WEB SECURITY

- Almost everything in today’s world relies on computer and internet.
  - Communications (emails, phones)
  - Transportation (car engine system, airplane navigation system)
  - Medicine (medical records, equipments)
  - Shopping (online store, online payments)
  - Entertainment (digital cables)

What is WEB SECURITY ??

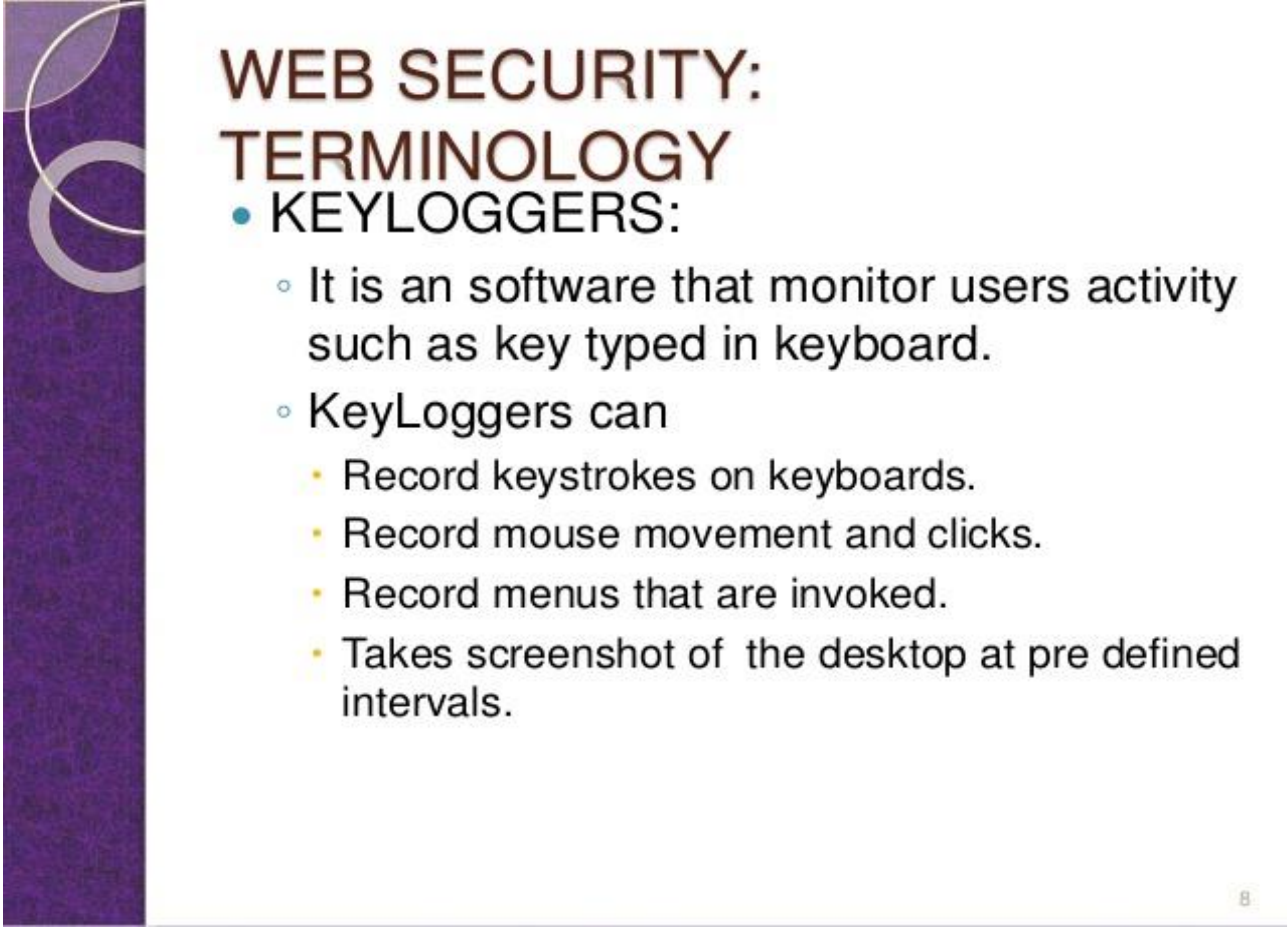
Web security , also known as “***cyber security*** “ involves protecting the information by protecting , preventing and responding to the attacks.

