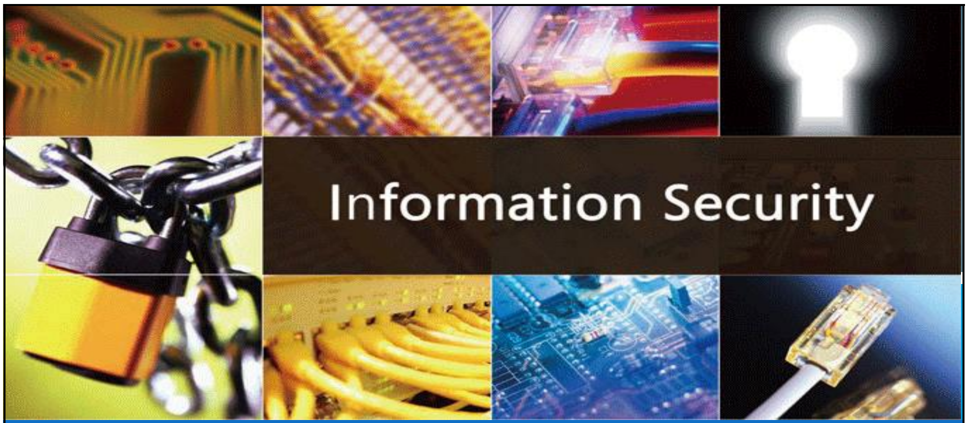


Internet Security Protocols and Standards

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

Contents

- Secure E-Mail and S/MIME
- DomainKeys Identified Mail
- Secure Sockets Layer (SSL)
- Transport Layer Security (TLS)
- HTTPS
- IPv4 and IPv6 Security – IPSec

Secure Email

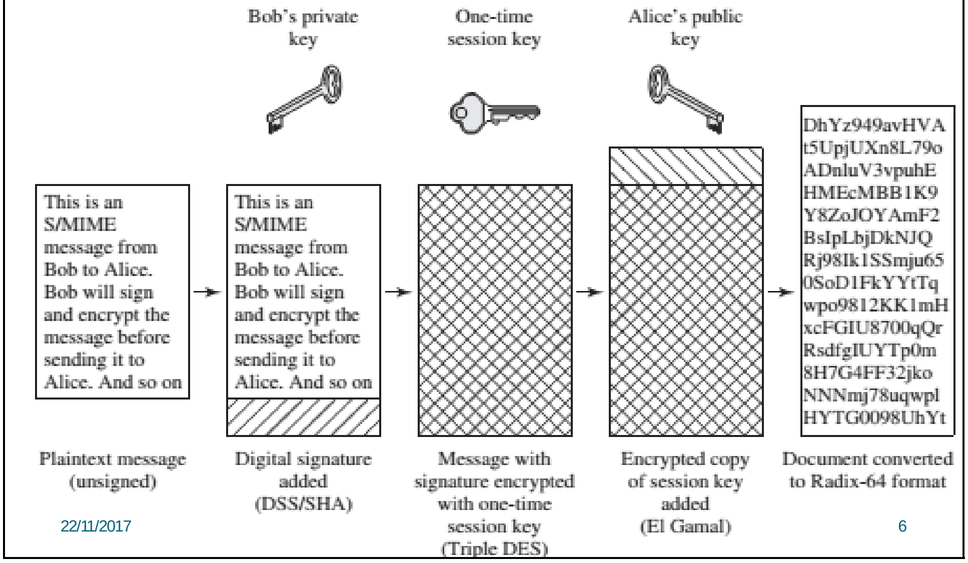
S/MIME

- MIME:
  - defines a simple header with To, From, Subject, and other fields
  - provides new header fields about the body: image, video
- S/MIME - Secure/Multipurpose Internet Mail Extension:
  - is a security enhancement to the MIME Internet e-mail format
  - based on technology from RSA Data Security.
  - ability to sign and/or encrypt e-mail messages

S/MIME functions

- **Enveloped data**: (= DES or 3DES, Dell-Hell for key exchange)
  - encrypted content
  - encrypted-content encryption keys for one or more recipients.
- **Signed data**: (= DSS and SHA-1)
  - the message digest of the content to be signed and then encrypting that with the private key of the signer.
- **Clear-signed data**:
  - Recipients without S/MIME capability can view these message content, although they cannot verify the signature.
- **Signed and enveloped data:**
  - Signed-only and encrypted-only entities may be nested, so that encrypted data may be signed and signed data or clear-signed data may be encrypted.

S/MIME example



Bob's private key

One-time session key

Alice's public key

This is an S/MIME message from Bob to Alice. Bob will sign and encrypt the message before sending it to Alice. And so on

This is an S/MIME message from Bob to Alice. Bob will sign and encrypt the message before sending it to Alice. And so on

DhYz949avHVA
t5UpjUXn8L79o
ADnluV3vpuhE
HMEcMBB1K9
Y8ZoJOYAmF2
BsIpLbjDkNJQ
Rj98Ik1SSmju65
0SoD1FkYYtTq
wpo9812KK1mH
xcFGIU8700qQr
RsdfgIUYTp0m
8H7G4FF32jko
NNNmj78uqwpl
HYTG0098UhYt

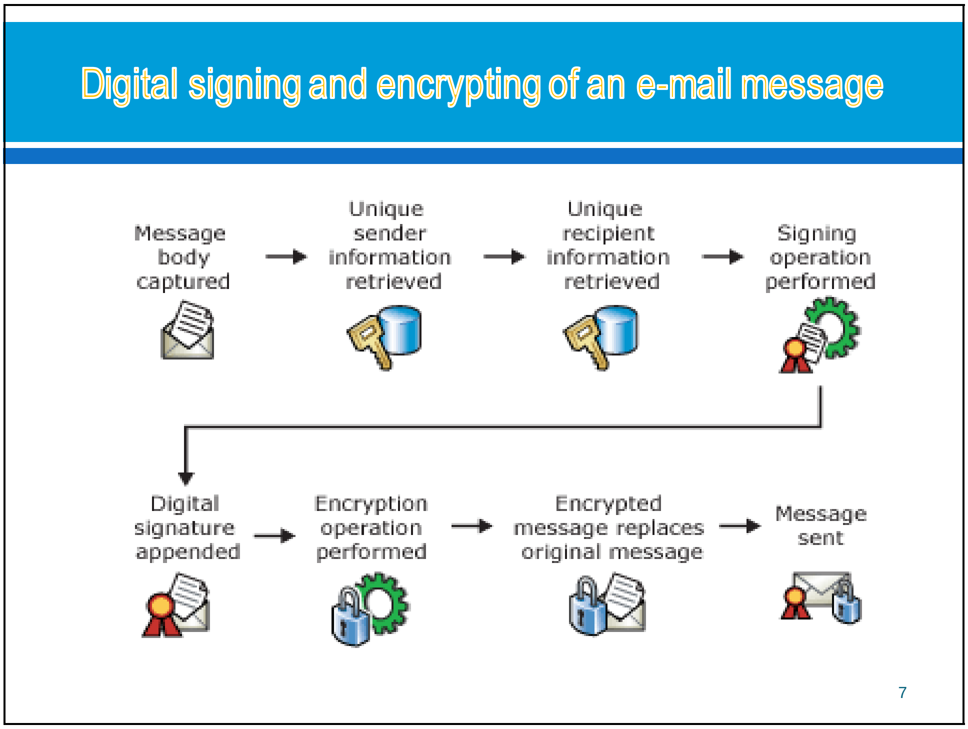
Plaintext message (unsigned)

Digital signature added (DSS/SHA)

Message with signature encrypted with one-time session key (Triple DES)

Encrypted copy of session key added (El Gamal)

