UNIVERSITY OF WESTMINSTER

Security Controls

6COSC019W- Cyber Security

Dr Ayman El Hajjar

February 19, 2024

School of Computer Science and Engineering
University of Westminster

Outline

Security Controls

SECURITY CONTROL

Control is defined as:

"An action, device, procedure, or other measure that reduces risk by eliminating or preventing a security violation, by minimizing the harm it can cause, or by discovering and reporting it to enable corrective action."

Control Classifications

- Management controls
  - Focus on security policies, planning, guidelines, and standards that influence the selection of operational and technical controls to reduce the risk of loss and to protect the organization's mission
  - These controls refer to issues that management needs to address
- Operational controls
  - Address the correct implementation and use of security policies and standards, ensuring consistency in security operations and correcting identified operational deficiencies
  - These controls relate to mechanisms and procedures that are primarily implemented by people rather than systems
  - They are used to improve the security of a system or group of systems

Control Classifications

- Technical controls
  - Involve the correct use of hardware and software security capabilities in systems
  - These range from simple to complex measures that work together to secure critical and sensitive data, information, and IT systems functions

Control Classes

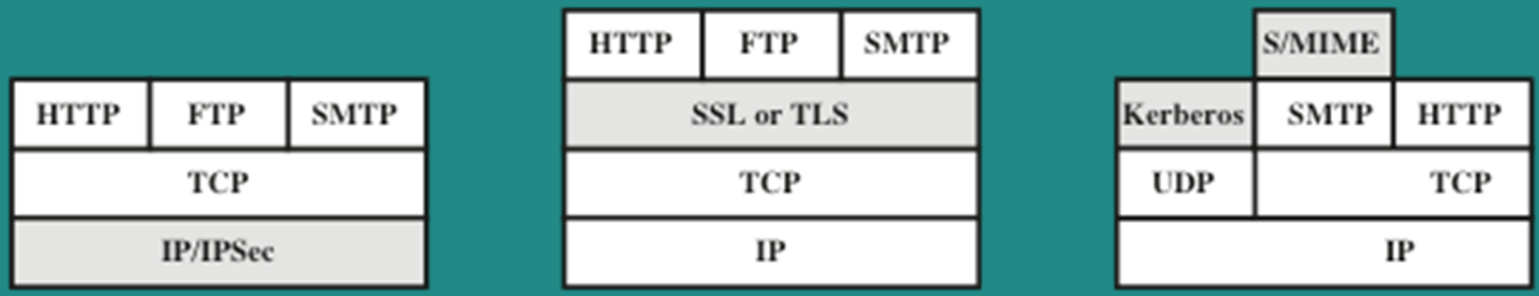
Each of the control classes may include the following:

- Supportive controls
  - Pervasive, generic, underlying technical IT security capabilities that are interrelated with, and used by, many other controls
- Preventative controls
  - Focus on preventing security breaches from occurring, by inhibiting attempts to violate security policies or exploit a vulnerability
- Detection and recovery controls
  - Focus on the response to a security breach, by warning of violations or attempted violations of security policies or the identified exploit of a vulnerability and by providing means to restore the resulting lost computing resources

