COMPUTER COMMUNICATION
EC 407

Syllabus

COURSE CODE	COURSE NAME	L-T-P-C	YEAR OF INTRODUCTION
EC407	COMPUTER COMMUNICATION	3-0-0-3	2016

Prerequisite: NIL

Course objectives:

- To give the basic concepts of computer network and working of layers, protocols and interfaces in a computer network.
- To introduce the fundamental techniques used in implementing secure network communications and give them an understanding of common threats and its defences.

Module	Course content (42 hrs)	Hours	End Sem. Exam Marks
I	Introduction to computer communication: Transmission modes - serial and parallel transmission, asynchronous, synchronous, simplex, half duplex, full duplex communication. Switching: circuit switching and packet switching	2	15%

Syllabus

	Networks: Network criteria, physical structures, network models, categories of networks, Interconnection of Networks: Internetwork	2	
	Network models: Layered tasks, OSI model, Layers in OSI model, TCP/IP protocol suite.	2	
II	Physical Layer: Guided and unguided transmission media (Co-axial cable, UTP,STP, Fiber optic cable)	2	15%
	Data Link Layer: Framing, Flow control (stop and wait , sliding window flow control)	2	
	Error control, Error detection(check sum, CRC), Bit stuffing, HDLC	2	
	Media access control: Ethernet (802.3), CSMA/CD, Logical link control, Wireless LAN (802.11), CSMA/CA	2	
FIRST INTERNAL EXAM			

Syllabus

III	Network Layer Logical addressing : IPv4 & IPV6	2	15%
	Address Resolution protocols (ARP, RARP)	2	
	Subnetting, Classless Routing(CIDR), ICMP, IGMP, DHCP	3	
	Virtual LAN, Networking devices (Hubs, Bridges & Switches)	1	
IV	Routing: Routing and Forwarding, Static routing and Dynamic routing	1	15%
	Routing Algorithms: Distance vector routing algorithm, Link state routing (Dijkstra's algorithm)	2	
	Routing Protocols: Routing Information protocol (RIP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), MPLS	3	
SECOND INTERNAL EXAM			
V	Transport Layer –UDP, TCP	1	20%
	Congestion Control & Quality of Service – Data traffic, Congestion, Congestion Control, QoS and Flow Characteristics	4	
	Application Layer – DNS, Remote Logging (Telnet), SMTP, FTP, WWW, HTTP, POP3, MIME, SNMP	3	

Syllabus

VI	Introduction to information system security, common attacks	1	20%
	Security at Application Layer (E-MAIL, PGP and S/MIME). Security at Transport Layer (SSL and TLS). Security at Network Layer (IPSec).	3	
	Defence and counter measures: Firewalls and their types. DMZ, Limitations of firewalls, Intrusion Detection Systems -Host based, Network based, and Hybrid IDSs	2	
END SEMESTER EXAM			

Question Paper Pattern

The question paper shall consist of three parts. Part A covers modules I and II, Part B covers modules III and IV, and Part C covers modules V and VI. Each part has three questions uniformly covering the two modules and each question can have maximum four subdivisions. In each part, any two questions are to be answered. Mark patterns are as per the syllabus with 90% for theory and 10% for logical/numerical problems, derivation and proof.

References

Text Books:

1. Behrouz A. Forouzan, Cryptography & Network Security , , IV Edition, Tata McGraw-Hill, 2008
2. J F Kurose and K W Ross, Computer Network A Top-down Approach Featuring the Internet, 3/e, Pearson Education, 2010

References:

1. Behrouz A Forouzan, Data Communications and Networking, 4/e, Tata McGraw-Hill, 2006.
2. Larry Peterson and Bruce S Davie: Computer Network- A System Approach, 4/e, Elsevier India, 2011.
3. S. Keshav, An Engineering Approach to Computer Networking, Pearson Education, 2005.
4. Achyut S.Godbole, Data Communication and Networking, 2e, McGraw Hill Education New Delhi, 2011

UNIT 6

Network Security

First security issue: Computer Security – protect data stored into computer

Network Security – ***protect data during transmissions & guarantee that data transmissions are authentic***

Security Requirements

Confidentiality – data accessed & read only by authorized parties

Integrity – data modification by authorized parties

Availability – data available to authorized parties

Network Security Problems (what to allow for):

Secrecy

Keeping information private (out of unauthorized parties)

Authentication

Proving one's identity, before revealing info

Non-repudiation

Showing (proving) that a message was sent; use of signatures

Integrity

Showing that a message wasn't modified

Attacks on Network Security

Passive Attacks

Nature of: eavesdropping (monitoring) on transmissions

Goal: to obtain information that is being transmitted;

Two types of passive attacks:

Release of message contents

Outsider learns content of transmission

Traffic analysis

By monitoring frequency and length of messages, even encrypted, nature of communication may be guessed

Difficult to detect, because attacks don't alter data; can be prevented, rather than detected; use of *encryption*

Active Attacks

Involve some data stream modification, or creation of a false stream

Masquerade

Pretending to be a different entity

Replay

Capture of data unit and retransmission for an unauthorized effect

Modification of messages

Some portion of a legitimate message is altered

Denial of service

Prevents or inhibits normal use of communications facilities

Easy to detect: detection may lead to a deterrent effect (helps prevention)

Hard to prevent (requires all time physical protection)

Masquerade: behaviour that is intended to prevent the truth about something unpleasant or not wanted from becoming known:

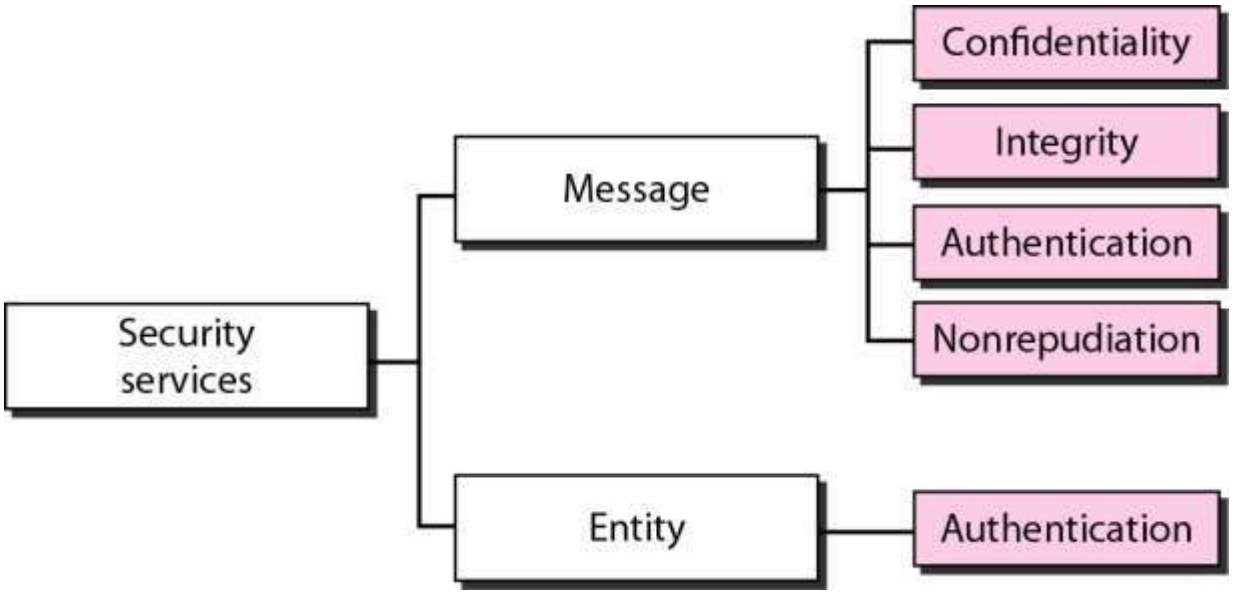
31-1 SECURITY SERVICES

Network security can provide five services. Four of these services are related to the message exchanged using the network. The fifth service provides entity authentication or identification.

Topics discussed in this section:

Message Confidentiality
Message Integrity
Message Authentication
Message Nonrepudiation
Entity Authentication

Figure 31.1 *Security services related to the message or entity*



32-1 IPSecurity (IPSec)

IPSecurity (IPSec) is a collection of protocols designed by the Internet Engineering Task Force (IETF) to provide security for a packet at the network level.

Topics discussed in this section:

Two Modes
Two Security Protocols

Figure 32.2 *TCP/IP protocol suite and IPSec at Network Layer*

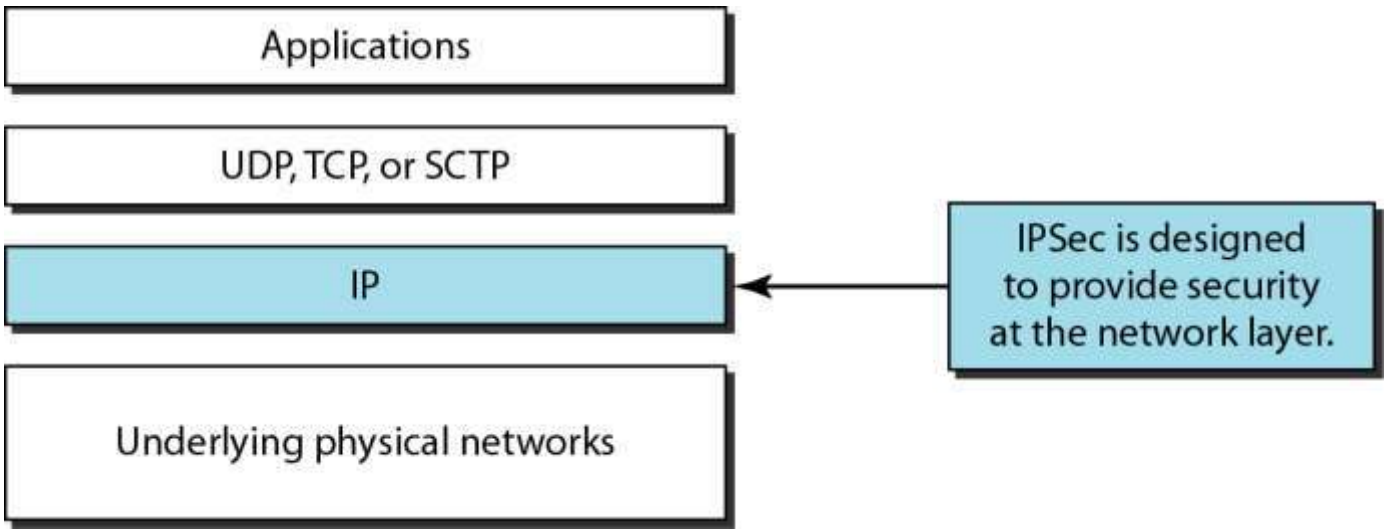
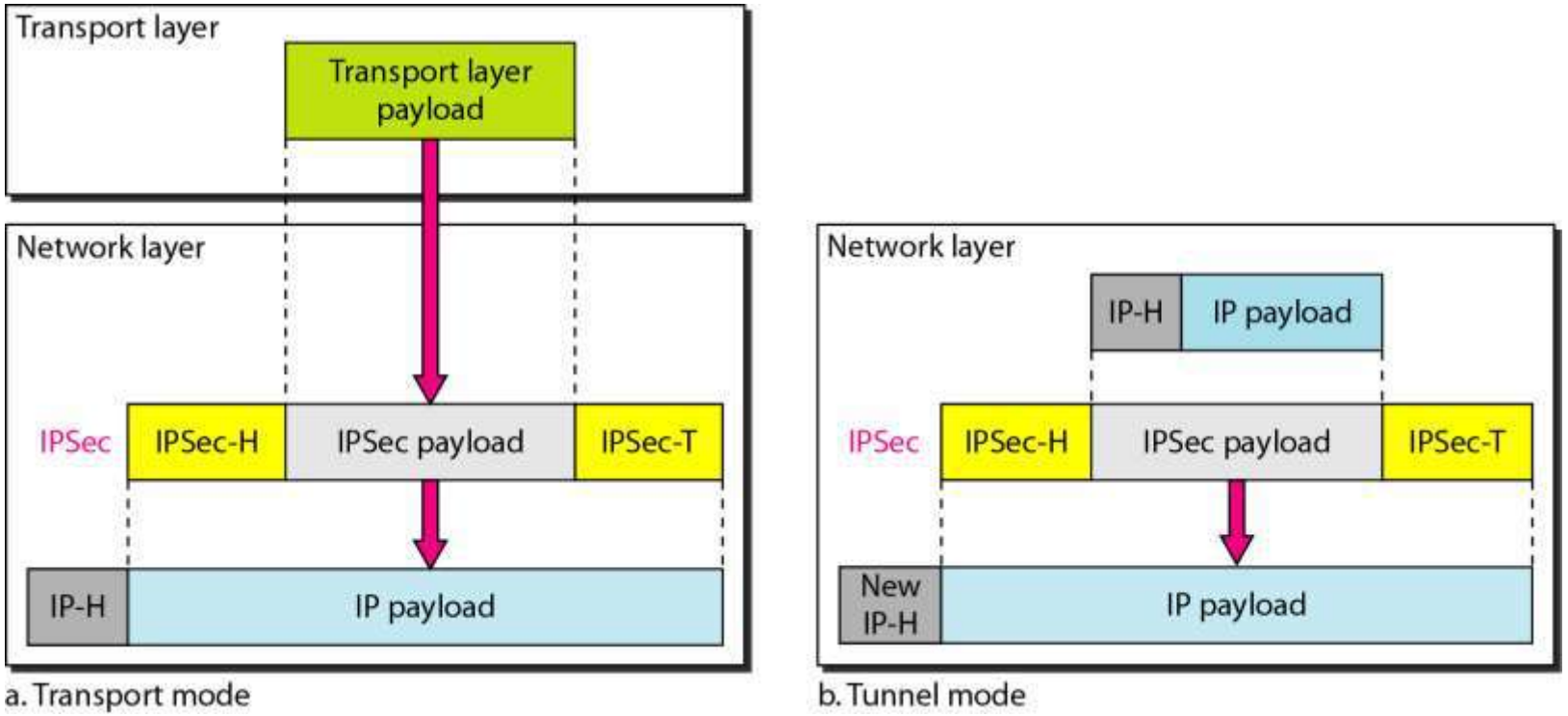


