UNIVERSITY OF
WESTMINSTER

Defensive Technologies- Securing the Network and Services

6COSC019- Cyber Security

Dr Ayman El Hajjar

March 13, 2023

School of Computer Science and Engineering
University of Westminster

OUTLINE

1. Internet Security Protocols and Standards
2. Network Layer Security
3. Transport Layer Security
4. Application Layer Security
   - Secure Shell (SSH)
   - Email Security

BEFORE WE START

Note

- **These are examples of protocols, possibly the mostly used.**
- **There are many others**

Session Overview

Internet Security Protocols and Standards

Network Layer Security

Transport Layer Security

Application Layer Security

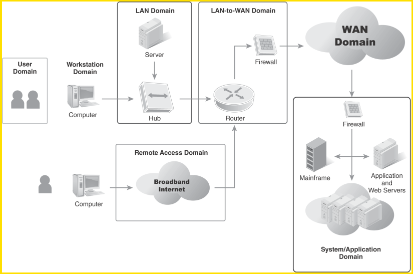
- Secure Shell (SSH)
- Email Security

Internet Security Protocols and Standards

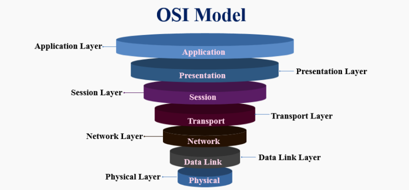
Protocols and Domains

Where we are

- Infrastructure Domains
- OSI layers

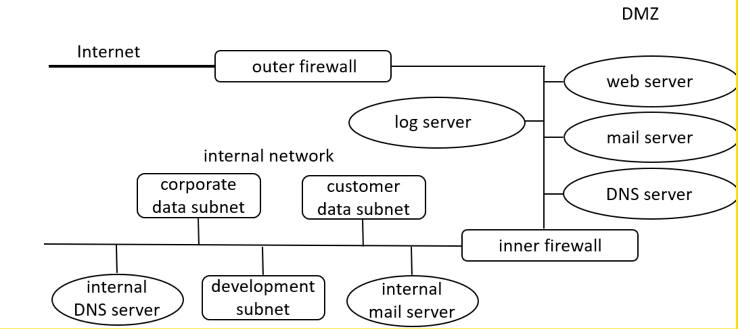


7 IT Infrastructure Domain



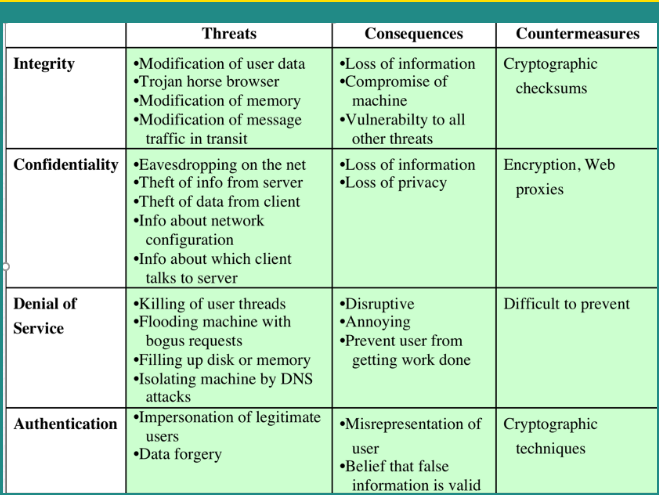
OSI Model

A typical Network Infrastructure



A typical Network Infrastructure

THREATS EXAMPLE ON A NETWORK

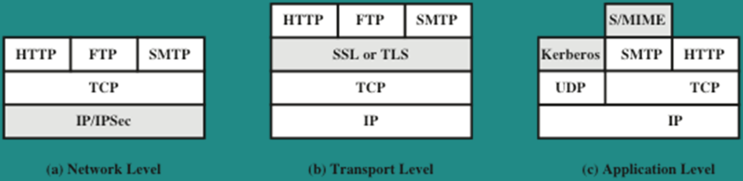


	Threats	Consequences	Countermeasures
Integrity	•Modification of user data •Trojan horse browser •Modification of memory •Modification of message traffic in transit	•Loss of information •Compromise of machine •Vulnerabilty to all other threats	Cryptographic checksums
Confidentiality	•Eavesdropping on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

Example of threats on a typical network

TCP/IP SECURITY SOLUTION

- A number of approaches to providing Internet security are possible.
  The various approaches that have been considered are similar in the services they provide in relation to to the TCP/IP protocol stack.



