Internet Security Protocols and Standards

Bojan Božić

By: William Stallings and Lawrie Brown

MIME and S/MIME

MIME

- Extension to the old RFC 822 specification of an Internet mail format
  - RFC 822 defines a simple heading with To, From, Subject
  - Assumes ASCII text format
- Provides a number of new header fields that define information about the body of the message

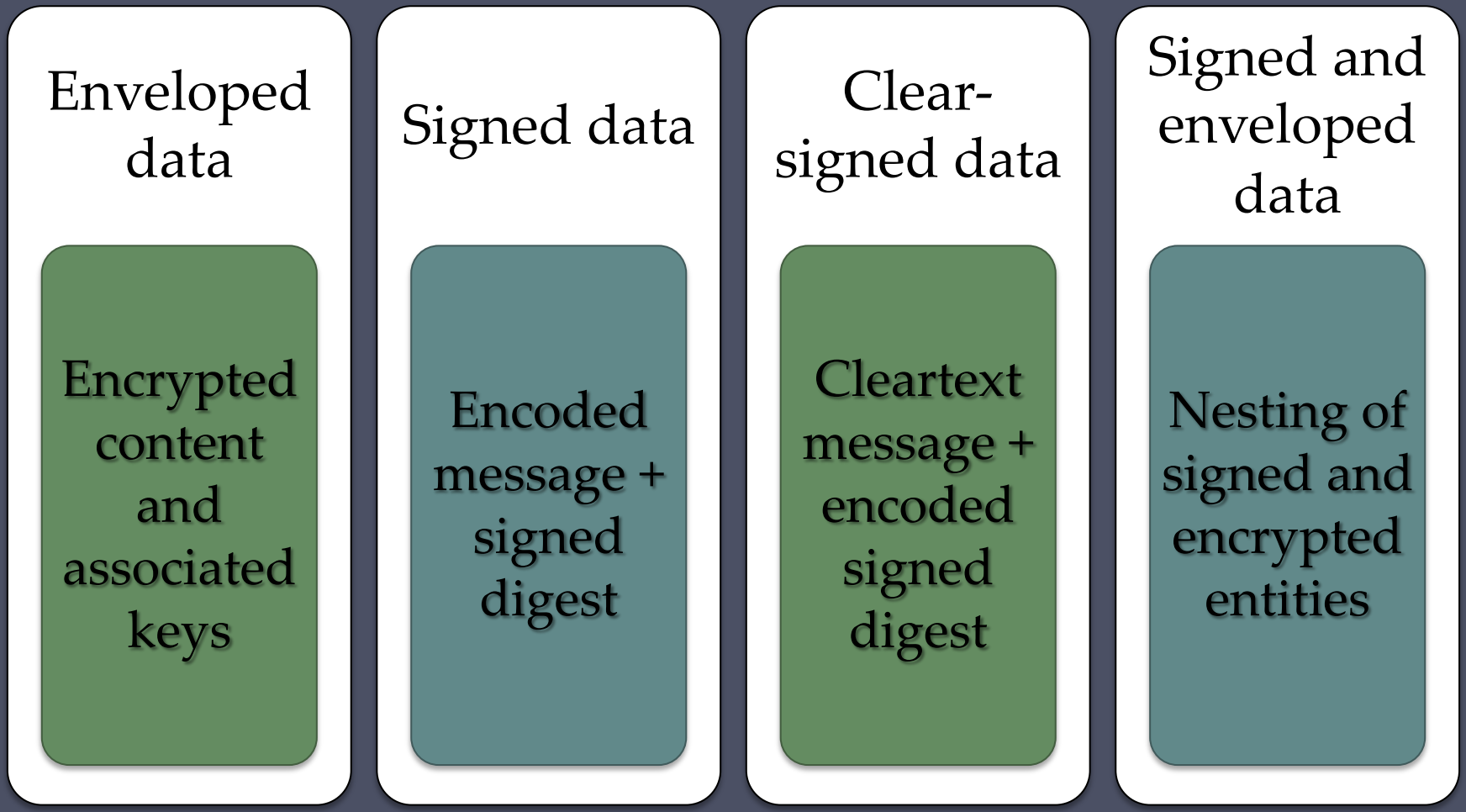
S/MIME

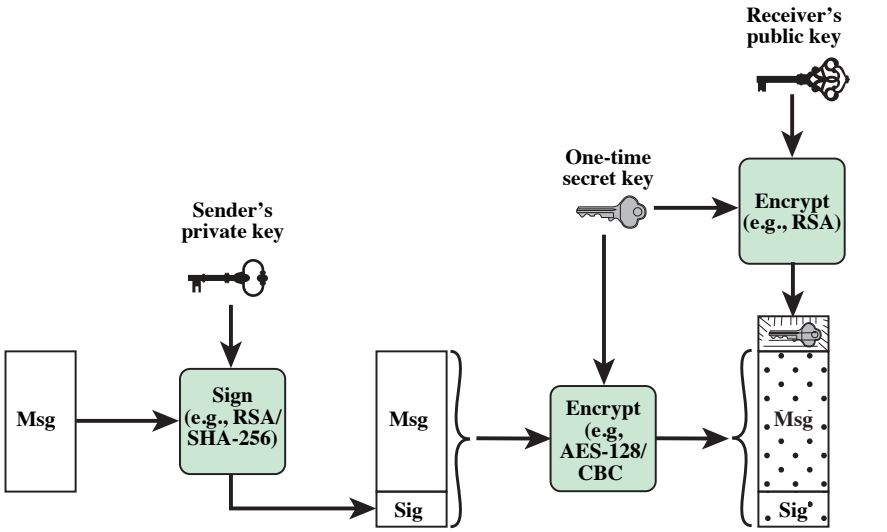
- Secure/Multipurpose Internet Mail Extension
- Security enhancement to the MIME Internet e-mail format
  - Based on technology from RSA Data Security
- Provides the ability to sign and/or encrypt e-mail messages