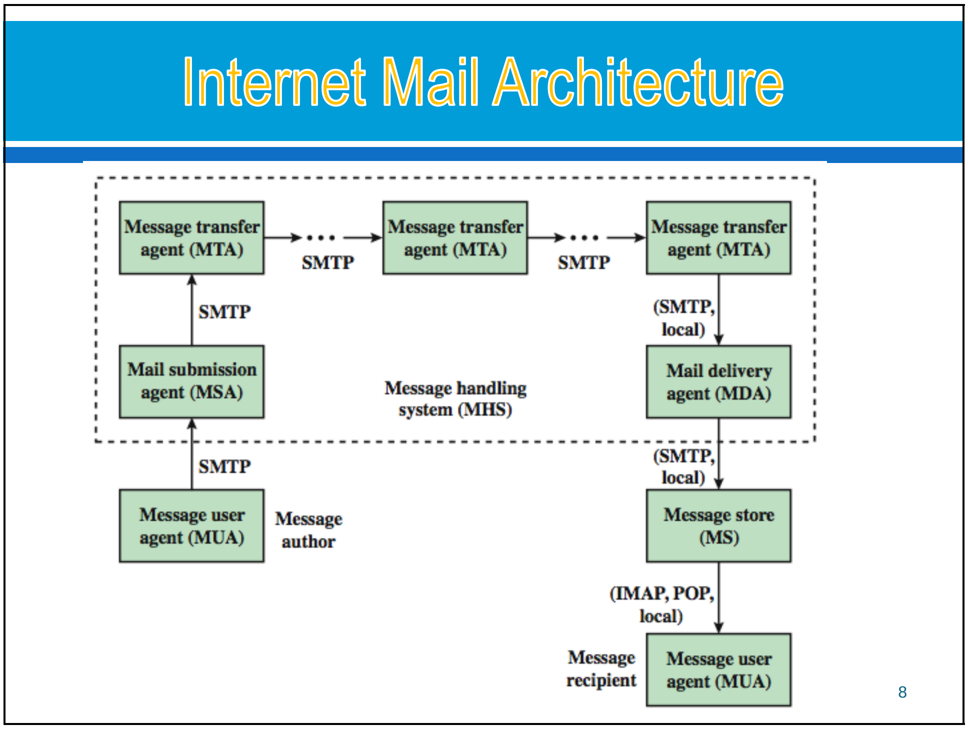
Document converted to Radix-64 format



Digital signing and encrypting of an e-mail message

Message body captured → Unique sender information retrieved → Unique recipient information retrieved → Signing operation performed

Digital signature appended → Encryption operation performed → Encrypted message replaces original message → Message sent



Internet Mail Architecture

Message transfer agent (MTA)

SMTP

Message transfer agent (MTA)

SMTP

Message transfer agent (MTA)

SMTP

(SMTP, local)

Mail submission agent (MSA)

Message handling system (MHS)

Mail delivery agent (MDA)

SMTP

(SMTP, local)

Message user agent (MUA)

Message author

Message store (MS)

(IMAP, POP, local)

Message recipient

Message user agent (MUA)

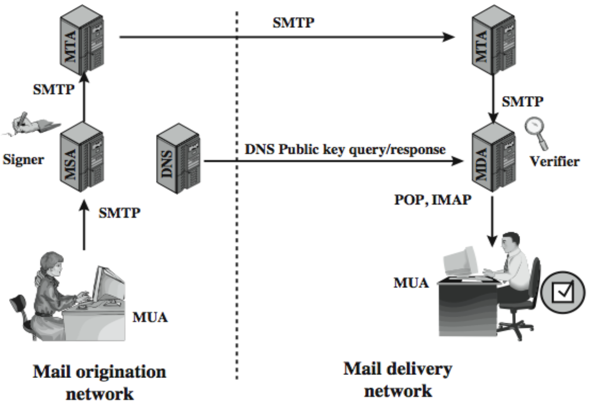
Email Threats

- see RFC 4684- *Analysis of Threats Motivating DomainKeys Identified Mail*
- describes the problem space in terms of:
  - range: low end, spammers, fraudsters
  - capabilities in terms of where submitted, signed, volume, routing naming etc
  - outside located attackers

9

DKIM Strategy

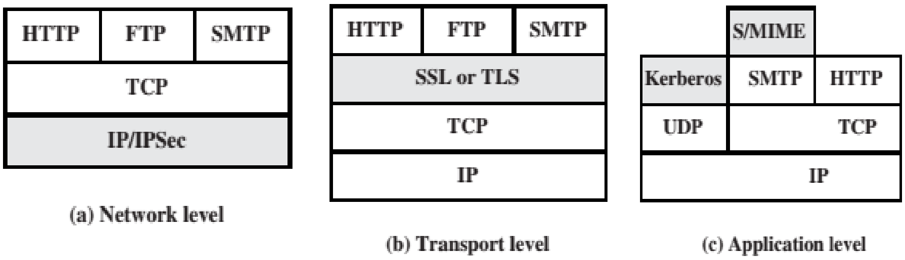
- to provide an email authentication technique
- transparent to user
  - MSA sign
  - MDA verify
- for pragmatic reasons



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

10

Security Facilities in the TCP/IP



(a) Network level

(b) Transport level

(c) Application level

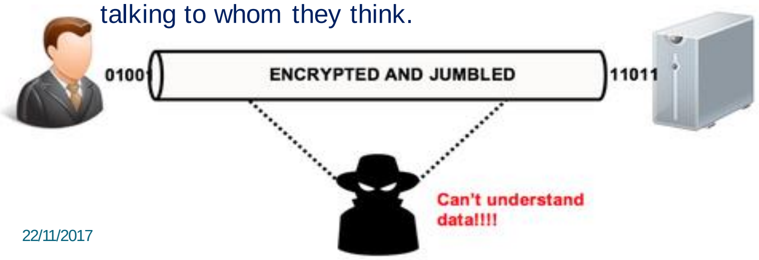
- transparent to end users and applications
- provides a general-purpose solution.
- includes a filtering capability so that only selected traffic need incur the overhead of IPsec processing.

- could be provided as part of the underlying protocol suite, therefore be transparent to applications.
- can be embedded in specific packages. Ex, Netscape and IE

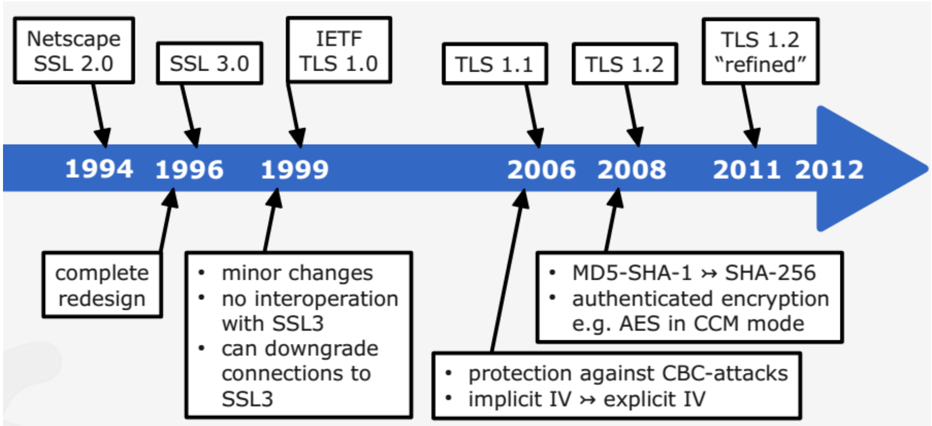
- Application-specific security services embedded within the particular application.
- the service can be tailored to the specific needs of a given application.

What is SSL/TLS?

- SSL/ TLS is used to secure communication between two parties using both asymmetric cryptography as well as symmetric cryptography to
  - provide data privacy, integrity, and authentication.
- A man in the middle is unable to read the contents of their messages.
  - Two parties are able to authenticate to ensure they really are talking to whom they think.



SSL/ TLS – History



- minor changes
- no interoperation with SSL3
- can downgrade connections to SSL3

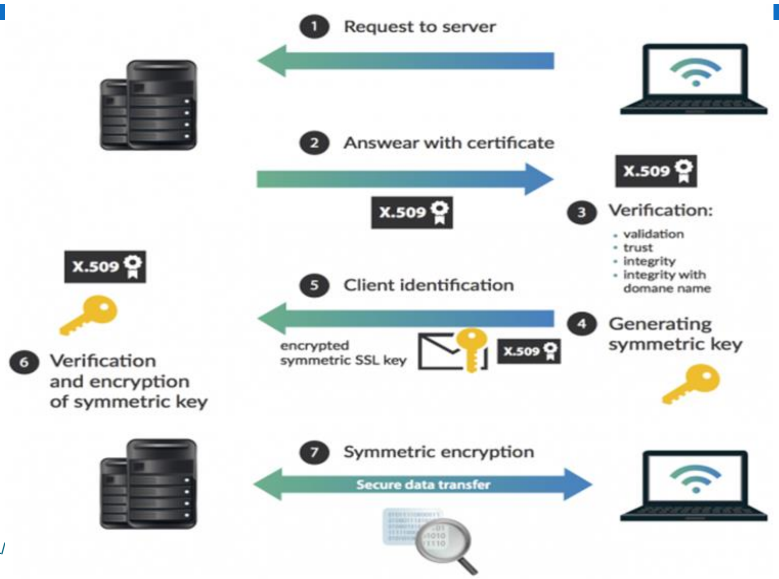
- MD5-SHA-1 ↣ SHA-256
- authenticated encryption e.g. AES in CCM mode

- protection against CBC-attacks
- implicit IV ↣ explicit IV

SSL certificate

- A tool that provides website protection and guarantees the confidentiality of data transmitted electronically.
- SSL certificates are registered on a particular domain name that contains information about the domain owner, his address, etc.
- Three basic types of SSL Certificates are issued by Certificate Authorities (CAs):
  - Domain Validated
  - Organization Validated
  - Extended Validation.

