

Chapter Four

Managing communication and network security

Remote access technologies

- Remote access technologies refer to the various methods and technologies that enable users to connect to computer systems or networks from a location other than the physical site.
- These technologies are essential for individuals or employees who need to access resources, data, or applications from outside the traditional office environment.
- remote access technology has reshaped modern work environments by promoting

Remote Access Modern Work Environments

- Flexibility and Work-Life Balance
- Increased Productivity
- Global Collaboration
- Cost Saving
- Advancements
 - Security and Compliance
 - Business Continuity
 - Employee Satisfaction and Retention
 - Challenges and Solutions

Common Remote access technologies

1. Virtual Private Network (VPN):

A VPN **establishes a secure and encrypted connection** over the internet, allowing users to access a private network from a remote location. This is often used for accessing company networks securely.

2. Remote Desktop Services (RDS):

RDS allows users to connect to a desktop environment or specific applications on a remote server. It provides a virtualized desktop experience, making it possible to access a remote computer as if you were sitting in front of it.

3. Cloud-Based Solutions:

Cloud services, such as cloud-based applications and storage, enable users to access resources hosted in the cloud from any device with an internet connection.

4. Secure Shell (SSH):

SSH is a cryptographic network protocol that provides a secure way to access and manage network devices remotely. It is

5. Mobile Device Management (MDM):

MDM solutions allow organizations to manage and secure mobile devices remotely. This is important for ensuring that mobile devices used for work are compliant with security policies.

6. Web-Based Remote Access:

Accessing resources and applications through a web browser, often utilizing HTTPS for secure connections.

7. Remote File Access:

- Tools like FTP (File Transfer Protocol), SFTP (Secure File Transfer Protocol), and cloud storage services enable users to access and transfer files remotely

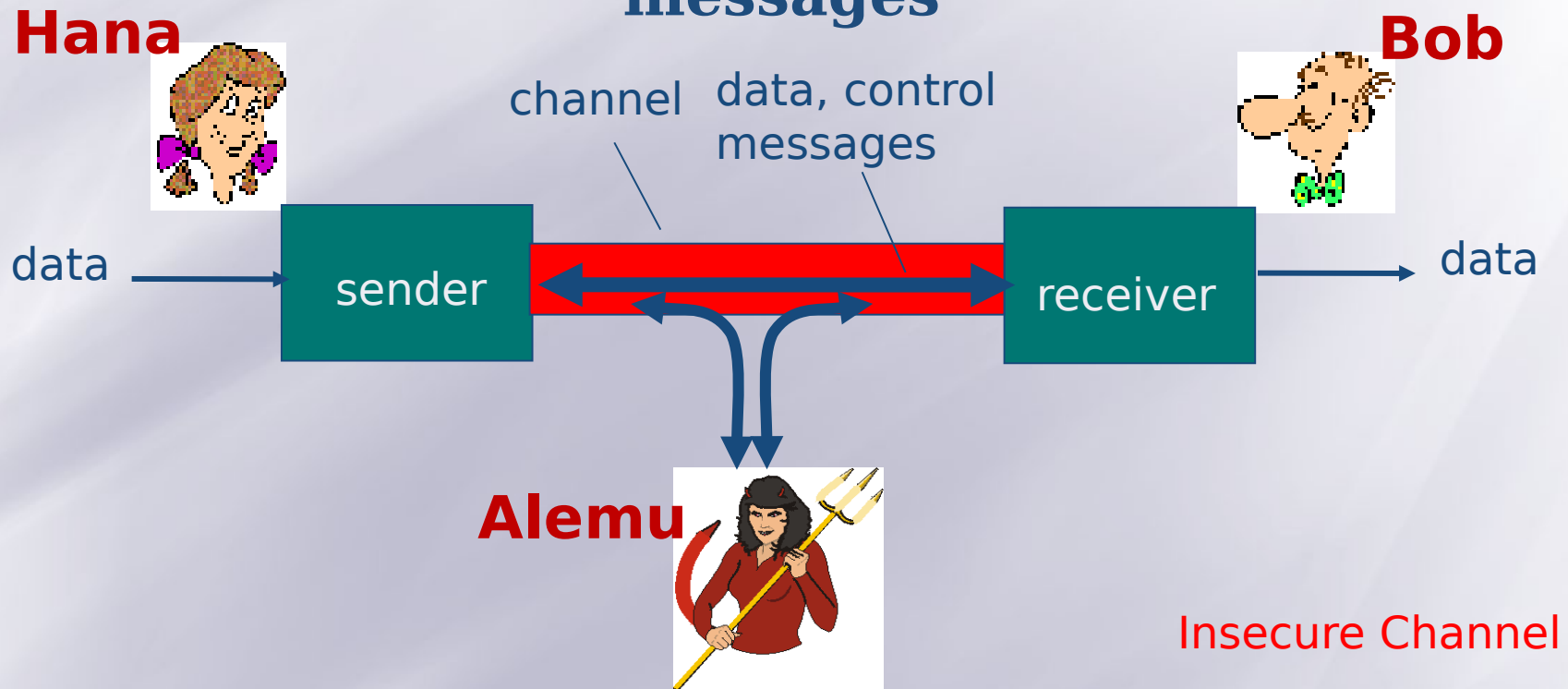
9. Remote Access Software:

- Various remote access software, such as TeamViewer, LogMeIn, or AnyDesk, Splashtop, allows users to connect to and control remote computers for support

Network Security

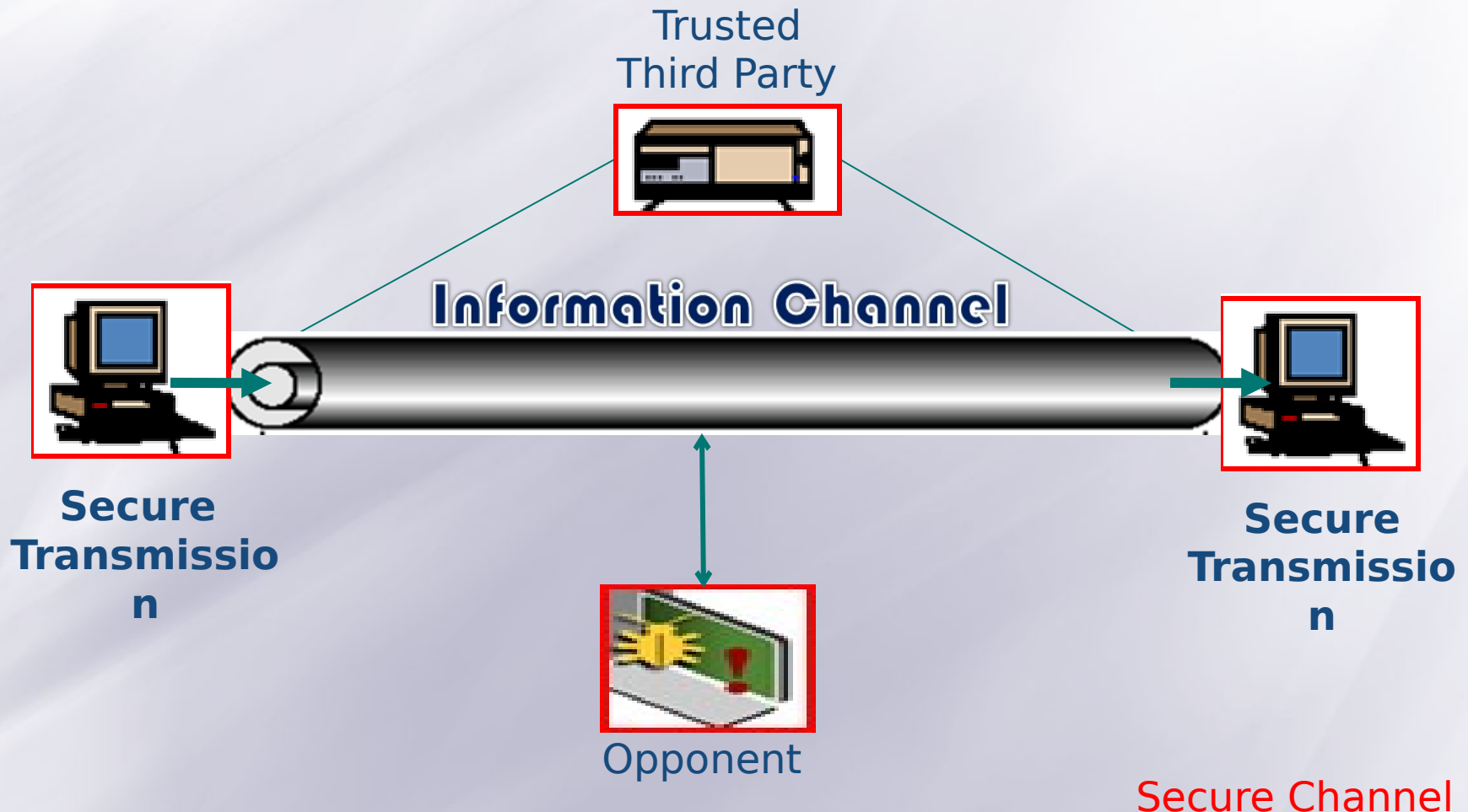
Hana, Bob and Alemu “Amies” and “Enemies”