Relative location of security facilities in the TCP/IP protocol stack

Network Layer Security

IP SECURITY

● RFC 1636: “Security in the Internet Architecture” issued in 1994 by the Internet Architecture Board (IAB)

Security area to secure in IP Security

✺ 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

- IPsec provides the capability to secure communications across a LAN, private and public WANs, and the Internet
- Examples include:
  - Secure branch office connectivity over the Internet
  - Secure remote access over the Internet
  - Establishing extranet and intranet connectivity with partners
  - Enhancing electronic commerce security
- Principal feature of IPsec is that it can encrypt and/or authenticate all traffic at the IP level
  - Thus all distributed applications (remote logon, client/server, e-mail, file transfer, Web access) can be secured

BENEFITS OF IPSEC

- When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter
- Traffic within a company or workgroup does not incur the overhead of security-related processing
- IPsec is below the transport layer (TCP, UDP) and so is transparent to applications
- There is no need to train users on security mechanisms
- This is useful for offsite workers and for setting up a secure virtual subnetwork within an organisation for sensitive applications

THE SCOPE OF IPSEC

- Provides two main functions:
  - A combined authentication/encryption function called Encapsulating Security Payload (ESP)
  - Key exchange function
- 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
- VPNs want both authentication and encryption

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 (Integrity)
  - Confidentiality (encryption)
  - Limited traffic flow (confidentiality)

TRANSPORT MODE

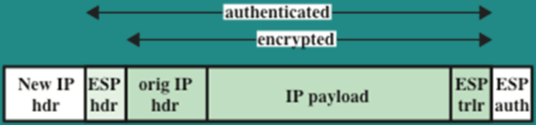
- Provides protection primarily for upper-layer protocols
- Examples include a TCP or UDP segment or an ICMP packet
- Typically used for end-to-end communication between two hosts
- ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header
- AH in transport mode authenticates the IP payload and selected portions of the IP header

TUNNEL MODE

- Provides protection to the entire IP packet
- Used when one or both ends of a security association (SA) are a security gateway
- A number of hosts on networks behind firewalls may engage in secure communications without implementing IPsec
- ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet, including the inner IP header
- AH in tunnel mode authenticates the entire inner IP packet and selected portions of the outer IP header

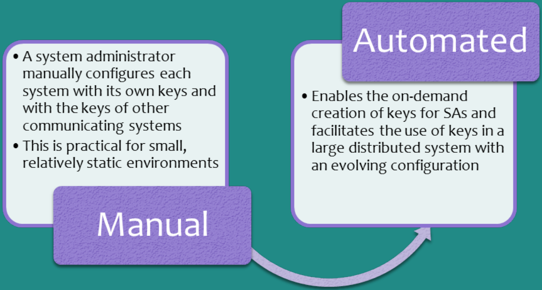
IPSec: Tunnel mode format

- Tunnel mode makes use of an IPsec function, a combined authentication/encryption function called Encapsulating Security Payload (ESP), and a key exchange function.
- For VPNs, both authentication and encryption are generally desired, because it is important both to (1) assure that unauthorized users do not penetrate the VPN, and (2) assure that eavesdroppers on the Internet cannot read messages sent over the VPN.



