

Electronic mail security
IP security
Web security

Prepared by Dr. Ayman Khallel

IT373
Information Security

Lecture 10



Course content

1. Overview of security concepts and definitions
2. Symmetric cryptography; modern encryption algorithms (DES, AES)
3. Modern data encryption standards
4. Block cipher cryptanalysis and usage
5. Modern stream ciphers
6. Asymmetric cryptography; public key cryptography,
7. Cryptographic Hash Functions
8. Message authentication
9. Digital signature and authentication protocols
10. Electronic mail security, IP security, web security.

Agenda

- **Introduction to Web Security**
 - Key Challenges and Risks
 - TLS and HTTPS for Web Protection
- **Email Security**
 - Email Protocols and Standards (RFC 5322)
 - Common Email Security Threats
 - Countermeasures: STARTTLS, S/MIME, DNSSEC, DANE
- **IP Security (IPsec)**
 - Overview and Applications of IPsec
 - IPsec Modes: Transport vs Tunnel Mode
 - Benefits and Use Cases

Web Security Considerations

- The World Wide Web is fundamentally a client/server application running over the Internet and TCP/IP intranets
- The following characteristics of Web usage suggest the need for tailored security tools:
 - Web servers are relatively easy to configure and manage
 - Web content is increasingly easy to develop
 - The underlying software is extraordinarily complex
 - May hide many potential security flaws
 - A Web server can be exploited as a launching pad into the corporation's or agency's entire computer complex
 - Casual and untrained (in security matters) users are common clients for Web-based services.
 - Such users are not necessarily aware of the security risks that exist and do not have the tools or knowledge to take effective countermeasures

Table 17.1 A Comparison of Threats on the Web

	Threats	Consequences	Countermeasures
Integrity	•Modification of user data •Trojan horse browser •Modification of memory •Modification of message traffic in transit	•Loss of information •Compromise of machine •Vulnerabilty to all other threats	Cryptographic checksums
Confidentiality	•Eavesdropping on the net •Theft of info from server •Theft of data from client •Info about network configuration •Info about which client talks to server	•Loss of information •Loss of privacy	Encryption, Web proxies
Denial of Service	•Killing of user threads •Flooding machine with bogus requests •Filling up disk or memory •Isolating machine by DNS attacks	•Disruptive •Annoying •Prevent user from getting work done	Difficult to prevent
Authentication	•Impersonation of legitimate users •Data forgery	•Misrepresentation of user •Belief that false information is valid	Cryptographic techniques



HTTP	FTP	SMTP
TCP		
IP/IPSec		

(a) Network Level

HTTP	FTP	SMTP
SSL or TLS		
TCP		
IP		

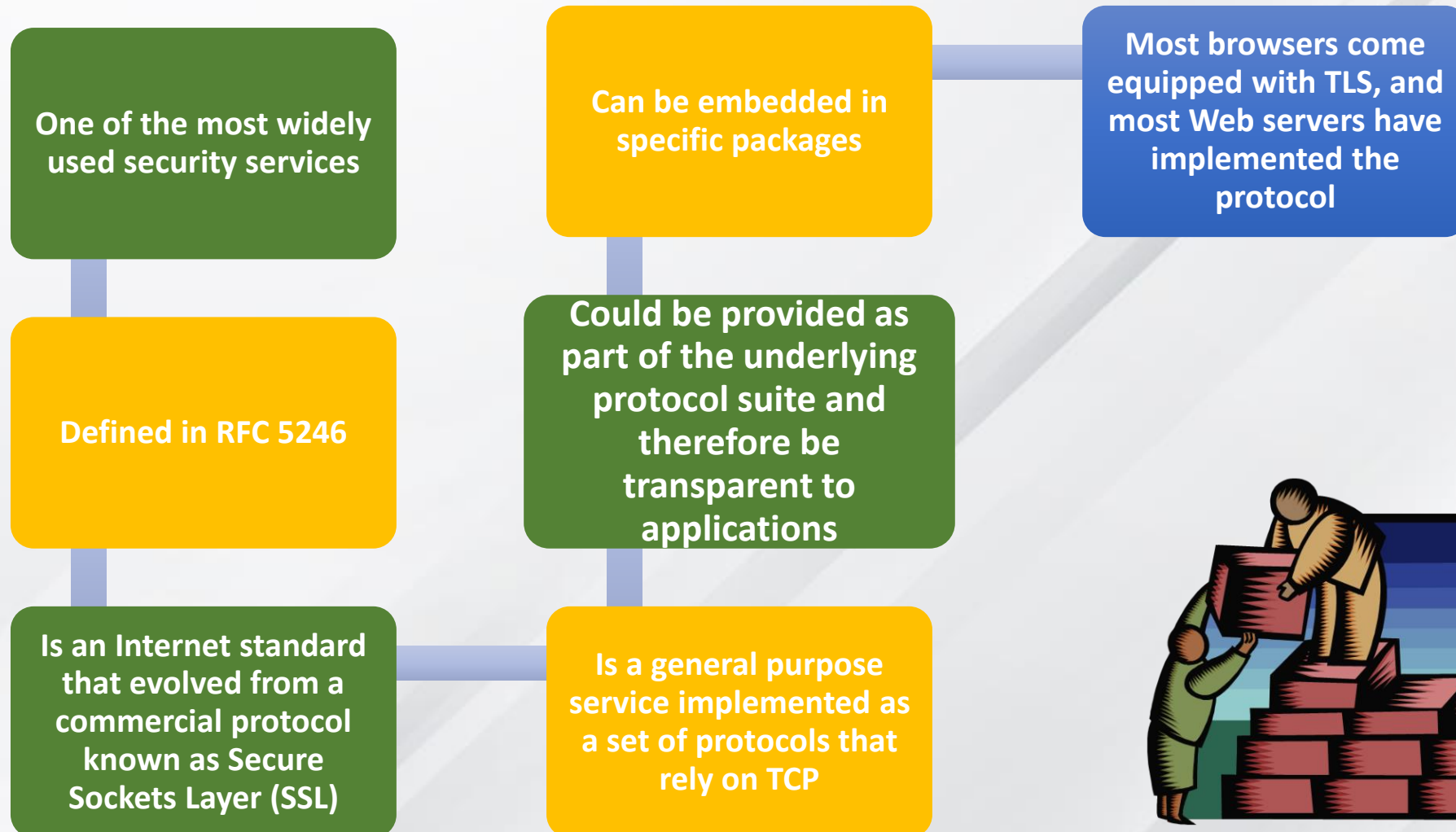
(b) Transport Level

	S/MIME	
Kerberos	SMTP	HTTP
UDP	TCP	
IP		

(c) Application Level

Figure 17.1 Relative Location of Security Facilities in the TCP/IP Protocol Stack

Transport Layer Security (TLS)