TECHNICAL CONTROLS- 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

Application layer controls

EMAIL SECURITY: MIME AND S/MIME

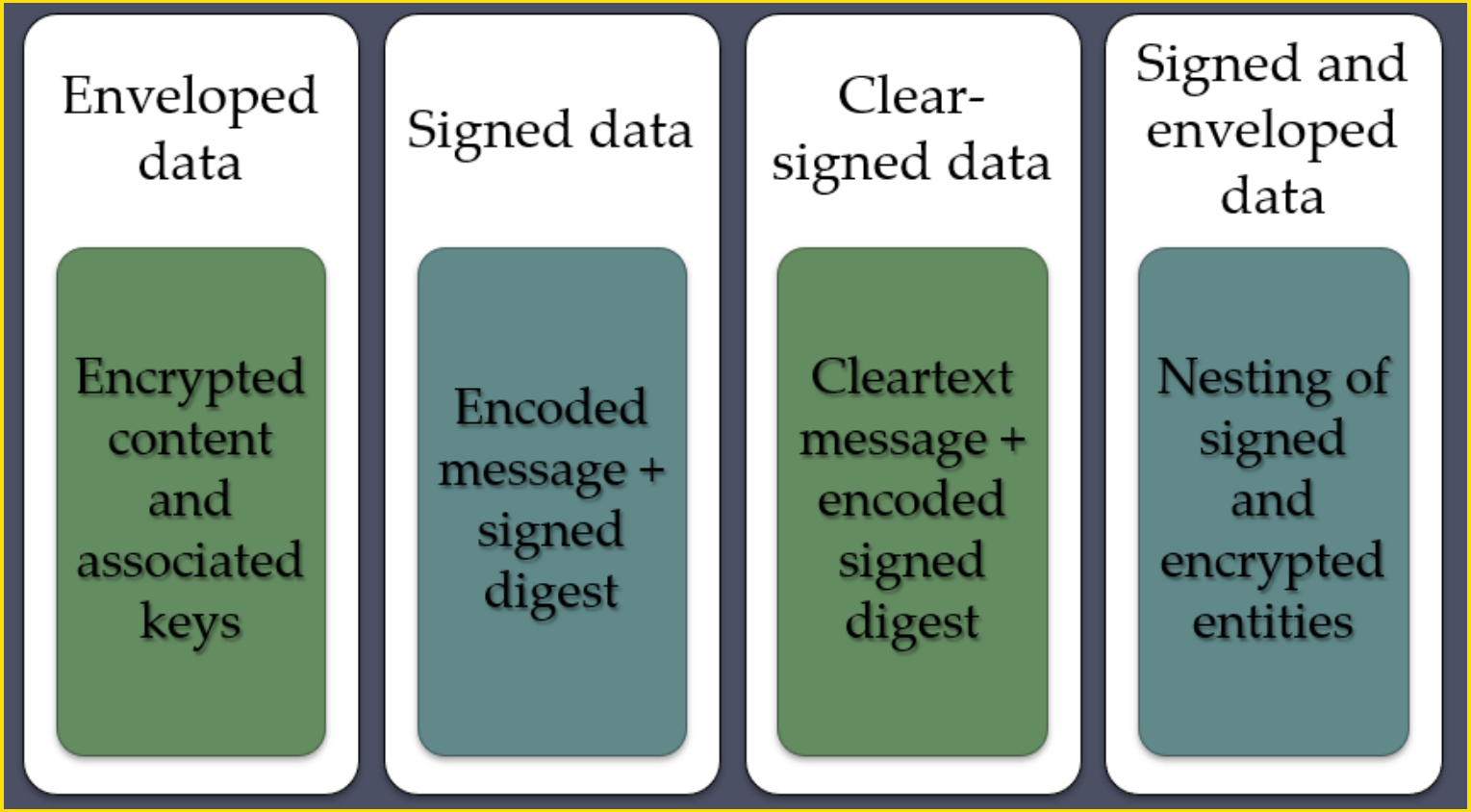