Table 22.1
S/MIME Content Types

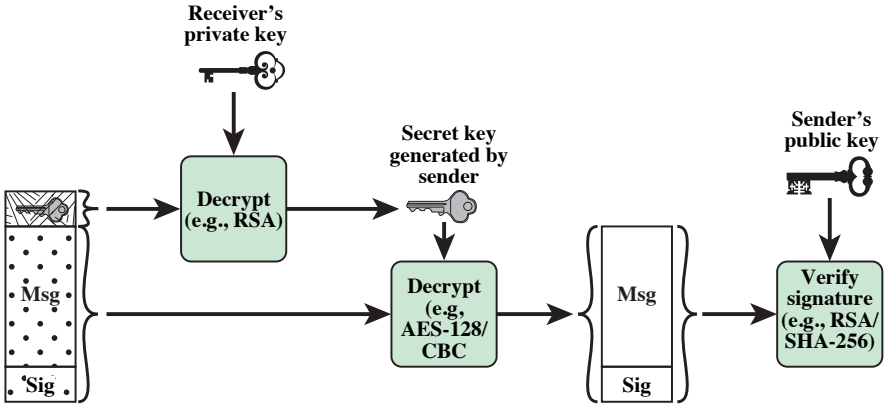
Type	Subtype	smime Parameter	Description
Multipart	Signed		A clear-signed message in two parts: one is the message and the other is the signature.
Application	pkcs7-mime	signedData	A signed S/MIME entity.
	pkcs7-mime	envelopedData	An encrypted S/MIME entity.
	pkcs7-mime	degenerate signedData	An entity containing only public-key certificates.
	pkcs7-mime	CompressedData	A compressed S/MIME entity.
	pkcs7-signature	signedData	The content type of the signature subpart of a multipart/signed message.

S/MIME Functions





(a) Sender signs, then encrypts message



(b) Receiver decrypts message, then verifies sender's signature

Figure 22.1 Simplified S/MIME Functional Flow

Signed and Clear-Signed Data

- The preferred algorithms used for signing S/MIME messages use either an RSA or a DSA signature of a SHA-256 message hash
- The process works as follows:
  - Take the message you want to send and map it into a fixed-length code of 256 bits using SHA-256
  - The 256-bit message digest is unique for this message making it virtually impossible for someone to alter this message or substitute another message and still come up with the same digest
  - S/MIME encrypts the digest using RSA and the sender's private RSA key
  - The result is the digital signature, which is attached to the message
  - Now, anyone who gets the message can recompute the message digest then decrypt the signature using RSA and the sender's public RSA key
  - Since this operation only involves encrypting and decrypting a 256-bit block, it takes up little time

Enveloped Data

- Default algorithms used for encrypting S/MIME messages are AES and RSA
  - S/MIME generates a pseudorandom secret key that is used to encrypt the message using AES or some other conventional encryption scheme
  - A new pseudorandom key is generated for each new message encryption
  - This session key is bound to the message and transmitted with it
  - The secret key is used as input to the public-key encryption algorithm, RSA, which encrypts the key with the recipient's public RSA key
  - On the receiving end, S/MIME uses the receiver's private RSA key to recover the secret key, then uses the secret key and AES to recover the plaintext message
  - If encryption is used alone, radix-64 is used to convert the ciphertext to ASCII format

DomainKeys Identified Mail (DKIM)

- Specification of cryptographically signing e-mail messages permitting a signing domain to claim responsibility for a message in the mail stream
- Proposed Internet Standard (RFC 4871: *DomainKeys Identified Mail (DKIM) Signatures)*
- Has been widely adopted by a range of e-mail providers