Tunnel mode format

Tunnel Mode and Transport Mode Functionality



Manual

- A system administrator manually configures each system with its own keys and with the keys of other communicating systems
- This is practical for small, relatively static environments

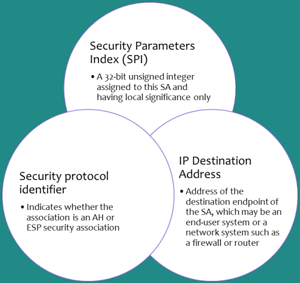
Automated

- Enables the on-demand creation of keys for SAs and facilitates the use of keys in a large distributed system with an evolving configuration

Tunnel Mode and Transport Mode Functionality

INTERNET KEY EXCHANGE (IKE)

- The key management portion of IPsec involves the determination and distribution of secret keys
  - A typical requirement is four keys for communication between two applications
  - Transmit and receive pairs for both integrity and confidentiality



Security Parameters Index (SPI)

- A 32-bit unsigned integer assigned to this SA and having local significance only

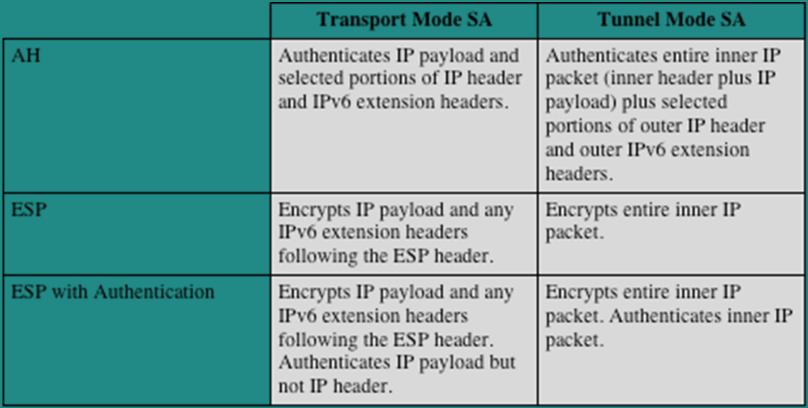
Security protocol identifier

- Indicates whether the association is an AH or ESP security association

IP Destination Address

- Address of the destination endpoint of the SA, which may be an end-user system or a network system such as a firewall or router

PROTOCOL OPERATION FOR ESP



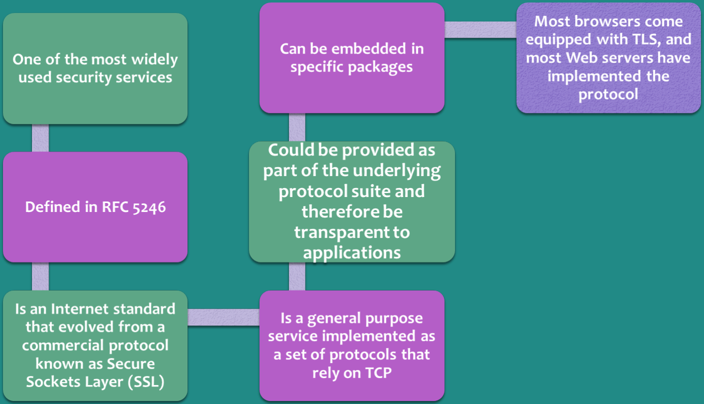
	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers.	Authenticates entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and outer IPv6 extension headers.
ESP	Encrypts IP payload and any IPv6 extension headers following the ESP header.	Encrypts entire inner IP packet.
ESP with Authentication	Encrypts IP payload and any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header.	Encrypts entire inner IP packet. Authenticates inner IP packet.

Transport Layer Security

TRANSPORT LAYER SECURITY

- 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

Transport layer Security - A definition



One of the most widely used security services

Defined in RFC 5246

Is an Internet standard that evolved from a commercial protocol known as Secure Sockets Layer (SSL)

Is a general purpose service implemented as a set of protocols that rely on TCP

Could be provided as part of the underlying protocol suite and therefore be transparent to applications

Can be embedded in specific packages

Most browsers come equipped with TLS, and most Web servers have implemented the protocol