Multipurpose Internet Mail Extension

- 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

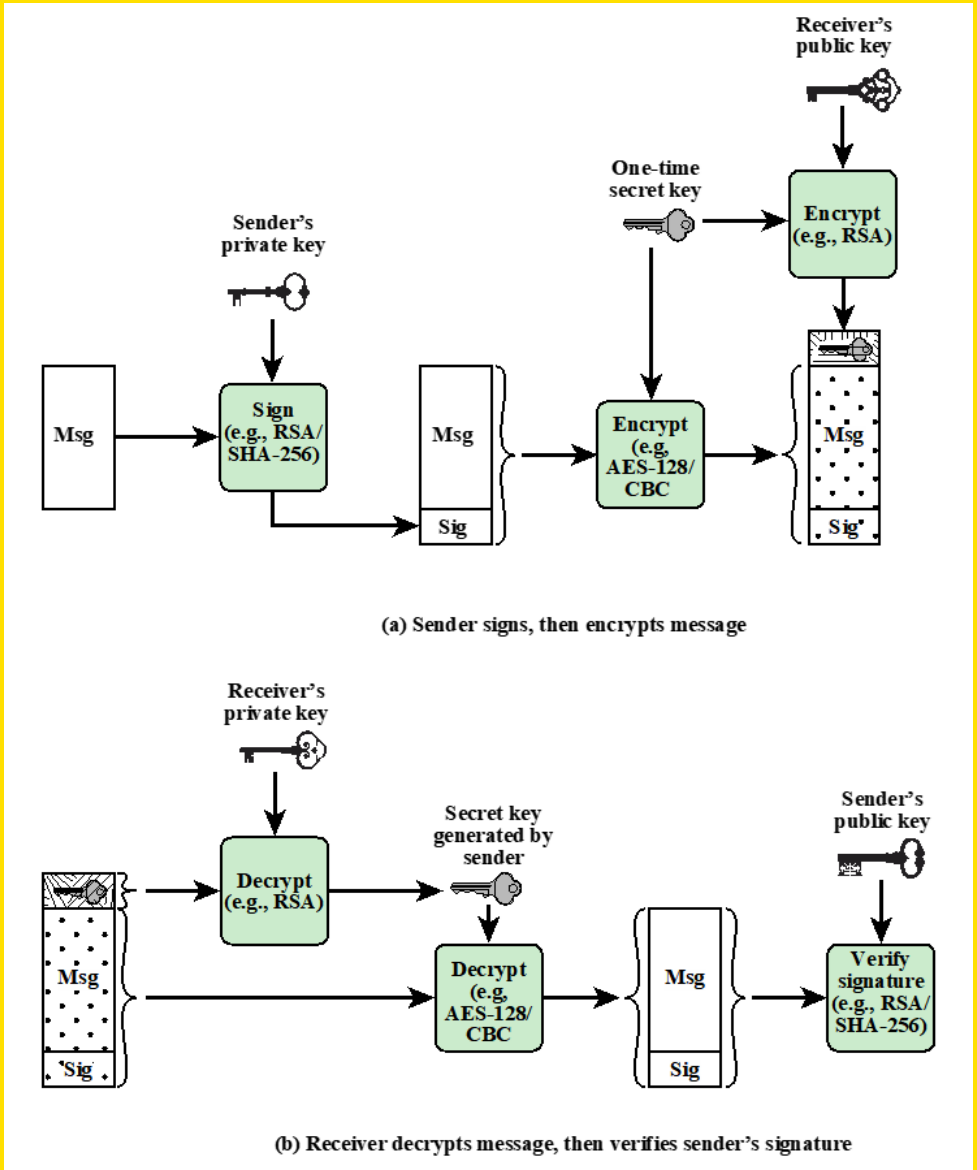
Secure/Multipurpose Internet Mail Extension