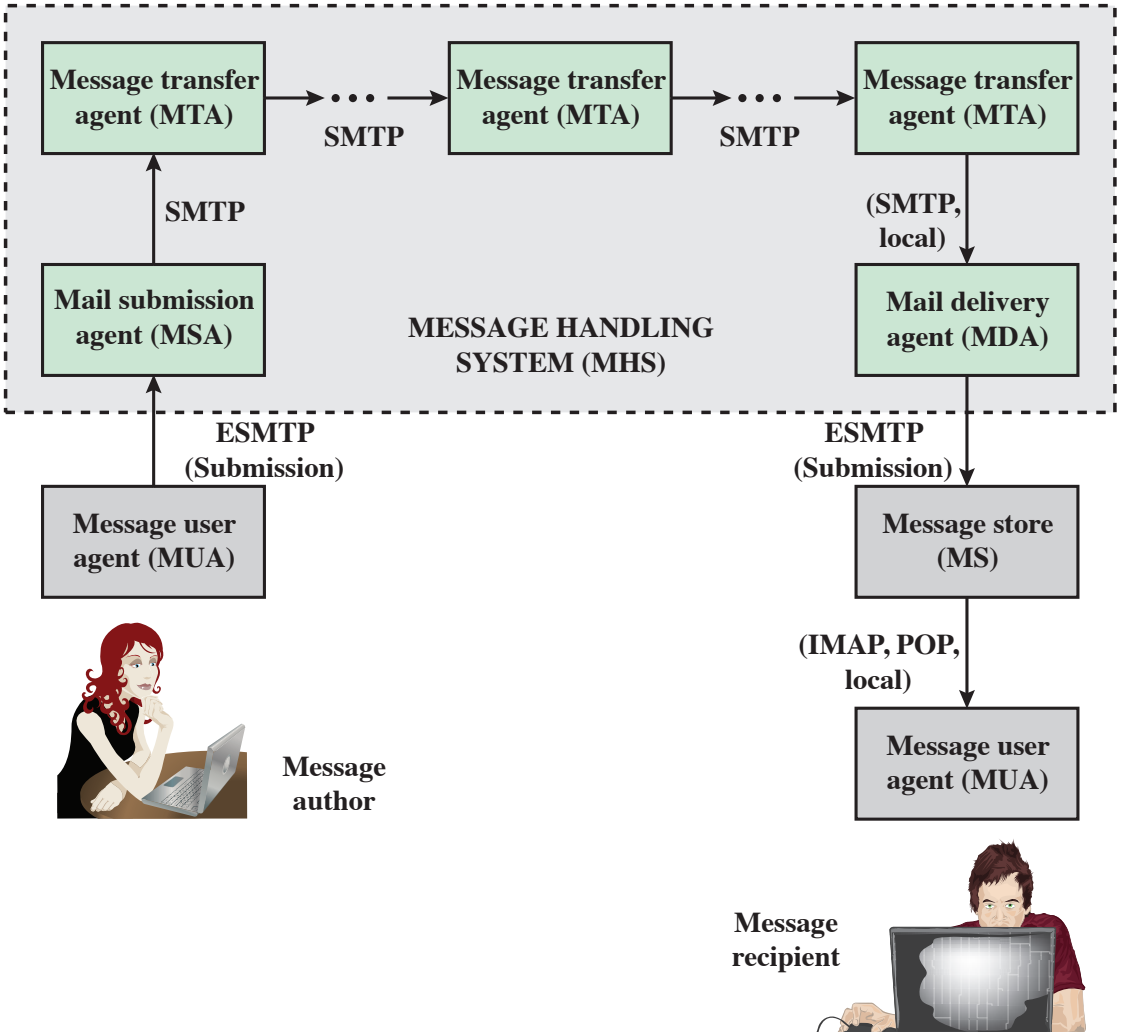
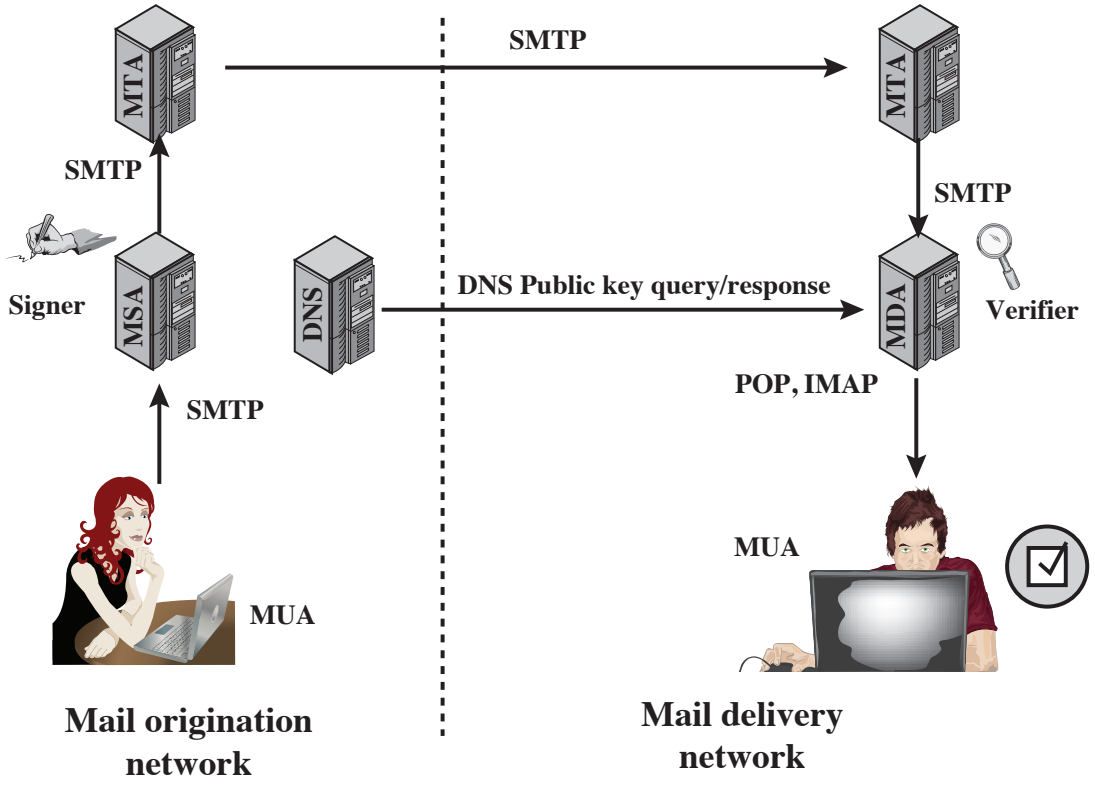


Figure 22.2 Function Modules and Standardized Protocols Used Between Them in the Internet Mail Architecture

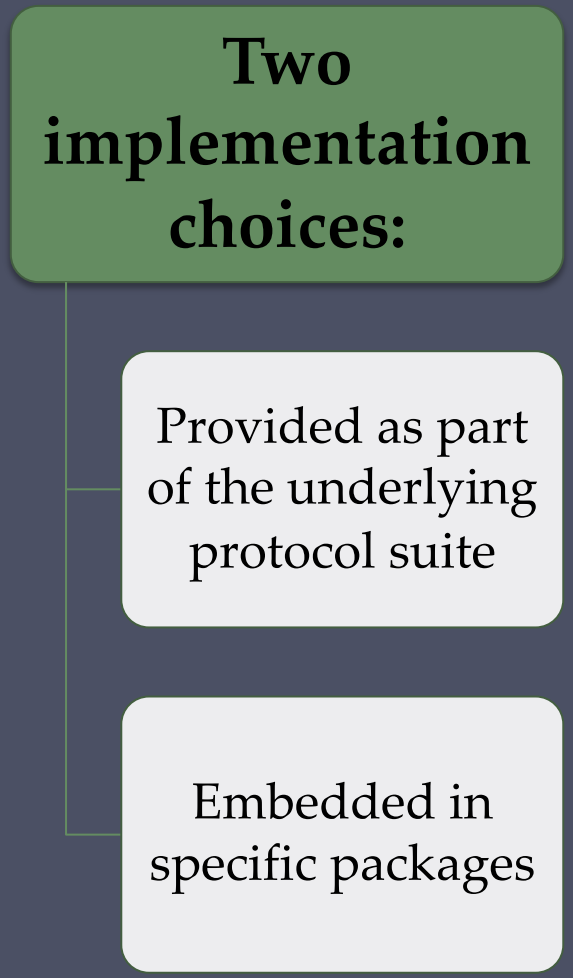


DNS = domain name system
MDA = mail delivery agent
MSA = mail submission agent
MTA = message transfer agent
MUA = message user agent

Figure 22.3 Simple Example of DKIM Deployment

Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

- One of the most widely used security services
- General-purpose service implemented as a set of protocols that rely on TCP
- Subsequently became Internet standard RFC4346: Transport Layer Security (TLS)