How SSL certificate works



1 Request to server

2 Answear with certificate

X.509

X.509

3 Verification:
- validation
- trust
- integrity
- integrity with domane name

4 Generating symmetric key

5 Client identification

encrypted symmetric SSL key

X.509

X.509

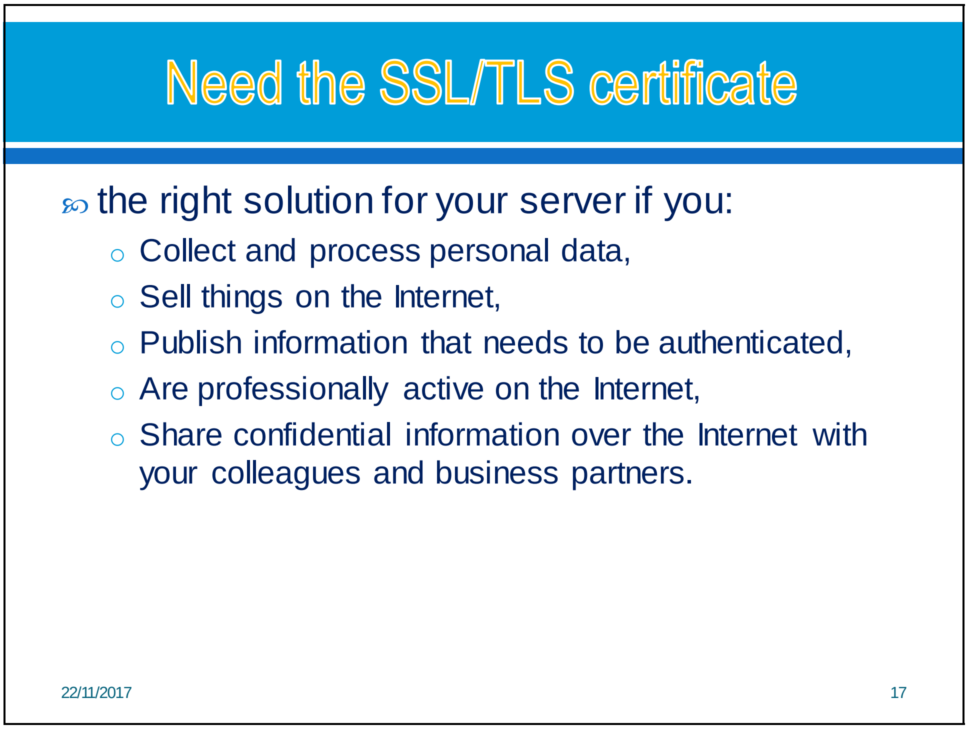
6 Verification and encryption of symmetric key

7 Symmetric encryption

Secure data transfer

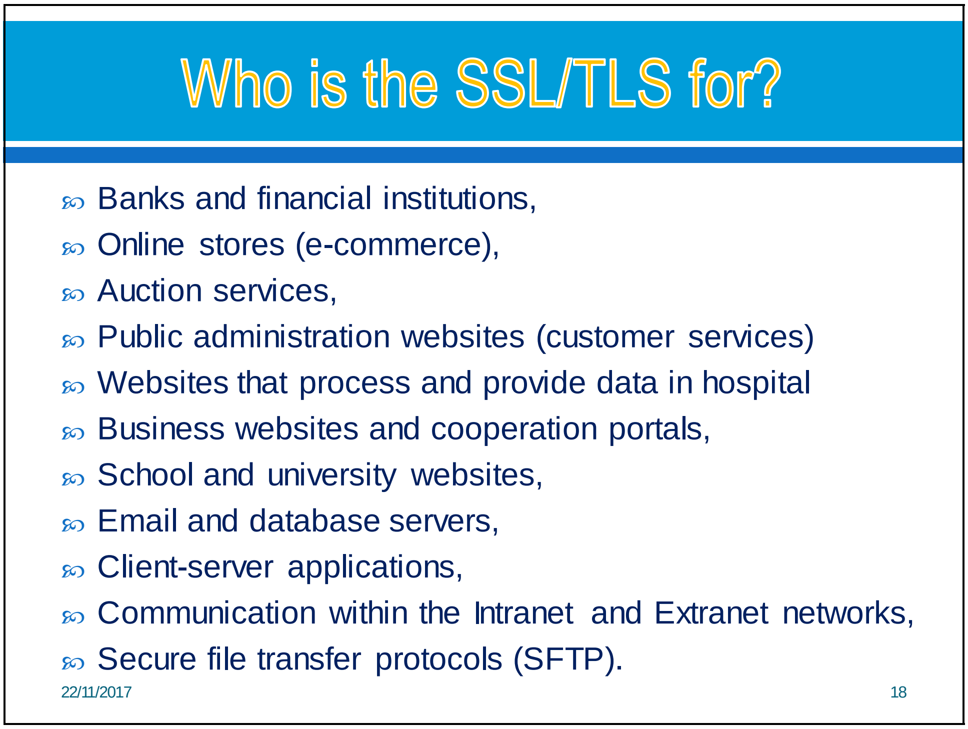
Benefits of TLS/SSL

- Strong authentication, message privacy, and integrity
  - secure transmitted data using encryption
  - data integrity through an integrity check value
  - help protect against masquerade attacks, man-in-the-middle, rollback attacks, and replay attacks.
- Interoperability: works with
  - most Web browsers and on most OS and Web Server
- Algorithm flexibility
  - authentication mechanisms, encryption algorithms, and hashing algorithms
- Ease of deployment:
  - transparently on a Windows Server
- Ease of use:
  - most of its operations are completely invisible to the client.
  - The client still be protected from attackers. (no need knowledge)



Need the SSL/TLS certificate

- the right solution for your server if you:
  - Collect and process personal data,
  - Sell things on the Internet,
  - Publish information that needs to be authenticated,
  - Are professionally active on the Internet,
  - Share confidential information over the Internet with your colleagues and business partners.



Who is the SSL/TLS for?

- Banks and financial institutions,
- Online stores (e-commerce),
- Auction services,
- Public administration websites (customer services)
- Websites that process and provide data in hospital
- Business websites and cooperation portals,
- School and university websites,
- Email and database servers,
- Client-server applications,
- Communication within the Intranet and Extranet networks,
- Secure file transfer protocols (SFTP).

Limitations of TLS/SSL

- Increased processor load
  - Cryptography, specifically public key operations, is CPU-intensive.
  - TLS uses the greatest resources while it is setting up connections.
- Administrative overhead
  - A TLS/SSL environment is complex and requires maintenance; the system administrator must configure the system and manage certificates.

Common TLS/SSL Scenarios

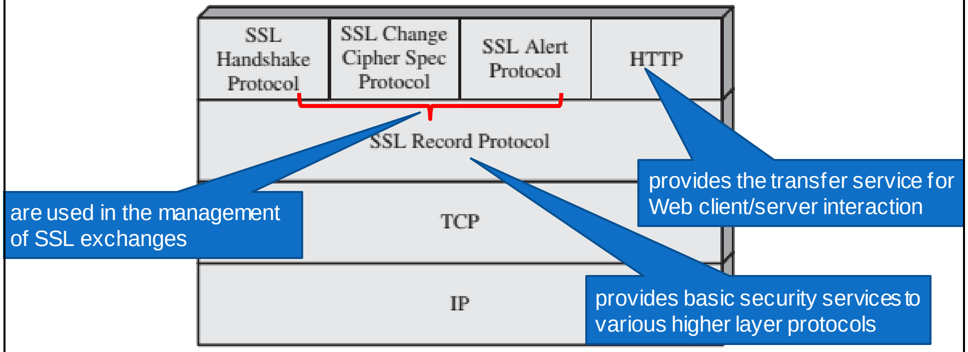
- SSL-secured transactions with an e-commerce Web site
  - certificate of the Web site is valid,
  - sends the client's credit card information as cipher text
  - must be enabled for the Web page: an order form..
- Authenticated client access to an SSL-secured Web site
  - Both the client and server need certificates from a mutually-trusted certification authority (CA)
- Remote access
  - provide authentication and data protection when users remotely log in to Windows-based systems or networks.
- SQL access
  - client or server can be configured to require encryption of the data that is transferred between them
- E-mail
  - protect data in a server-to-server exchange allows companies to use the Internet to securely transfer e-mail among divisions within the same company

SSL concepts

- **Connection:**
  - A connection is a transport that provides a suitable type of service.
  - Connections are peer-to-peer relationships.
  - The connections are transient.
  - Every connection is associated with one session.
- **Session:**
  - An association between a client and a server.
  - Sessions are created by the Handshake Protocol.
  - Sessions define a set of cryptographic security parameters which can be shared among multiple connections.
  - Sessions are used to avoid the expensive negotiation of new security parameters for each connection.