- 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 FUNCTIONS



SIMPLIFIED S/MIME FUNCTIONAL FLOW



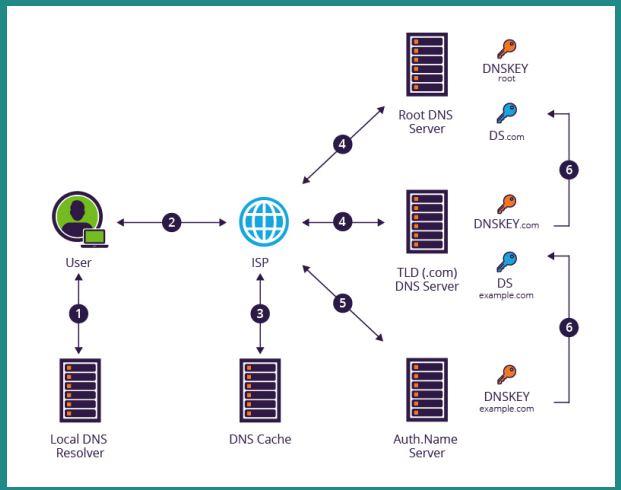
PRETTY GOOD PRIVACY (PGP) CRYPTOGRAPHY

- Another standard for electronic-mail encryption and digital signatures
- Use a Public Private Keys (PPK) method
  - Users can sign one another's public keys, adding some degree of confidence to a key's validity
  - Someone who signs another's public key acts as an introducer for that person to someone else so that if someone trusts the introducer, they should also trust the person who's being introduced
  - Pretty Good Privacy (PGP) is often used to encrypt documents that can be shared via e-mail over the open Internet
- S/MIME and Open PGP use proprietary encryption techniques and handle digital signatures differently

DNS THREATS PREVENTION

- To prevent DNS Hijacking and DNS Pharming, DNS Security (DNSSEC) is deployed to ensure:
  - Authenticity of DNS answer origin
  - Integrity of reply
  - Authenticity of denial of existence
  - Accomplishes this by signing DNS replies at each step of the way
  - Uses public-key cryptography to sign responses

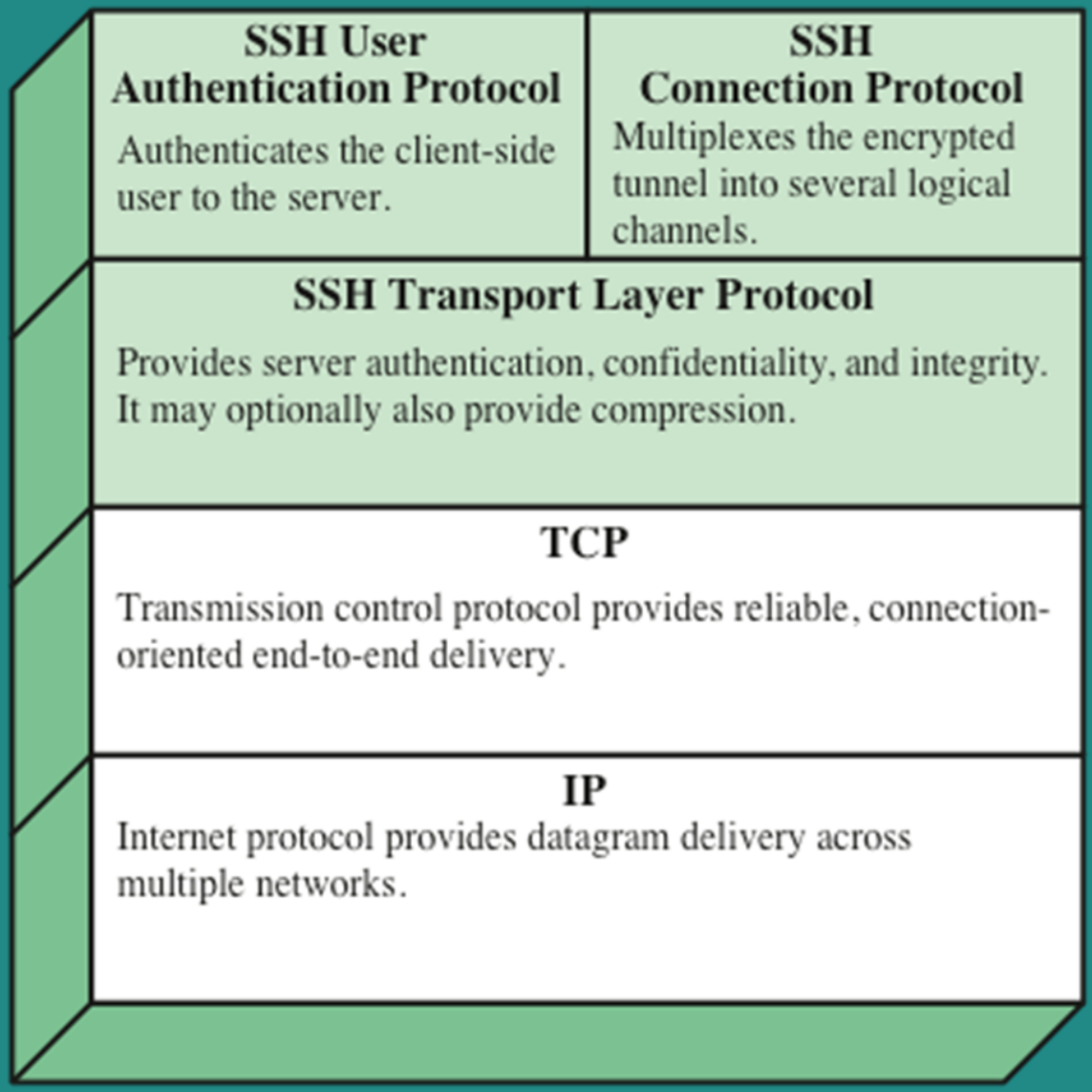
- DNSSEC adds considerable load to dns servers with packet sizes considerably larger than 512 byte size of UDP packets