Figure 32.3 *Transport mode and tunnel modes of IPSec protocol*



Note

IPSec in the transport mode does not protect the IP header; it only protects the information coming from the transport layer.

Figure 32.4 *Transport mode in action*

Host to host protection of data
Authentication and encryption at sender side
Authentication and decryption at receiver side

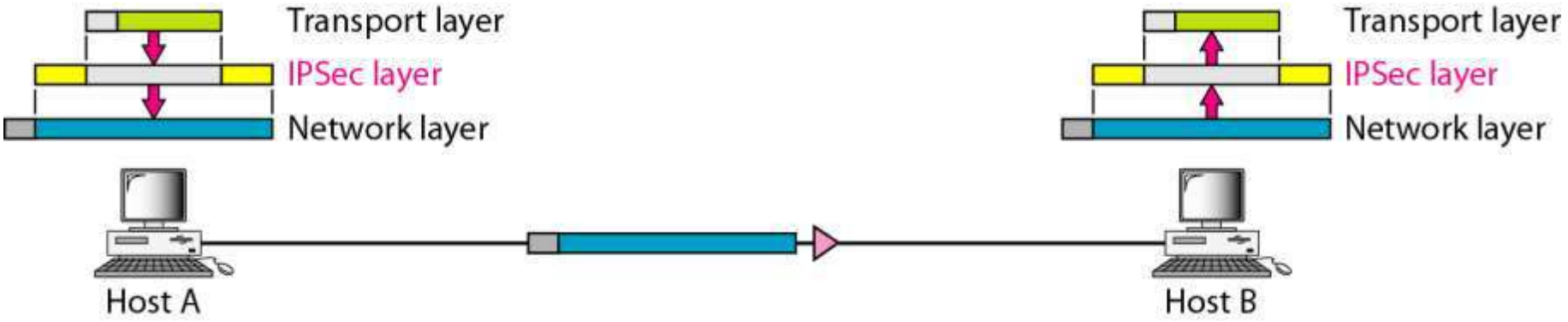
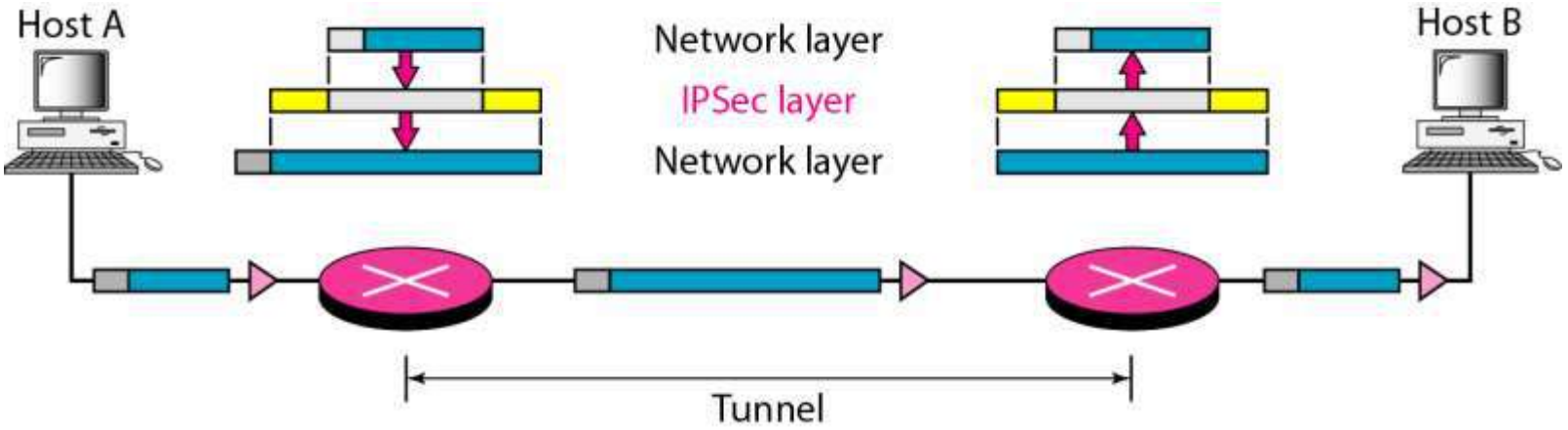


Figure 32.5 *Tunnel mode in action*

It takes an IP packet, including header, Applies IPsec methods to all packets and then adds new IP header

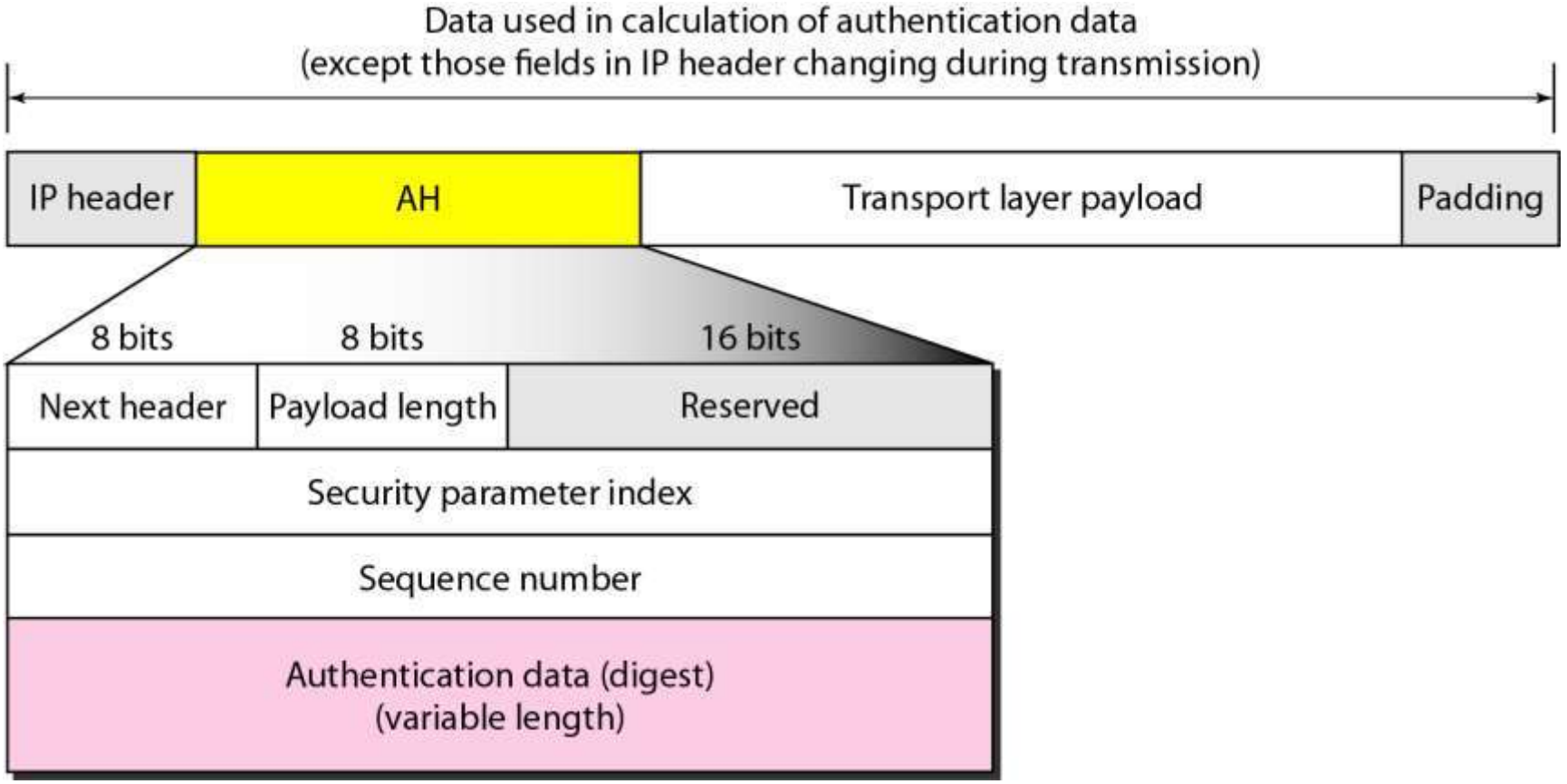
Between host and a router, between router and a router



Note

IPSec in tunnel mode protects the original IP header.

Figure 32.6 *Authentication Header (AH) Protocol in transport mode*



Note

The AH Protocol provides source authentication and data integrity,
but not privacy.

Authentication Header Protocol (AHP)

To authenticate the source host and to ensure the integrity of the payload

The **Authentication Header (AH) Protocol** is designed to authenticate the source host and to ensure the integrity of the payload carried in the IP packet. The protocol uses a hash function and a symmetric key to create a message digest; the digest is inserted in the authentication header. The AH is then placed in the appropriate location based on the mode (transport or tunnel).

Authentication Header Protocol (AHP)

The addition of an authentication header follows these steps:

1. An authentication header is added to the payload with the authentication data field set to zero.
2. Padding may be added to make the total length even for a particular hashing algorithm.
3. Hashing is based on the total packet. However, only those fields of the IP header that do not change during transmission are included in the calculation of the message digest (authentication data).
4. The authentication data are inserted in the authentication header.
5. The IP header is added after the value of the protocol field is changed to 51.

Hash algorithm is a function that converts a data string into a numeric string output of fixed length. The output string is generally much smaller than the original data.

Authentication Header Protocol (AHP)

A brief description of each field follows:

- **Next header.** The 8-bit next-header field defines the type of payload carried by the IP datagram (such as TCP, UDP, ICMP, or OSPF). It has the same function as the protocol field in the IP header before encapsulation. In other words, the process copies the value of the protocol field in the IP datagram to this field. The value of the protocol field in the new IP datagram is now set to 51 to show that the packet carries an authentication header.
- **Payload length.** The name of this 8-bit field is misleading. It does not define the length of the payload; it defines the length of the authentication header in 4-byte multiples, but it does not include the first 8 bytes.
- **Security parameter index.** The 32-bit security parameter index (SPI) field plays the role of a virtual-circuit identifier and is the same for all packets sent during a connection called a security association (discussed later).
- **Sequence number.** A 32-bit sequence number provides ordering information for a sequence of datagrams. The sequence numbers prevent a playback. Note that the sequence number is not repeated even if a packet is retransmitted. A sequence number does not wrap around after it reaches 2^{32}; a new connection must be established.
- **Authentication data.** Finally, the authentication data field is the result of applying a hash function to the entire IP datagram except for the fields that are changed during transit (e.g., time-to-live).