Bob and **Hana** want to communicate securely
Alemu may intrude to intercept, delete or add messages



Network Security

Model for Secure Transmission



Network Security

Introduction

≡ In today's highly networked world, **computer security** is highly dependent on **network security**

≡ Focus is on:

- **Internet/Intranet** security issues in **TCP/IP** based networks (application, transport and network) link and physical layers are not also free from attack

- Attacks that use security holes of the network protocol and their defenses

≡ Does not include attacks that use

Network Security

Concerns in Network Security

- ≡ **Confidentiality:** only sender and intended receiver should “understand” message contents
- ≡ **Authentication:** sender and receiver want to confirm identity of each other
- ≡ **Message integrity:** sender and receiver want to ensure message not altered (in transit, or afterwards) without detection
- ≡ **Access and availability:** services must be accessible and available to users

Network Security/ Types of Attacks

Passive attacks

- ≡ Listen to the network and make use of the information without altering
 - Passive **wiretapping** attack
 - **Traffic analysis**
- ≡ Most networks use a broadcast medium and it is easy to access other machines packets
 - Utilities such as **EtherDetect** and **tcpdump**

Network Security/ Types of Attacks

Active attacks

☰ An active attack threatens the **integrity** and **availability** of data being transmitted

- The transmitted data is fully controlled by the intruder
- The attacker can **modify, extend, delete** or **play** any data

☰ This is quite possible in TCP/IP since the frames and packets are not protected in terms of authenticity and integrity

☰ Denial of service or **degrading** of service attack

- **Prevention** of authorized access to resources
- Examples
 - **E-mail bombing**: flooding someone's mail store
 - **Smurf attack**: Sending a “ping” multicast or broadcast with a spoofed IP of a victim. The recipients will respond with a “pong” to the victim
 - There had been reports of incidences of **distributed denial of service attacks** against major sites such as **Amazon, Yahoo, CNN and eBay**

Network Security/ Types of Attacks

Active attacks ...

- ☰ **Spoofing** attack: a situation in which one person or program imitates another by falsifying data and thereby gaining an illegitimate advantage.
 - **IP spoofing**
 - Putting a wrong IP address in the source IP address of an IP packet
 - **DNS spoofing**
 - Changing the DNS information so that it directs to a wrong machine
 - **URL spoofing/Webpage phishing**
 - A legitimate web page such as a bank's site is reproduced in "look and feel" on another server under control of the attacker
 - **E-mail address spoofing**
 - **Session hijacking**

Network Security/ Protocols and Vulnerabilities

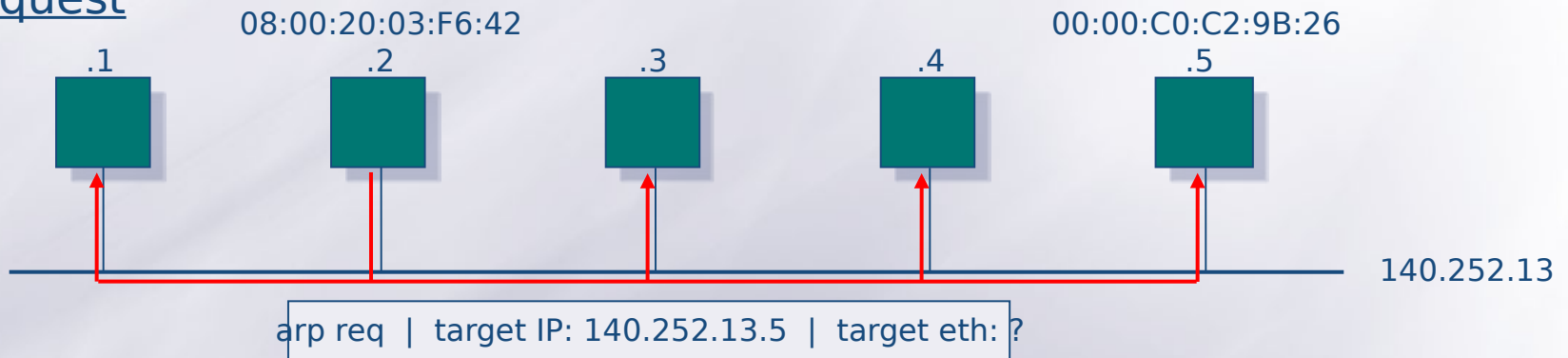
Security in TCP/IP Networks

- ≡ TCP/IP was **designed** to be used by a **trusted** group of users
- ≡ The protocols are **not designed** to **withstand attacks**
- ≡ Internet is now used by **all** sorts of **people**
- ≡ Attackers exploit **vulnerabilities** of every protocol to achieve their goals
- ≡ The next slides show some attacks at each layer of the **TCP/IP stack**

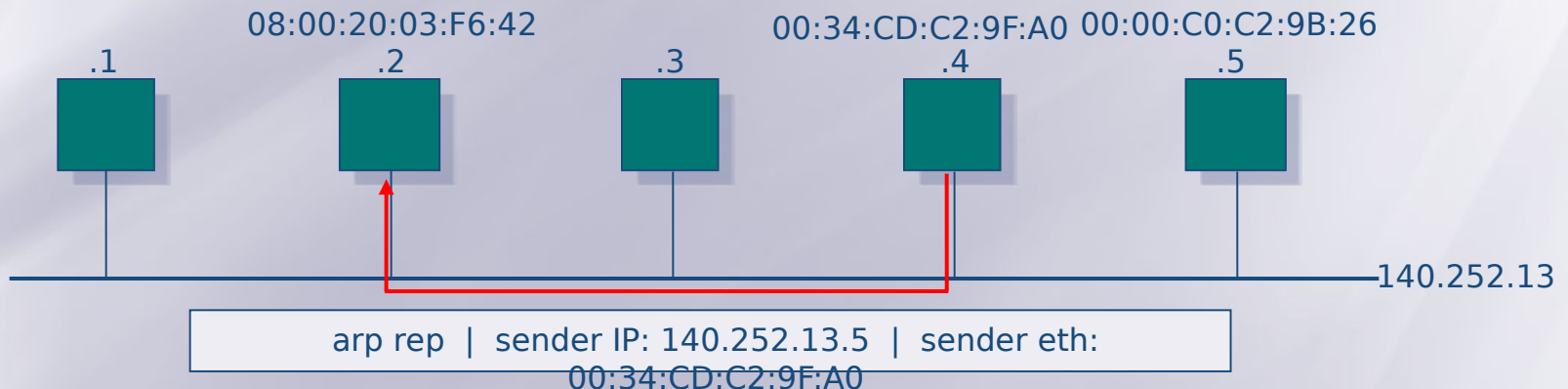
Network Security/ Protocols and Vulnerabilities

Link and Physical Layers: ARP Spoofing, Wiretapping

Request



Reply



Read more on ARP Spoofing and Wiretapping!

Network Security/ Protocols and Vulnerabilities

Network Layer: IP Vulnerabilities

- ≡ IP packets can be intercepted
 - In the LAN broadcast
 - In routers and switches
- ≡ Since the packets are not protected they can be easily read
- ≡ Since IP packets are not authenticated they can be easily modified
- ≡ Even if the user encrypts his/her data it will still be vulnerable to traffic analysis attack
- ≡ Information exchanged between routers to maintain their routing tables is not authenticated

Network Security/ Protocols and Vulnerabilities

Network Layer: IP security (IPSec) overview

☰ IPSec is a set of security algorithms plus a general framework that allows a pair of communicating entities to use whichever algorithms provide security appropriate for the communication.