WEB SECURITY: TERMNOLOGY

- HACKERS: People who strive to exploit weaknesses in software and computer for their own gain.
- VIRUSES: Infects your computer before actually u can do something.
- WORMS: Propagates without users intervention.
- TROJAN: A software that claims to do something while in fact doing something in background.

WEB SECURITY: TERNINOLOGY

- RANSOMWARE:
  - A form of Trojan that has been since 1989, as known as ‘PC CYBORG’ Trojan.
  - It affects the user computer by encrypting the user’s personal files.
  - The victim then contacted and offered the decrypt key in exchange of cash.



WEB SECURITY: TERMINOLOGY

- KEYLOGGERS:
  - It is an software that monitor users activity such as key typed in keyboard.
  - KeyLoggers can
    - Record keystrokes on keyboards.
    - Record mouse movement and clicks.
    - Record menus that are invoked.
    - Takes screenshot of the desktop at pre defined intervals.

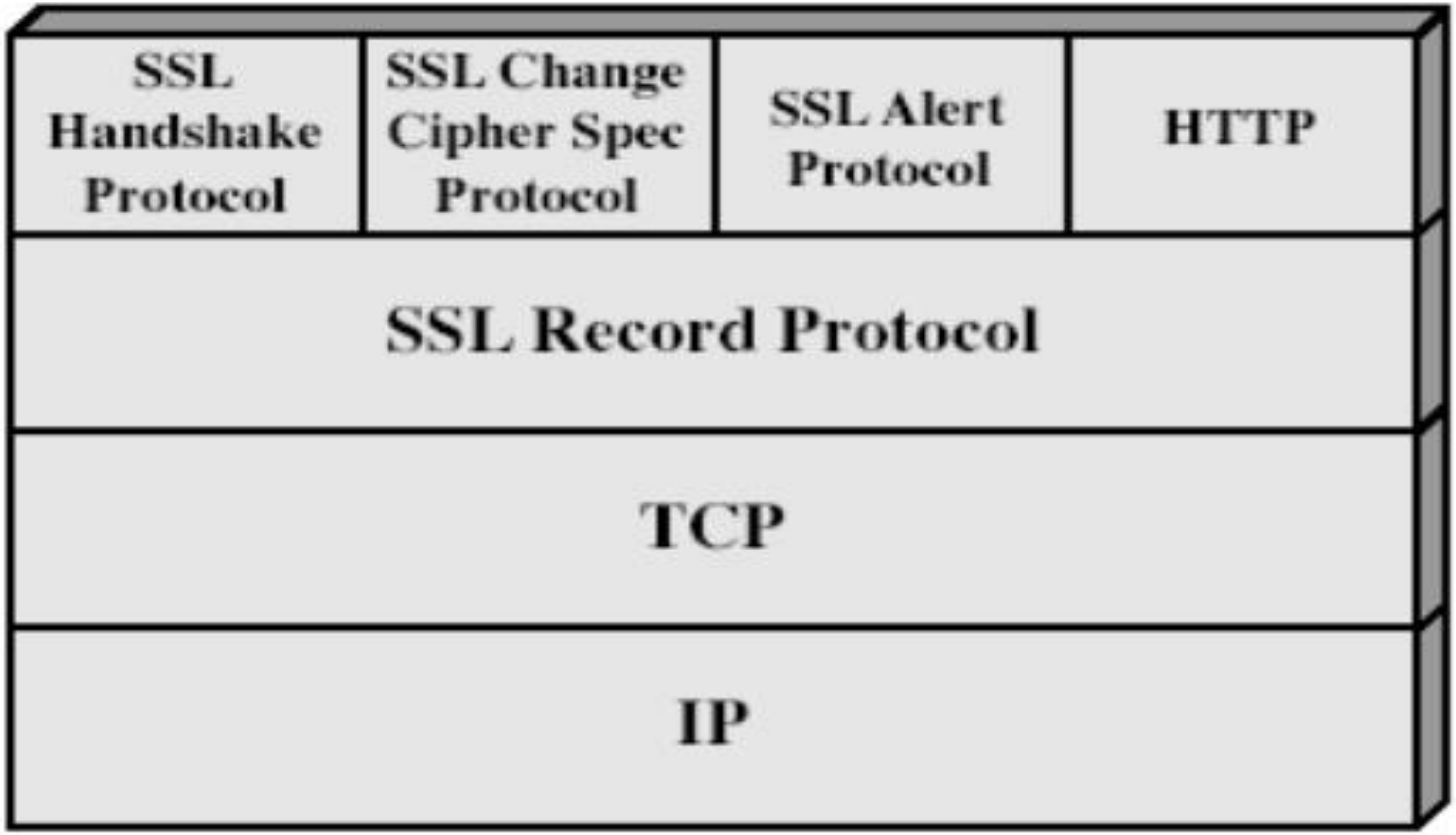
Web Security

- 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.

What is SSL?

- SSL – Secure Socket Layer ƒt provides a secure transport connection between applications (e.g., a web server and a browser)
- SSL was developed by Netscape
- uses TCP to provide a reliable end-to-end service
- SSL has two layers of protocols SSL v3.0 was specified in an Internet Draft (1996) ƒt evolved into RFC 246 and was renamed to TLS (Transport Layer Security)
- TLS can be viewed as SSL v3.1