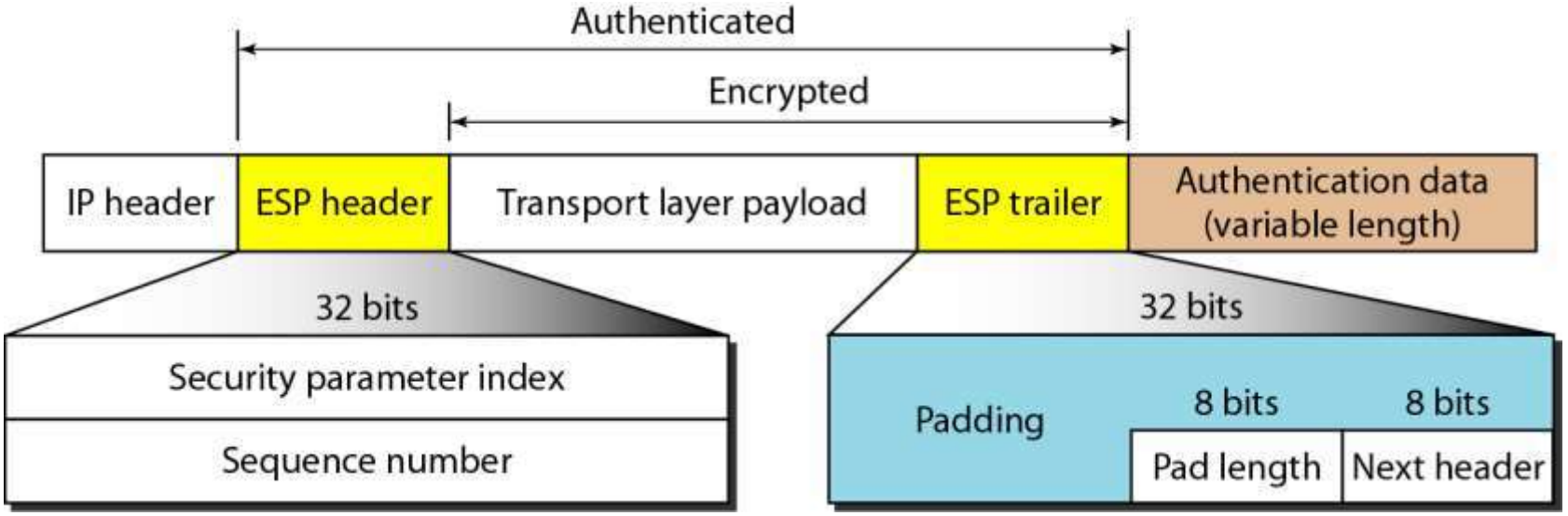
Note

Encapsulating Security Payload

Note

ESP provides source authentication, data integrity, and privacy.

Figure 32.7 *Encapsulating Security Payload (ESP) Protocol in transport mode*



Encapsulating Security Payload (ESP) Protocol in transport mode

The ESP procedure follows these steps:

1. An ESP trailer is added to the payload.
2. The payload and the trailer are encrypted.
3. The ESP header is added.
4. The ESP header, payload, and ESP trailer are used to create the authentication data.
5. The authentication data are added to the end of the ESP trailer.
6. The IP header is added after the protocol value is changed to 50.

Encapsulating Security Payload (ESP) Protocol in transport mode

- **Security parameter index.** The 32-bit security parameter index field is similar to that defined for the AH Protocol.
- **Sequence number.** The 32-bit sequence number field is similar to that defined for the AH Protocol.
- **Padding.** This variable-length field (0 to 255 bytes) of 0s serves as padding.
- **Pad length.** The 8-bit pad length field defines the number of padding bytes. The value is between 0 and 255; the maximum value is rare.
- **Next header.** The 8-bit next-header field is similar to that defined in the AH Protocol. It serves the same purpose as the protocol field in the IP header before encapsulation.
- **Authentication data.** Finally, the authentication data field is the result of applying an authentication scheme to parts of the datagram. Note the difference between the authentication data in AH and ESP. In AH, part of the IP header is included in the calculation of the authentication data; in ESP, it is not.

Table 32.1 *IPSec services*

Services	*AH*	*ESP*
Access control	Yes	Yes
Message authentication (message integrity)	Yes	Yes
Entity authentication (data source authentication)	Yes	Yes
Confidentiality	No	Yes
Replay attack protection	Yes	Yes

SSL/TLS

Figure 32.14 *Location of SSL and TLS in the Internet model*

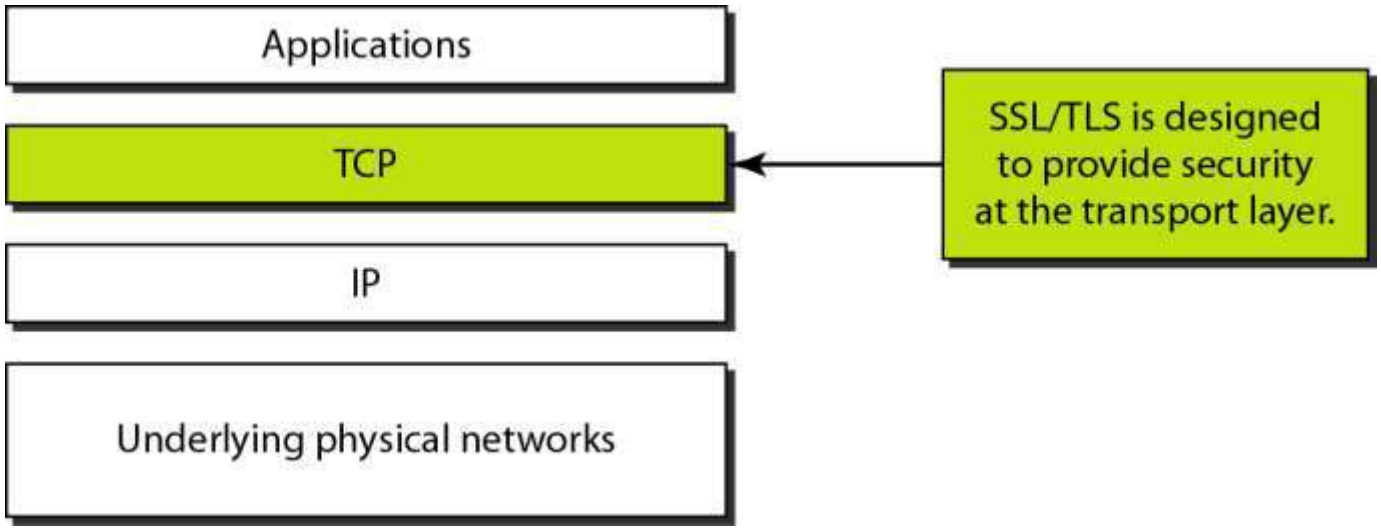
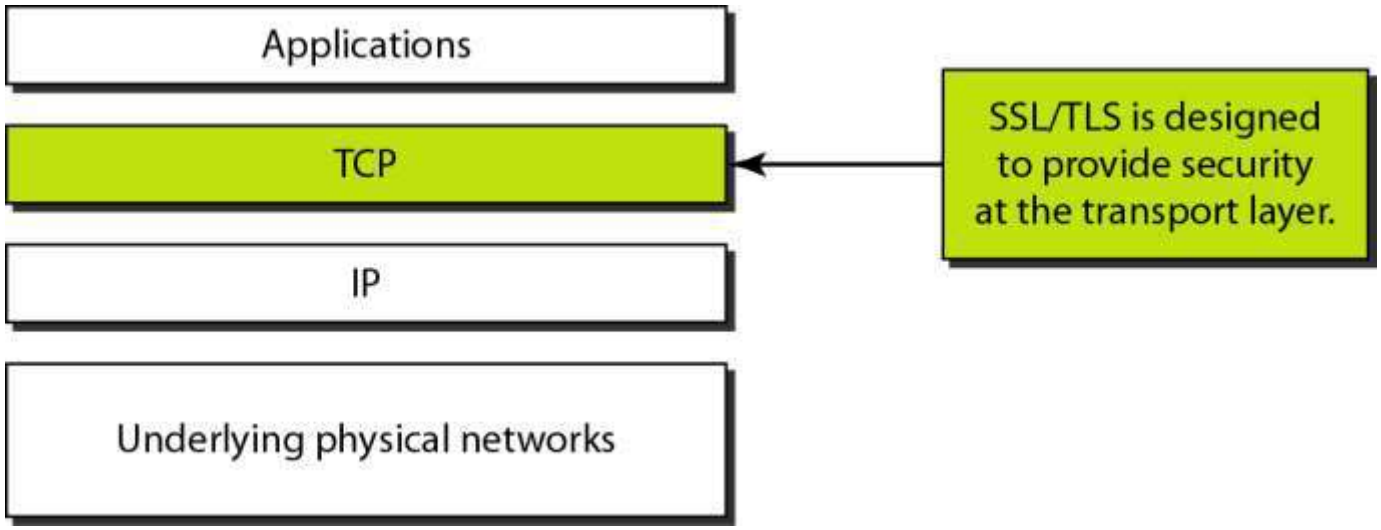


Figure 32.14 *Location of SSL and TLS in the Internet model*



SSL –Secure Socket Layer Protocol
TLS- Transport Layer Security

SSL –Secure Socket Layer Protocol

- Used to provide security and compression services to data generated from application layer.
- It receives data from application normally from HTTP
- This is compressed(optional), signed and encrypted
- The data is then passed to TCP

Fragmentation

First, SSL divides the data into blocks of 2^{14} bytes or less.

Compression

Each fragment of data is compressed by using one of the lossless compression methods negotiated between the client and server. This service is optional.

Message Integrity

To preserve the integrity of data, SSL uses a keyed-hash function to create a MAC.

Confidentiality

To provide confidentiality, the original data and the MAC are encrypted using symmetric-key cryptography.

Framing

A header is added to the encrypted payload. The payload is then passed to a reliable transport layer protocol.

Message Authentication Code is typically the result of a one way hashing algorithm used to determine whether the input data has been modified.

Security Parameters

Cipher Suite and Cryptographic secrets

The combination of key exchange, hash, and encryption algorithms defines a **cipher suite** for each SSL session. Each suite starts with the term *SSL*, followed by the key-exchange algorithm. The word *WITH* separates the key exchange algorithm from the encryption and hash algorithms.

Security Parameters

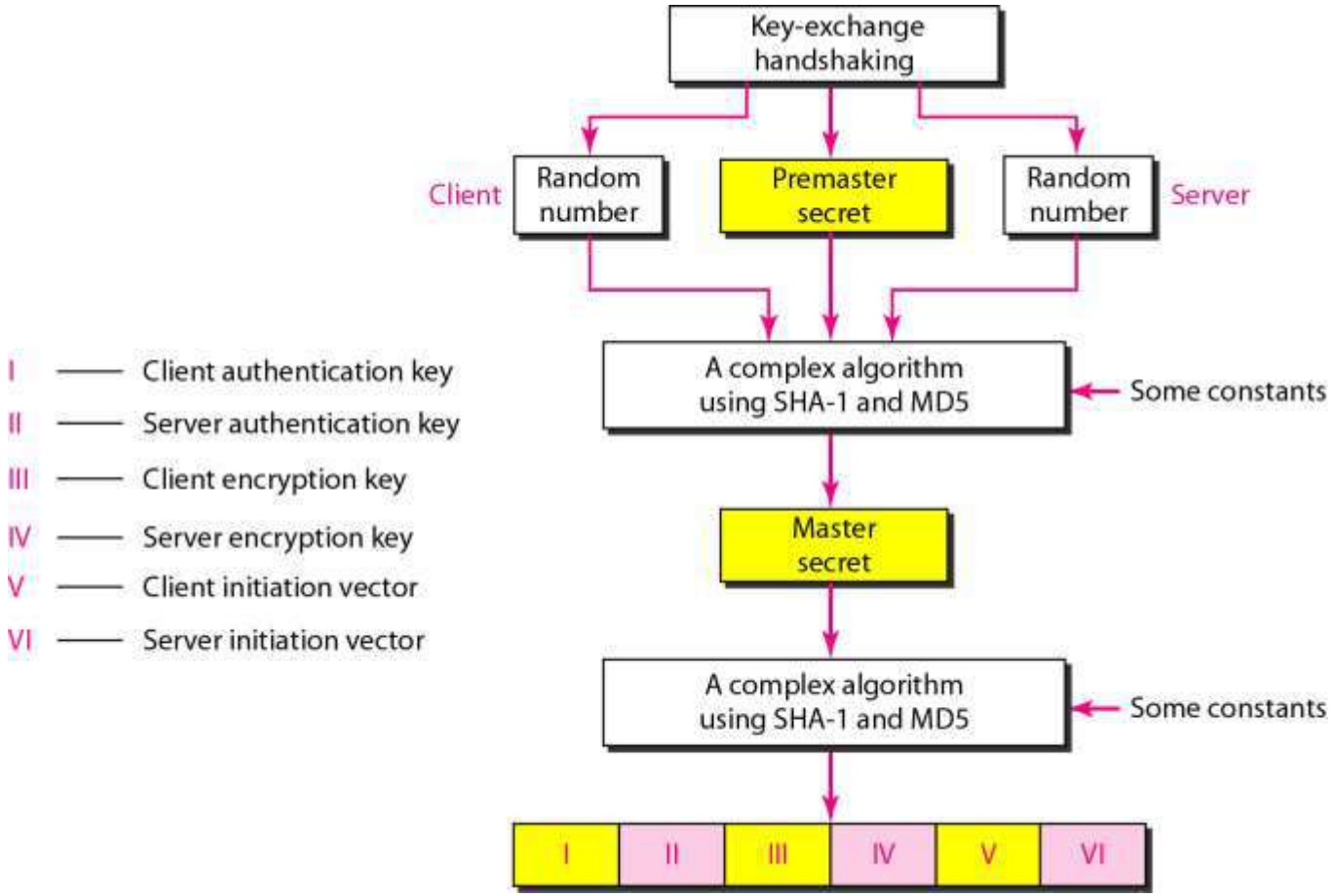
Cryptographic secrets

The second part of security parameters is often referred to as cryptographic secrets. To achieve message integrity and confidentiality, SSL needs six cryptographic secrets, four keys, and two IVs.