☰ Applications of IPSec

- Secure branch office connectivity over the Internet
- Secure remote access over the Internet
- Establishing extranet and intranet

Network Security/ Protocols and Vulnerabilities

Network Layer: IP security (IPSec) overview ...

☰ Benefits of IPSec

- Transparent to applications (below transport layer)
- Provide security for individual users

☰ IPSec can assure that:

- A router or neighbor **advertisement** comes from an **authorized router**
- A **redirect** message comes from the router to which the **initial** packet was sent
- A routing update is **not forged**

Network Security/ Protocols and Vulnerabilities

Network Layer: IP security (IPSec)

≡ Network-layer secrecy:

- Sending host encrypts the data in IP datagram
- TCP and UDP segments; ICMP and SNMP messages

≡ Network-layer authentication

- Destination host can authenticate source IP address

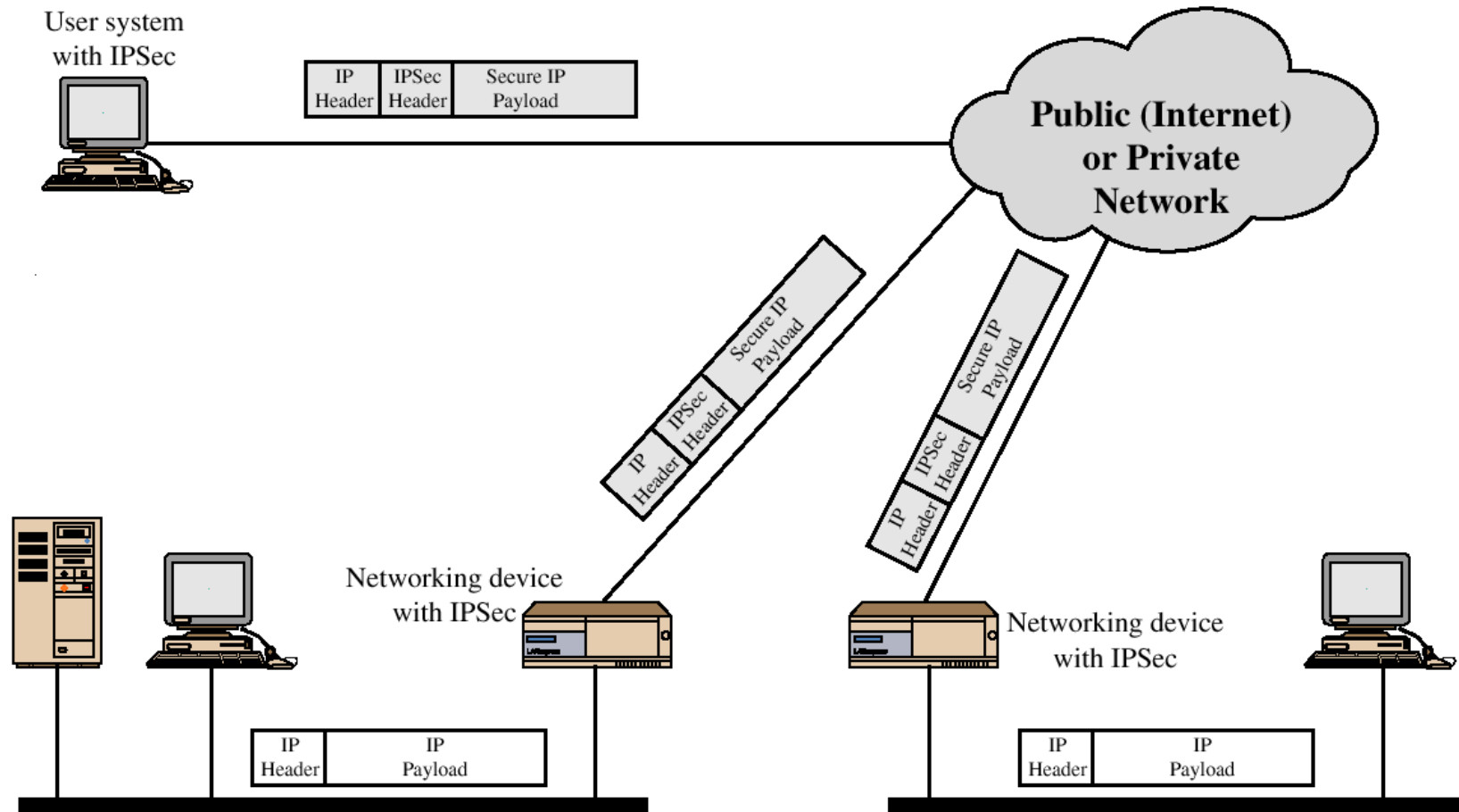
≡ Two principal protocols

- Authentication header (AH) protocol
- Encapsulation security payload (ESP) protocol

≡ Both AH and ESP provide confidentiality

Network Security/ Protocols and Vulnerabilities

Network Layer: IP security scenario ...



Network Security/ Protocols and Vulnerabilities

Network Layer: IPSec - Security Associations (SA)

- ≡ SA is a one way relationship between a sender and a receiver that provides security services (authentication and confidentiality)
- ≡ SA is uniquely identified by:
 - Security Parameters Index (SPI) in the enclosed extension header of AH or ESP
 - AH: Authentication Header (Authentication)
 - ESP: Encapsulating Security Payload (both authentication and confidentiality)
 - IP Destination address in the IPv4/IPv6 header
- ≡ Both AH and ESP support two modes of use
 - Transport Mode: Protection for upper layer protocols (TCP, UDP)
 - Tunnel Mode: Protection to the entire IP packet

Network Security/ Protocols and Vulnerabilities

Network Layer: IPSec AH Authentication



**(a) Before
AH**

← authenticated except for mutable fields →

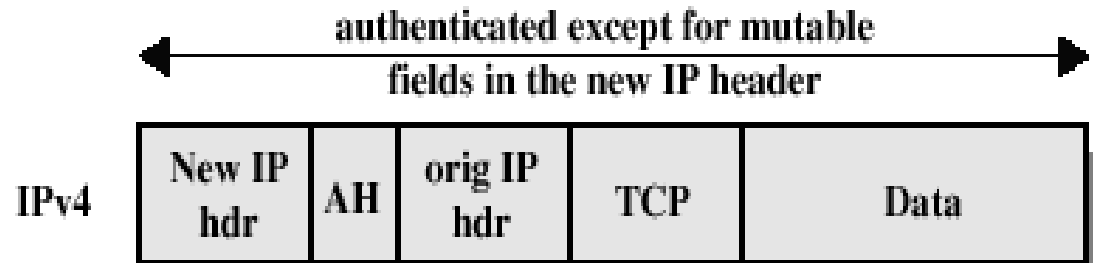


**(b) Transport
Mode**

Network Security/ Protocols and Vulnerabilities

Network Layer: IPSec AH Authentication

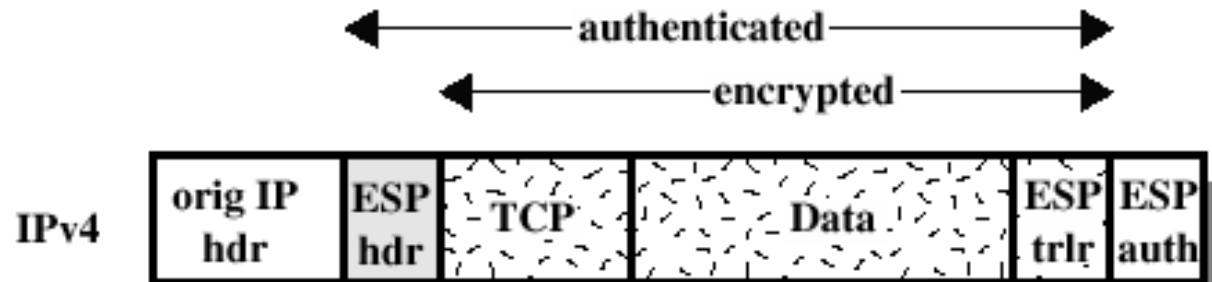
...