SSL Architecture

- SSL is designed to make use of TCP to provide a reliable end-to-end secure service.
- SSL is not a single protocol but rather two layers of protocols



are used in the management of SSL exchanges

provides the transfer service for Web client/server interaction

provides basic security services to various higher layer protocols

Figure 16.2 SSL Protocol Stack

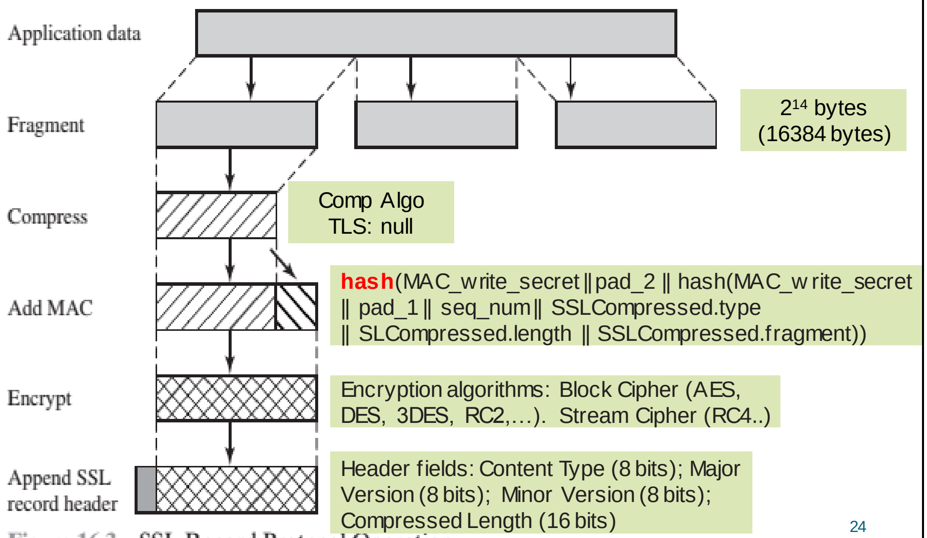
SSL Record Protocol

- The SSL Record Protocol provides two services for SSL connections:
  - **Confidentiality:**

    The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads.
  - **Message Integrity:**

    The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC).

SSL Record Protocol Operation



2^{14} bytes (16384 bytes)

Comp Algo
TLS: null

hash(MAC_write_secret || pad_2 || hash(MAC_w rite_secret || pad_1 || seq_num || SSLCompressed.type || SLCompressed.length || SSLCompressed.fragment))

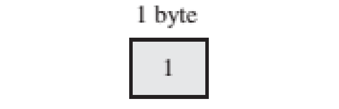
Encryption algorithms: Block Cipher (AES, DES, 3DES, RC2,…). Stream Cipher (RC4..)

Header fields: Content Type (8 bits); Major Version (8 bits); Minor Version (8 bits); Compressed Length (16 bits)

Figure 16.3 SSL Record Protocol Operation

Change Cipher Spec Protocol

- Change Cipher Spec Protocol:
  - is the simplest.
  - consists of a single message:
    - consists of a single byte with the value 1
    - to cause the pending state to be copied into the current state, which updates the cipher suite to be used on this connection.

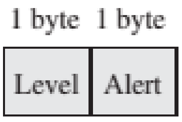

1 byte

1

(a) Change Cipher Spec Protocol

Alert protocol

- The Alert Protocol:
  - is used to convey SSL-related alerts to the peer entity.
  - alert messages are compressed and encrypted, as specified by the current state.
  - Each message in this protocol consists of two bytes
    - The first byte takes the value warning (1) or fatal (2) to convey the severity of the message.
    - The second byte contains a code that indicates the specific alert

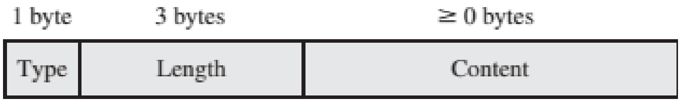

1 byte 1 byte

Level Alert

(b) Alert Protocol

Handshake Protocol

- Handshake Protocol
  - The most complex part of SSL
  - This protocol allows the server and client to authenticate each other and to negotiate an encryption and MAC algorithm and cryptographic keys to be used to protect data sent in an SSL record.
  - It is used before any application data is transmitted.
  - It consists of a series of messages exchanged by client and server. Each message has three fields:
    - **Type (1 byte):** Indicates one of 10 messages. Table 16.2 lists the defined message types.
    - **Length (3 bytes):** The length of the message in bytes.
    - **Content(bytes):** The parameters associated w ith this message



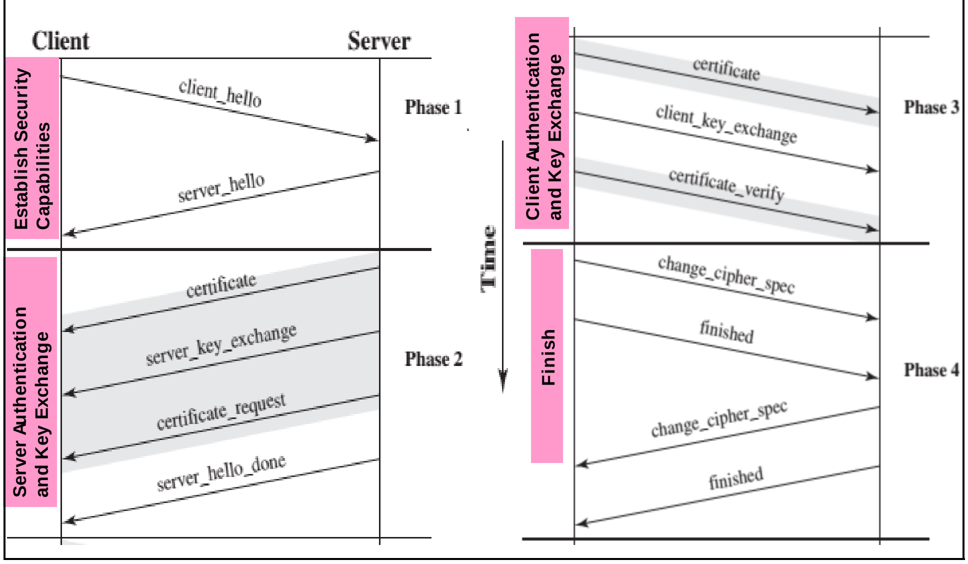
1 byte	3 bytes	≥ 0 bytes
Type	Length	Content

(c) Handshake Protocol

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

Handshake Protocol Action



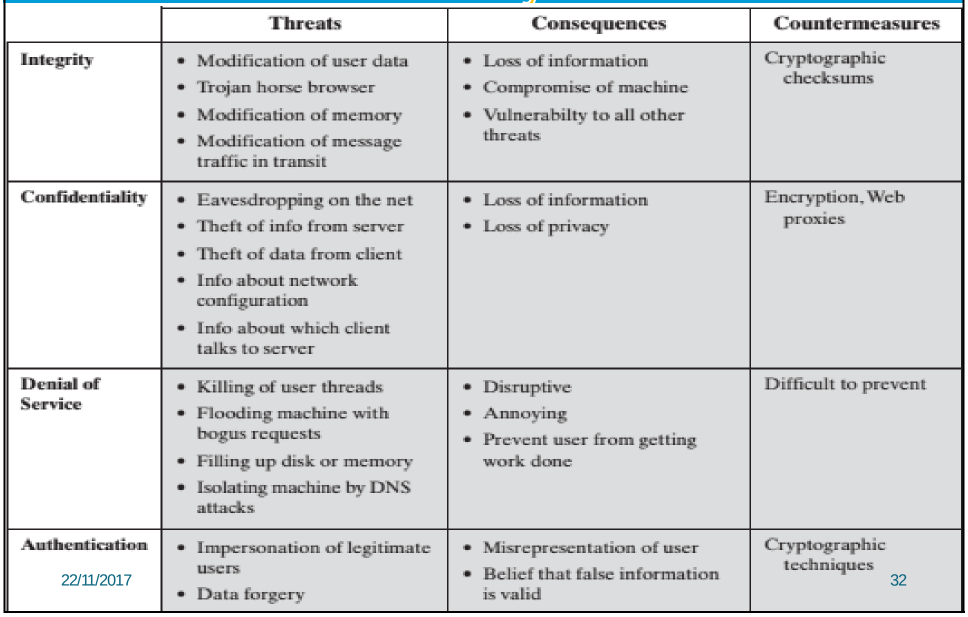
Transport Layer Security

- TLS is an IETF standardization initiative whose goal is to produce an Internet standard version of SSL.
- TLS is defined as a Proposed Internet Standard in RFC 5246
- It is very similar to SSLv3.
- There are minor differences:
  - record format version number
  - uses HMAC for MAC
  - a pseudo-random function expands secrets: based on HMAC using SHA-1 or MD5
  - has additional alert codes
  - some changes in supported ciphers
  - changes in certificate types & negotiations
  - changes in crypto computations & padding