SSL Architecture



SSL Handshake Protocol

SSL Change Cipher Spec Protocol

SSL Alert Protocol

HTTP

SSL Record Protocol

TCP

IP

SSL Components

SSL HANDSHAKE PROTOCOL	SSL RECORD PROTOCOL	SSL ALERT PROTOCOL	SSL CHANGE CIPHER SPEC PROTOCOL
• Negotiation of security algorithms and parameters. • Key exchange. • Server authentication and optionally client authentication.	• Fragmentation. • Compression. • Encryption. • Message authentication and integrity protection.	• Error message (fatal alerts and warning)	• A single message that indicates the end of SSL handshake.

Sessions and Connections

- An SSL session is a connection between client and server.
- Sessions are stateful ; the session state includes security algorithm and parameters.
- A session may include multiple secure connection between same server and client.
- Connections of the same session share the session state.
- Sessions are used to avoid expensive negotiation of new security parameters for each state.

Session States…

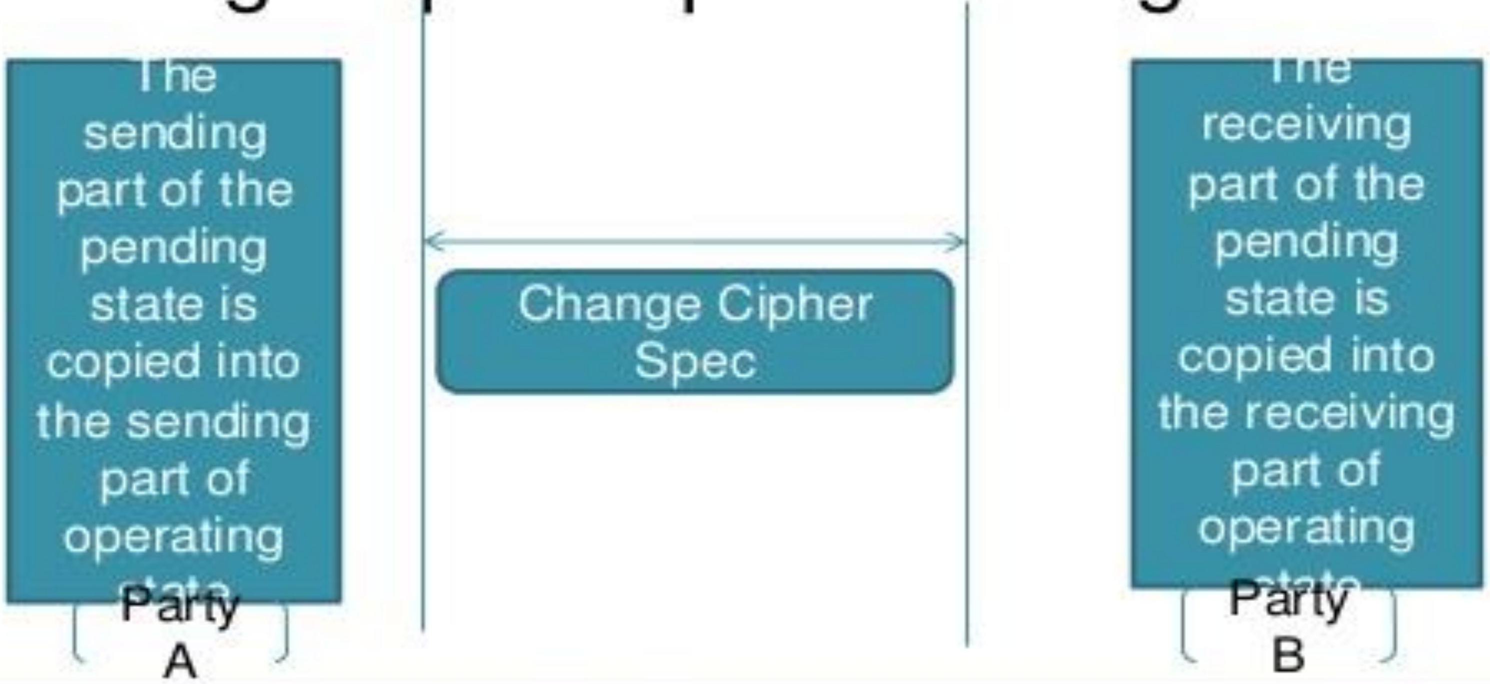
- Session state
  - Session identifier – arbitrary byte sequence chosen by the server to identify the session.
  - Peer certificate – may be null.
  - Compression method.
  - Cipher Spec – bulk data encryption algorithm and MAC algorithm (eg. DES, MD5).
  - Master key – a 48 byte secret key is used in between client and server.
  - Resumable – a flag indicating whether the session can be used to initiate new connections.