**(c) Tunnel
Mode**

Network Security/ Protocols and Vulnerabilities

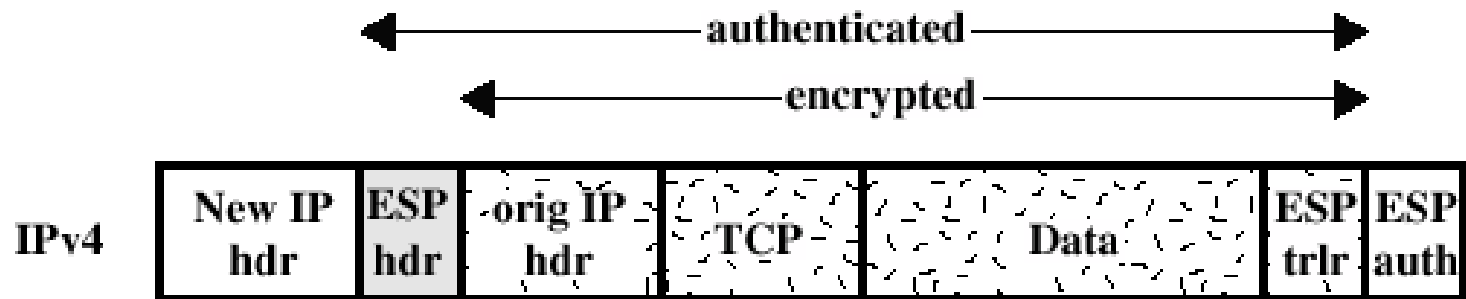
Network Layer: IPSec ESP Encryption and Authentication



a) Transport Mode

Network Security/ Protocols and Vulnerabilities

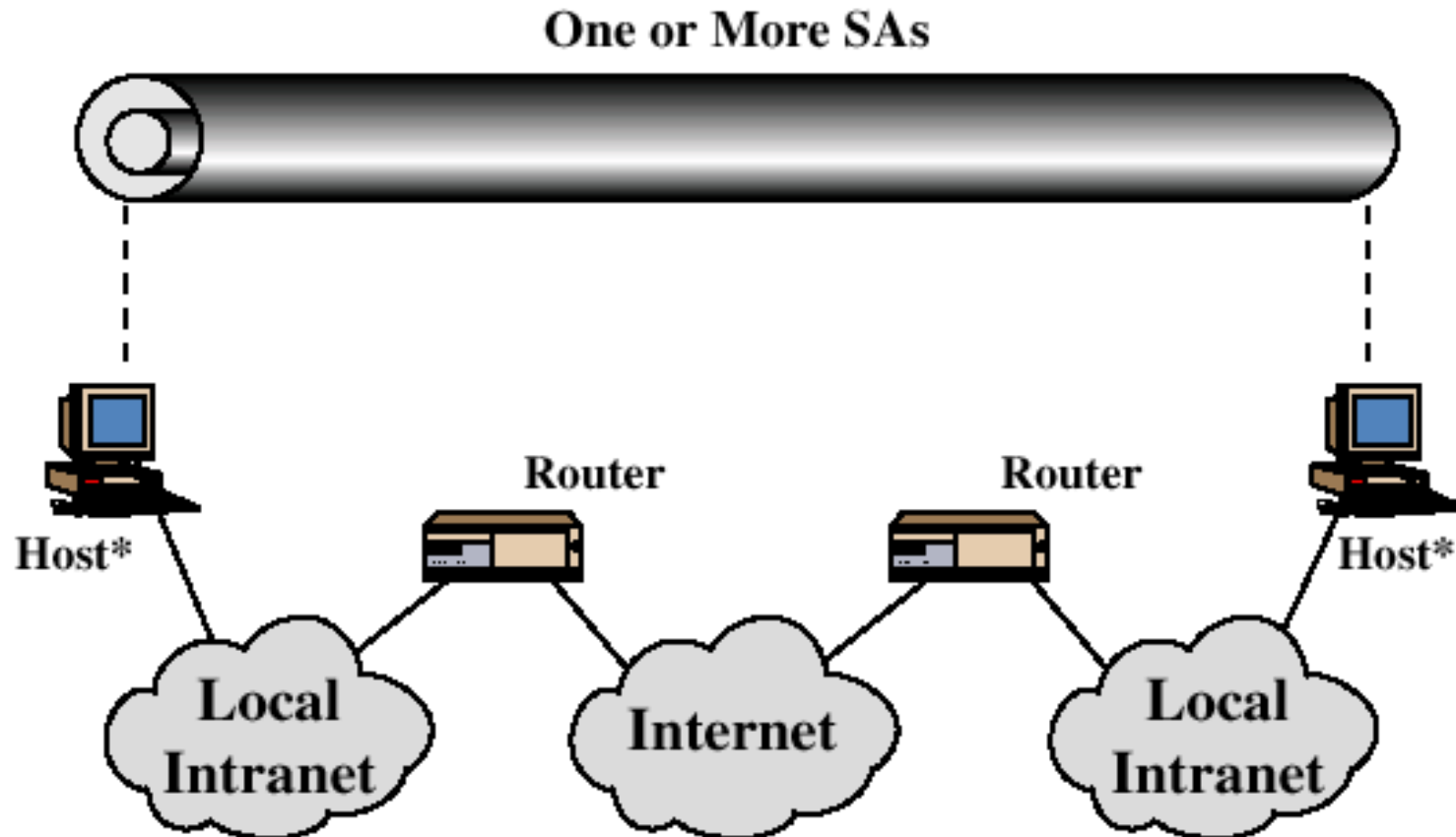
Network Layer: IPSec ESP Encryption and Authentication...