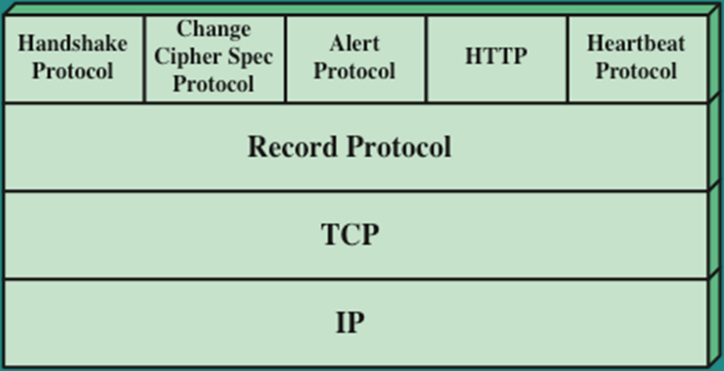
Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

- 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)
- Two implementation choices:
  - Provided as part of the underlying protocol suite
  - Embedded in specific packages

SSL/TLS PROTOCOL STACK

- TLS is designed to make use of TCP to provide a reliable end-to-end secure service.
- The TLS Record Protocol provides basic security services to various higher layer protocols.
- Three higher-layer protocols are defined as part of TLS:
  - The Handshake Protocol;
  - The Change Cipher Spec Protocol;
  - and the Alert Protocol.
- These TLS specific protocols are used in the management of TLS exchanges.
- A fourth protocol, the Heartbeat Protocol, is defined in a separate RFC.

SSL/TLS PROTOCOL STACK



Handshake Protocol

Change Cipher Spec Protocol

Alert Protocol

HTTP

Heartbeat Protocol

Record Protocol

TCP

IP

TLS CONCEPTS

- Two important TLS concepts are the TLS session and the TLS connection which are defined in the specification.
  - TLS Session:
    - Created by the Handshake Protocol
    - Define a set of cryptographic parameters
    - Used to avoid the expensive negotiation of new security parameters for each connection
  - TLS Connection:
    - A transport layer protocol that provides a suitable type of service
    - Peer-to-peer relationships
    - Every connection is associated with one session

TLS Record Protocol Operation

- TLS Record Protocol defines two services for TLS connections:
  - Confidentiality: The Handshake Protocol defines a shared secret key that is used for conventional encryption of TSL payloads. The message is compressed before being concatenated with the MAC and encrypted, with a range of ciphers being supported as shown.
  - Message Integrity: The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC), which is similar to HMAC

TLS Record Protocol Operation

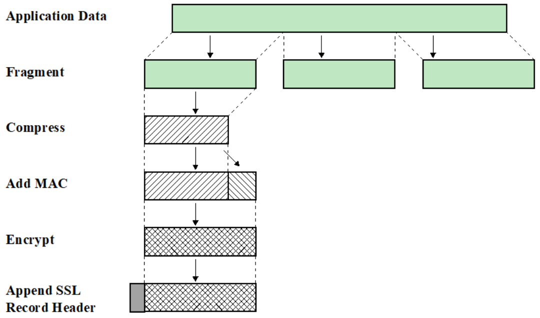
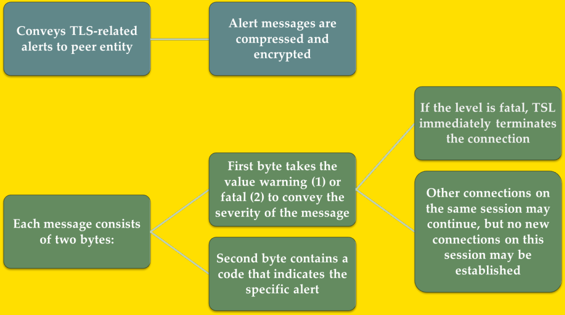


Figure 22.5 TLS Record Protocol Operation

ALERT PROTOCOL



Conveys TLS-related alerts to peer entity

Alert messages are compressed and encrypted

Each message consists of two bytes:

First byte takes the value warning (1) or fatal (2) to convey the severity of the message