Connection States…

- Connection State
  - Server and client random – random byte sequence is chosen by the client and server for new connection.
  - Server write MAC secret – secret key is used in MAC operations on data sent by the server.
  - Client write MAC secret – secret key is used in MAC operations on data sent by the client.
  - Server write key – secret encryption key for data, encrypted by the server.
  - Client write key – secret encryption key for data, encrypted by the client.

How States changes??

- Operating state: current using state
- Pending state: state to be used
- Operating state < Pending state: at the transmission and reception of change cipher spec message



The sending part of the pending state is copied into the sending part of operating state

Party A

Change Cipher Spec

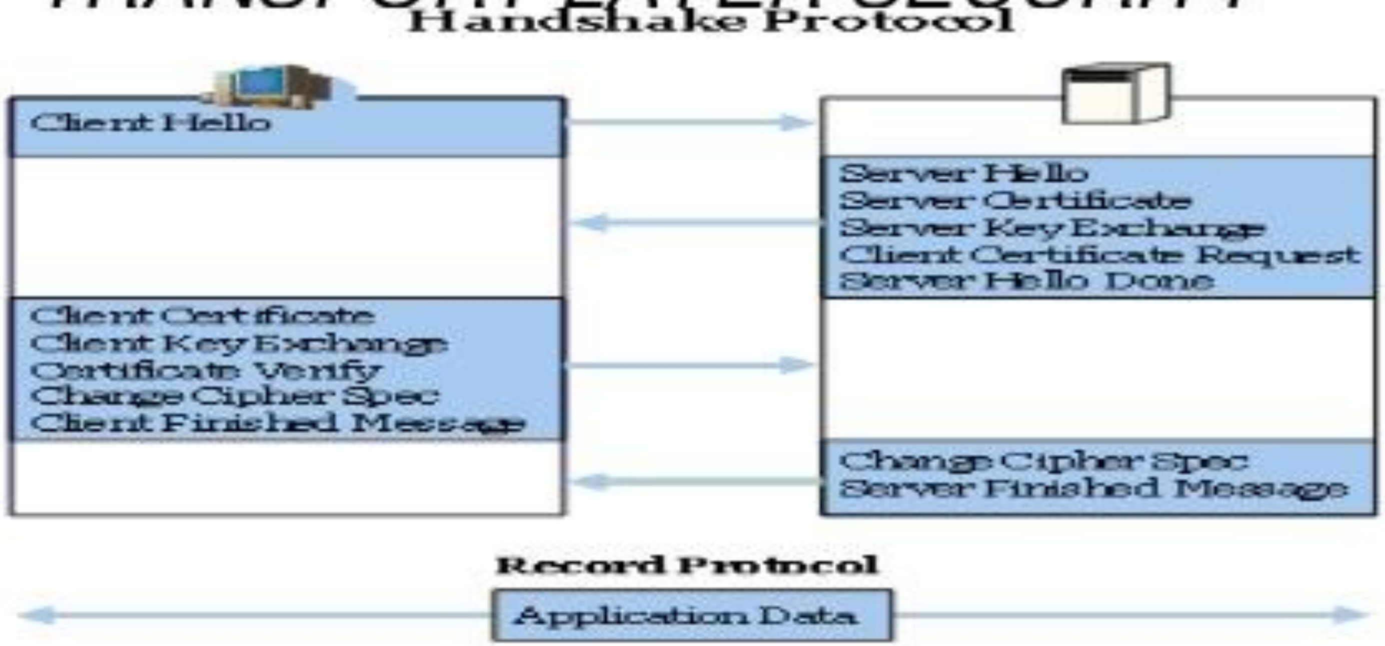
The receiving part of the pending state is copied into the receiving part of operating state