b) Tunnel mode

Network Security/ Protocols and Vulnerabilities

Network Layer: Combination of Security Associations

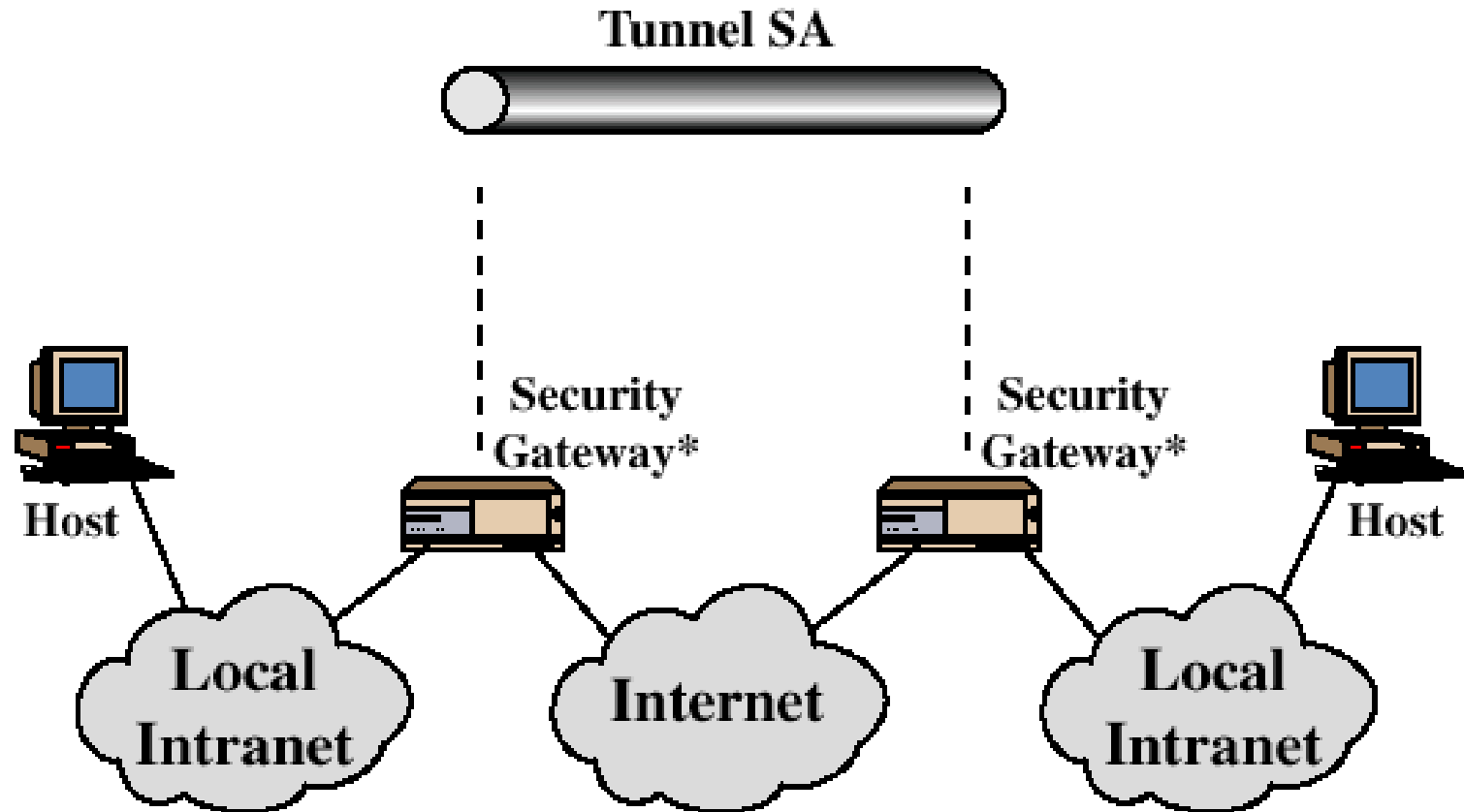


(a) Case 1

** Implements
IPSec*

Network Security/ Protocols and Vulnerabilities

Network Layer: Combination of Security Associations ...

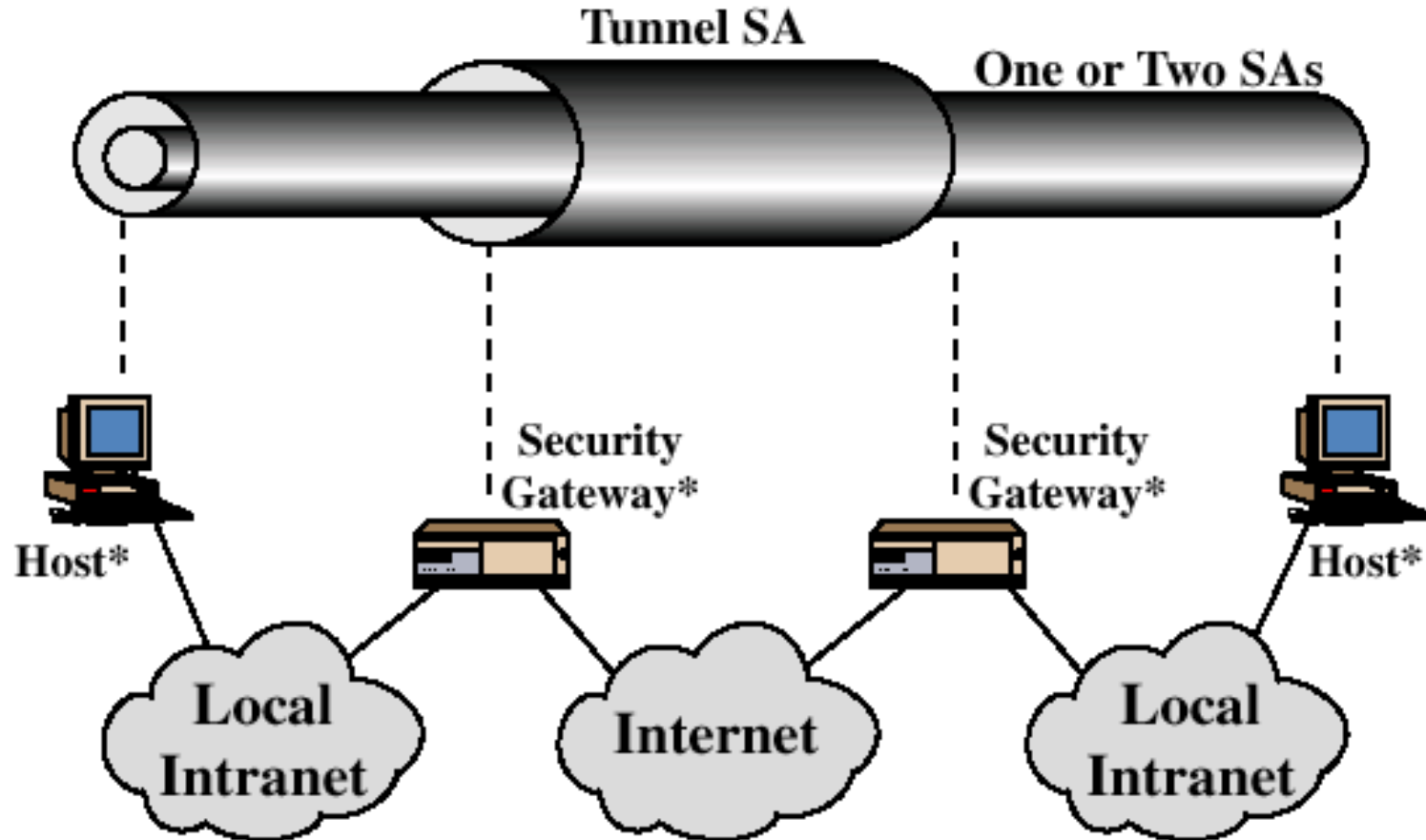


(b) Case 2

** Implements
IPSec*

Network Security/ Protocols and Vulnerabilities

Network Layer: Combination of Security Associations

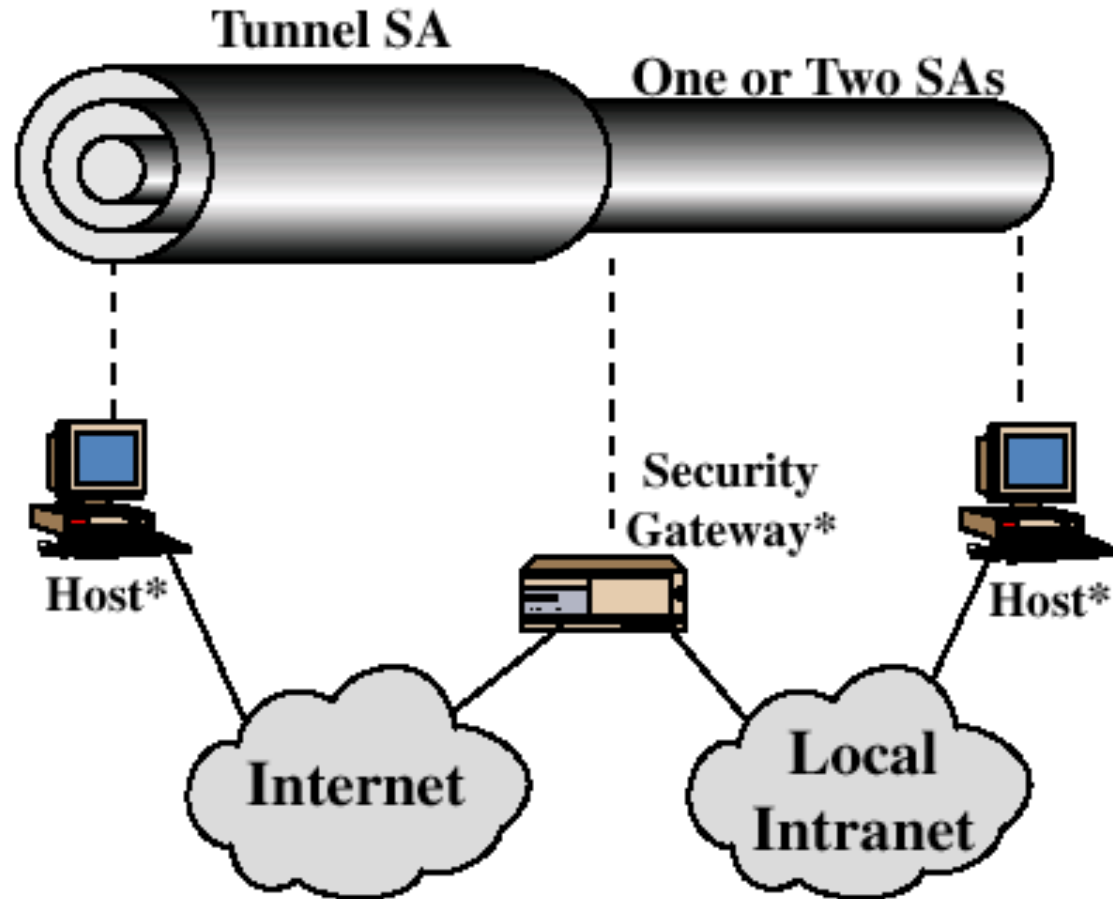


(c) Case 3

** Implements
IPSec*

Network Security/ Protocols and Vulnerabilities

Network Layer: Combination of Security Associations



(d) Case 4

* *Implements
IPSec*

Network Security/ Protocols and Vulnerabilities

IPSec: Encryption, Authentication... Summary

- ≡ **IPSec** provides authentication, confidentiality, and key management at the level of IP packets.
- ≡ IP-level authentication is provided by inserting an **Authentication Header** (AH) into the packets.
- ≡ IP-level confidentiality is provided by inserting an **Encapsulating Security Payload** (ESP) header into the packets. An ESP header can also do the job of the AH header by providing authentication in addition to confidentiality.
- ≡ Before ESP can be used, it is necessary for the two ends of a communication link to exchange the **secret key** that will be used for **encryption**. Similarly, AH needs an **authentication key**.
- ≡ IPSec is a specification for the IP-level security features that are built into the **IPv6** internet protocol. These security features can also be used with the **IPv4** internet protocol.