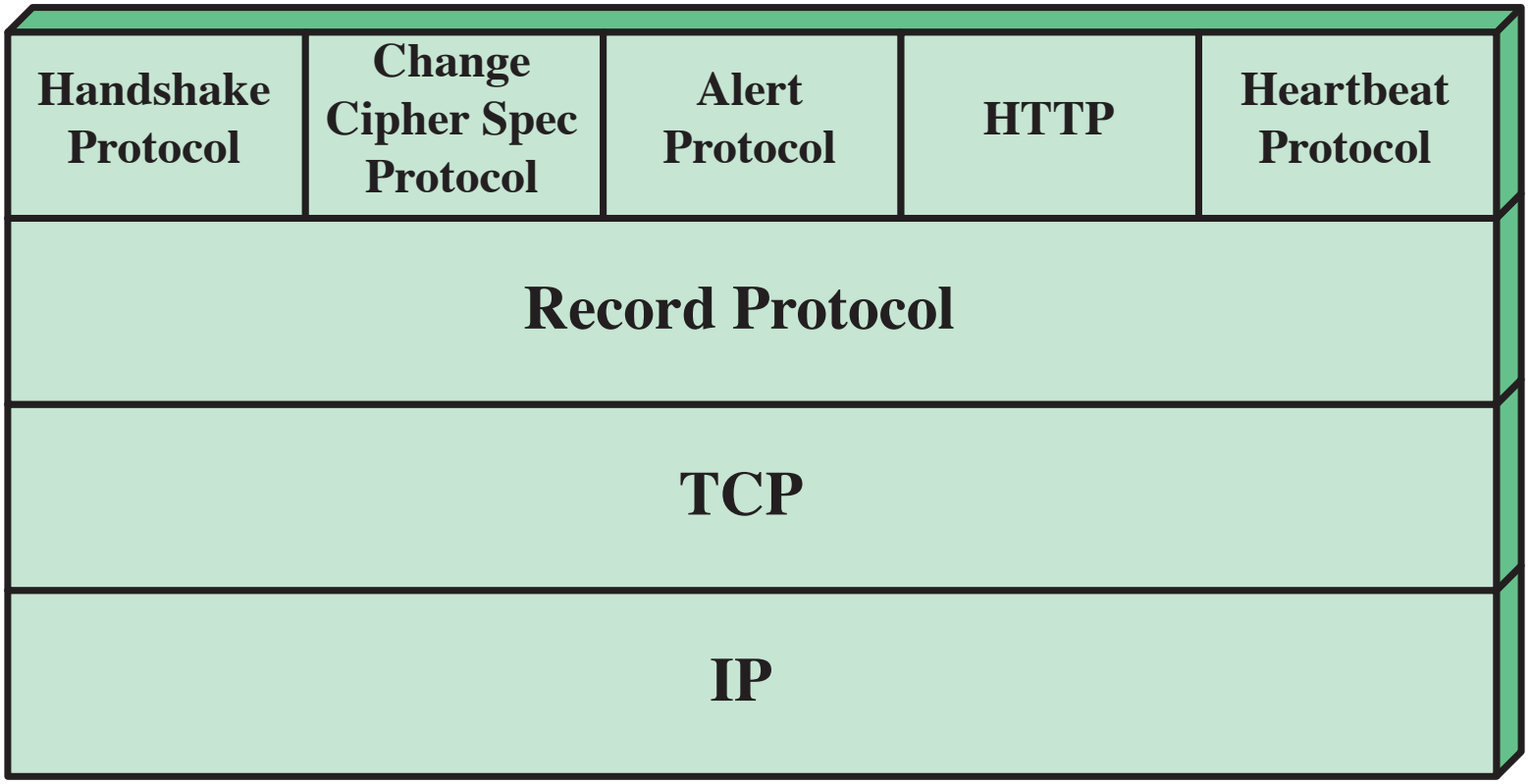


Figure 22.4 SSL/TLS Protocol Stack

TLS Concepts

TLS Session

- An association between a client and a server
- Created by the Handshake Protocol
- Define a set of cryptographic security parameters
- Used to avoid the expensive negotiation of new security parameters for each connection

TLS Connection

- A transport (in the OSI layering model definition) that provides a suitable type of service
- Peer-to-peer relationships
- Transient
- Every connection is associated with one session