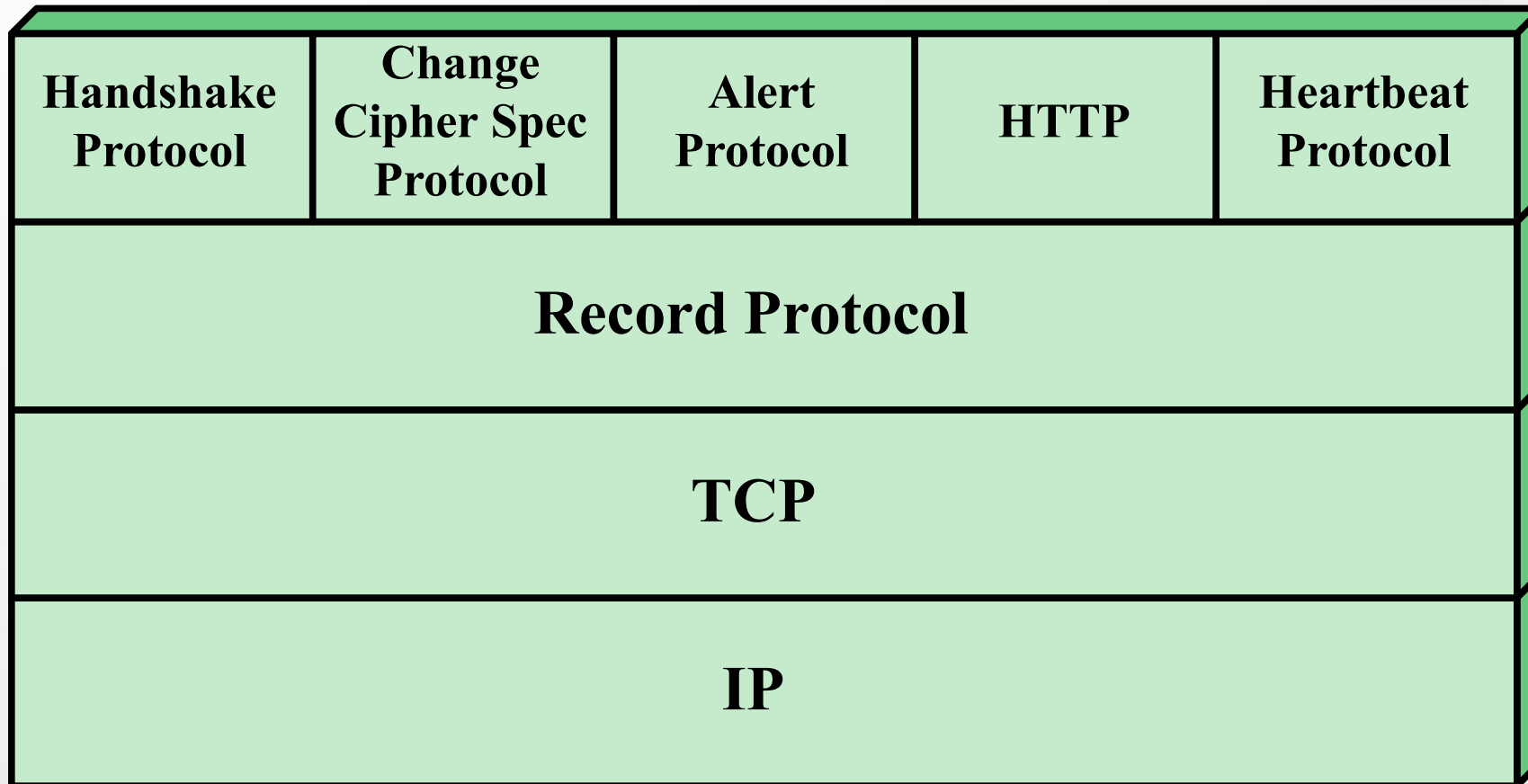


Figure 17.2 SSL/TLS Protocol Stack

TLS Architecture

- Two important TLS concepts are:

TLS connection

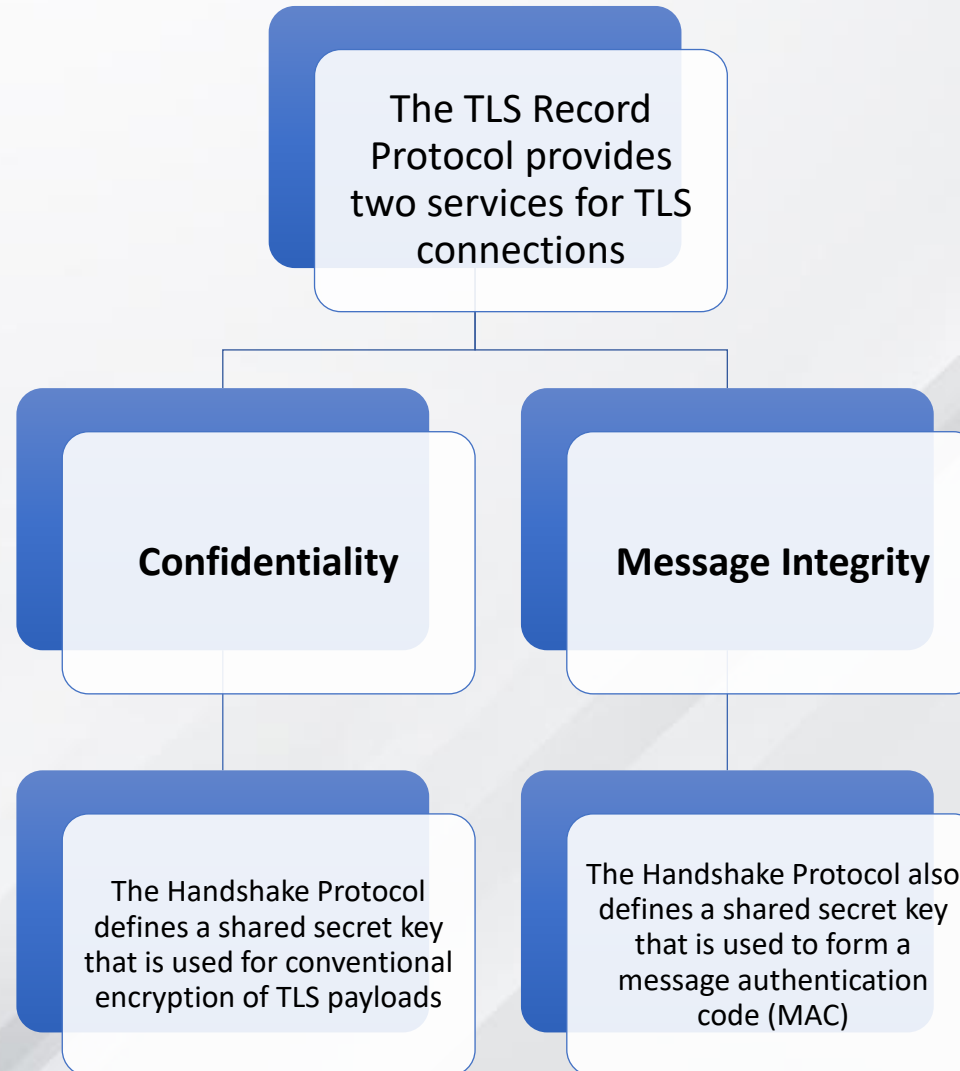
- A transport that provides a suitable type of service
- For TLS such connections are peer-to-peer relationships
- Connections are transient
- Every connection is associated with one session

TLS session

- An association between a client and a server
- Created by the Handshake Protocol
- Define a set of cryptographic security parameters which can be shared among multiple connections
- Are used to avoid the expensive negotiation of new security parameters for each connection