DNSSEC Signing

SECURE SHELL (SSH)

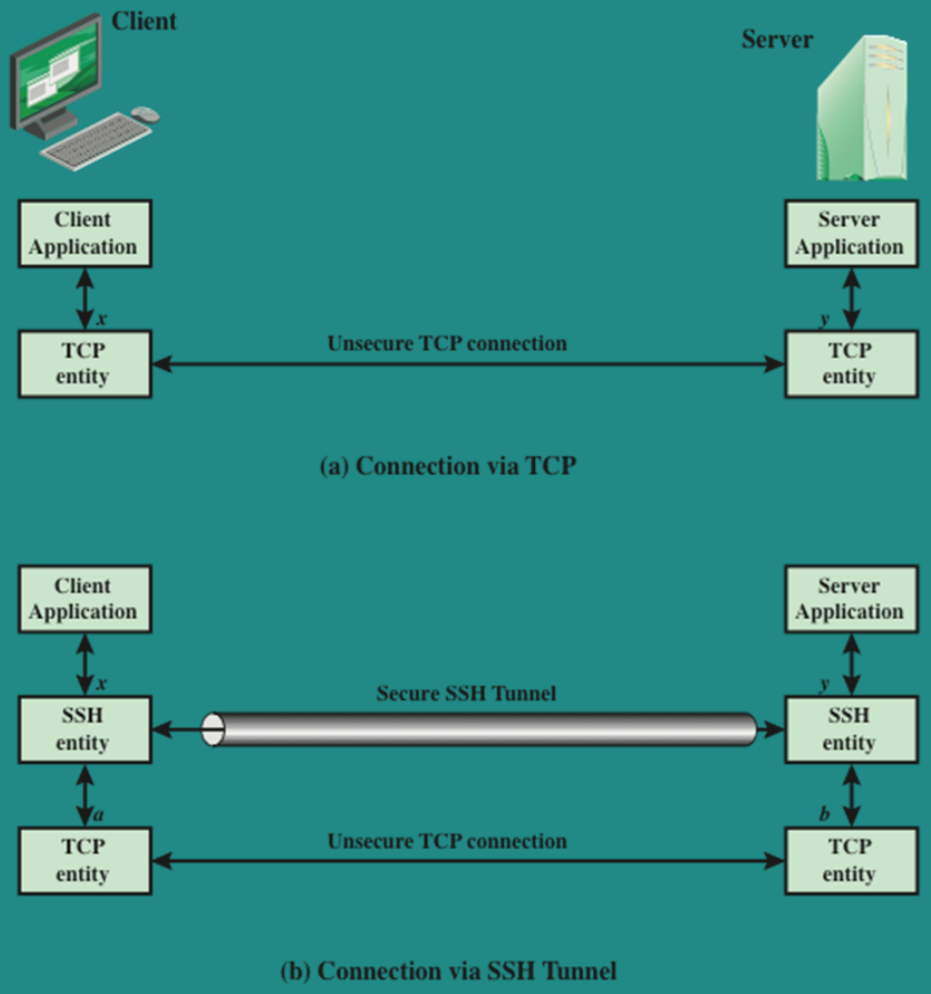
- A protocol for secure network communications designed to be relatively simple and inexpensive to implement
- The initial version, SSH1 was focused on providing a secure remote logon facility to replace TELNET and other remote login schemes that provided no security
- SSH also provides a more general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