Note

The client and the server have six different cryptography secrets.

Figure 32.15 *Creation of cryptographic secrets in SSL*

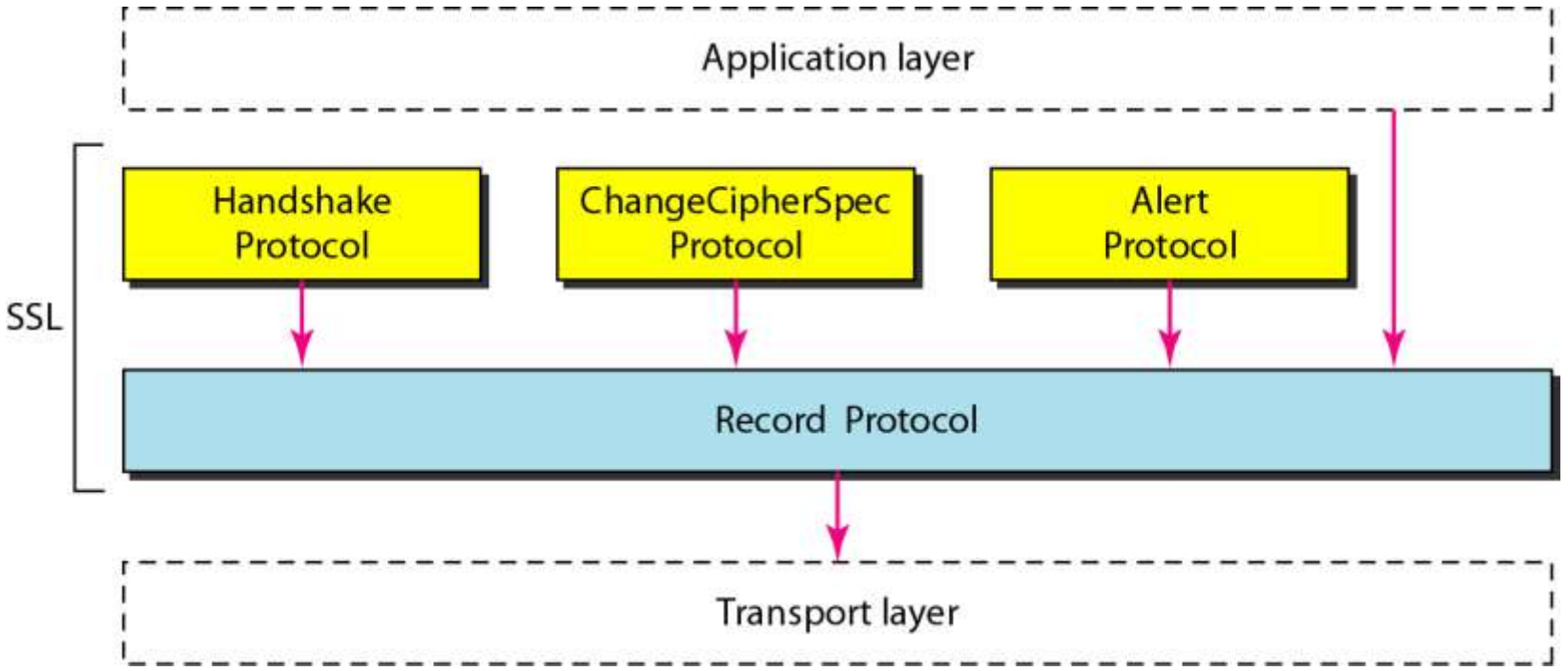


Creation of cryptographic secrets in SSL

1. The client and server exchange two random numbers; one is created by the client and the other by the server.
2. The client and server exchange one **premaster secret** by using one of the key-exchange algorithms
3. A 48-byte **master secret** is created from the premaster secret by applying two hash functions (SHA-1 and MD5).
4. The master secret is used to create variable-length secrets by applying the same set of hash functions and prepending with different constants.

However, the designers of SSL decided that they needed two-levels of connectivity: **session** and **connection.** A session between two systems is an association that can last for a long time; a connection can be established and broken several times during a session.

Figure 32.16 *Four SSL protocols*



Four SSL protocols

The **Record Protocol** is the carrier. It carries messages from three other protocols as well as the data coming from the application layer. Messages from the Record Protocol are payloads to the transport layer, normally TCP.

The **Handshake Protocol** provides security parameters for the Record Protocol. It establishes a cipher set and provides keys and security parameters. It also authenticates the server to the client and the client to the server, if needed.

The **ChangeCipherSpec Protocol** is used for signaling the readiness of cryptographic secrets. The **Alert Protocol** is used to report abnormal conditions.

TLS

Introduction

TLS Record Protocol

TLS Handshake Protocol

Summary

Introduction

- Transport Layer Security (TLS)
- TLS provides transport layer security for Internet applications
- It provides for confidentiality and data integrity over a connection between two end points
- TLS operates on a reliable transport, such as TCP, and is itself layered into
  - TLS Record Protocol
  - TLS Handshake Protocol

TLS Record Protocol

- TLS Record Protocol layers on top of a reliable connection-oriented transport, such as TCP
- TLS Record Protocol
  - provides data confidentiality using symmetric key cryptography
  - provides data integrity using a keyed message authentication checksum (MAC)
- The keys are generated uniquely for each session based on the security parameters agreed during the TLS handshake

- Basic operation of the TLS 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

TLS Handshake Protocol

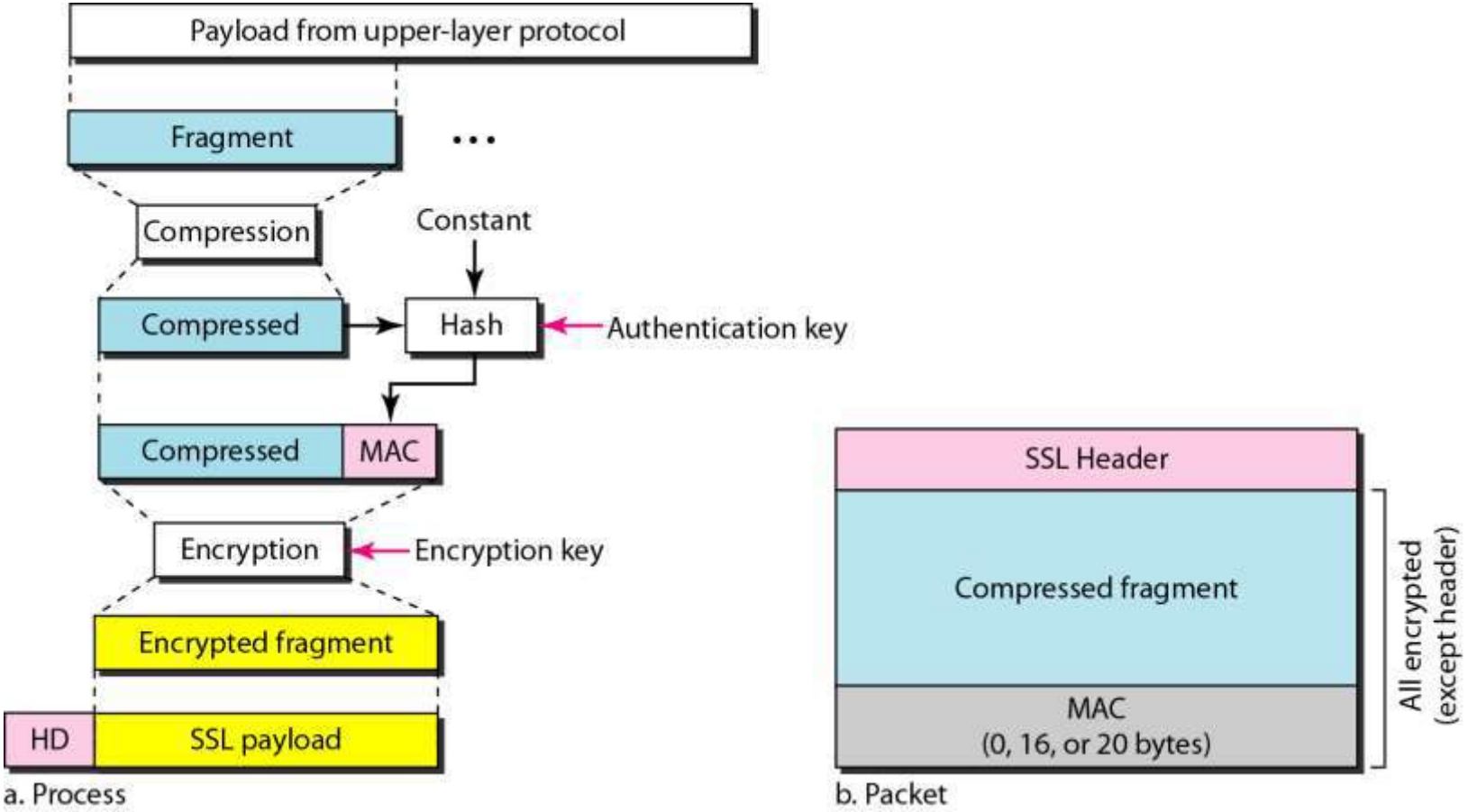
- TLS Handshake Protocol is layered on top of the TLS Record Protocol
- TLS Handshake Protocol is used to
  - authenticate the client and the server
  - exchange cryptographic keys
  - negotiate the used encryption and data integrity algorithms before the applications start to communicate with each other

Summary

- TLS protocol provides transport layer security for Internet applications and confidentiality using symmetric key cryptography and data integrity using a keyed MAC
- It also includes functionality for client and server authentication using public key cryptography

Figure 32.17 *Handshake Protocol*

Figure 32.18 *Processing done by the Record Protocol*



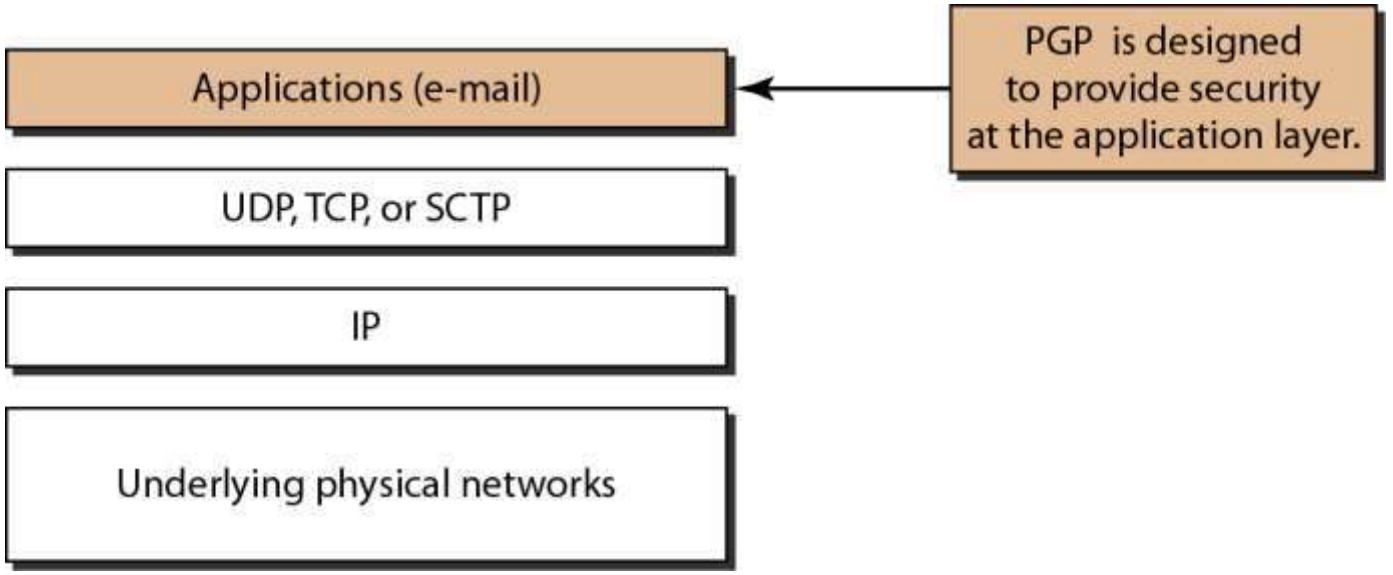
32-3 PGP

One of the protocols to provide security at the application layer is Pretty Good Privacy (PGP). PGP is designed to create authenticated and confidential e-mails.