Party B

- **SSL session**
  - an association between client & server
  - created by the Handshake Protocol
  - define a set of cryptographic parameters
  - may be shared by multiple SSL connections
- **SSL connection**
  - a transient, peer-to-peer, communications link
  - associated with 1 SSL session

SSL Handshake Protocol

- Handshake protocol is used to exchange all the information required by both sides for the exchange of actual application data by the *TRANSPORT LAYER SECURITY*



Handshake Protocol

Client Hello

Server Hello
Server Certificate
Server Key Exchange
Client Certificate Request
Server Hello Done

Client Certificate
Client Key Exchange
Certificate Verify
Change Cipher Spec
Client Finished Message

Change Cipher Spec
Server Finished Message

Record Protocol

Application Data

SSL Record Protocol

- **confidentiality**
  - using symmetric encryption with a shared secret key defined by Handshake Protocol
  - IDEA, RC2-40, DES-40, DES, 3DES, Fortezza, RC4-40, RC4-128
  - message is compressed before encryption
- **message integrity**
  - using a MAC with shared secret key
  - similar to HMAC but with different padding

SSL Change Cipher Spec Protocol

- one of 3 SSL specific protocols which use the SSL Record protocol
- a single message
- causes pending state to become current
- hence updating the cipher suite in use.

SSL Alert Protocol

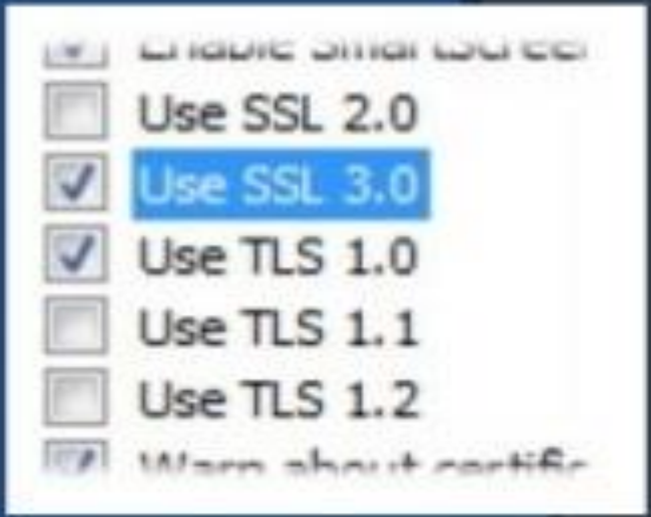
- conveys SSL-related alerts to peer entity
- severity
  - warning or fatal
- specific alert
  - unexpected message, bad record mac, decompression failure, handshake failure, illegal parameter
  - close notify, no certificate, bad certificate, unsupported certificate, certificate revoked, certificate expired, certificate unknown
- compressed & encrypted like all SSL data

Web security

- Web is now widely used by businesses, government firms and individuals.
- but Internet & Web space are vulnerable.
- have a variety of threats related to
  - **Integrity** : Someone might alter content
  - **Confidentiality** : Anyone can see content
  - **Denial of service**
  - **Authentication** : Not clear who you are talking with
- need added security mechanisms

Introduction (contd.)