SSH transport layer packets exchange

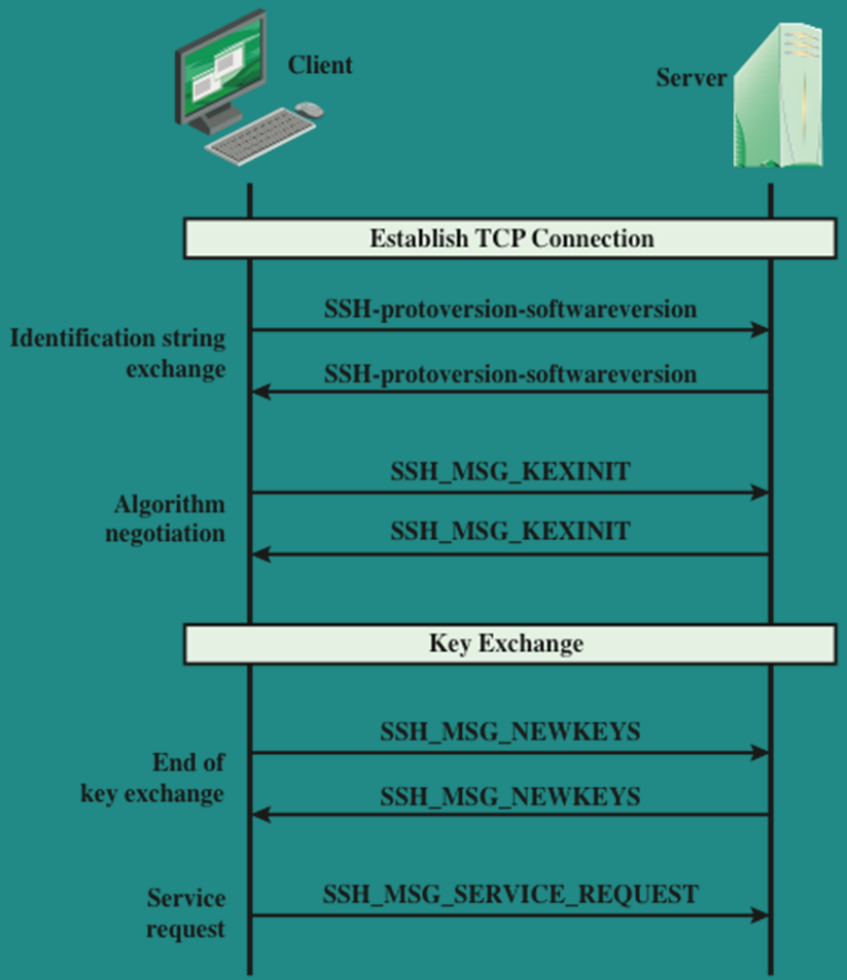
SSH PROTOCOL PACKET EXCHANGE

- 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

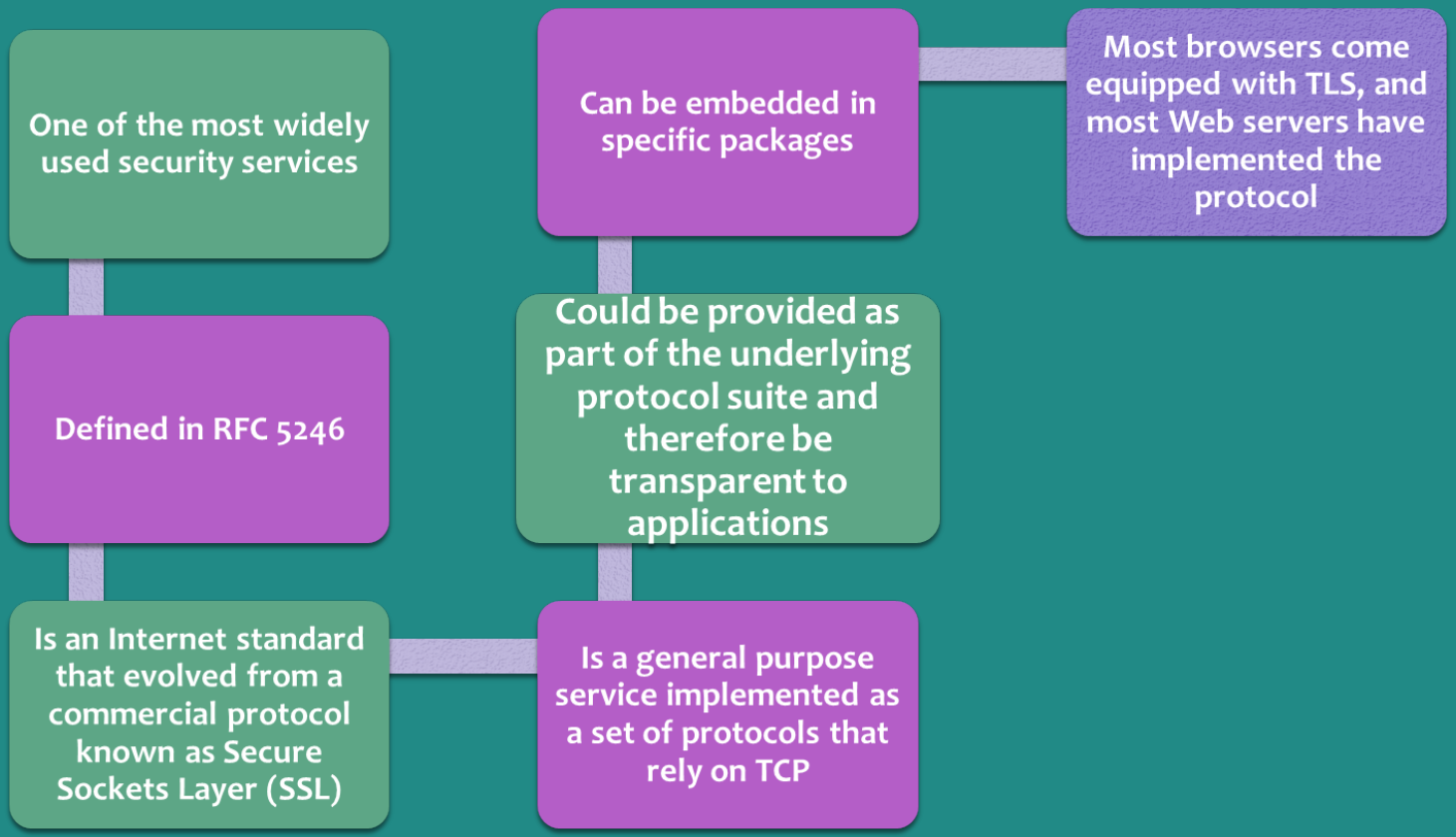
SSH PROTOCOL STACK



SSH protocol stack

Host to Host/Transport layer Controls

TRANSPORT LAYER SECURITY - A DEFINITION



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.