Topics discussed in this section:

Security Parameters
Services
A Scenario
PGP Algorithms
Key Rings

Figure 32.19 *Position of PGP in the TCP/IP protocol suite*



Note

In PGP, the sender of the message needs to include the identifiers of the
algorithms used in the message as well as the values of the keys.

Services

Plain text(simplest case)

Message authentication

Alice create a digest of the message and signs it with her private key. Bob verifies the message with Alic's public key

Compression

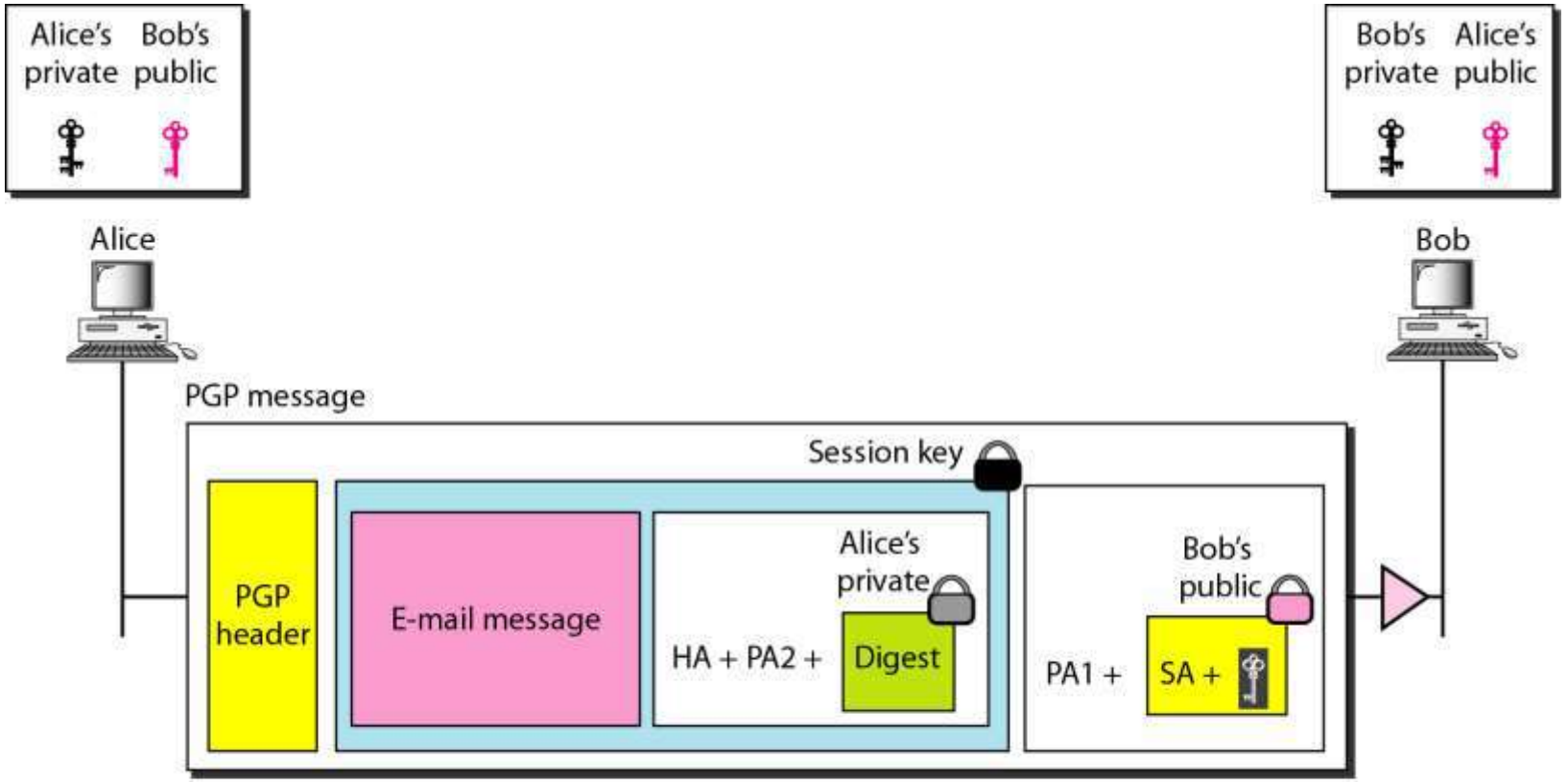
Confidentiality with one-time session

Alice, the sender can create a session key, use the session key to encrypt the message and digest, this session key is encrypted with Bob's public key and send along with the message.

Code conversion :To convert other characters not in ASCII

Segmentation

Figure 32.20 *A scenario in which an e-mail message is authenticated and encrypted*



PA1: Public-key algorithm 1 (for encrypting session key)
PA2: Public-key algorithm (for encrypting the digest)
SA: Symmetric-key algorithm identification (for encrypting message and digest)
HA: Hash algorithm identification (for creating digest)

Sender Side

1. Alice creates a session key(for symmetric encryption/decryption) session key is encrypted and concatenates with identity of the algorithm. The result is encrypted with Bob's public key. Also adds the identity of the algorithm

2.
   a. Alice authenticates the message (e-mail) by using a public-key signature algorithm and encrypts it with her private key. The result is called the signature. Alice appends the identification of the public key (used for encryption) as well as the identification of the hash algorithm (used for authentication) to the signature. This part of the message contains the signature and two extra pieces of information: the encryption algorithm and the hash algorithm.
   b. Alice concatenates the three pieces of information created above with the message (e-mail) and encrypts the whole thing, using the session key created in step 1.
3. Alice combines the results of steps 1 and 2 and sends them to Bob (after adding the appropriate PGP header).

Receiver Side

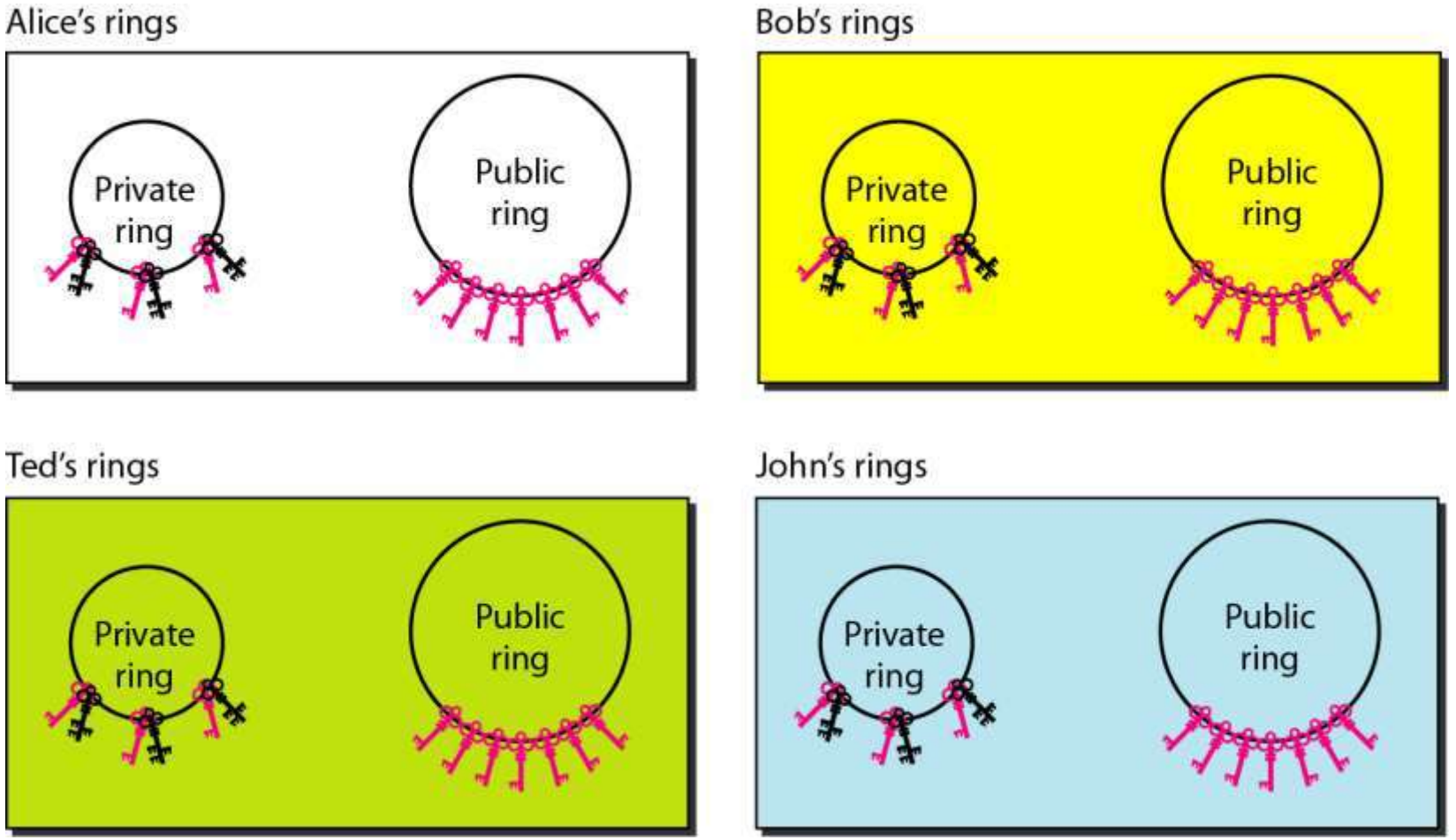
The following shows the steps used in this scenario at Bob's side after he has received the PGP packet:

1. Bob uses his private key to decrypt the combination of the session key and symmetric-key algorithm identification.
2. Bob uses the session key and the algorithm obtained in step 1 to decrypt the rest of the PGP message. Bob now has the content of the message, the identification of the public algorithm used for creating and encrypting the signature, and the identification of the hash algorithm used to create the hash out of the message.
3. Bob uses Alice's public key and the algorithm defined by PA2 to decrypt the digest.
4. Bob uses the hash algorithm defined by HA to create a hash out of message he obtained in step 2.
5. Bob compares the hash created in step 4 and the hash he decrypted in step 3. If the two are identical, he accepts the message; otherwise, he discards the message.

Table 32.4 *PGP Algorithms*

Algorithm	*ID*	*Description*
Public key	1	RSA (encryption or signing)
	2	RSA (for encryption only)
	3	RSA (for signing only)
	17	DSS (for signing)
Hash algorithm	1	MD5
	2	SHA-1
	3	RIPE-MD
Encryption	0	No encryption
	1	IDEA
	2	Triple DES
	9	AES

Figure 32.21 *Rings*



Note

In PGP, there can be multiple paths from fully or partially trusted authorities to any subject.

Email Security

Threats to Email

- Message interception
  - Emails sent in clear text over the Internet.
- Message modification
  - Anyone with system admin rights on the mail servers your message visits can not only read your message, but also delete or change the message before it reaches its destination (and the recipient won't be able to tell if the message has been modified).
- False messages
  - It is very easy to create an email with someone else's name and address. SMTP servers don't check for sender authenticity.

Threats to Email

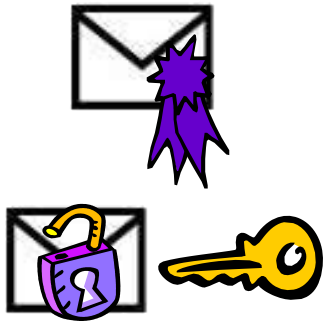
- Message Replay
  - Messages can be saved, modified, and re-sent later.
- Repudiation
  - You can't prove that someone sent you a message since email messages can be forged.