TLS Record Protocol



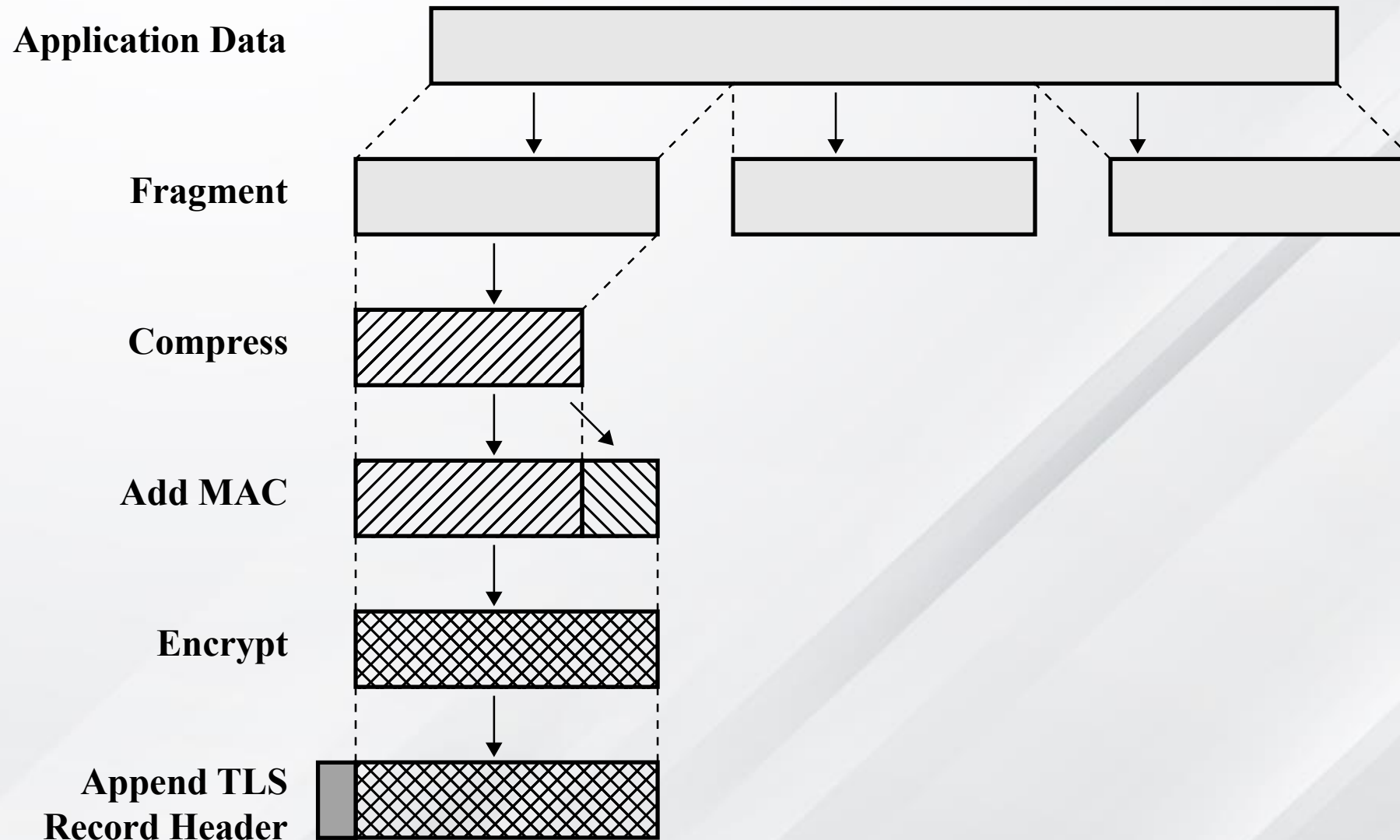


Figure 17.3 TLS Record Protocol Operation

encrypted

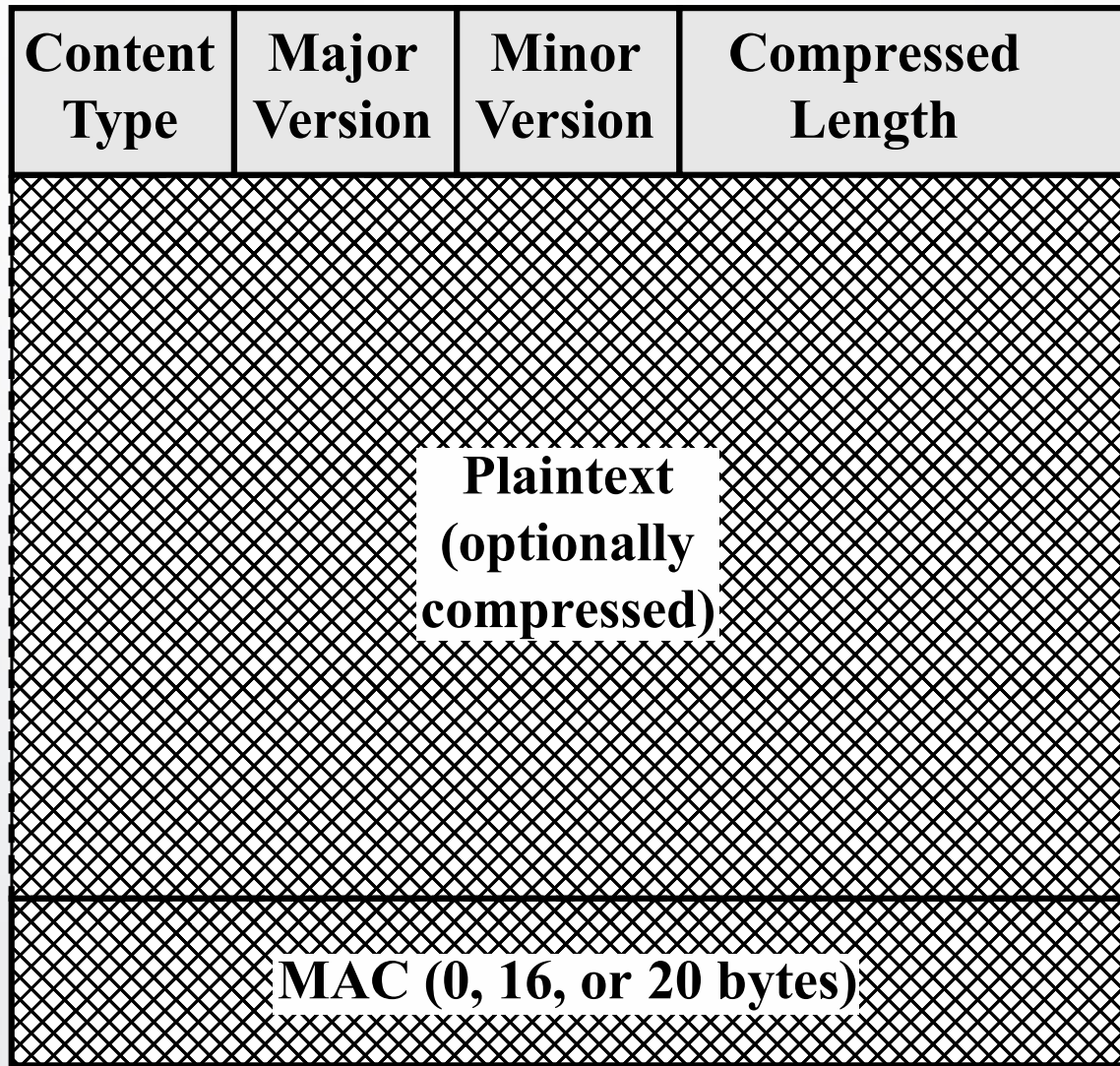


Figure 17.4 SSL Record Format

Here is a list of the Message Types in TLS:

- Change Cipher Spec (0x14)
- Alert (0x15)
- Handshake (0x16)
- Application Data (0x17)
- Heartbeat (0x18) (*Deprecated in TLS 1.2 and removed in TLS 1.3*)

Handshake Protocol Message Types:

- ClientHello (0x01)
- ServerHello (0x02)
- Certificate (0x0B)
- ServerKeyExchange (0x0C)
- CertificateRequest (0x0D)
- ServerHelloDone (0x0E)
- CertificateVerify (0x0F)
- ClientKeyExchange (0x10)
- Finished (0x14)



Table 17.2 SSL Handshake Protocol Message Types

Message Type	Parameters
hello_request	null
client_hello	version, random, session id, cipher suite, compression method
server_hello	version, random, session id, cipher suite, compression method
certificate	chain of X.509v3 certificates
server_key_exchange	parameters, signature
certificate_request	type, authorities
server_done	null
certificate_verify	signature
client_key_exchange	parameters, signature
finished	hash value



(Table is on page 522 in the textbook)

Phase 1. Establish Security Capabilities

Purpose: Initialize the connection and define security parameters for the session.