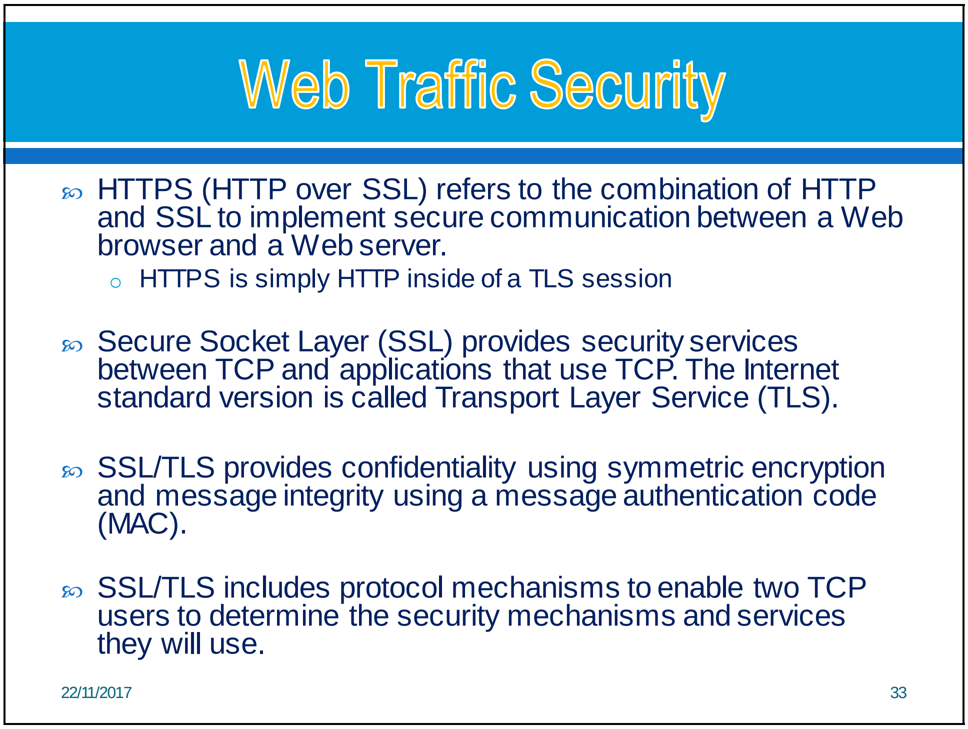
Web security

- Web now widely used by business, government, individuals
- but *Internet & Web are vulnerable*
- have a *variety of threats*
  - Integrity
  - Confidentiality
  - denial of service
  - authentication
- need *added security mechanisms*

Web security threats

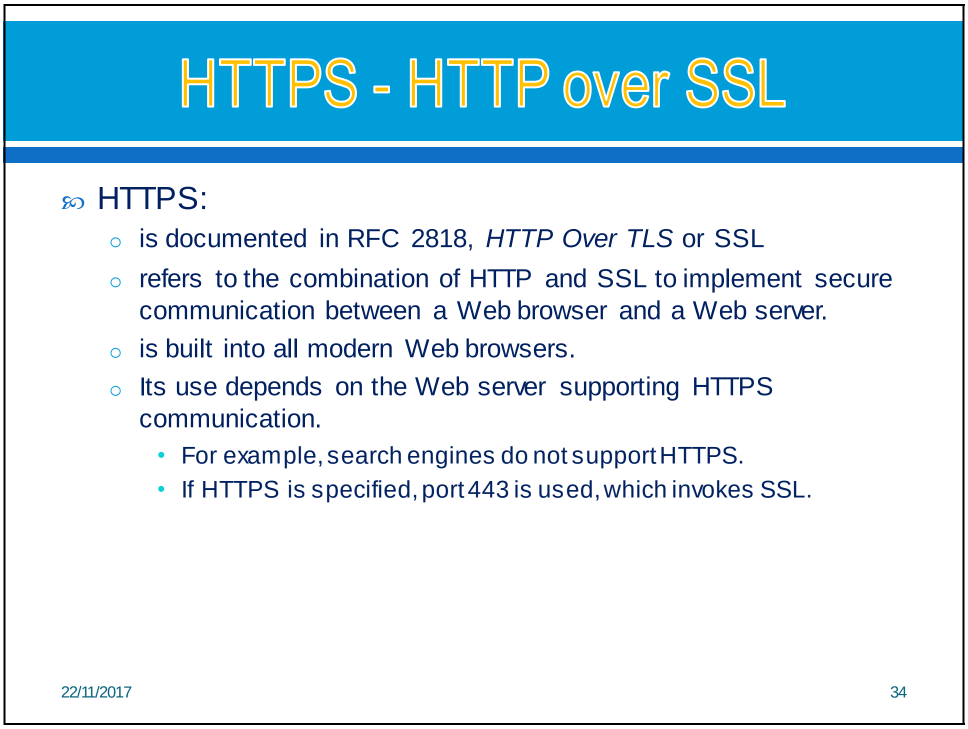


	Threats	Consequences	Countermeasures
Integrity	• Modification of user data • Trojan horse browser • Modification of memory • Modification of message traffic in transit	• Loss of information • Compromise of machine • Vulnerabilty to all other threats	Cryptographic checksums
Confidentiality	• Eavesdropping 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



Web Traffic Security

- HTTPS (HTTP over SSL) refers to the combination of HTTP and SSL to implement secure communication between a Web browser and a Web server.
  - HTTPS is simply HTTP inside of a TLS session
- Secure Socket Layer (SSL) provides security services between TCP and applications that use TCP. The Internet standard version is called Transport Layer Service (TLS).
- SSL/TLS provides confidentiality using symmetric encryption and message integrity using a message authentication code (MAC).
- SSL/TLS includes protocol mechanisms to enable two TCP users to determine the security mechanisms and services they will use.



HTTPS - HTTP over SSL

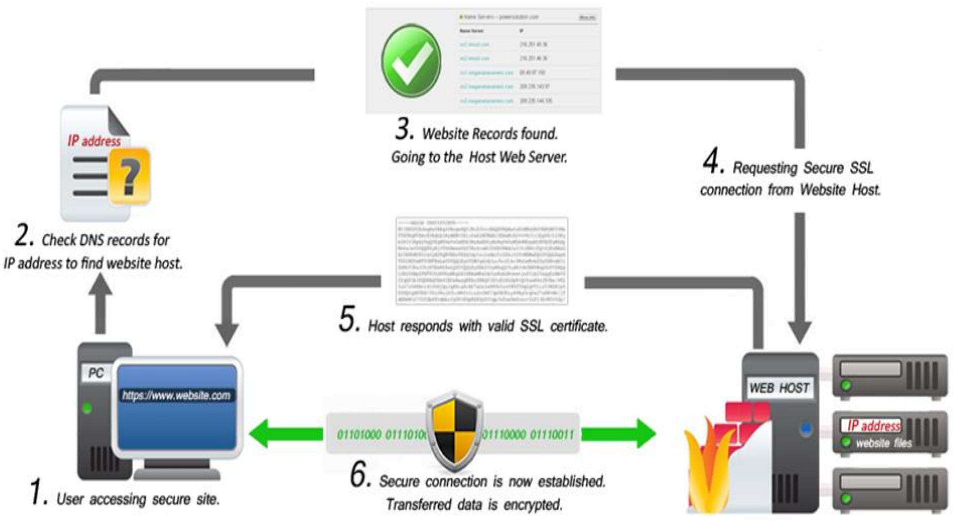
- HTTPS:
  - is documented in RFC 2818, *HTTP Over TLS* or SSL
  - refers to the combination of HTTP and SSL to implement secure communication between a Web browser and a Web server.
  - is built into all modern Web browsers.
  - Its use depends on the Web server supporting HTTPS communication.
    - For example, search engines do not support HTTPS.
    - If HTTPS is specified, port 443 is used, which invokes SSL.

HTTPS - HTTP over SSL

- When HTTPS is used, the following elements of the communication are encrypted:
  - URL of the requested document
  - Contents of the document
  - Contents of browser forms (filled in by browser user)
  - Cookies sent from browser to server and from server to browser
  - Contents of HTTP header
- There is no fundamental change in using HTTP over either SSL or TLS, and both implementations are referred to as HTTPS.

How does HTTPS works?