Solutions

- First, let's review the requirements for secure email.
  - Sender authenticity
  - Nonrepudiation
  - Message integrity
  - Message confidentiality

Solutions

- What do we need to meet these requirements?
  - Digital Signatures
    - Solves integrity, authenticity, and nonrepudiation problems.
  - Encryption
    - Solves confidentiality problem.



Secure E-Mail Systems

- Both of these systems provide encryption and digital signatures for security.
  - Secure Multipurpose Internet Mail Extensions (S/MIME)
  - Pretty Good Privacy (PGP)

S/MIME

- Stands for Secure/Multipurpose Internet Mail Extension
- Security enhancement to the MIME internet e-mail format

MIME – Header Files

- There are five message header fields
  - MIME-Version
  - Content-Type
  - Content-Transferring Encoding
  - Content-ID
  - Content-Description

MIME – Content Types

- Message
  - Rfc822
  - Partial
  - External-body
- Image
  - Jpeg
  - Gif
- Video
  - mpeg

Mime – Content Type

- Audio
  - Basic
- Application
  - PostScript
  - Octet-stream

MIME – Content Transferring Encoding

- Two types
  - Quoted printable
    - Used when data consists largely of octets.
    - Limits message lines to 76 characters.
  - Base64 transfer encoding
    - Common for encoding arbitrary binary data.

S/MIME Functionality

- S/MIME provides the following functions
  - Enveloped Data
    - Consists of encrypted content
  - Signed Data
    - Contains a digital signature
  - Clear-signed data
    - Encoded digital signature
  - Signed and enveloped data
    - Encrypted and Signed data

S/MIME – Cryptographic Algorithms

- Create message digest to form digital signature
  - Must use SHA-1, Should support MD5
- Encrypt message digest to form signature
  - Must support DSS, Should support RSA
- Encrypt session key for transmission
  - Should support Diffie-Hellman, Must support RSA

S/MIME – Cryptographic Algorithms

- Encrypt message for transmission with one-time session key
  - Must support triple DES, Should support AES, Should support RC2/40
- Create a message authentication code
  - Must support HMAC with SHA-1, Should support HMAC with SHA-1

S/MIME – User Agent Role

- Key generation
  - Generating key with RSA
- Registration
  - Register a user's public key must be registered with a certification authority
- Certificate storage and retrieval
  - Access to a local list of certificates in order to verify incoming signatures and encrypt outgoing

S/MIME – Enhanced Security Services

- Signed receipts
  - The receiver returns a signed receipt back to the sender to verify the message arrived
- Secure mailing lists
  - Sending to multiple recipients at once securely by using a public key for the whole mailing list

32-4 FIREWALLS

All previous security measures cannot prevent Eve from sending a harmful message to a system. To control access to a system, we need firewalls. A firewall is a device installed between the internal network of an organization and the rest of the Internet. It is designed to forward some packets and filter (not forward) others.

Topics discussed in this section:

Packet-Filter Firewall
Proxy Firewall

Figure 32.22 *Firewall*

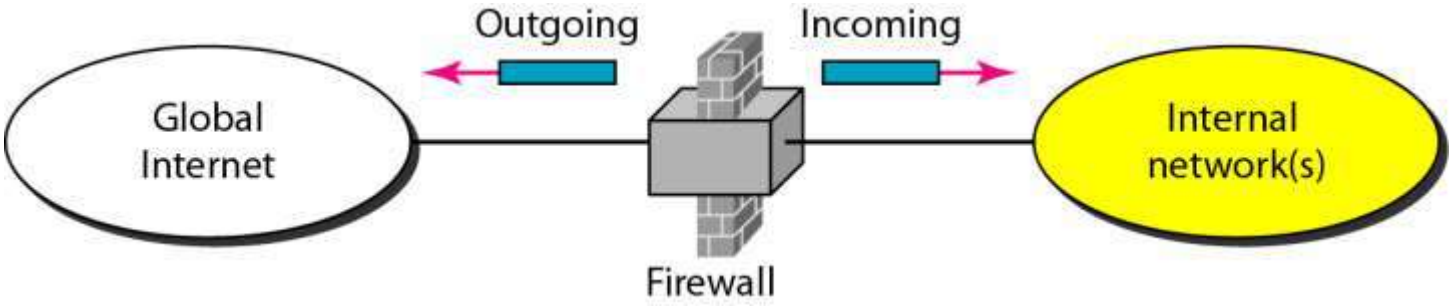
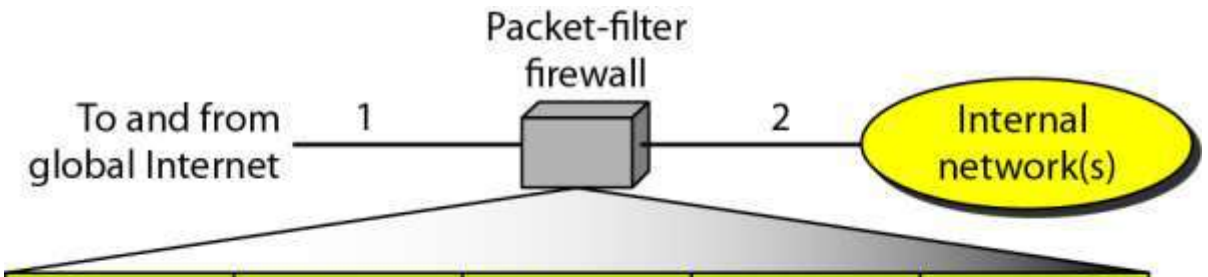


Figure 32.23 *Packet-filter firewall*

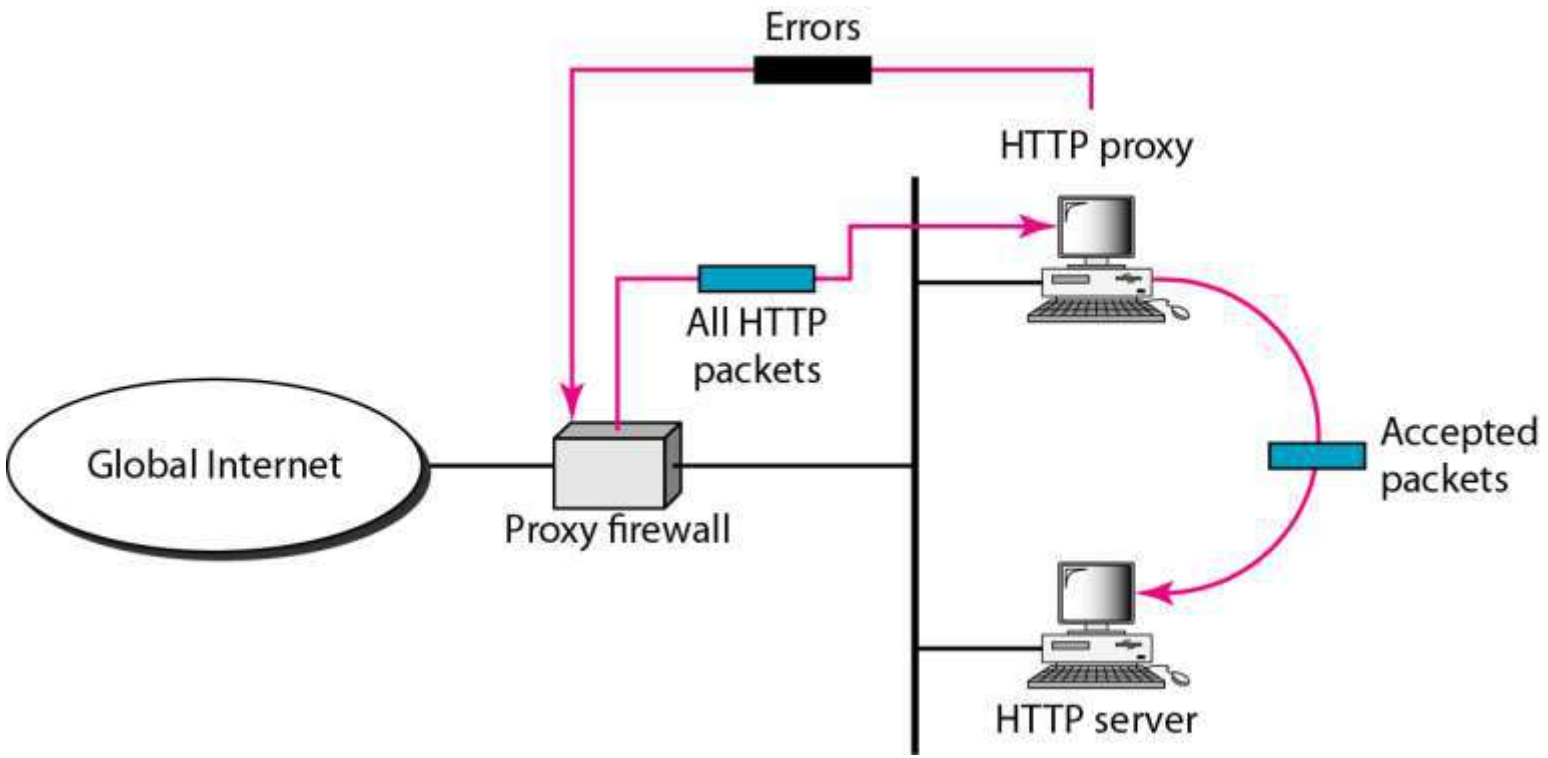


Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	80	*	*

Note

A packet-filter firewall filters at the network or transport layer.

Figure 32.24 *Proxy firewall*



Note

A proxy firewall filters at the application layer.

Intrusion Detection System (IDS)

❖An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.

❖Although intrusion detection systems monitor networks for potentially malicious activity, they are also prone to false alarms (false positives).

❖Consequently, organizations need to fine-tune their IDS products when they first install them. That means properly configuring their intrusion detection systems to recognize what normal traffic on their network looks like compared to potentially malicious activity.

Different types of intrusion detection systems

1. Network intrusion detection system (NIDS)
2. Host intrusion detection systems (HIDS)
3. Hybrid intrusion detection systems
4. Signature-based intrusion detection systems
5. Anomaly-based intrusion detection systems

Network Intrusion Detection System:

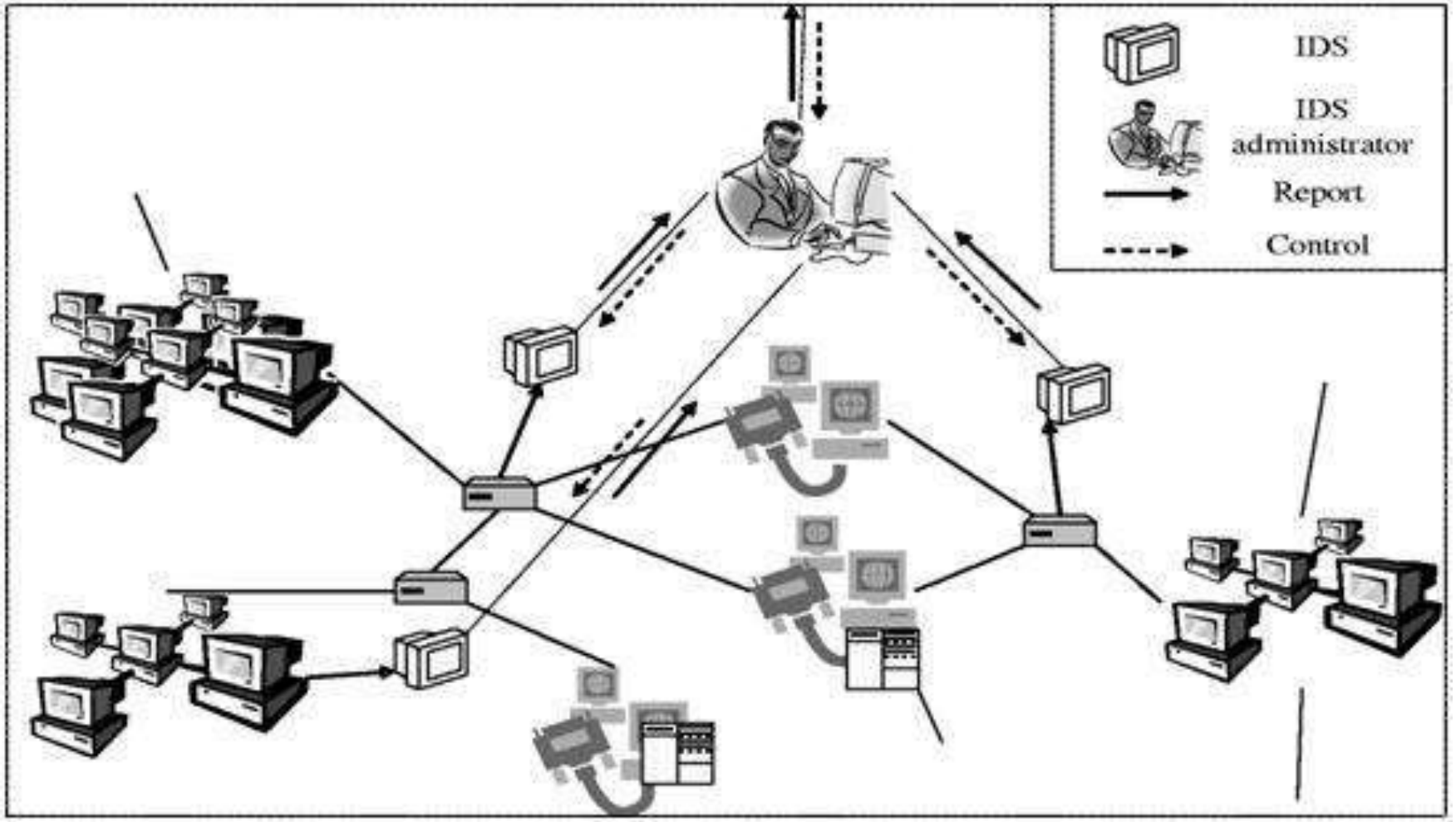
❖This system monitors the traffic on individual networks or subnets by continuously analyzing the traffic and comparing it with the known attacks in the library.