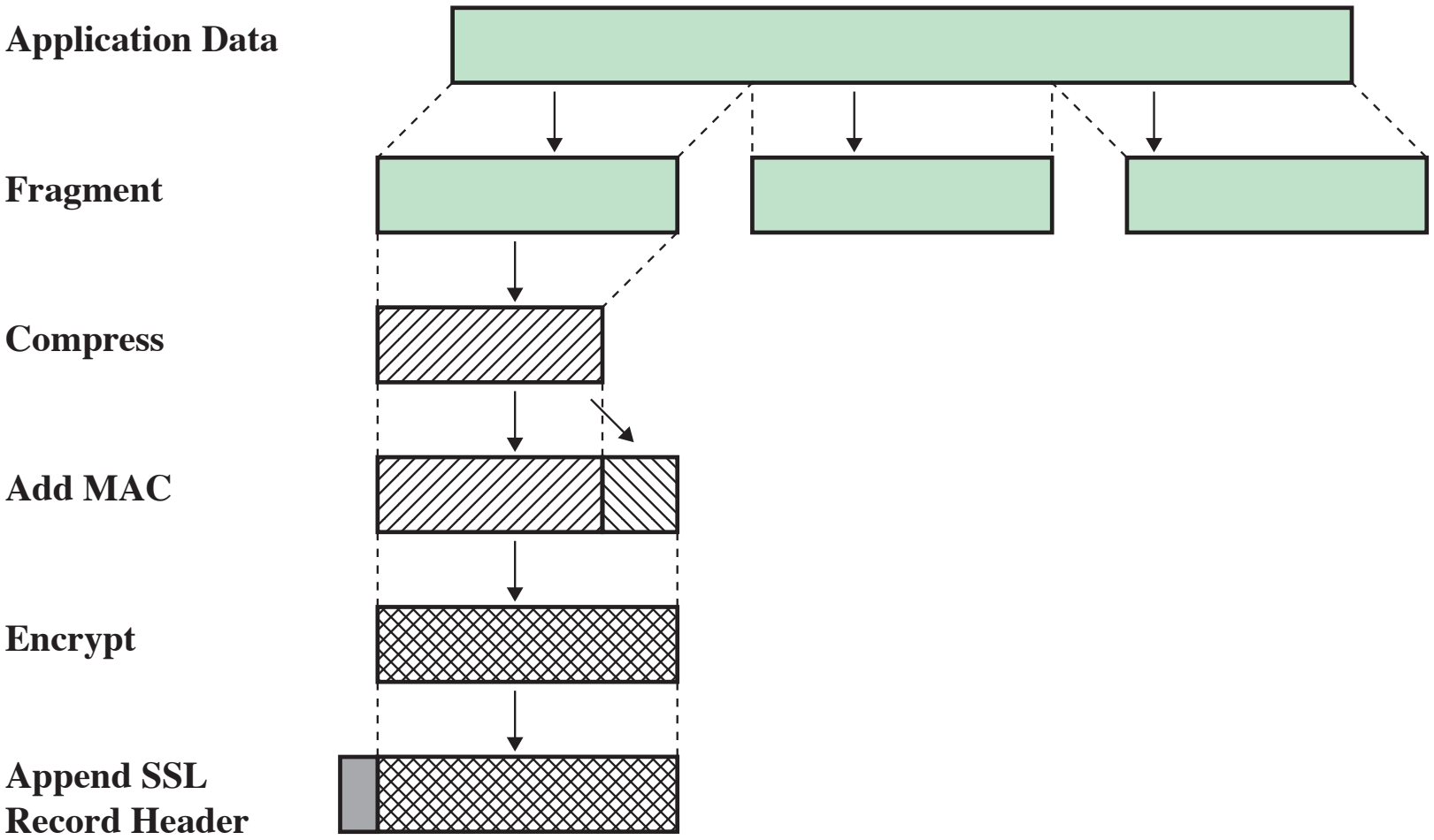
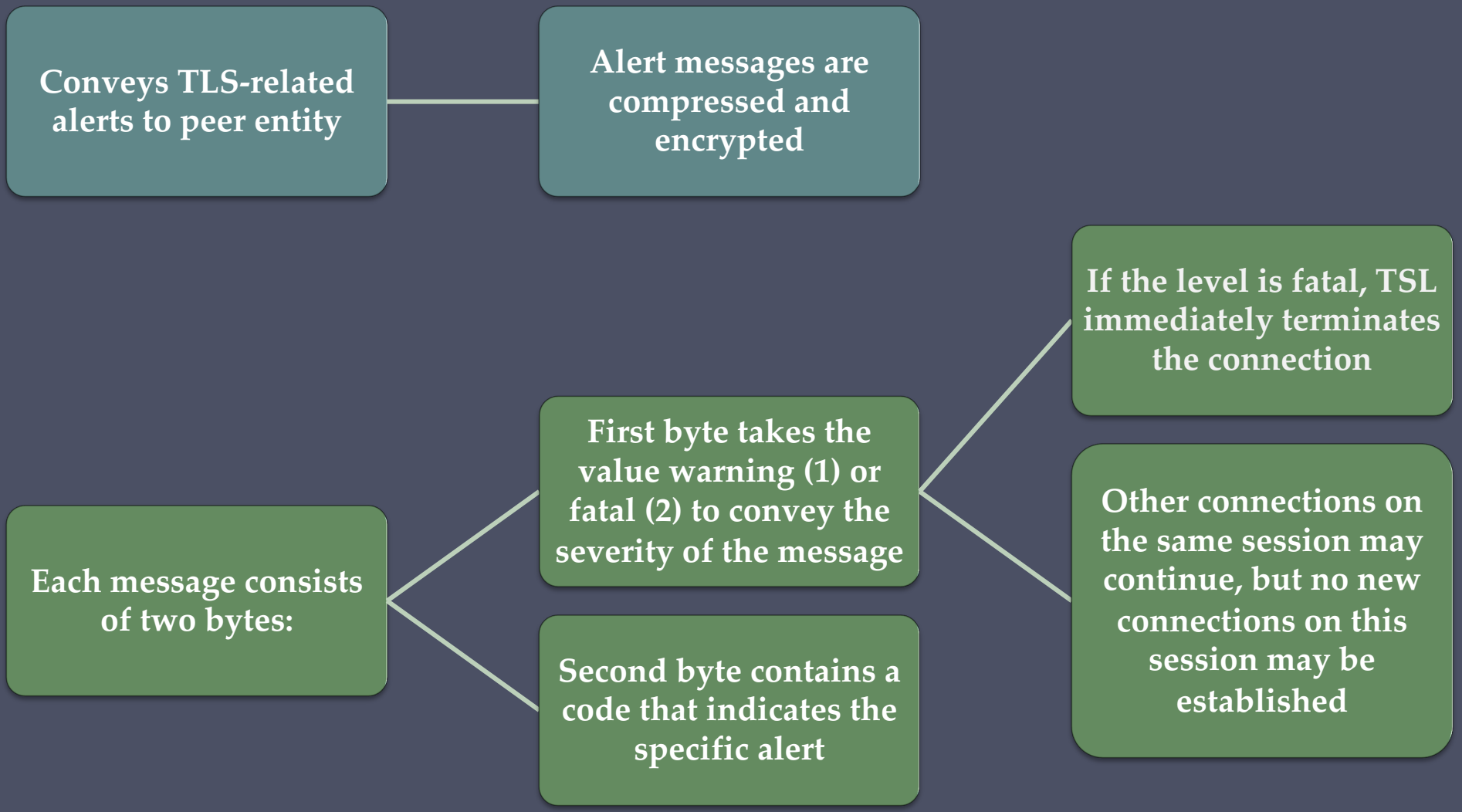


Figure 22.5 TLS Record Protocol Operation

Change Cipher Spec Protocol

- One of four TLS specific protocols that use the TLS Record Protocol
- Is the simplest
- Consists of a single message which consists of a single byte with the value 1
- Sole purpose of this message is to cause pending state to be copied into the current state
- Hence updating the cipher suite in use

Alert Protocol



Handshake Protocol

- Most complex part of TLS
- Is used before any application data are transmitted
- Allows server and client to:

- Comprises a series of messages exchanged by client and server
- Exchange has four phases