Network Security/ Protocols and Vulnerabilities

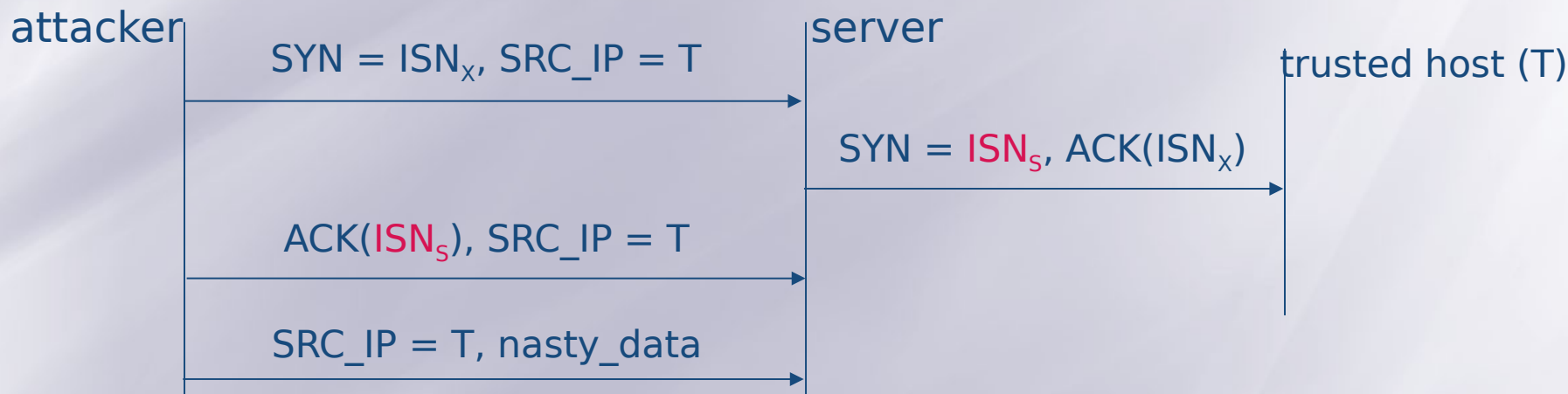
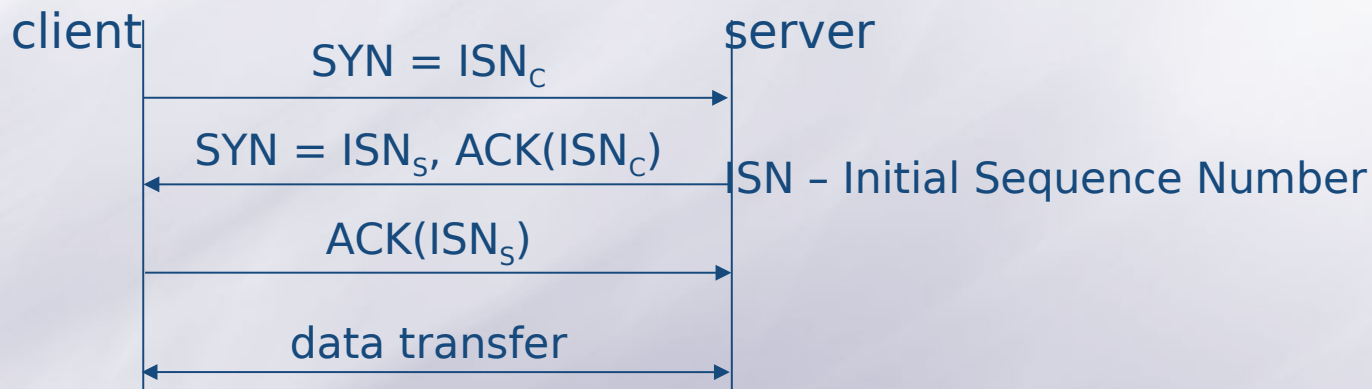
Transport Layer : TCP SYNC attack

- Sequence Number: monotonically increasing 32 bits long counter that provides anti-replay function
- Sequence numbers are initialized with a “random” value during connection setup
- The RFC(request for comment) suggests that the ISN (Initial Sequence Number) is incremented by one at least every 4 μ s
- In many implementations, it is computationally feasible to guess the next ISN number
- If successful, an attacker can impersonate

Network Security/ Protocols and Vulnerabilities

Transport Layer : TCP SYNC attack ...

3 way handshake



Impact of TCP SYN attack on Networks

- ✓ **Service Disruption:** Legitimate users find it difficult or impossible to access the affected service.
- ✓ **Resource Strain:** The server's resources, including memory and processing power, are consumed by the flood of bogus requests.
- ✓ **Potential System Failures:** In extreme cases, the server might crash or malfunction due to the overwhelming number of half-open connections.

Hence, some mitigation techniques are

- Firewall and proxies server
- SYN Cookies
- Reducing SYN-RECEIVED Timer and so on

Network Security/ Protocols and Vulnerabilities

SSL/TLS Protocols

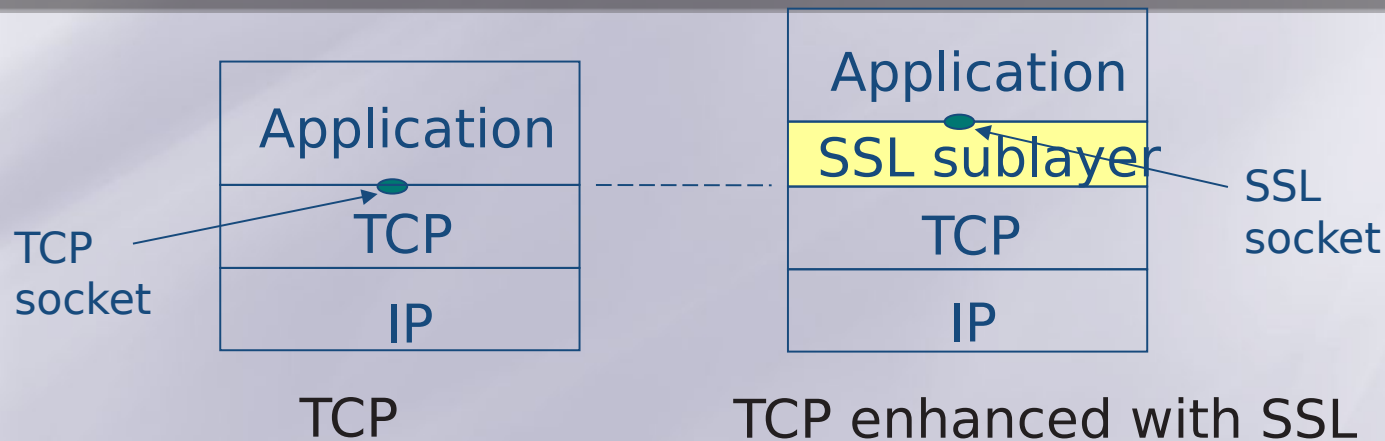
Secure Socket Layer (SSL)

- Widely deployed, “real-world” security protocol
- Considered as the de-facto standard for Internet security
- First designed by Netscape in 1994
- Evolved through versions 1.0, 2.0 and 3.0
- Version 3.0 is renamed to TLS by IETF/Internet Engineering Task Force (Sometimes called SSL 3.1)

Network Security/ Protocols and Vulnerabilities

SSL/TLS Protocols

- Provides transport layer security to any TCP-based application using SSL services.
e.g., between Web browsers, servers for e-commerce
- Provides security services like server authentication, data encryption, client authentication



Network Security/ Protocols and Vulnerabilities

SSL/TLS Protocols ...