❖If an attack is detected, an alert is sent to the system administration.

❖It is placed mostly at important points in the network so that it can keep an eye on the traffic travelling to and from the different devices on the network.

❖The IDS is placed along the network boundary or between the network and the server.

❖An advantage of this system is that it can be deployed easily and at low cost, without having to be loaded for each system.


IDS
IDS administrator
Report
Control

Host Intrusion Detection System:

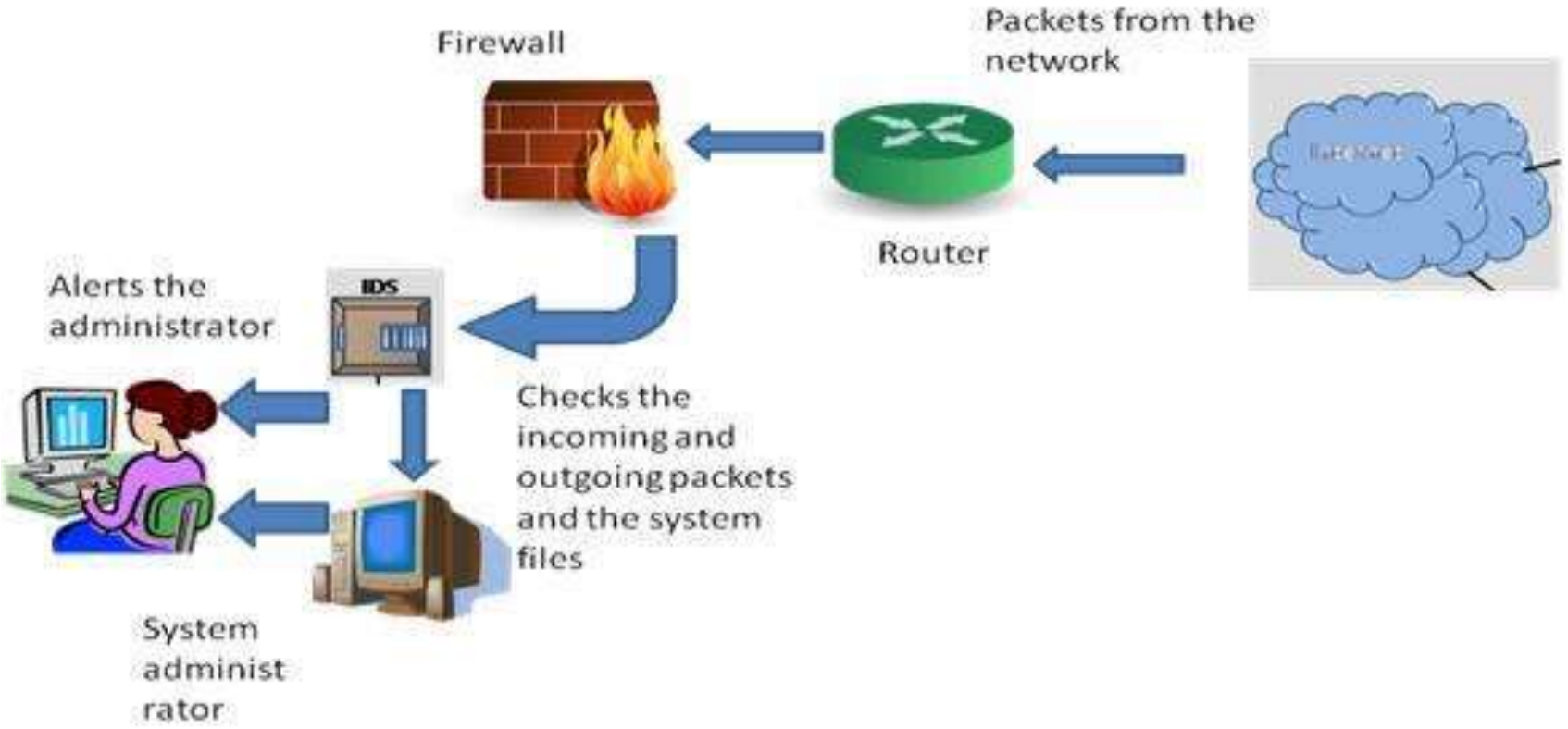
❖Such system works on individual systems where the network connection to the system, i.e. incoming and outgoing of packets are constantly monitored and also the auditing of system files is done

❖ In case of any discrepancy, the system administrator is alerted about the same.

❖This system monitors the operating system of the computer. The IDS is installed on the computer.

❖Advantage of this system is it can accurately monitor the whole system and does not require installation of any other hardware.

Host Intrusion Detection System:



Comparison

Host Based

- Narrow in scope (watches only **specific** host activities)
- More complex setup
- Better for detecting attacks from the **inside**
- **More expensive** to implement
- Detection is based on what any **single host** can record
- Does not see packet headers
- Usually only responds **after** a suspicious log entry has been made
- OS-specific
- Detects local attacks before they hit the network
- Verifies success or failure of attacks

Network Based

- Broad in scope (watches **all** network activities)
- Easier setup
- Better for detecting attacks from the **outside**
- **Less expensive** to implement
- Detection is based on what can be recorded on the **entire network**
- Examines packet headers
- Near **real-time** response
- OS-independent
- Detects network attacks as payload is analyzed
- Detects unsuccessful attack attempts

Host Intrusion Detection System:

❖Such system works on individual systems where the network connection to the system, i.e. incoming and outgoing of packets are constantly monitored and also the auditing of system files is done

❖ In case of any discrepancy, the system administrator is alerted about the same.

❖This system monitors the operating system of the computer. The IDS is installed on the computer.

❖Advantage of this system is it can accurately monitor the whole system and does not require installation of any other hardware.

Hybrid Intrusion Detection

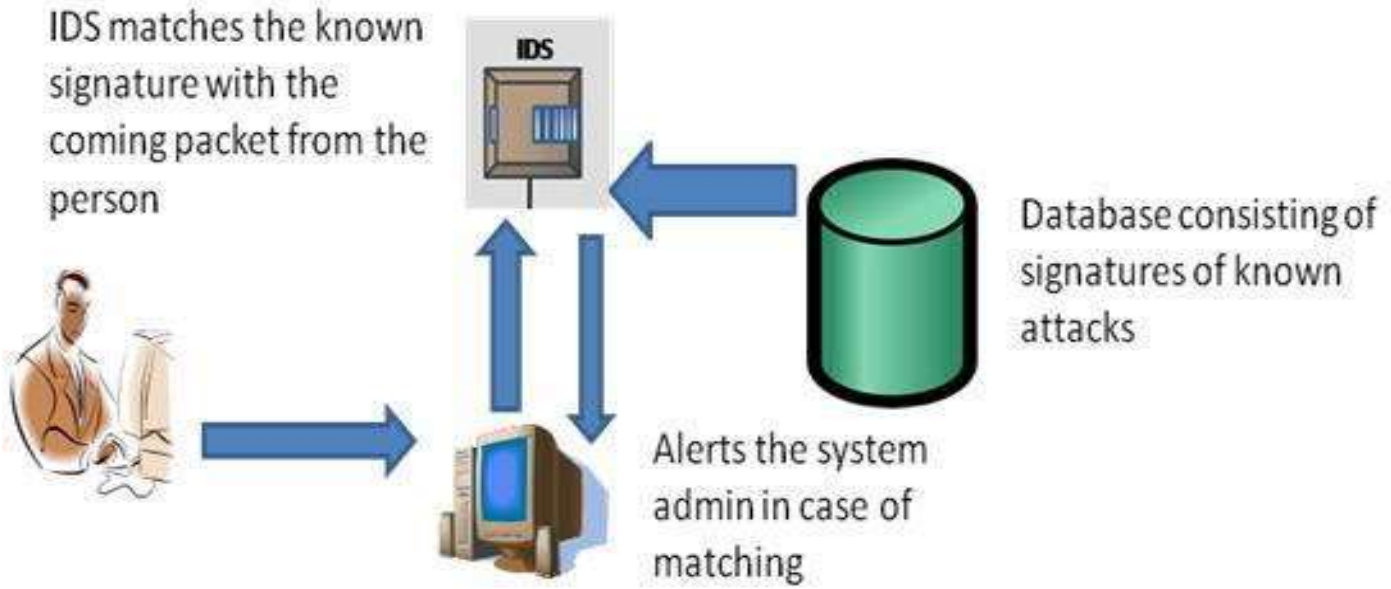
- Are systems that combine both Host-based IDS, which monitors events occurring on the host system and Network-based IDS, which monitors network traffic, functionality on the same security platform.
- A Hybrid IDS, can monitor system and application events and verify a file system's integrity like a Host-based IDS, but only serves to analyze network traffic destined for the device itself.
- A Hybrid IDS is often deployed on an organization's most critical servers.

Signature based Intrusion Detection System:

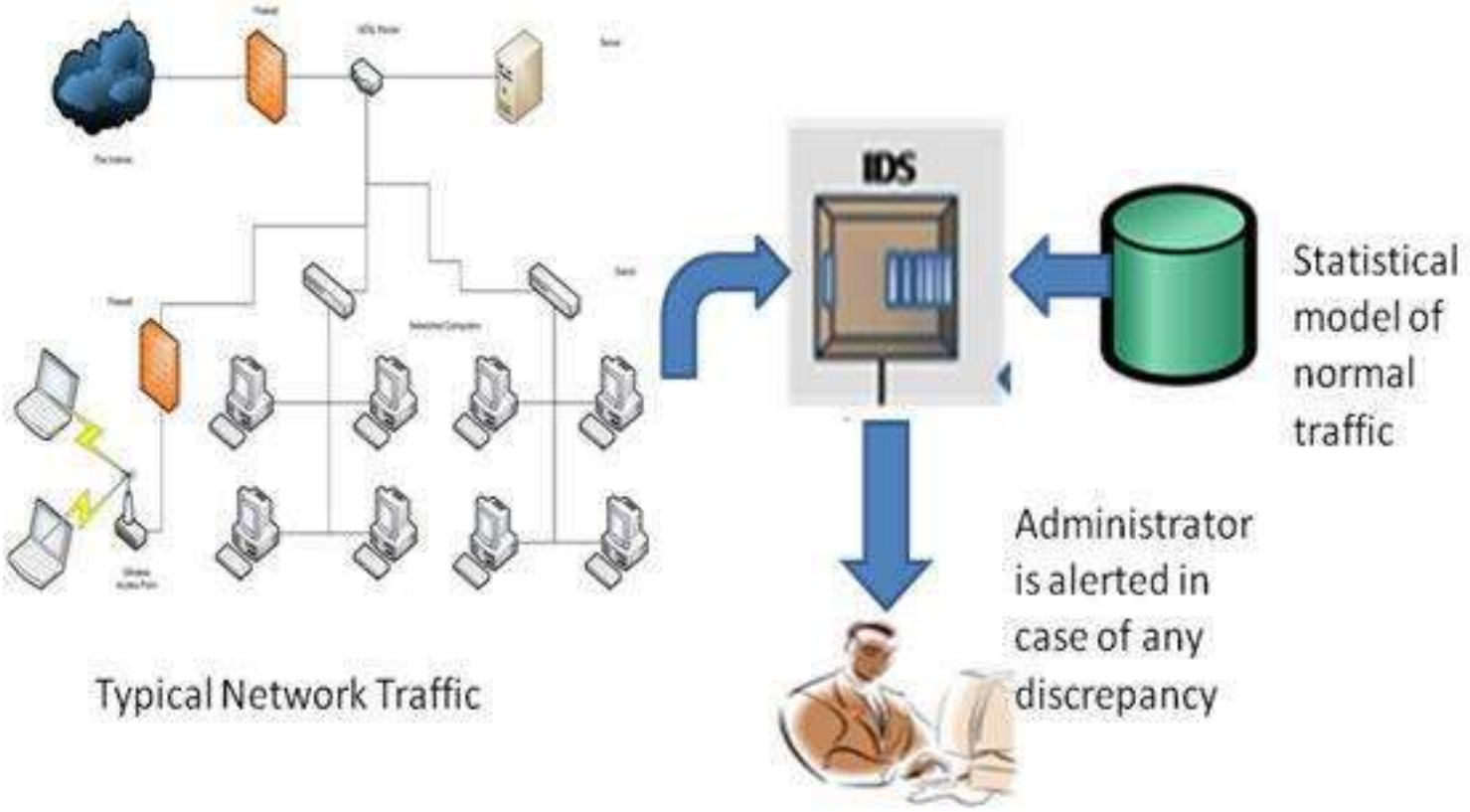
❖This system works on the principle of matching.