If the level is fatal, TSL immediately terminates the connection

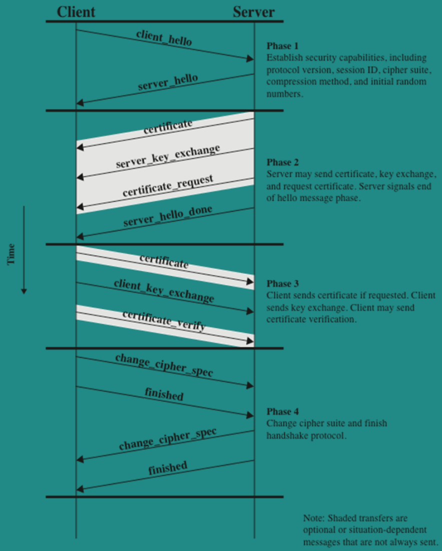
Other connections on the same session may continue, but no new connections on this session may be established

Second byte contains a code that indicates the specific alert

TLS HANDSHAKE MESSAGES

- Most complex part of TLS
- Is used before any application data are transmitted
- Allows server and client to:
  - ✺ Authenticate Each Other → Negotiate encryption and MAC algorithms → Negotiate cryptographic keys to be used
- Comprises a series of messages exchanged by client and server
- Exchange has four phases

HANDSHAKE PROTOCOL ACTION



Phase 1
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.

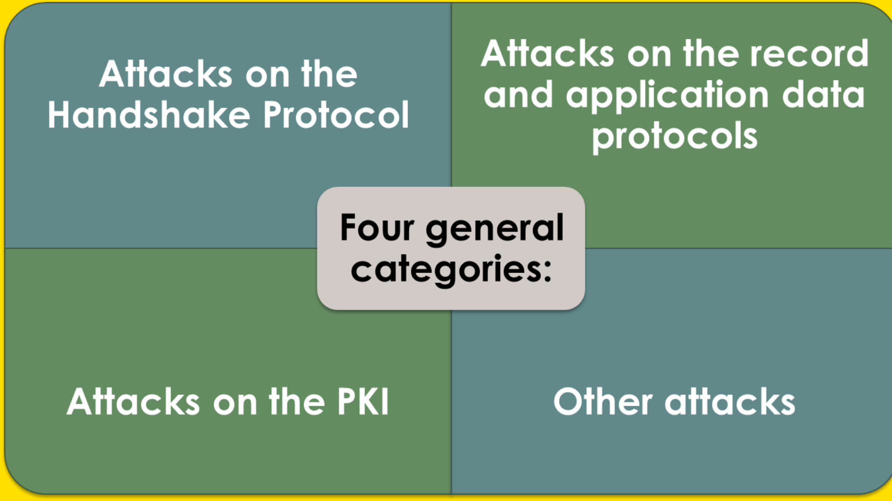
Phase 2
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.

Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.

Phase 4
Change cipher suite and finish handshake protocol.

Note: Shaded transfers are optional or situation-dependent messages that are not always sent.

SSL/TLS ATTACKS



Four general categories:

Attacks on the Handshake Protocol

Attacks on the record and application data protocols

Attacks on the PKI

Other attacks

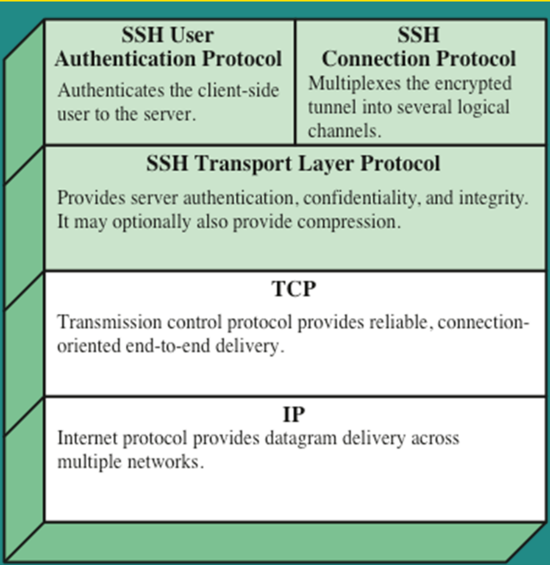
HTTPS (HTTP over SSL)

- 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

Application Layer Security

SECURE SHELL (SSH)

- A protocol for secure network communications designed to be relatively simple and inexpensive to implement
- The initial version, SSH1 was focused on providing a secure remote logon facility to replace TELNET and other remote logon schemes that provided no security
- SSH also provides a more general client/server capability and can be used for such network functions as file transfer and e-mail
- SSH2 fixes a number of security flaws in the original scheme.
- SSH client and server applications are widely available for most operating systems



SSH User Authentication Protocol

Authenticates the client-side user to the server.