- ≡ **SSL** is used extensively by web browsers to provide secure connections for transferring sensitive data.
- ≡ SSL-protected HTTP transfer uses port 443 (instead of port 80), and is identified with a special URL method - **https**.
 - For example: <https://www.gmail.com/> would cause an SSL-enabled browser to open a secure SSL session to port 443 at www.gmail.com.
- ≡ SSL, like most modern security protocols, is based on [cryptography](#).
- ≡ When an SSL session is established, the server begins by announcing a public key to the client, no encryption is in use initially.
 - Both parties (and any eavesdropper) can read this key.
- ≡ The client then transmits information to the server in a way that no one else could decode using the server's

Network Security/ Protocols and Vulnerabilities

Application layer: DNS spoofing

- ≡ If the attacker has access to a name server it can modify it so that it gives false information
 - Ex: redirecting *www.ebay.com* to map to own (attacker's) IP address
- ≡ The cache of a DNS name server can be poisoned with false information using some simple techniques

Network Security/ Protocols and Vulnerabilities

E-mail Security

- ≡ **E-mails** transit through various servers before reaching their destinations
- ≡ By default, they are visible by anybody who has access to the servers
- ≡ **SMTP** protocol has security holes and operational limitations
- ≡ E-mail security can be improved using tools and protocols like: PGP and S-MIME
 - **PGP**: Pretty Good Privacy
 - **S-MIME**: Secure Multi-Purpose Internet Mail Extension

Network Security/ Protocols and Vulnerabilities

E-Mail Security - SMTP

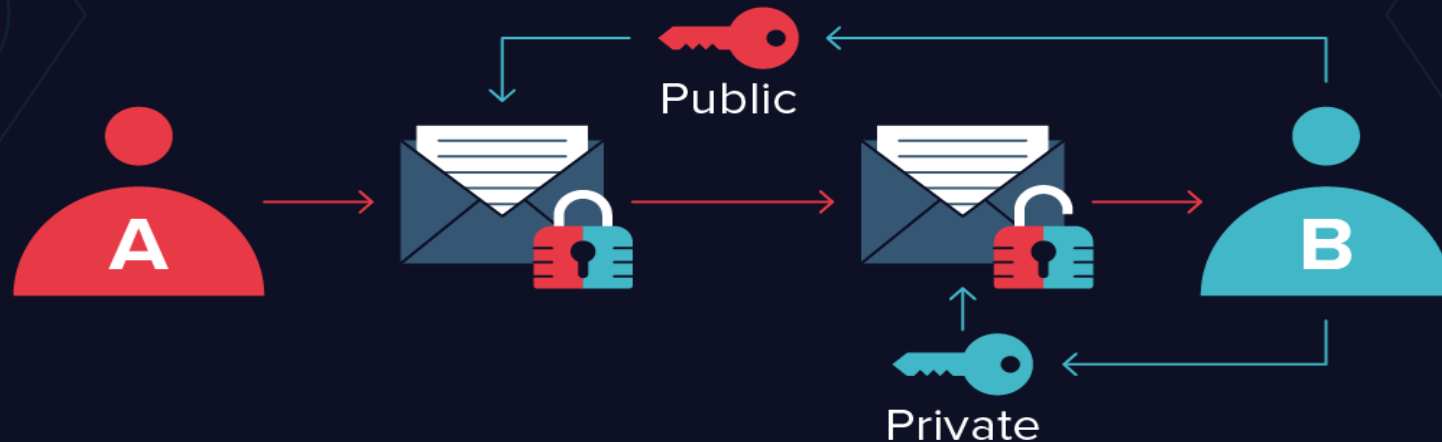
-  **SMTP Limitations - Can not transmit, or has a problem with:**
 - Executable files, or other binary files (jpeg image)
 - “national language” characters (non-ASCII)
 - Messages over a certain size
 - ASCII to EBCDIC(Extended Binary Coded Decimal Interchange Code) **translation problems**
 - Lines longer than a certain length (72 to 254 characters)

Network Security/ Protocols and Vulnerabilities

E-mail Security - PGP

-  Philip R. Zimmerman is the creator of PGP (Pretty Good Protocol)
-  PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications.
-  Example ProtonMail
-  Five services of PGP
 - Digital Signature
 - Message Encryption
 - Compression
 - E-mail Compatibility

HOW PGP ENCRYPTION WORKS



1. User A wants to send User B a private email
2. User B generates a public and private key
3. User B keeps the private key and sends back the public key
4. User A encrypts their message using the public key
5. User A sends the private encrypted message
6. User B decrypts the message with the private key

MIME(Multi-purpose Mail Extension) is a techniques used to describes transfer of a multimedia including audio, video and pictures.

E-mail Security - S/MIME Functions

-  **Enveloped Data:** Encrypted content and encrypted session keys for recipients
-  **Signed Data:** Message Digest encrypted with private key of “signer.”
-  **Clear-Signed Data:** Signed but not encrypted
-  **Signed and Enveloped Data:** Various orderings for encrypting and signing.

PGP	S/MIME
It is designed for processing the plain texts	designed to process email as well as many multimedia files.
less costly as compared to S/MIME.	comparatively expensive.
good for personal as well as office use.	good for industrial use.
less efficient than S/MIME.	more efficient than PGP.
depends on user key exchange.	it relies on a hierarchically valid certificate for key exchange.
contains 4096 public keys.	only 1024 public keys
standard for strong encryption.	the standard for strong encryption but has some drawbacks

Network Security/ Protocols and Vulnerabilities

Application layer: Web browser

☰ Types of Web threats and counter measures:

- **Integrity**
 - Data, memory and/or message modification
 - Trojan horse browser
 - ☐ **Cryptographic checksums**
- **Confidentiality**
 - Eavesdropping
 - Theft of data from client & information from Server
 - Access to information about network configuration
 - Access to information about which client is communicating
 - ☐ **Encryption**
- **Denial of Service**
 - Killing of user thread
 - Machine flooding
 - Filling up disk/memory
 - Isolating machine by DNS attacks
 - ☐ **Detection and action (suspicious pattern)**
- **Authentication**
 - Impersonation
 - Data forgery
 - ☐ **Cryptographic techniques**

Network Security/ Protocols and Vulnerabilities

Web Security: Secure Electronic Transactions (SET)

- ≡ An open encryption and security specification.
- ≡ Protect credit card transaction on the Internet.
- ≡ Companies involved:
 - MasterCard, Visa, IBM, Microsoft, Netscape, RSA, Terisa and Verisign
- ≡ Not a payment system but enables users to employ the existing credit card payment infrastructure on an open network (Internet) in a secure