❖The data is analyzed and compared with the signature of known attacks. Incase of any matching, an alert is issued.

❖An advantage of this system is it has more accuracy and standard alarms understood by user.



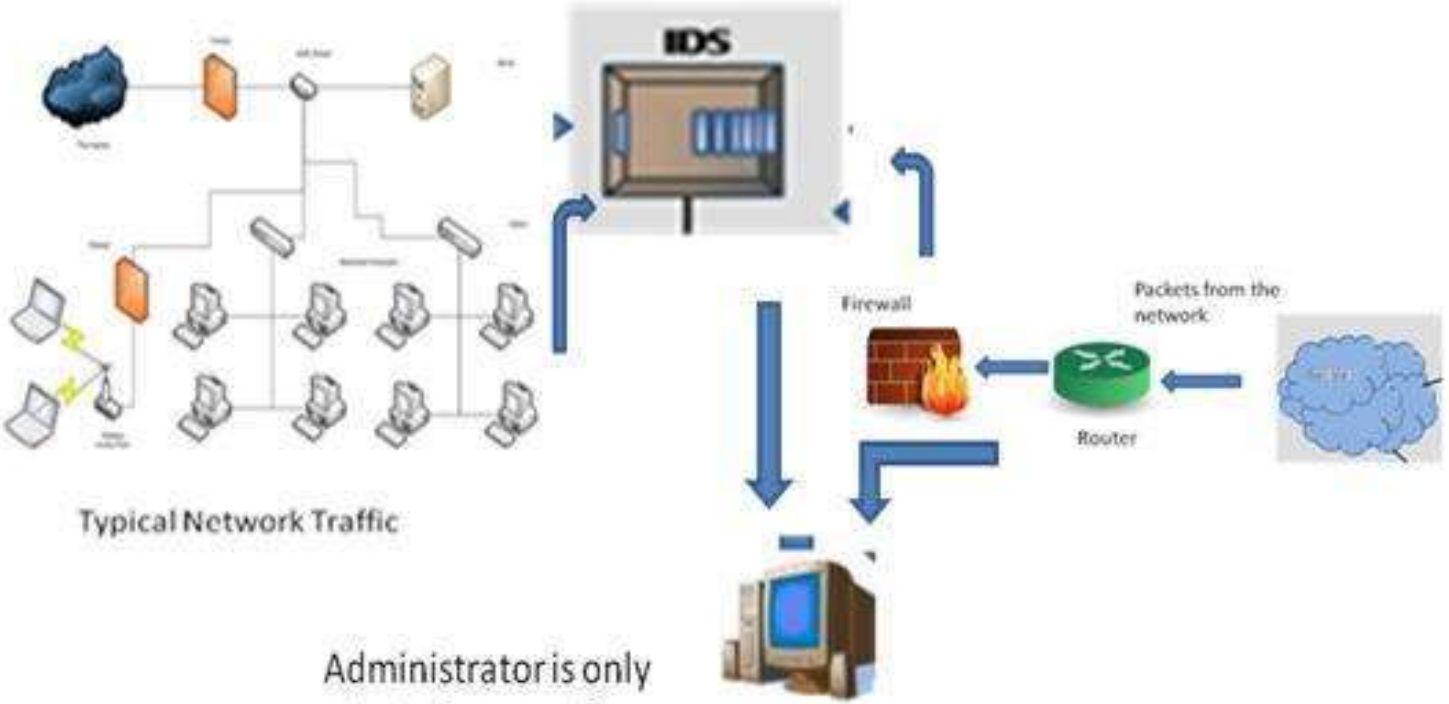
Anomaly based Intrusion Detection System:



Passive Intrusion Detection System:

❖It simply detects the kind of malware operation and issues an alert to the system or network administrator. (What we have been seeing till now!).

❖The required action is then taken by the administrator.



Reactive Intrusion Detection System:

It not only detects the threat but also performs specific action by resetting the suspicious connection or blocks the network traffic from the suspicious source.

It is also known as Intrusion Prevention System.

Typical Features of an Intrusion Detection System:

- It monitors and analysis 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 analysis of patterns based on known attacks.
- It detects errors in system configuration.
- It detects and cautions if the system is in danger.

Advantages of Intrusion Detection Systems

❖The network or computer is constantly monitored for any invasion or attack.

❖The system can be modified and changed according to needs of specific client and can help outside as well as inner threats to the system and network.

❖It effectively prevents any damage to the network.

❖It provides user friendly interface which allows easy security management systems.

❖Any alterations to files and directories on the system can be easily detected and reported.

Domain Name System (DNS)

Domain Name System (DNS)

❖DNS, or the Domain Name System, translates human readable domain names (for example, www.amazon.com) to machine readable IP addresses (for example, 192.0.2.44).

❖The Internet's DNS system works much like a phone book by managing the mapping between names and numbers.

❖DNS servers translate requests for names into IP addresses, controlling which server an end user will reach when they type a domain name into their web browser.

❖These requests are called queries.

Types of DNS Service

An authoritative DNS

❖Its service provides an update mechanism that developers use to manage their public DNS names.

❖It then answers DNS queries, translating domain names into IP address so computers can communicate with each other.

❖Authoritative DNS has the final authority over a domain and is responsible for providing answers to recursive DNS servers with the IP address information.

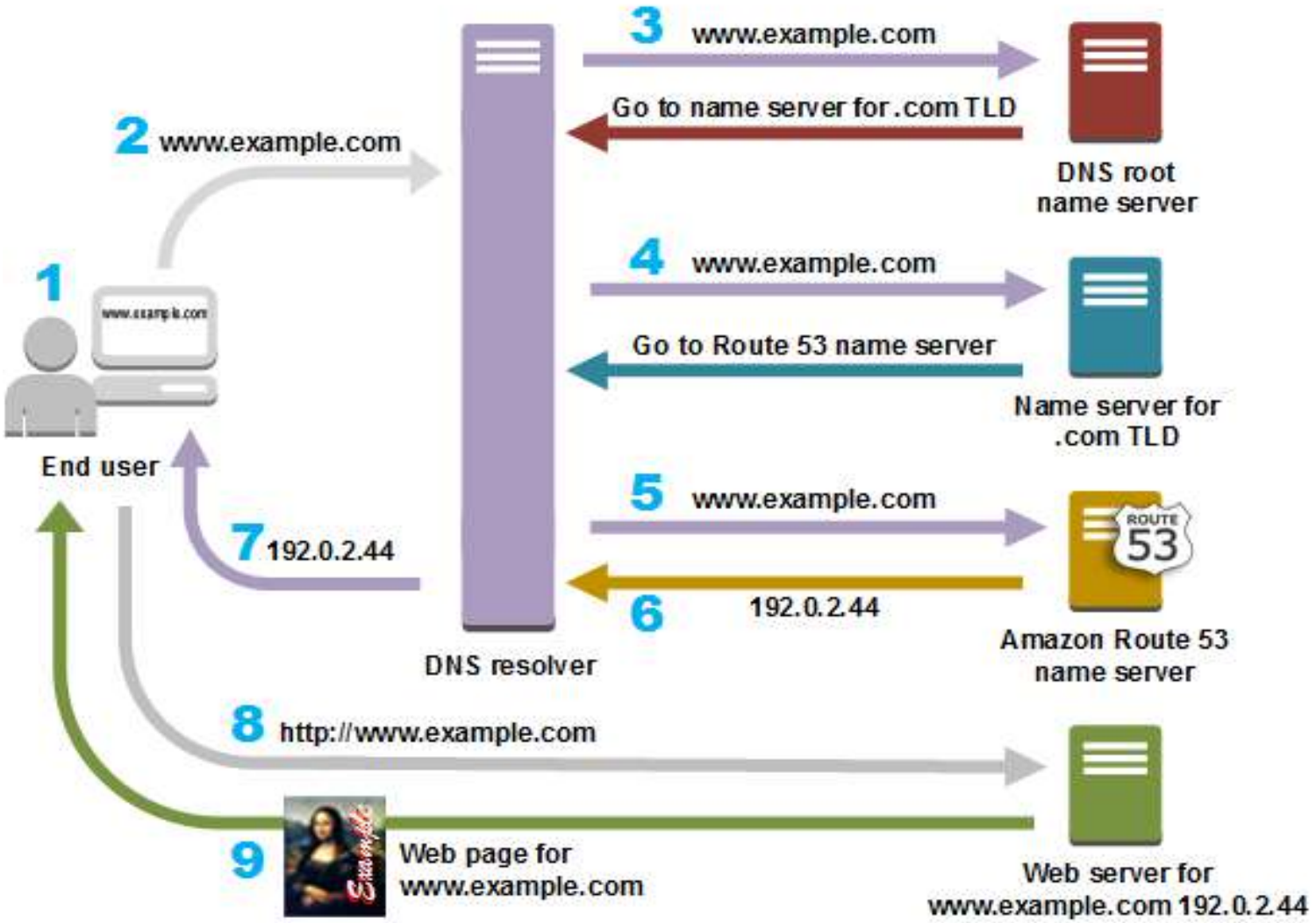
Types of DNS Service

❖Recursive DNS: Clients typically do not make queries directly to authoritative DNS services. Instead, they generally connect to another type of DNS service known a resolver, or a recursive DNS service.

If a recursive DNS has the DNS reference cached, or stored for a period of time, then it answers the DNS query by providing the source or IP information.

If not, it passes the query to one or more authoritative DNS servers to find the information.

How Does DNS Route Traffic To Your Web Application?



Domain Name System (DNS)

1. A user opens a web browser, enters www.example.com in the address bar, and presses Enter.

2. The request for www.example.com is routed to a DNS resolver, which is typically managed by the user's Internet service provider (ISP), such as a cable Internet provider, a DSL broadband provider, or a corporate network.

3. The DNS resolver for the ISP forwards the request for www.example.com to a DNS root name server.

4. The DNS resolver for the ISP forwards the request for www.example.com again, this time to one of the TLD name servers for .com domains. The name server for .com domains responds to the request with the names of the four Amazon Route 53 name servers that are associated with the example.com domain.

Domain Name System (DNS)

5. The DNS resolver for the ISP chooses an Amazon Route 53 name server and forwards the request for www.example.com to that name server.

6. The Amazon Route 53 name server looks in the example.com hosted zone for the www.example.com record, gets the associated value, such as the IP address for a web server, 192.0.2.44, and returns the IP address to the DNS resolver.

7. The DNS resolver for the ISP finally has the IP address that the user needs. The resolver returns that value to the web browser. The DNS resolver also caches (stores) the IP address for example.com for an amount of time that you specify so that it can respond more quickly the next time someone browses to example.com. For more information, see time to live (TTL).

8. The web browser sends a request for www.example.com to the IP address that it got from the DNS resolver. This is where your content is, for example, a web server running on an Amazon EC2 instance or an Amazon S3 bucket that's configured as a website endpoint.

9. The web server or other resource at 192.0.2.44 returns the web page for www.example.com to the web browser, and the web browser displays the page.