The message includes the following parameters:

1. **Version:**
 - Highest TLS version supported by the client.
2. **Random:**
 - 32-bit timestamp + 28 bytes from a secure random number generator.
 - Used as nonces to prevent replay attacks during key exchange.
3. **Session ID:**
 - **Nonzero:** Requests an update to an existing session or a new connection within the session.
 - **Zero:** Requests a new connection with a new session.
4. **CipherSuite:**
 - List of cryptographic algorithm combinations supported by the client (key exchange + CipherSpec).
 - Listed in order of preference.
5. **Compression Method:**
 - List of supported compression methods.

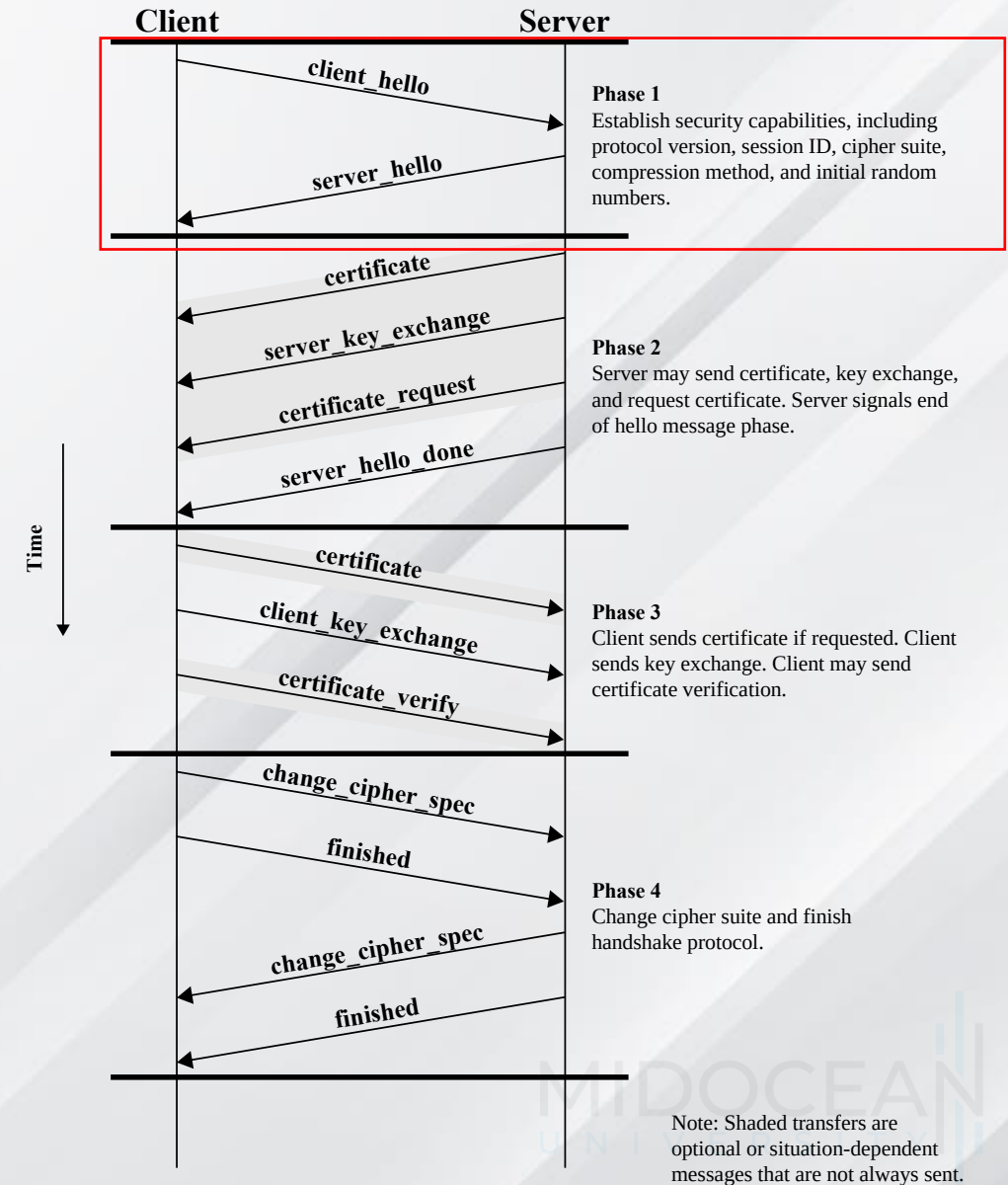


Figure 17.6 Handshake Protocol Action



Phase 2. Server Authentication and Key Exchange

Purpose: Authenticate the server and exchange key parameters.

- **Certificate**
 - Includes one or more X.509 certificates.
- **Server Key Exchange**
 - Sent when key exchange parameters are not included in the certificate.
- **Request Certificate (Optional)**
 - Sent by the server to request the client's certificate.
 - Indicates that the server requires client authentication.
- **Server Done**
 1. Indicates the end of server messages.
 2. Has no parameters.
 3. Server waits for the client's response.