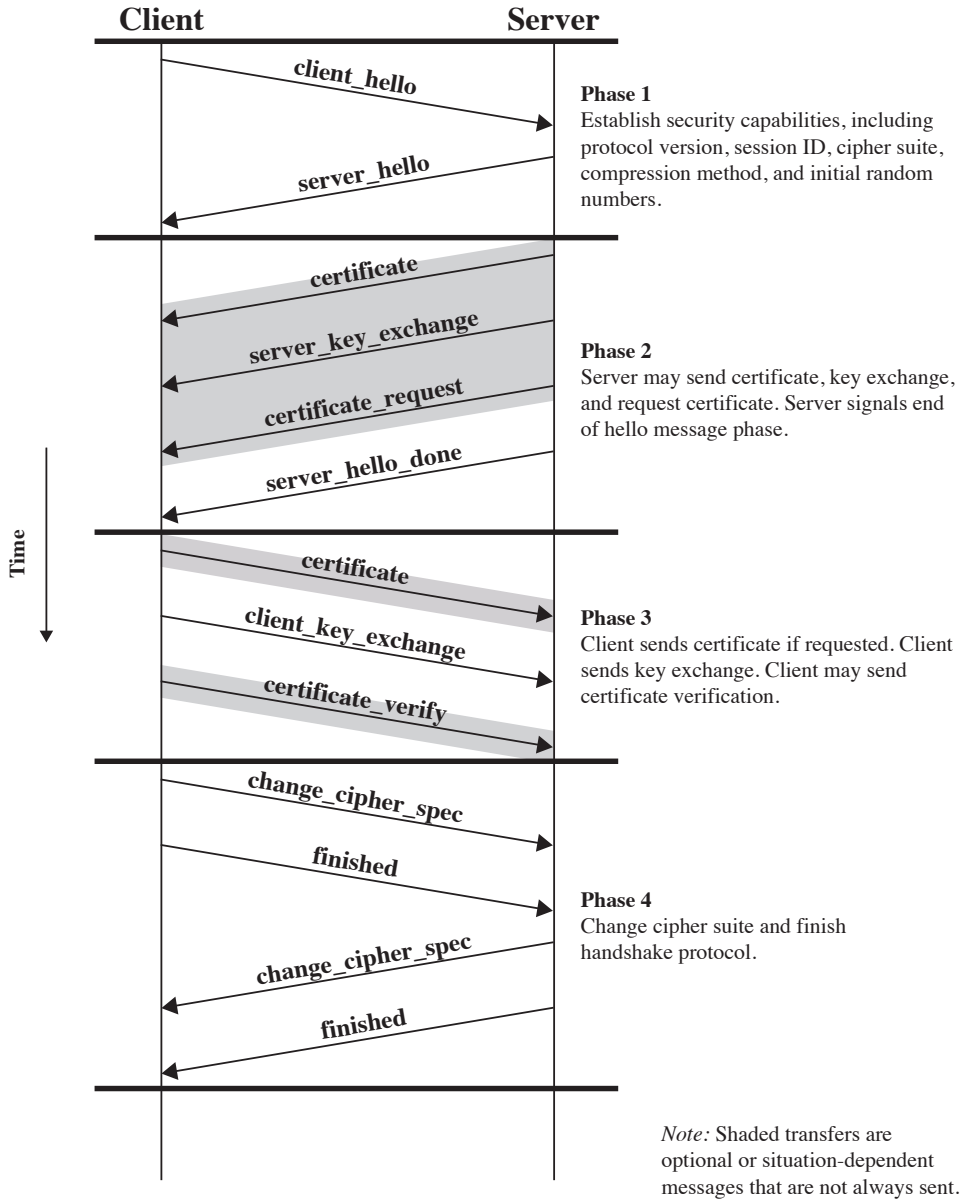
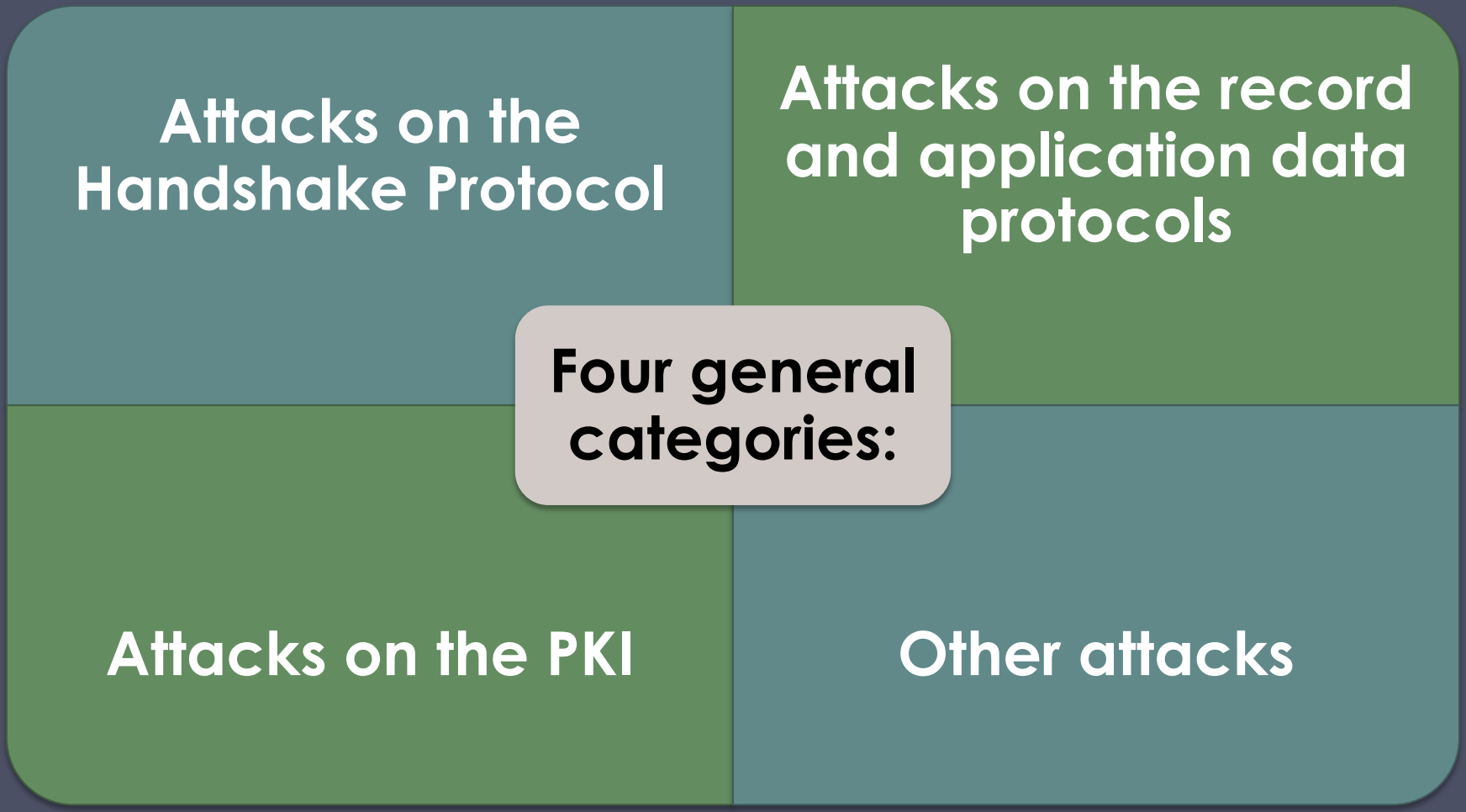