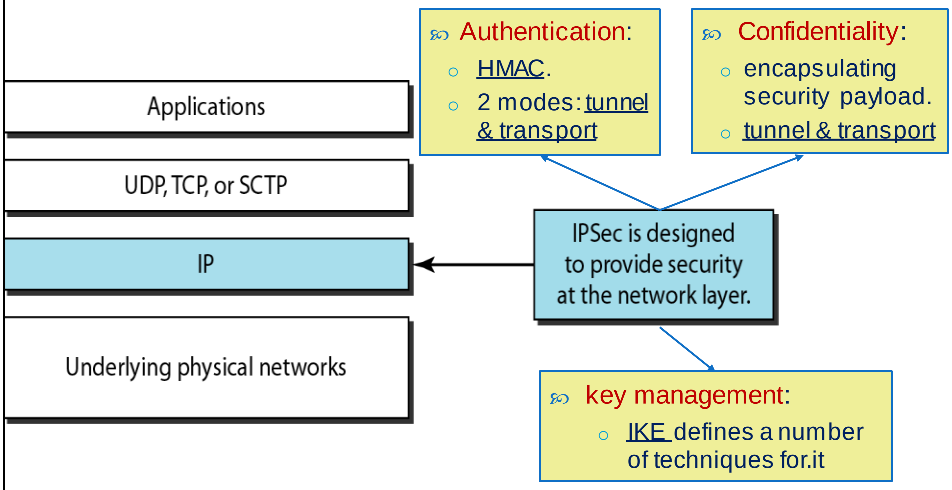
This presumes that SSL has already been issued by SSL issuing authority.


3. Website Records found.
Going to the Host Web Server.
IP address
2. Check DNS records for
IP address to find website host.
4. Requesting Secure SSL
connection from Website Host.
5. Host responds with valid SSL certificate.
PC
https://www.website.com
1. User accessing secure site.
01101000 0111010
01110000 01110011
6. Secure connection is now established.
Transferred data is encrypted.
WEB HOST
IP address
website files

IP Security Issues

- Eavesdropping
- Modification of packets in transit
- Identity spoofing (forged source IP addresses)
- Denial of service
- Many solutions are application-specific
- TLS for Web, S/MIME for email, SSH for remote login
- IPsec aims to provide a framework of open standards for secure communications over IP
- Protect every protocol running on top of IPv4 and IPv6

TCP/IP protocol suite and IPSec



- Authentication:
  - HMAC.
  - 2 modes: tunnel & transport
- Confidentiality:
  - encapsulating security payload.
  - tunnel & transport

IPSec is designed to provide security at the network layer.

- key management:
  - IKE defines a number of techniques for.it

Applications of IPsec

- IPsec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet.
  - **Secure branch office connectivity over the Internet:** saving costs and network management overhead.
  - **Secure remote access over the Internet:** reduces the cost of toll charges for traveling employees and telecommuters.
  - **Establishing extranet and intranet connectivity with partners:** ensuring authentication and confidentiality and providing a key exchange mechanism.
  - **Enhancing electronic commerce security:** guarantees data is both encrypted and authenticate.

An IP Security Scenario

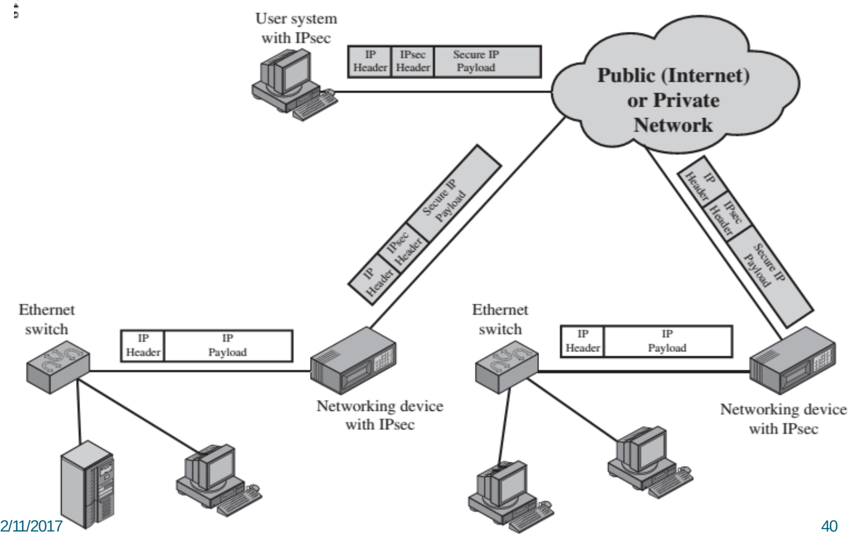


Figure 19.1 An IP Security Scenario

IPsec Protocol Suite

- Authentication Header (AH) protocol
  - For authenticating and securing data
  - IP protocol 51
- Encapsulating Security Payload (ESP) protocol
  - For encrypting, authenticating, and securing data
  - IP protocol 50
- Internet Key Exchange (IKE) protocol
  - For negotiating security parameters and establishing authenticated keys
  - Uses UDP port 500 for ISAKMP

Authentication Header (AH)

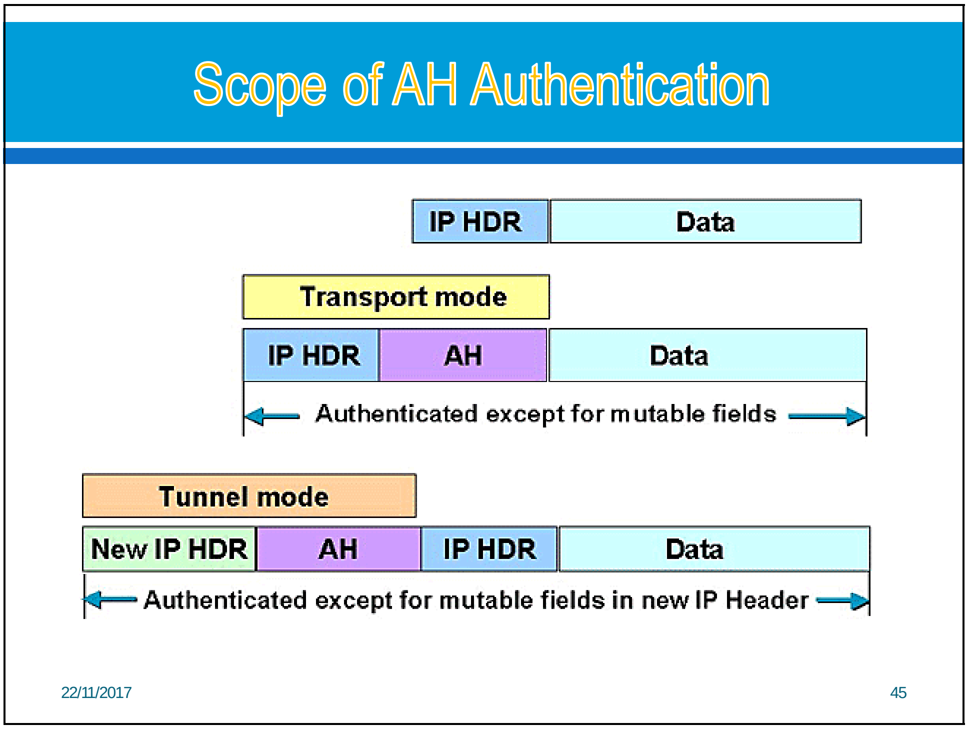
- Authentication Header (AH) - RFC4302
  - is an extension header
  - Provide data origin **authenticatio**n for IP datagrams
  - provide connectionless **integrity** and
  - provide protection against replays.

Encapsulating Security Payload (ESP)

- Encapsulating Security Payload (ESP) RFC4303
  - consists of an **encapsulating** header and trailer used to provide encryption or combined encryption/authentication
  - ESP can be used to provide:
    - **confidentiality**,
    - Data origin **authentication**,
    - connectionless **integrity,**
    - an anti-replay service (a form of partial sequence integrity),
    - and (limited) traffic flow confidentiality.
  - ESP can work with a variety of encryption and authentication algorithms

Packet Encapsulation in IPsec

- AH and ESP support 2 modes: transport and tunnel mode
- Transport mode:
  - provides *protection* primarily for *upper-layer protocols*.
  - extends to the *payload* of an IP packet.
  - is used for end-to-end communication between
  - to encrypt & *optionally* authenticate IP data
    - can do traffic analysis but is efficient
    - good for ESP host-to-host traffic
- Tunnel mode:
  - provides *protection* to the *entire IP packet*.
  - Packet travels *through a tunnel* from one point a IP network to another
  - encrypts entire IP packet
  - add new header for next hop
  - no routers on way can examine inner IP header
  - good for VPNs, gateway to gateway security