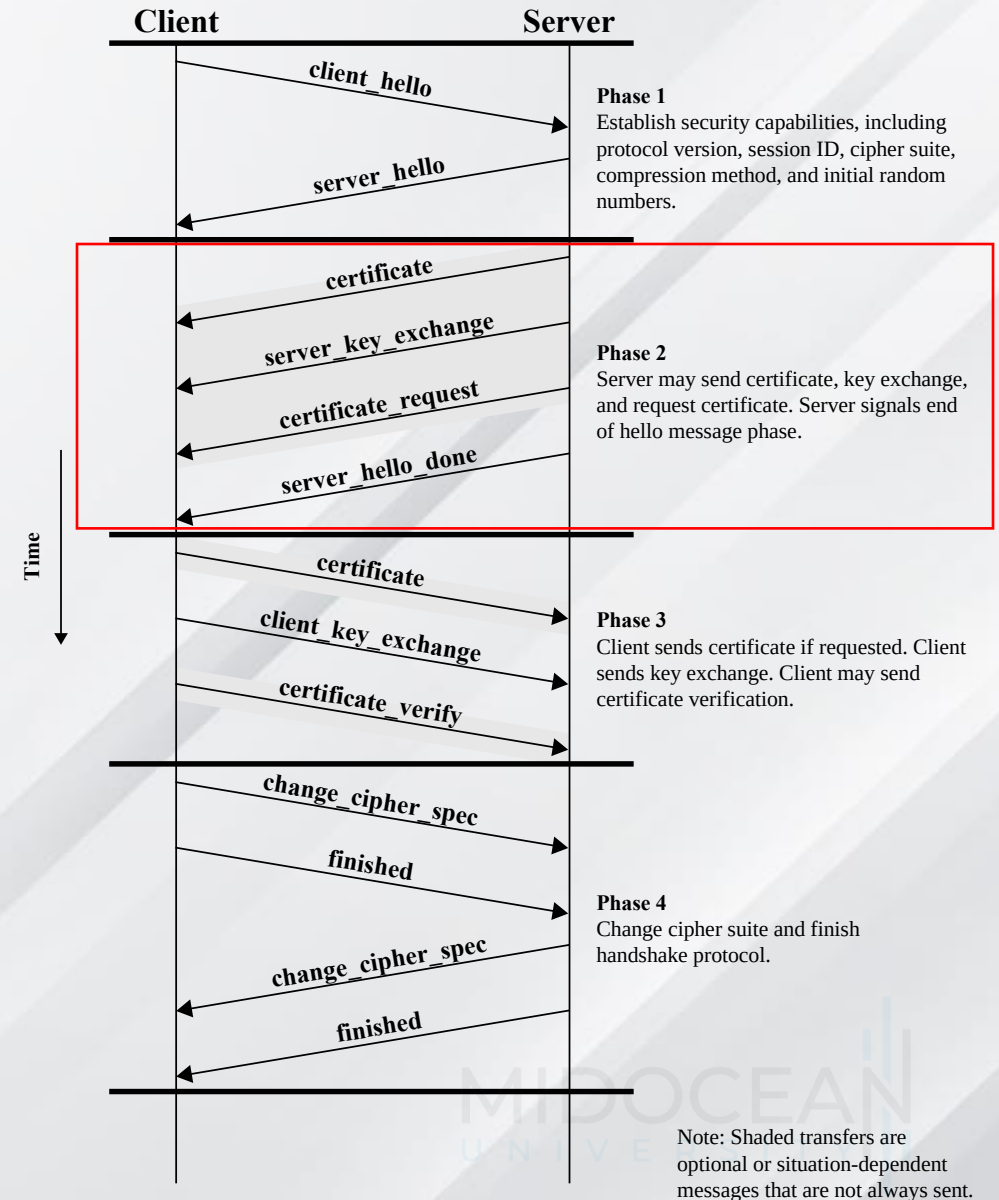


Figure 17.6 Handshake Protocol Action



Phase 3. Client Authentication and Key Exchange

Purpose: Authenticate the client (if required) and establish shared secrets for secure communication.

- **Verification by the Client**
 - Ensures the server's certificate (if provided) is valid.
 - Confirms that the server_hello parameters are acceptable.
- **Certificate Message (Optional)**
 - Sent if the server requested client authentication.
 - If no suitable certificate exists, the client sends a **no_certificate alert**.
- **Client Key Exchange (Mandatory)**
 - Content depends on the key exchange method:
 - **RSA:** Sends a 48-byte pre-master secret encrypted with the server's public key.
 - **Ephemeral/Anonymous Diffie-Hellman:** Sends the client's public Diffie-Hellman parameters.
 - **Fixed Diffie-Hellman:** No content; parameters already sent in the client's certificate.
- **Certificate Verify (Optional)**
 - Sent if the client provided a certificate with signing capability.
 - Provides explicit verification of the client's certificate.

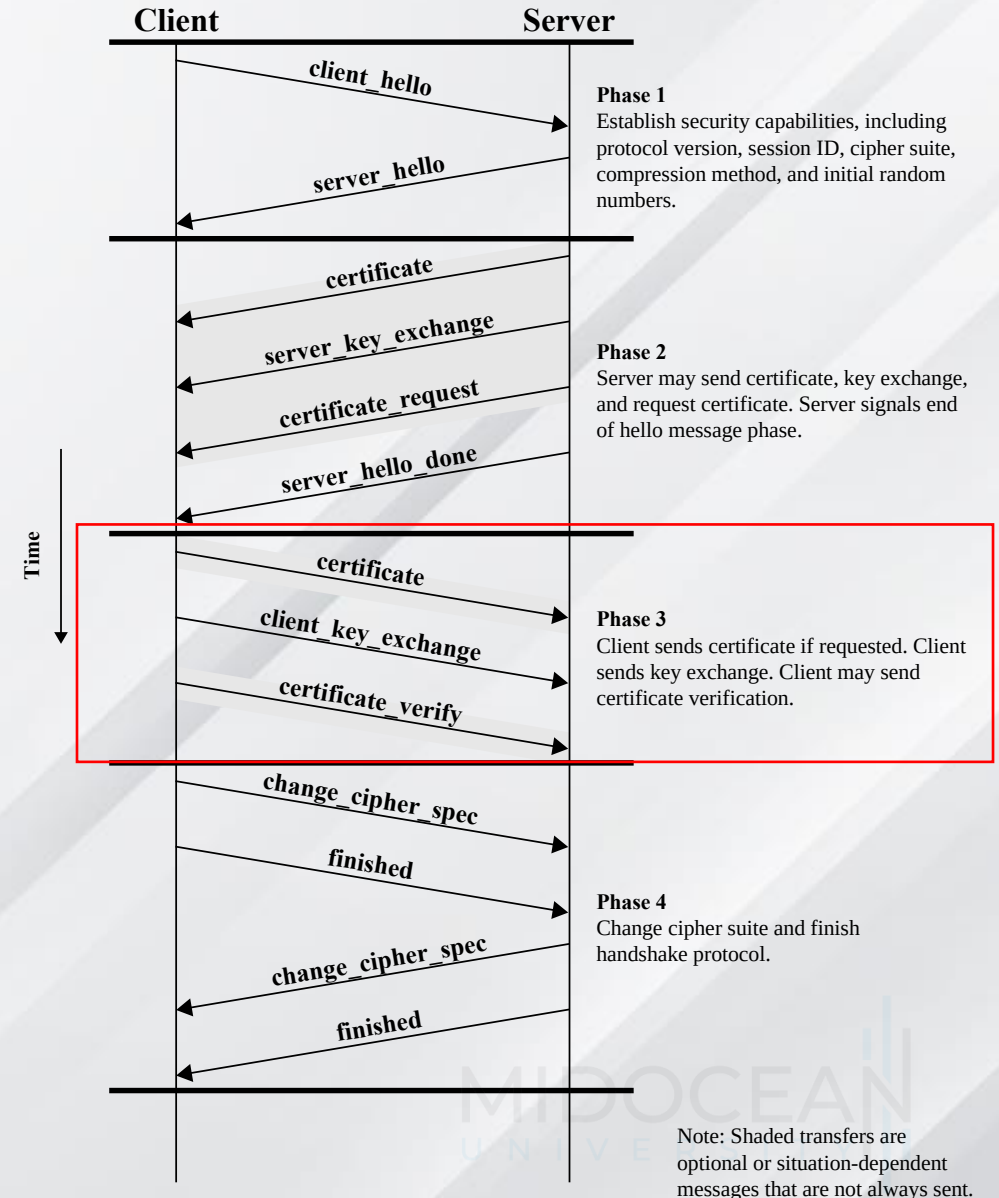


Figure 17.6 Handshake Protocol Action



Phase 4. Finish

Purpose: Finalize the secure connection and begin encrypted communication.

- **Client Actions:**
 - Sends a **change_cipher_spec** message:
 - Copies the pending CipherSpec to the current CipherSpec.
 - Uses the **Change Cipher Spec Protocol** (not part of the Handshake Protocol).
 - Sends a **finished** message:
 - First message encrypted with new algorithms, keys, and secrets.
 - Verifies the success of key exchange and authentication.
- **Server Actions:**
 - Sends its **change_cipher_spec** message:
 - Copies the pending CipherSpec to the current CipherSpec.
 - Sends its **finished** message:
 - Verifies the handshake from the server's side.