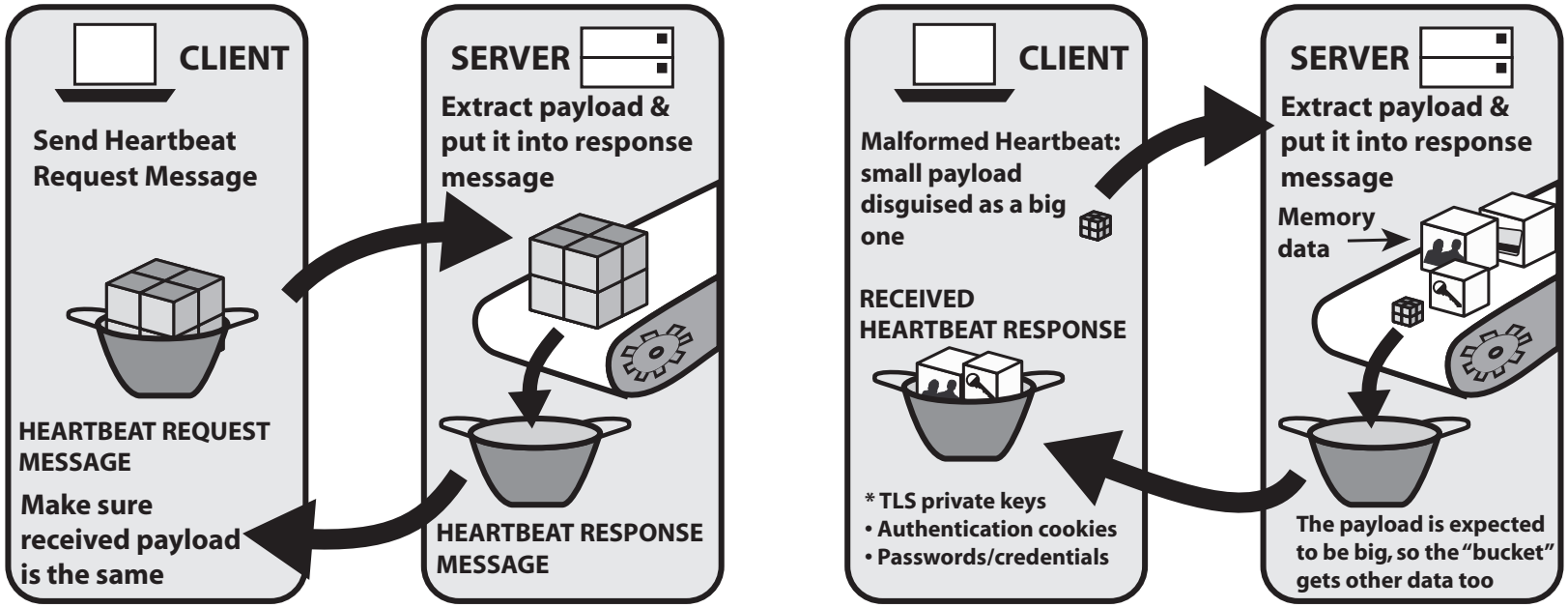
Figure 22.6 Handshake Protocol Action

Heartbeat Protocol

- A periodic signal generated by hardware or software to indicate normal operation or to synchronize other parts of a system
- Typically used to monitor the availability of a protocol entity
- Defined in 2012 in RFC 6250
- Runs on top of the TLS Record Protocol
- Use is established during Phase 1 of the Handshake Protocol
- Each peer indicates whether it supports heartbeats
- Serves two purposes:
  - Assures the sender that the recipient is still alive
  - Generates activity across the connection during idle periods

SSL/TLS Attacks





(a) How TLS Heartbeat Protocol works

(b) How TLS Heartbleed exploit works

Figure 22.7 The Heartbleed Exploit

Source: BAE Systems

HTTPS (HTTP over SSL)

- Combination of HTTP and SSL to implement secure communication between a Web browser and a Web server
- Built into all modern Web browsers
  - Search engines do not support HTTPS
  - URL addresses begin with https://
- Documented in RFC 2818, HTTP Over TLS
- Agent acting as the HTTP client also acts as the TLS client
- Closure of an HTTPS connection requires that TLS close the connection with the peer TLS entity on the remote side, which will involve closing the underlying TCP connection

IP Security (IPsec)

- Various application security mechanisms
  - S/MIME, Kerberos, SSL/HTTPS
- Security concerns cross protocol layers
- Would like security implemented by the network for all applications
- Authentication and encryption security features included in next-generation IPv6
- Also usable in existing IPv4

Benefits of IPsec

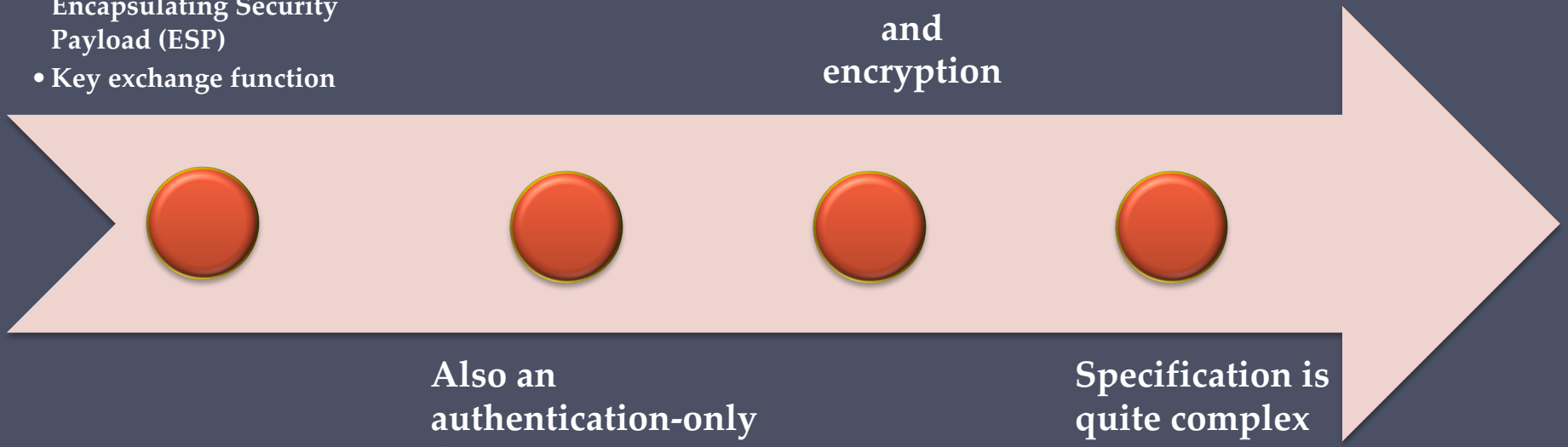
- When implemented in a firewall or router, it provides strong security to all traffic crossing the perimeter
- In a firewall it is resistant to bypass
- Below transport layer, hence transparent to applications
- Can be transparent to end users
- Can provide security for individual users
- Secures routing architecture