Network Security/ Protocols and Vulnerabilities

Web Security: Secure Electronic Transaction Services

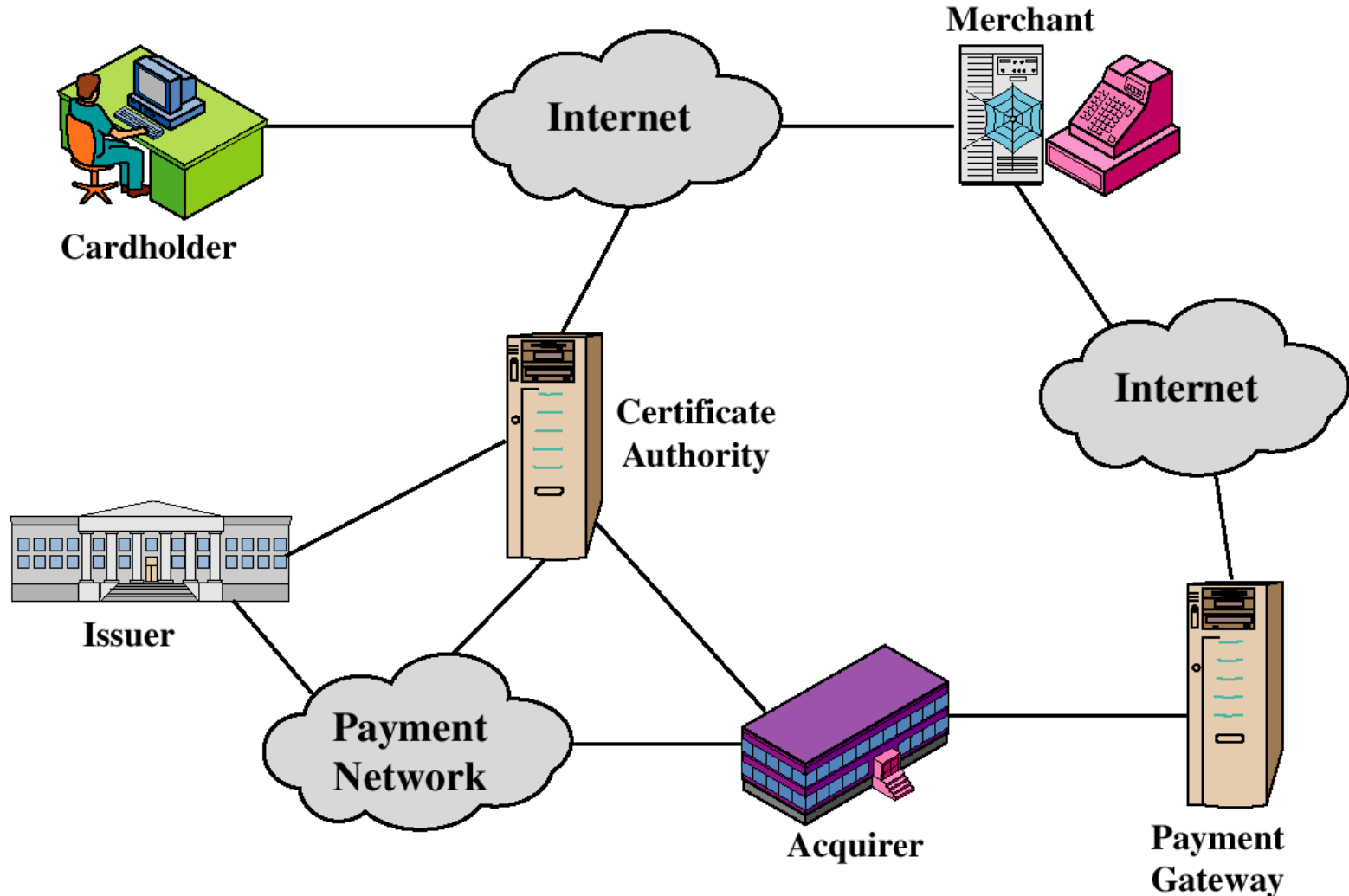
- ☰ Provides a secure communication channel in a transaction.
- ☰ Provides trust by the use of X.509v3 digital certificates.

☰ Key Features of SET:

- Confidentiality of information
- Integrity of data
- Cardholder account authentication
- Merchant authentication

Network Security/ Protocols and Vulnerabilities

Web Security: SET Participants



Network Security/ Protocols and Vulnerabilities

Web Security: SET Participants ...

- ≡ **Cardholder:** Authorized holder of Payment Card
- ≡ **Merchant:** Has goods to sell to the Cardholder.
- ≡ **Issuer:** Financial institution (such as bank) - connected with the Cardholder.
- ≡ **Acquirer:** Verifies that a card account is active and the proposed purchase does not exceed the credit limit - Connected with the Merchant.
- ≡ **Payment gateway:** Operated by the acquirer or a designated third party that processes merchant payment messages
- ≡ **Certification Authority:** Trusted entity to issue

Network Security/ Protocols and Vulnerabilities

Web Security: SET (Sequence of events for transactions)

1. The **customer** opens an account.
2. The **customer** receives a certificate.
3. **Merchants** have their own certificates.
4. The **customer** places an order.
5. The **merchant** is verified.
6. The **order** and payment are sent.
7. The **merchant** request payment authorization.
8. The **merchant** confirm the order.
9. The **merchant** provides the goods or service.

Network Security/ Protocols and Vulnerabilities

Web Security: SET - Dual Signature

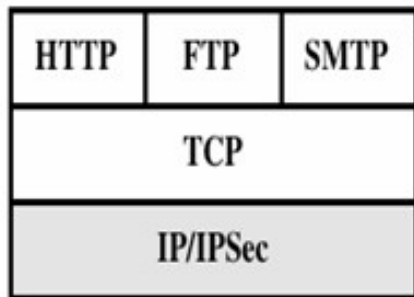
- ≡ Dual signature is an important **innovation by SET**
- ≡ Used to **link** two messages that are intended for **two different recipients**.
- ≡ The customer wants to send Order Information (**OI**) to the merchant and Payment Information (**PI**) to the bank.
- ≡ Merchant - Does not need to know customer's CC number.
- ≡ Bank - Does not need to know details of customer's order.

Privacy!!

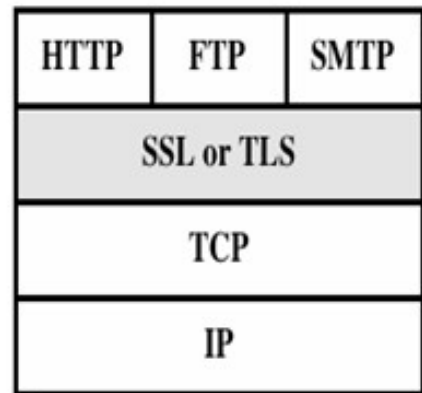
- ≡ The two items however must be linked

Network Security/ Summary

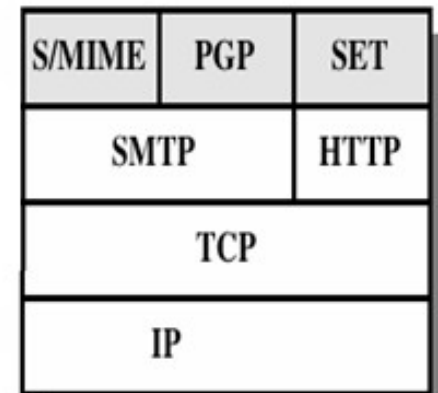
Security features in the TCP/IP protocol stack



(a) Network Level



(b) Transport Level



(c) Application Level

Network Security/ Summary

☰ Use of IP Security (IPSec) (Figure a)

- Transparent to applications
- Provide general purpose solution
- Provides filtering capability

☰ Security just above TCP (Figure b)

- SSL: **Secure Socket Layer**
- TLS: **Transport Layer Security**
- SSL/TLS could be provided as part of the underlying protocol suite => **Transparent to applications**
- Alternatively, can be embedded into applications
 - Example: Netscape and Microsoft Explorer browsers are equipped with SSL

☰ Application specific security services (Figure c)

- Embedded within specific application
- Best examples are SET (**Secure Electronic**

Network Security/ Summary

Security-enhanced application

☰ Solution to most application layer security problems are tackled by developing security-enhanced application protocols

☰ Examples

- For FTP => FTPS
- For HTTP => HTTPS
- For SMTP => SMTPS
- For DNS => DNSSEC

Directory security concern

- **A directory** is a location for storing files on a computer.
- **Directory security** involves controlling access to directories or folders on a computer system.
- Main goal to ensure that only authorized users or processes can view, modify, or execute the contents of a directory.

Some common directory security mechanisms:

1. **File System Permissions:** is a permission settings that specify what actions can be performed by the owner, the group, and others.
2. **Read, Write, and Execute Permissions:**
 - **Read (r):** Allows users to list the contents of a directory.
 - **Write (w):** Permits users to create, modify, or delete files within the directory.

3. **User Groups:** have a permissions set for the owner, the group, and others
4. **Access Control Lists (ACLs):** allow administrators to define more **detailed and specific permissions** for users or groups.
5. **Ownership:** the owner has special privileges, including the **ability to modify permissions** and content within the directory.
6. **Group Memberships and inheritance**
8. **Security Contexts:** Certain systems, such as Linux with **SELinux (Security-Enhanced Linux)**, allow directories to have security contexts associated with them. These contexts define additional **security attributes**, specifying the type and source of access.
9. **Encryption and authentication**
10. **Logging and auditing** allow administrators to