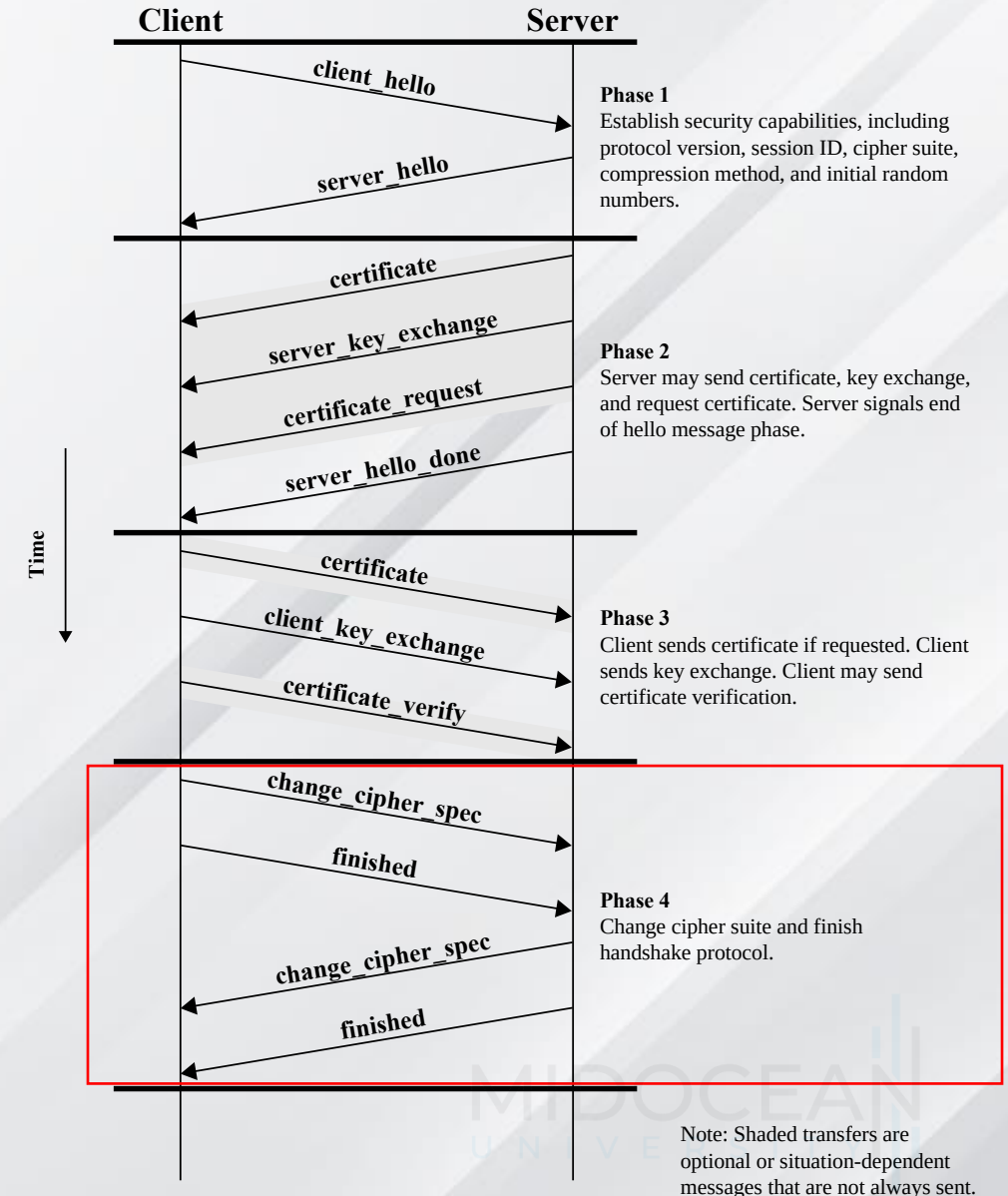


Figure 17.6 Handshake Protocol Action



Hyper Text Transfer Protocol Secure (HTTPS)

- The secure version of HTTP
- HTTPS encrypts all communications between the browser and the website
- Data sent using HTTPS provides three important areas of protection:
 - Encryption
 - Data integrity
 - Authentication



Electronic mail security



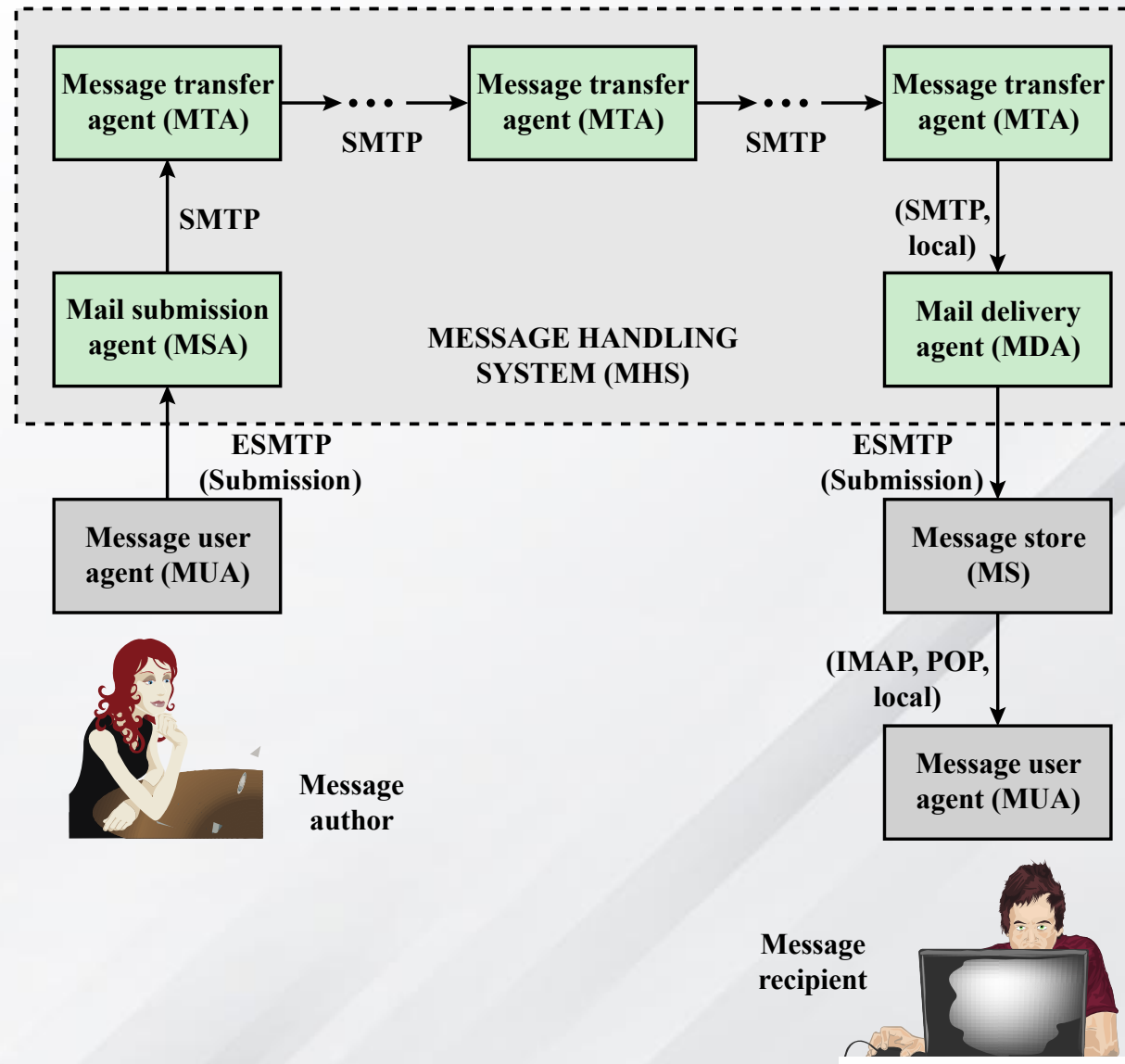


Figure 19.1 Function Modules and Standardized Protocols Used Between Them in the Internet Mail Architecture

Email Protocols

Two types of protocols are used for transferring email:

Used to send and transfer emails between mail servers.

- Simple Mail Transfer Protocol (SMTP)

Used to retrieve emails from the mail server to the client.

- IMAP and POP are the most commonly used



RFC 5322

- Defines a format for text messages that are sent using electronic mail
- Messages are viewed as having an envelope and contents
 - The envelope contains whatever information is needed to accomplish transmission and delivery
 - The contents compose the object to be delivered to the recipient
 - RFC 5322 standard applies only to the contents
- The content standard includes a set of header fields that may be used by the mail system to create the envelope



Example Message

Date: October 8, 2009 2:15:49 PM EDT

From: "William Stallings" <ws@shore.net>

Subject: The Syntax in RFC 5322

To: Smith@Other-host.com

Cc: Jones@Yet-Another-Host.com

Hello. This section begins the actual message body, which is delimited from the message heading by a blank line.