The Scope of IPsec

Provides two main functions:

- A combined authentication/encryption function called Encapsulating Security Payload (ESP)
- Key exchange function

VPNs want both authentication and encryption



Also an authentication-only function, implemented using an Authentication Header (AH)

- Because message authentication is provided by ESP, the use of AH is included in IPsecv3 for backward compatibility but should not be used in new applications

Specification is quite complex

- Numerous RFC's 2401/4302/ 4303/4306

Security Associations

- A one-way relationship between sender and receiver that affords security for traffic flow
  - If a peer relationship is needed for two-way secure exchange then two security associations are required
- Is uniquely identified by the Destination Address in the IPv4 or IPv6 header and the SPI in the enclosed extension header (AH or ESP)

Defined by 3 parameters:

- Security Parameter Index (SPI)
- IP Destination Address
- Protocol Identifier

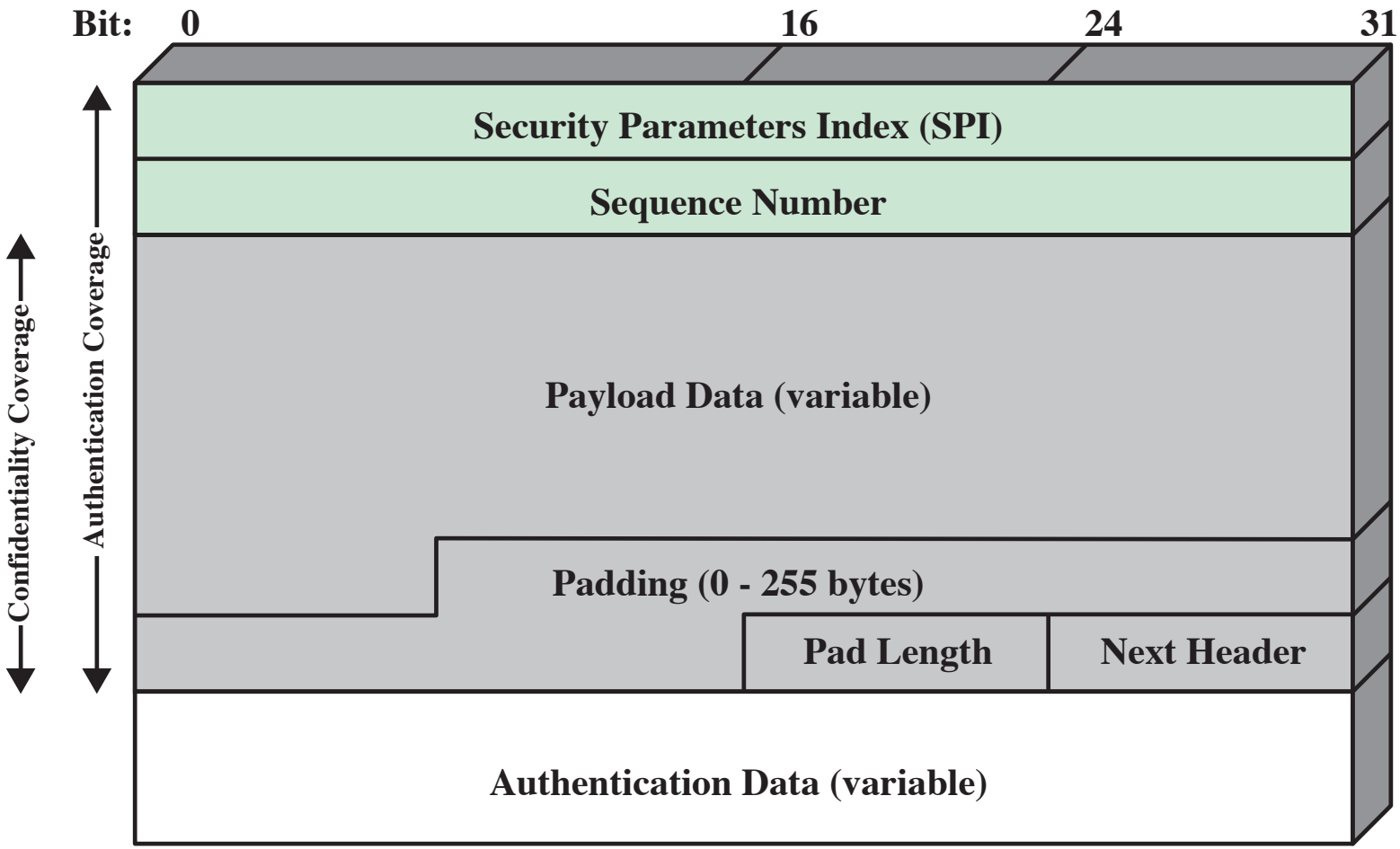


Figure 22.8 IPSec ESP Format

Transport and Tunnel Modes

Transport Mode

- Extends to the payload of an IP packet
- Typically used for end-to-end communication between two hosts
- ESP encrypts and optionally authenticates the IP payload but not the IP header

Tunnel Mode

- Provides protection to the entire IP packet
- The entire original packet travels through a tunnel from one point of an IP network to another
- Used when one or both ends of a security association are a security gateway
- A number of hosts on networks behind firewalls may engage in secure communications without implementing IPsec

Summary

- Secure E-mail and S/MIME
  - MIME
  - S/MIME
- DomainKeys identified mail
  - Internet mail architecture
  - DKIM strategy
- SSL and TLS
  - TLS architecture
  - TLS protocols
  - TLS attacks
  - SSL/TLS attacks
- HTTPS
  - Connection institution
  - Connection closure
- IPv4 and IPv6 security
  - IP security overview
  - The scope of IPsec
  - Security associations
  - Encapsulating security payload
  - Transport and tunnel modes