging you to act or respond quickly, stop and think about it. Remember that fraudsters use this as a tactic to capture your sensitive data
- Never reply to a suspicious text without doing proper research and verifying the source
- Never try calling a contact number mentioned in the text message from an unknown number

Cybercrime against individual: Pharming

- Pharming is a tactic used by criminals to redirect a legitimate web site to a fraudulent site.

- Unlike phishing and its variations, pharming does not try to trick you into clicking a URL or talk you into providing sensitive information.

- Instead, it uses malicious code to redirect you to the criminal’s site without your consent or knowledge, making it more difficult to detect.

Cybercrime against individual: Spamming

- Spamming means sending multiple copies of unsolicited mails or mass e-mails such as chain letters.

- Spammers create spams

- Most widely recognized is e-mail spam

- Other are: instant messaging spam, web search engine spam, spam in blogs, online classified ads spam, socoal networking spam

Cybercrime against individual: Spamming

- Search engine spam:
- Some web authors use “subversive techniques” to ensure that their site appears more frequently or higher number in returned results
- This is strongly discouraged by search engines and there are fines/penalties for this
- Those who continuously subvert or spam the search engine may be permanently excluded from search engine
- Therefore following web publishing techniques should be avoided:

Repeating keywords, non related keywords, redirection, IP cloaking, duplication of pages with different URLs, hidden links etc.

IP cloaking is the process of delivering different versions of a website to search engines than to human readers. It is often used to boost a site's search ranking, as it allows sites to recognize when engines such as Google are requesting data before sending them a version of their page that is full of keywords.

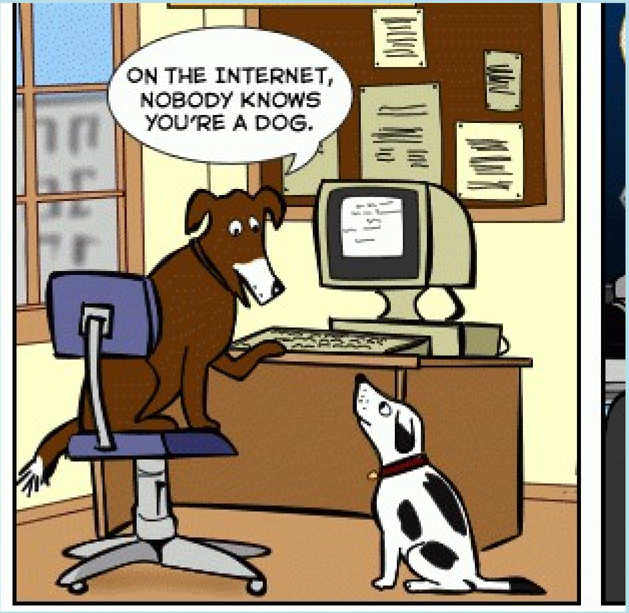
Cybercrime against individual: Cyberdefamation

- The term defamation is used to define the injury that is caused to the reputation of a person in the eyes of a third person.
- The injury can be done by words oral or written, or by signs or by visible representations.

- Cyber defamation is publishing of defamatory material against another person with the help of computers or internet.
- If someone publishes some defamatory statement about some other person on a website or send emails containing defamatory material to other persons with the intention to defame the other person about whom the statement has been made would amount to cyber defamation.

Cybercrime against individual: Cyberdefamation

- There are two main types of defamation: libel, or written defamation, and slander, or verbal defamation.
- When a potentially defamatory statement is made online or through social media -- such as via Facebook or Linkedin that involves the written (or "posted") word, and so it is considered libel.



Cybercrime against individual: Cyberstalking and harassment

- The repeated use of electronic communications to harass or frighten someone, for example by sending threatening emails.

- Cyberstalking can include many things including threats, demand for sex, false **accusations** (claim that someone has done something illegal or wrong), defamation, slander, libel, identity theft, and **vandalism** (willful or malicious destruction or defacement of public or private property.).

- Cyberstalking is often used in conjunction with offline stalking, as both are an expression of a desire to control, intimidate, or manipulate a victim.

- A cyberstalker may be someone the victim is familiar with, or a complete stranger, and is a criminal offense.

- Stalking may be followed by serious violent acts such as physical harm to the victim and the same has to be treated and viewed seriously.

Cybercrime against individual: Cyberstalking and harassment

- **Types of stalkers:**
- **Online Stalkers:**
- Communicate with victim directly with the help of internet (E-mail and Chat rooms) rather than using cellphone or telephone

- **Offline Stalker:**
- Follow the victim, watch daily routine of victim,
- Searching personal profiles and websites to gather information

Cybercrime against individual: Cyberstalking and harassment

- **How do they Operate**

- Collect all personal information about the victim such as name, family background, Telephone Numbers of residence and work place, daily routine of the victim, address of residence and place of work, date of birth etc. If the stalker is one of the acquaintances of the victim he can easily get this information. If stalker is a stranger to victim, he collects the information from the internet resources such as various profiles, the victim may have filled in while opening the chat or e-mail account or while signing an account with some website.