Email Security Threats

- Authenticity-related threats
 - Could result in unauthorized access to an enterprise's email system
- Integrity-related threats
 - Could result in unauthorized modification of email content
- Confidentiality-related threats
 - Could result in unauthorized disclosure of sensitive information
- Availability-related threats
 - Could prevent end users from being able to send or receive mail

Threat	Impact on Purported Sender	Impact on Receiver	Mitigation
Email sent by unauthorized MTA in enterprise (e.g. malware botnet)	Loss of reputation, valid email from enterprise may be blocked as possible spam/phishing attack.	UBE and/or email containing malicious links may be delivered into user inboxes	Deployment of domain-based authentication techniques. Use of digital signatures over email.
Email message sent using spoofed or unregistered sending domain	Loss of reputation, valid email from enterprise may be blocked as possible spam/phishing attack.	UBE and/or email containing malicious links may be delivered into user inboxes	Deployment of domain-based authentication techniques. Use of digital signatures over email.
Email message sent using forged sending address or email address (i.e. phishing, spear phishing)	Loss of reputation, valid email from enterprise may be blocked as possible spam/phishing attack.	UBE and/or email containing malicious links may be delivered. Users may inadvertently divulge sensitive information or PII.	Deployment of domain-based authentication techniques. Use of digital signatures over email.

Table 19.3
Email Threats and Mitigations

Threat	Impact on Purported Sender	Impact on Receiver	Mitigation
Email modified in transit	Leak of sensitive information or Personally Identifiable Information (PII).	Leak of sensitive information, altered message may contain malicious information	Use of TLS to encrypt email transfer between server. Use of end-to-end email encryption.
Disclosure of sensitive information (e.g. PII) via monitoring and capturing of email traffic	Leak of sensitive information or PII.	Leak of sensitive information, altered message may contain malicious information	Use of TLS to encrypt email transfer between server. Use of end-to-end email encryption.
Unsolicited Bulk Email (UBE) (i.e. spam)	None, unless purported sender is spoofed.	UBE and/or email containing malicious links may be delivered into user inboxes	Techniques to address UBE.
DoS/DDoS attack against an enterprises' email servers	Inability to send email.	Inability to receive email.	Multiple mail servers, use of cloud-based email providers.

Table 19.3
Email Threats and Mitigations

Counter Threat Protocols

- SP800-177 recommends use of a variety of standardized protocols as a means for countering threats:
 - STARTTLS
 - An SMTP security extension that provides authentication, integrity, non-repudiation and confidentiality for the entire SMTP message by running SMTP over TLS
 - S/MIME
 - Provides authentication, integrity, non-repudiation and confidentiality of the message body carried in SMTP messages
 - DNS Security Extensions (DNSSEC)
 - Provides authentication and integrity protection of DNS data, and is an underlying tool used by various email security protocols
 - DNS-based Authentication of Named Entities (DANE)
 - Is designed to overcome problems in the certificate authority (CA) system by providing an alternative channel for authenticating public keys based on DNSSEC, with the result that the same trust relationships used to certify IP addresses are used to certify servers operating on those addresses



IP Security

Dr. Ayman Khallel



IP Security Overview

- RFC 1636
 - “Security in the Internet Architecture”
 - Issued in 1994 by the Internet Architecture Board (IAB)
 - Identifies key areas for security mechanisms
 - Need to secure the network infrastructure from unauthorized monitoring and control of network traffic
 - Need to secure end-user-to-end-user traffic using authentication and encryption mechanisms
 - IAB included authentication and encryption as necessary security features in the next generation IP (IPv6)
 - The IPsec specification now exists as a set of Internet standards

Applications of IPsec

- **Secure Branch Office Connectivity**
 - Build secure Virtual Private Networks (VPNs) over the Internet or public WAN.
 - Reduces reliance on private networks, saving costs and network management overhead.
- **Secure Remote Access**
 - End users with IPsec-equipped systems can access company networks securely over the Internet.
 - Reduces toll charges for traveling employees and telecommuters.
- **Extranet and Intranet Connectivity**
 - Secures communication with partners, ensuring authentication and confidentiality.
 - Provides key exchange mechanisms.
- **Enhanced E-commerce Security**
 - IPsec complements built-in security protocols of Web and e-commerce applications.
 - Adds an additional layer of encryption and authentication to network traffic.



Benefits of IPsec

- **Strong Perimeter Security**

- IPsec in firewalls or routers provides robust security for all traffic crossing the network perimeter.
- Traffic within the company or workgroup remains unaffected by security overhead.

- **Firewall Resistance to Bypass**

- If all external traffic must use IP and the firewall is the only point of entry from the Internet, IPsec ensures strong protection against bypass.

- **Transparency to Applications**

- IPsec operates below the transport layer (TCP, UDP), making it transparent to applications.
- No need for changes to software on user or server systems when IPsec is implemented in a firewall or router.

- **Minimal User Involvement**

- IPsec can be transparent to end users: no need for training, issuing keying material, or revoking keys when users leave the organization.

- **Security for Individual Users**

- Can provide security for offsite workers or create a secure virtual subnetwork within the organization for sensitive applications.

IPsec Services

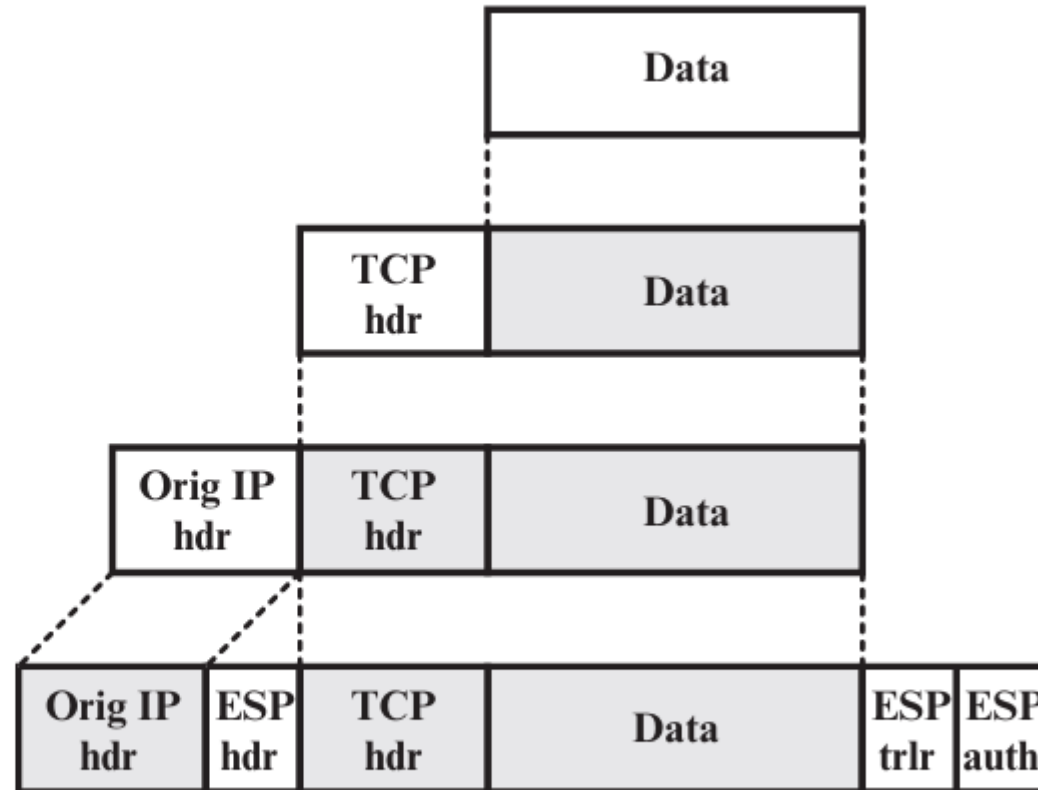
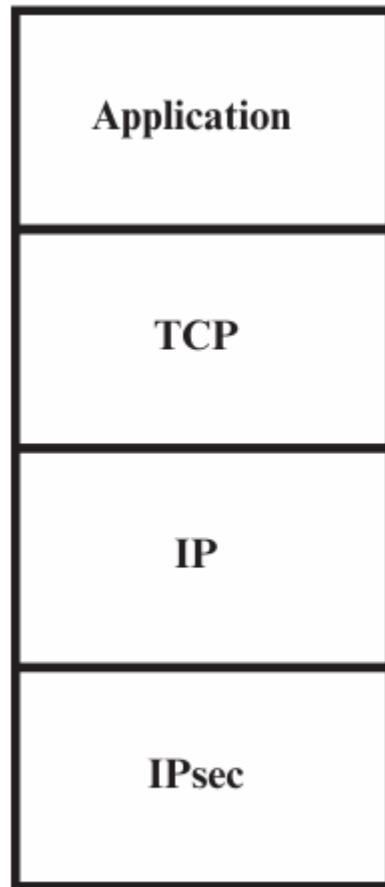
- IPsec provides security services at the IP layer by enabling a system to:
 - Select required security protocols
 - Determine the algorithm(s) to use for the service(s)
 - Put in place any cryptographic keys required to provide the requested services
- RFC 4301 lists the following services:
 - Access control
 - Connectionless integrity
 - Data origin authentication
 - Rejection of replayed packets (a form of partial sequence integrity)
 - Confidentiality (encryption)
 - Limited traffic flow confidentiality