Scope of AH Authentication

IP HDR | Data

Transport mode

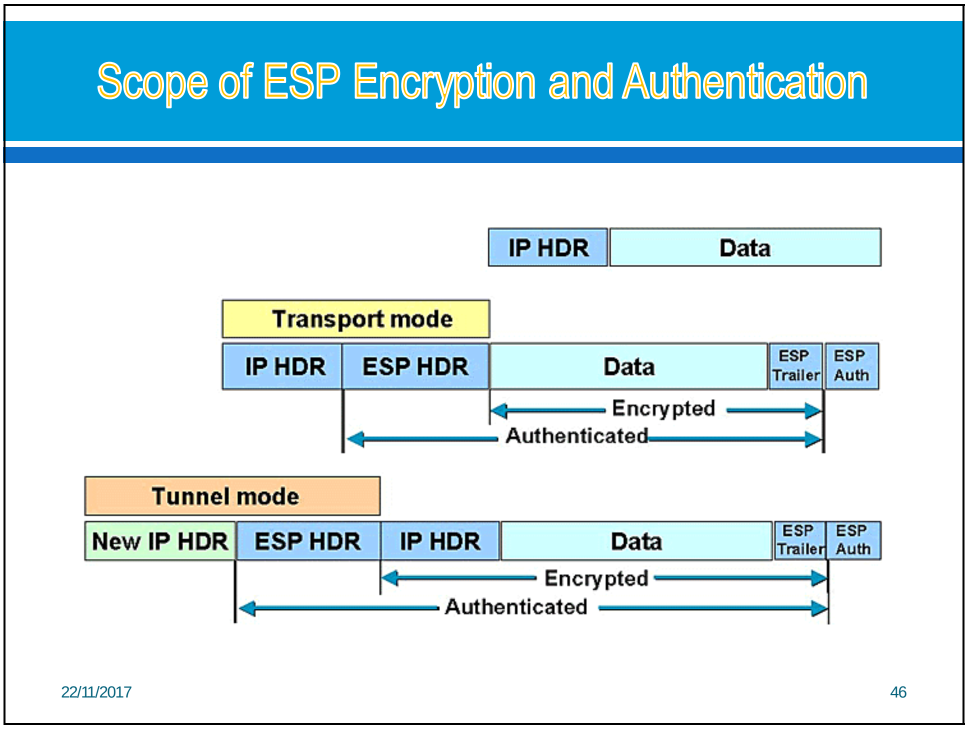
IP HDR | AH | Data

Authenticated except for mutable fields

Tunnel mode

New IP HDR | AH | IP HDR | Data

Authenticated except for mutable fields in new IP Header



Scope of ESP Encryption and Authentication

IP HDR | Data

Transport mode

IP HDR | ESP HDR | Data | ESP Trailer | ESP Auth

Encrypted

Authenticated

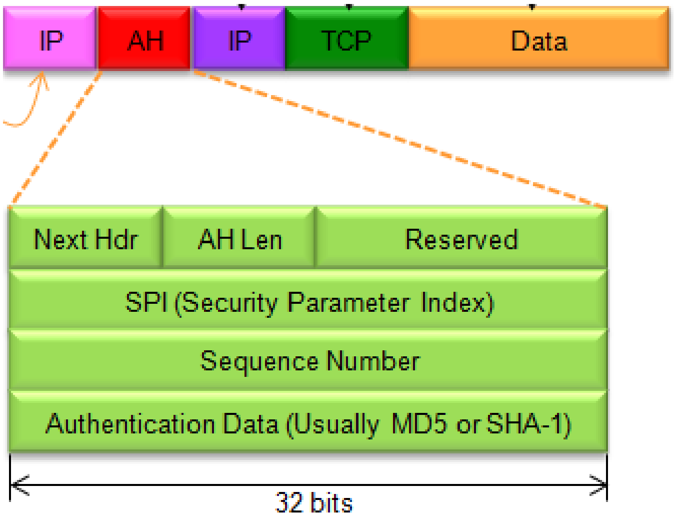
Tunnel mode

New IP HDR | ESP HDR | IP HDR | Data | ESP Trailer | ESP Auth

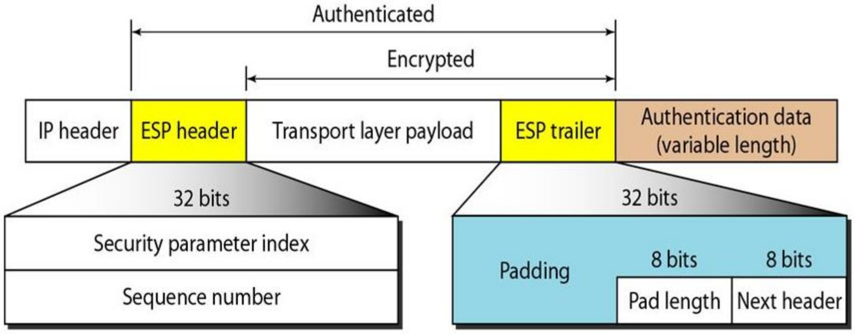
Encrypted

Authenticated

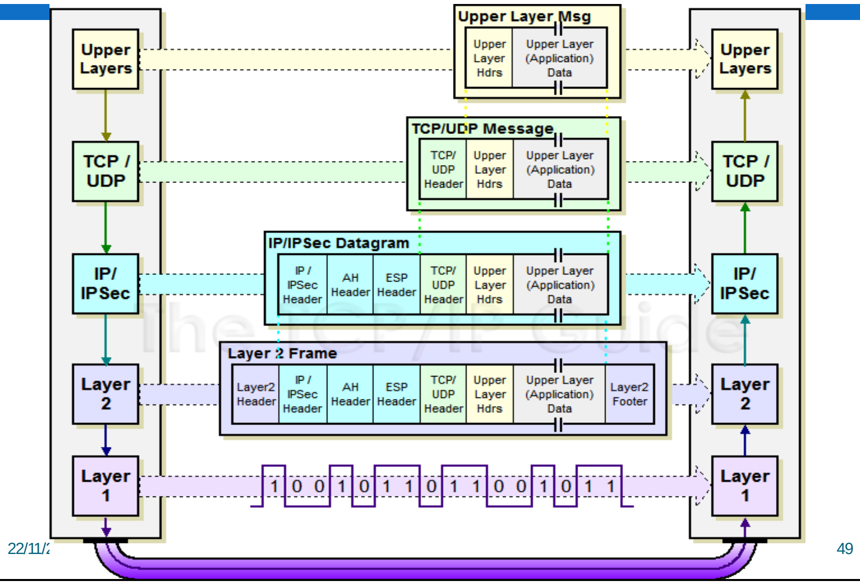
AH Packet Format


IP
AH
IP
TCP
Data
Next Hdr
AH Len
Reserved
SPI (Security Parameter Index)
Sequence Number
Authentication Data (Usually MD5 or SHA-1)
32 bits