SSH Connection Protocol

Multiplexes the encrypted tunnel into several logical channels.

SSH Transport Layer Protocol

Provides server authentication, confidentiality, and integrity. It may optionally also provide compression.

TCP

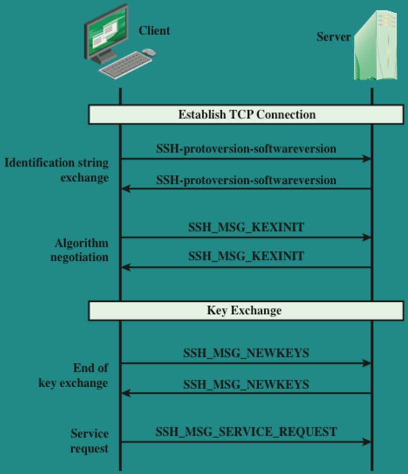
Transmission control protocol provides reliable, connection-oriented end-to-end delivery.

IP

Internet protocol provides datagram delivery across multiple networks.

SSH transport layer packets exchange

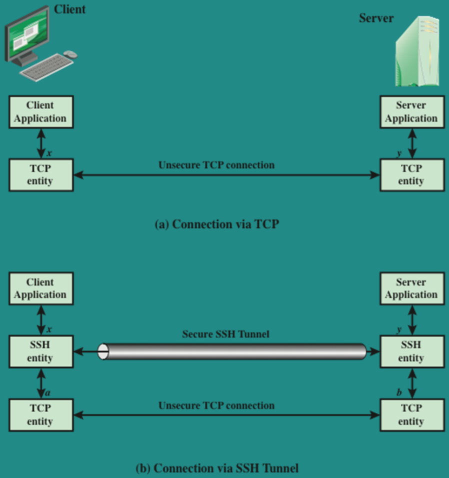
SSH PROTOCOL STACK



SSH protocol stack

SSH PROTOCOL PACKET EXCHANGE

- First, the client establishes a TCP connection to the server.
- This is done via the TCP protocol and is not part of the Transport Layer Protocol.
- Once the connection is established, the client and server exchange packets in the data field of a TCP segment.



SSH protocol packet exchanges

Email Security: MIME and S/MIME

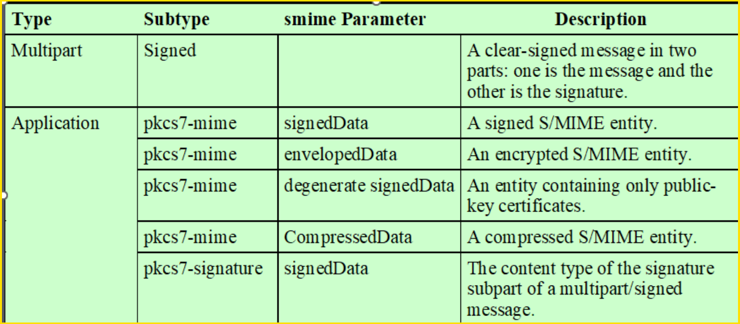
MIME

- Extension to the old RFC 822 specification for mail format
  - ✷ 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