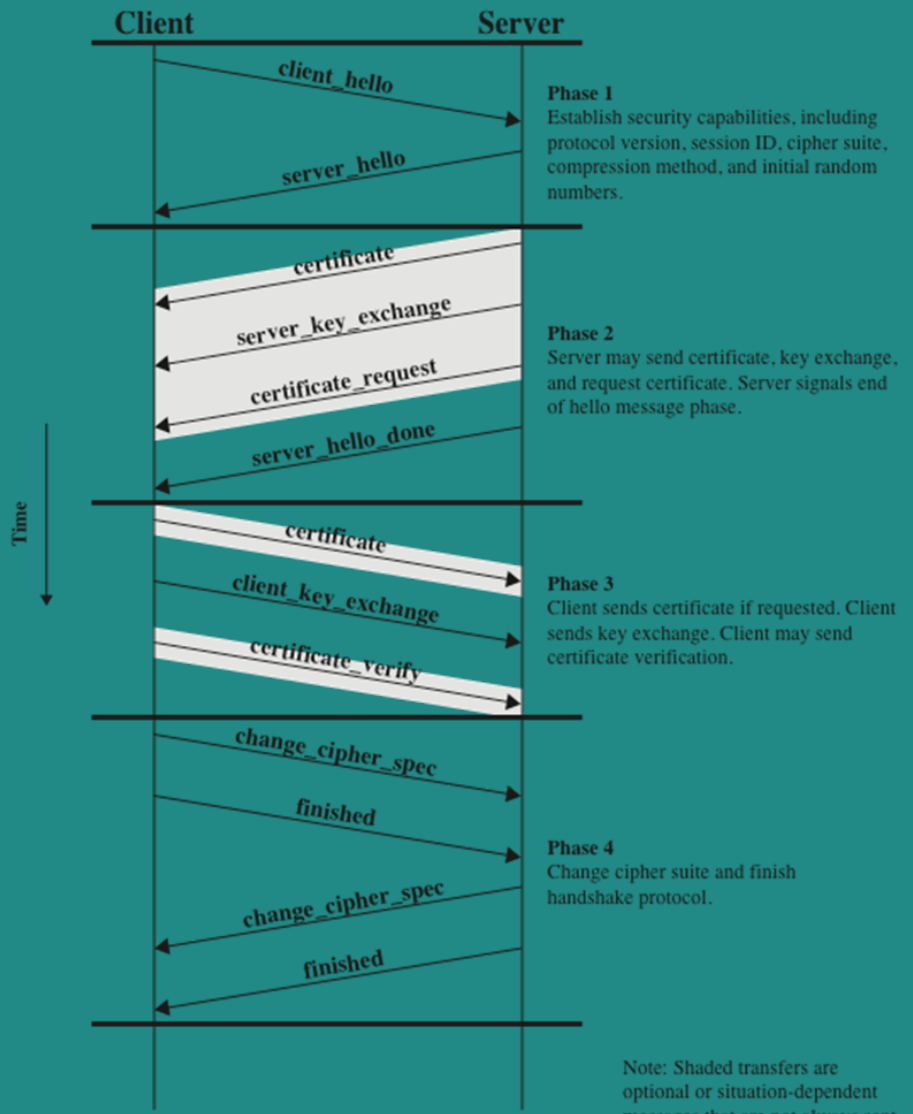
TLS Concepts

- 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 Handshake messages

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

HANDSHAKE PROTOCOL ACTION



HTTPS (HTTP OVER TSL)

- Combination of HTTP and TLS (RFC 2818, HTTP Over TLS) to implement secure communication between a Web browser and a Web server
- Built into all modern Web browsers
  - URL addresses begin with https://
- 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

Network Layer Security

IP Security

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

Security for IP & Networks

- Need to secure the network infrastructure from unauthorised monitoring and control of network traffic
- Need to secure end-user-to-end-user traffic using authentication and encryption mechanisms

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

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/confidentiality)

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

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 unauthorised users do not penetrate the VPN, and (2) assure that eavesdroppers on the Internet cannot read messages sent over the VPN.

Tunnel mode format

REFERENCES

- The lecture notes and contents were compiled from my own notes and from various sources.
- Figures and tables are from the recommended books
- **The lecture notes are very detailed. If you attend the lecture, you should be able to understand the topics.**
- **You can use any of the recommended readings! You do not need to read all the chapters!**
- **Recommended Readings note:** Focus on what was covered in the class.
  - Chapter 13- Attack and Defence, CEH v11 Certified Ethical Hacker Study Guide
  - SQL Injection on Owasp site Link
  - Chapter 8, Malicious Software and Attack Vectors, Fundamentals of Information Systems Security
  - Chapter 15, 16 & 17, CyBOK, The Cyber Security Body of Knowledge