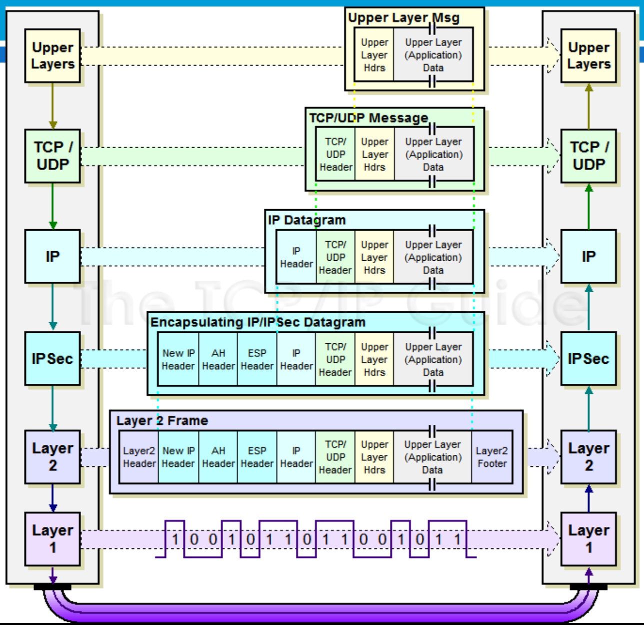
ESP Packet Format

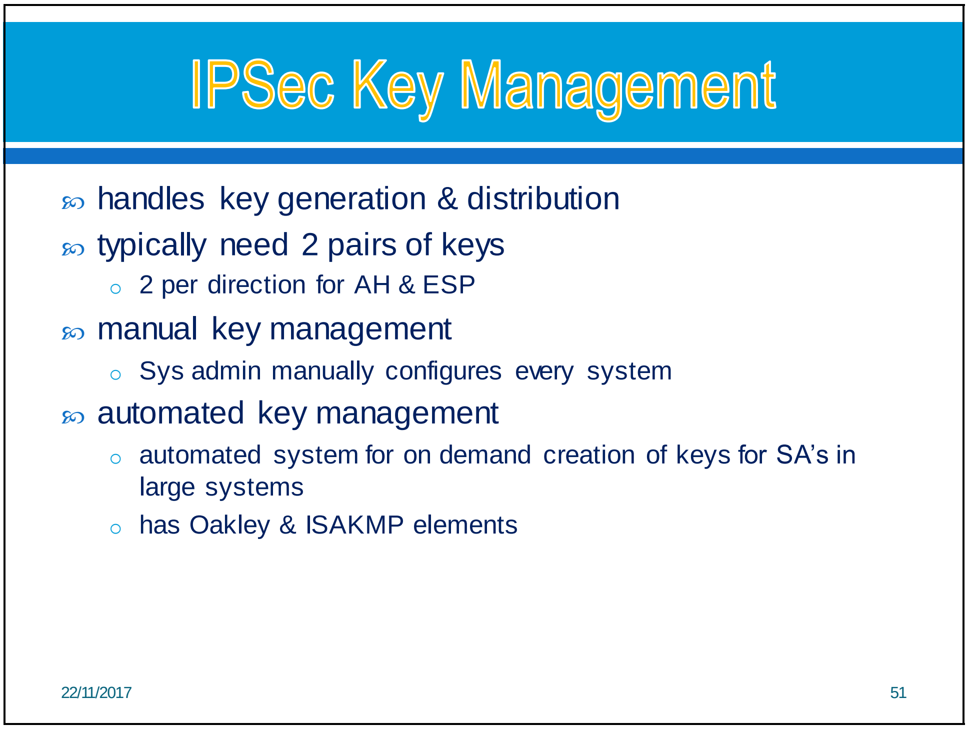


IPSec Transport Mode Operation



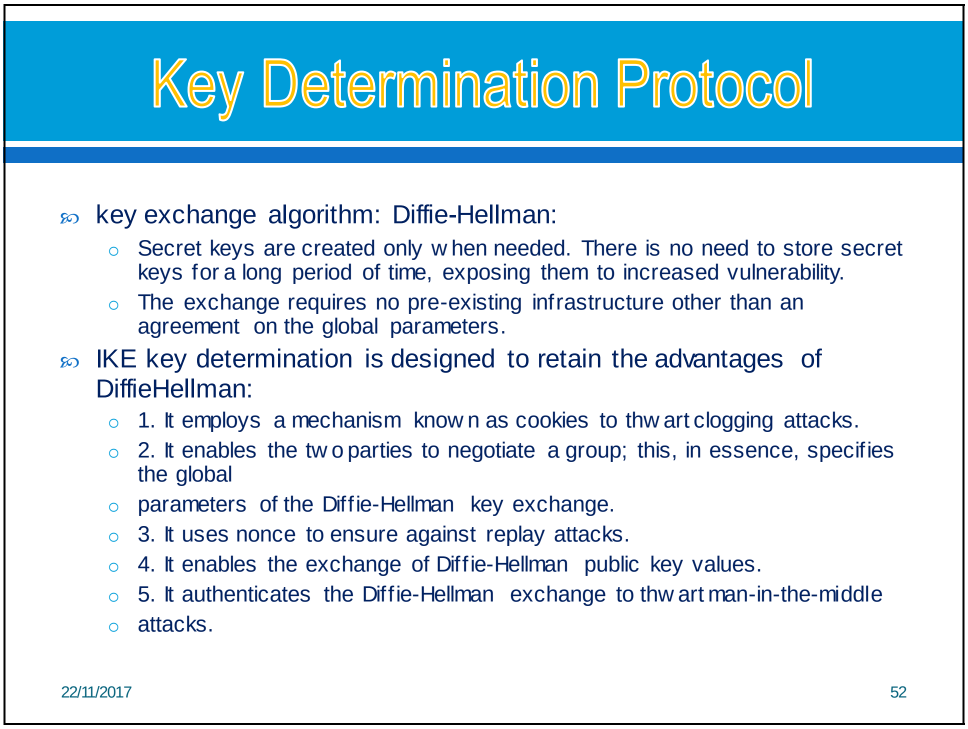
IPSec Tunnel Mode Operation





IPSec Key Management

- handles key generation & distribution
- typically need 2 pairs of keys
  - 2 per direction for AH & ESP
- manual key management
  - Sys admin manually configures every system
- automated key management
  - automated system for on demand creation of keys for SA’s in large systems
  - has Oakley & ISAKMP elements



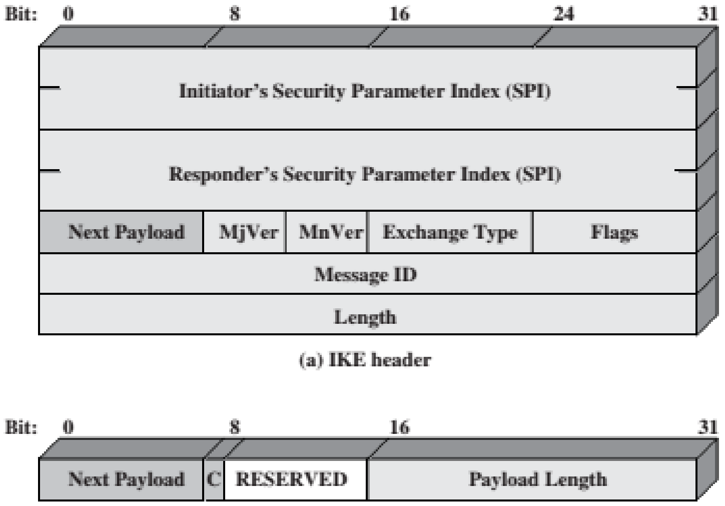
Key Determination Protocol

- key exchange algorithm: Diffie-Hellman:
  - Secret keys are created only when needed. There is no need to store secret keys for a long period of time, exposing them to increased vulnerability.
  - The exchange requires no pre-existing infrastructure other than an agreement on the global parameters.
- IKE key determination is designed to retain the advantages of DiffieHellman:
  - 1. It employs a mechanism known as cookies to thwart clogging attacks.
  - 2. It enables the two parties to negotiate a group; this, in essence, specifies the global
  - parameters of the Diffie-Hellman key exchange.
  - 3. It uses nonce to ensure against replay attacks.
  - 4. It enables the exchange of Diffie-Hellman public key values.
  - 5. It authenticates the Diffie-Hellman exchange to thwart man-in-the-middle
  - attacks.

IKE's Responsibilities in IPsec Protocol

- Negotiates IPsec tunnel characteristics between two IPsec peers
- Negotiates IPsec protocol parameters
- Exchanges public keys
- Authenticates both sides
- Manages keys after the exchange
- Automates entire key-exchange process

IKE Formats



Bit: 0 8 16 24 31

Initiator's Security Parameter Index (SPI)

Responder's Security Parameter Index (SPI)

Next Payload | MjVer | MnVer | Exchange Type | Flags

Message ID

Length

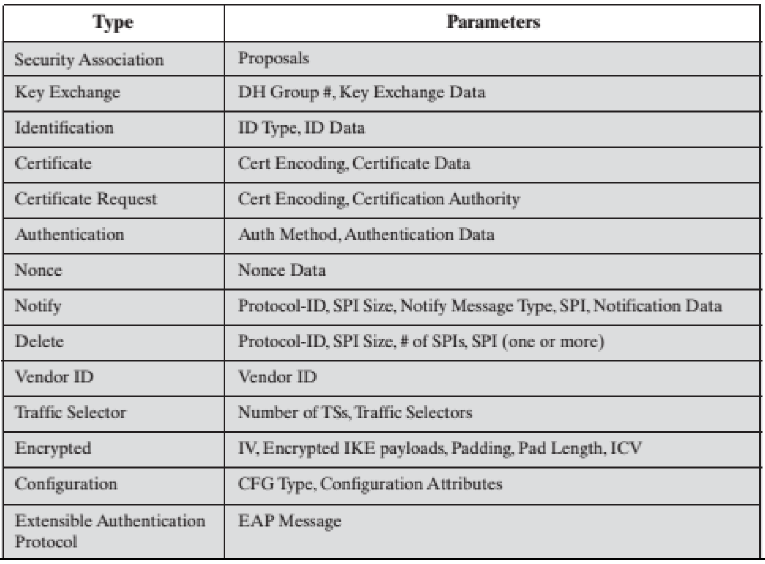
(a) IKE header

Bit: 0 8 16 31

Next Payload | C | RESERVED | Payload Length

(b) Generic Payload header

IKE Payload Types



Type	Parameters
Security Association	Proposals
Key Exchange	DH Group #, Key Exchange Data
Identification	ID Type, ID Data
Certificate	Cert Encoding, Certificate Data
Certificate Request	Cert Encoding, Certification Authority
Authentication	Auth Method, Authentication Data
Nonce	Nonce Data
Notify	Protocol-ID, SPI Size, Notify Message Type, SPI, Notification Data
Delete	Protocol-ID, SPI Size, # of SPIs, SPI (one or more)
Vendor ID	Vendor ID
Traffic Selector	Number of TSs, Traffic Selectors
Encrypted	IV, Encrypted IKE payloads, Padding, Pad Length, ICV
Configuration	CFG Type, Configuration Attributes
Extensible Authentication Protocol	EAP Message

Q & A