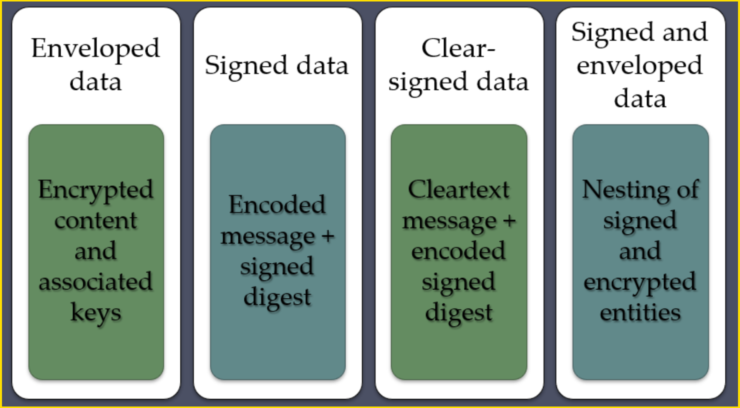
- Secure/Multipurpose Internet Mail Extension
- Security enhancement to the MIME Internet e-mail format
  - ✷ Based on technology from RSA Data Security
- Provides the ability to sign and/or encrypt e-mail messages

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



Enveloped data

Encrypted content and associated keys

Signed data

Encoded message + signed digest

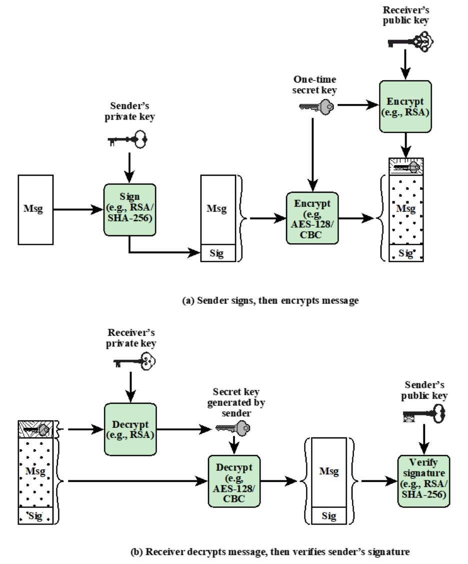
Clear-signed data

Cleartext message + encoded signed digest

Signed and enveloped data

Nesting of signed and encrypted entities

Simplified S/MIME Functional Flow


Receiver's public key
One-time secret key
Encrypt (e.g., RSA)
Sender's private key
Msg
Sign (e.g., RSA/ SHA-256)
Msg
Sig
Encrypt (e.g. AES-128/ CBC
Msg
Sig
(a) Sender signs, then encrypts message
Receiver's private key
Secret key generated by sender
Sender's public key
Msg
Sig
Decrypt (e.g., RSA)
Decrypt (e.g. AES-128/ CBC
Msg
Sig
Verify signature (e.g., RSA/ SHA-256)
(b) Receiver decrypts message, then verifies sender's signature

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

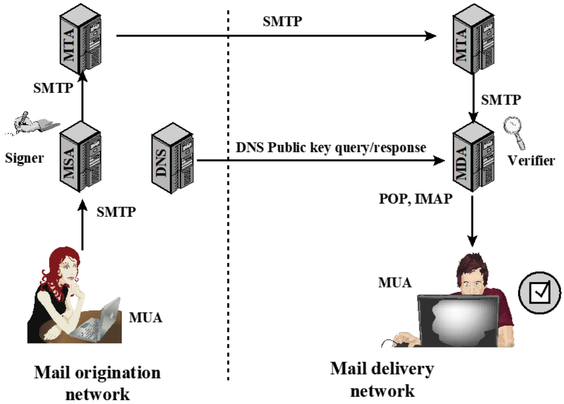
ENVELOPED DATA

- Default algorithms used for encrypting S/MIME messages are AES and RSA
  - ✺ S/MIME generates a pseudorandom secret key to encrypt the message using AES or RSA
  - ✺ 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

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

Simple Example of DKIM Deployment



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

REFERENCES

- The lecture notes and contents were compiled from my own notes and from various sources.
- Figures and tables are from the recommended books
- **Recommended Readings note:** Focus on what was covered in the class. Other parts will come later in other lectures.
  - ✺ Chapter 22,23- Computer Security: Principles and Practice, , William Stallings and Lawrie Brown
  - ✺ Chapter 15, 19- CyBOK, The Cyber Security Body of Knowledge