Transport Mode

- **Protection Level:** Protects only the **payload** of an IP packet (upper-layer protocols).
- **Examples:** TCP/UDP segments, ICMP packets.
- **Operation:**
 - **IPv4:** Protects the data following the IP header.
 - **IPv6:** Protects the data following both the IP header and any extension headers (except destination options header).
- **Security:**
 - **ESP in Transport Mode:** Encrypts and optionally authenticates the IP payload but not the IP header.
 - **AH in Transport Mode:** Authenticates the IP payload and selected portions of the IP header.
- **Use Case:** Ideal for **end-to-end communication** between hosts (e.g., client-server or workstation-to-workstation).



Transport Mode



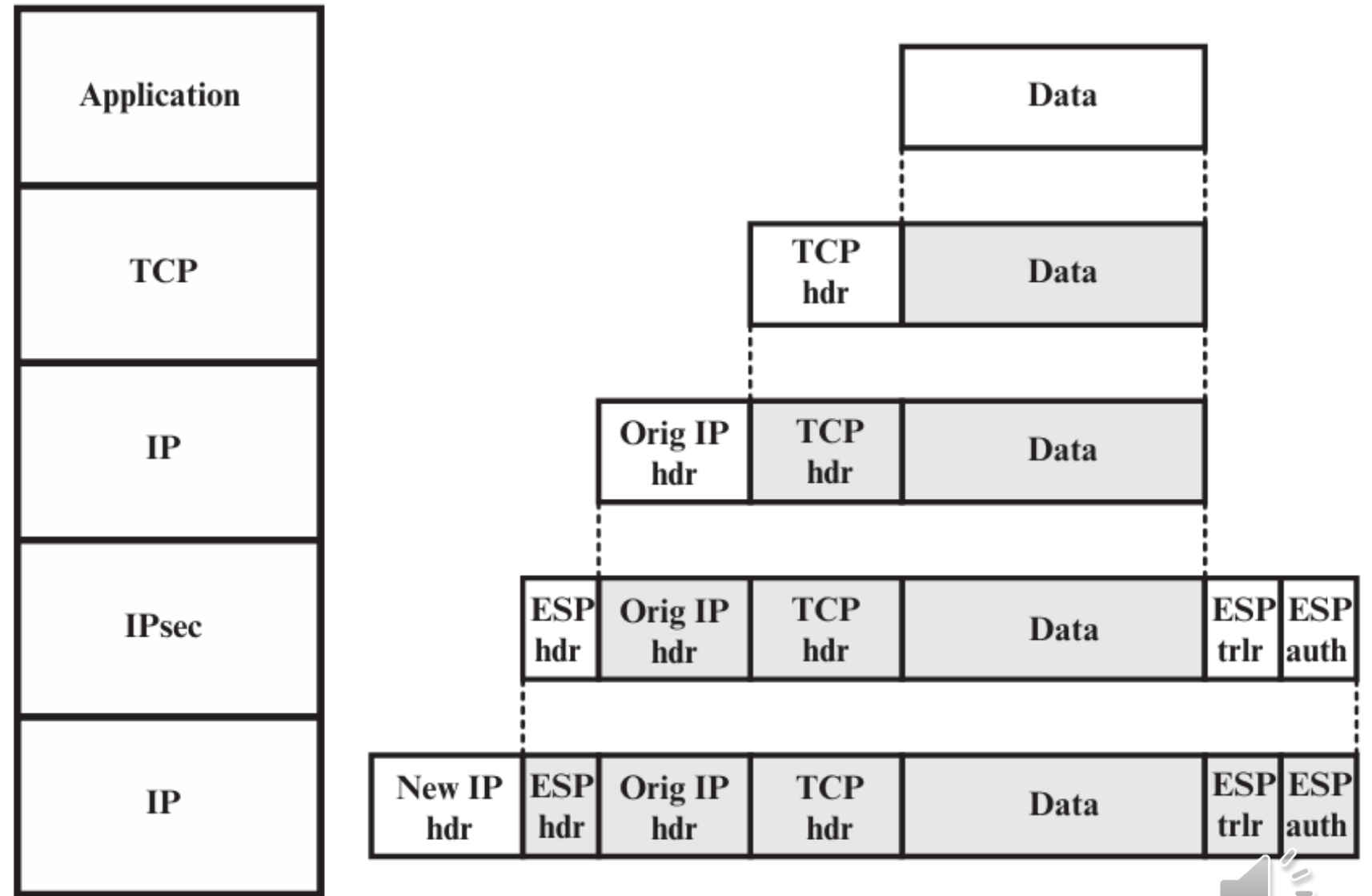
(a) Transport mode



Tunnel Mode

- **Protection Level:** Protects **the entire IP packet**.
- **Operation:**
 - After adding AH or ESP fields, the entire packet (including new security fields) becomes the payload of a **new outer IP packet** with a new IP header.
 - The original packet is encapsulated, and the new outer packet is routed across the network.
 - Intermediate routers can only inspect the outer IP header, providing added security.
- **Use Case:**
 - Used when one or both ends of the security association (SA) are **security gateways** (e.g., firewalls, routers).
 - Enables secure communication between **multiple hosts behind firewalls** without needing to implement IPsec on each host.

Tunnel Mode



(b) Tunnel mode

Summary

- **Web Security Considerations**

- **Threats:** Complex software, untrained users, and exploitable servers.
- **Solution:** **TLS/HTTPS** ensures encryption, integrity, and authentication.

- **Email Security**

- **Threats:** Authenticity, integrity, confidentiality, and availability issues.
- **Solutions:** STARTTLS, S/MIME, DNSSEC, and DANE secure email communication.

- **IPsec Security**

- **Applications:** VPNs, remote access, secure communications, e-commerce.
- **Modes:**
 - **Transport:** End-to-end payload protection.
 - **Tunnel:** Full packet protection via gateways.





Thank You