- The stalker may post this information on any website related to sex-services or dating services, posing as if the victim is posting this information and invite the people to call the victim on her telephone numbers to have sexual services. Stalker even uses very filthy and obscene language to invite the interested persons.

- People of all kind from nook and corner of the World, who come across this information, start calling the victim at her residence and/or work place, asking for sexual services or relationships.

- Some stalkers subscribe the e-mail account of the victim to innumerable pornographic and sex sites, because of which victim starts receiving such kind of unsolicited e-mails.

Cybercrime against property: Credit card frauds

- Credit card fraud is a wide-ranging term for theft and fraud committed using or involving a payment card, such as a credit card or debit card, as a fraudulent source of funds in a transaction.
- The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account.

- **Credit Card Skimming**
- Credit card skimming is a type of credit card theft where crooks use a small device to steal credit card information in an otherwise legitimate credit or debit card transaction.
- When a credit or debit card is swiped through a skimmer, the device captures and stores all the details stored in the card's magnetic strip.
- Thieves use the stolen data to make fraudulent charges either online or with a counterfeit credit card.

Cybercrime against property: Intellectual property crimes

- These include:
  - Software piracy: illegal copying of programs, distribution of copies of software
  - Copyright infringement
  - Trademarks violations
  - Theft of computer source code

Cybercrime against property: Internet time theft

- The usage of the Internet hours by an unauthorized person which is actually paid by another person.

Cybercrime against organization: Denial of Service attacks

- Denial-of-service (or DoS) attacks are usually launched to make a particular service unavailable to someone who is authorized to use it.

- These attacks may be launched using one single computer or many computers across the world.

- In the latter scenario, the attack is known as a distributed denial of service attack.

Cybercrime against organization:
Email Bombing, Logic Bomb & Trojan Horse

❖ **Email Bombing:**

- Sending large numbers of mails to the individual or company or mail servers thereby ultimately resulting into crashing.
- Email Bombing is sending large number to a email id in a single click.

❖ **Logic Bomb:**

- Its an event dependent program, as soon as the designated event occurs, it crashes the computer, release a virus or any other harmful possibilities.

❖ **Trojan Horse:**

- An unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

Cybercrime against organization: Salami Attack/Salami Technique

- Used for committing financial crimes
- When negligible amounts are removed & accumulated in to something larger.
- E.g. bank employee inserts program into bank servers, that deducts very small amount say Rs. 2 from account of every customer
- This is unnoticeable but bank employee will make huge amount

Cybercrime against organization: Data diddling

- This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

Cybercrime against organization: Software Piracy

- Software piracy is the illegal copying, distribution, or use of software.

Cybercrime against society: Forgery

- Currency notes, revenue stamps, mark sheets etc can be forged using computers and high quality scanners and printers

Cybercrime against society: Cyberterrorism

- Any person, group or organization who, with terrorist intent, utilizes a computer or computer network and thereby knowingly engages in or attempts to engage in terrorist act commits the offence of cyberterrorism

Cybercrime against society:
Web Jacking

- Hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money.

Categories of Cybercrime

- Cybercrime can be categorized based on:
  1. Target of the crime
  2. Whether crime occurs as a single event or as a series of event

Cyber Attack Meaning : Attack in which Cyber criminals can be targeted against person, property or organization include government, business and social.

Categories of Cybercrime:

1. Crime Targeted at Person (individual)
2. Crime Targeted at Assets
3. Cyber Crime Against Organization
4. Cyber attacks using single event
5. Cyber attacks considering series of event

How Cyber Criminals Plan cyber Attacks

- Cyber Criminals use many tool and methods to locate vulnerability of their victim.
- Attackers can be categorized as inside attacker or outside attacker.
- Attacks perform within the organization is called inside attack whereas attacker get information from outside is called outside attack.
- Inside attack are always more dangerous than outside, because inside attackers has get more resources than outsider.

- Following are three major phases are involved in planning of cyber crime.
  1. **Reconnaissance**
  2. **Scanning and scrutinizing**
  3. **Launching an attack**

Social Engineering

- Involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders.

- **Classification of Social Engineering:**

1. Human-based Social Engineering e.g. impersonation
2. Computer-based Social Engineering e.g. phishing, fake emails
3. Mobile-based Social Engineering e.g. SMS

Ransomware

Ransomware is a kind of malware attack that restricts access to your devices or files and displays a pop-up message that demands payment for the restriction to be removed.

✓ Restricts access to devices

✓ Contains malicious attachments.