- **Secure Sockets Layer (SSL)**
  - Developed by Netscape Corporation
  - Versions 1, 2, and 3 (released in 1996)
- **Transport Layer Security (TLS)**
  - Successor of SSL
  - IETF standards track protocol, based on SSL 3.0
  - Last updated in RFC 5246 (2008)



☑ Enable SmartScree

□ Use SSL 2.0

☑ Use SSL 3.0

☑ Use TLS 1.0

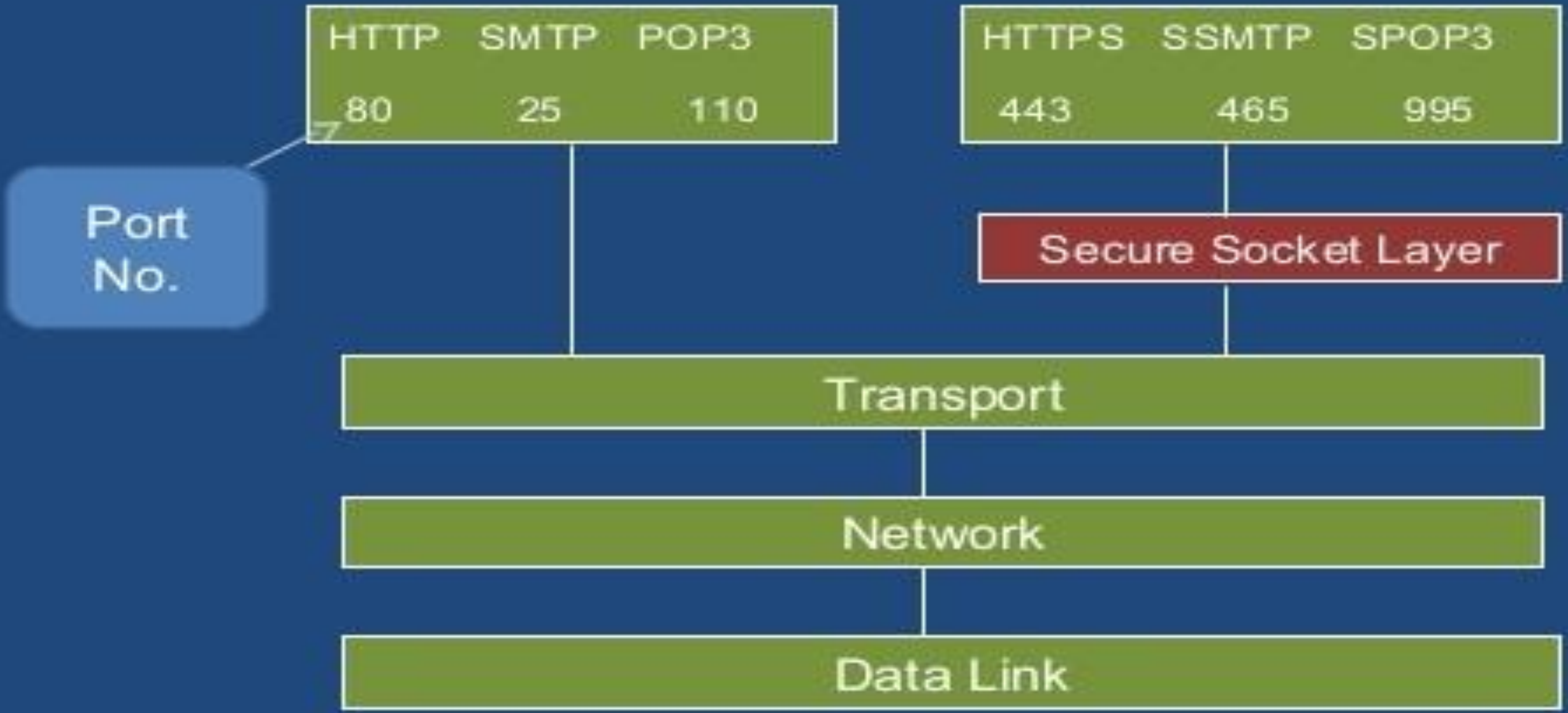
□ Use TLS 1.1

□ Use TLS 1.2

☑ Warn about certific

SECURE SOCKET LAYER (SSL)

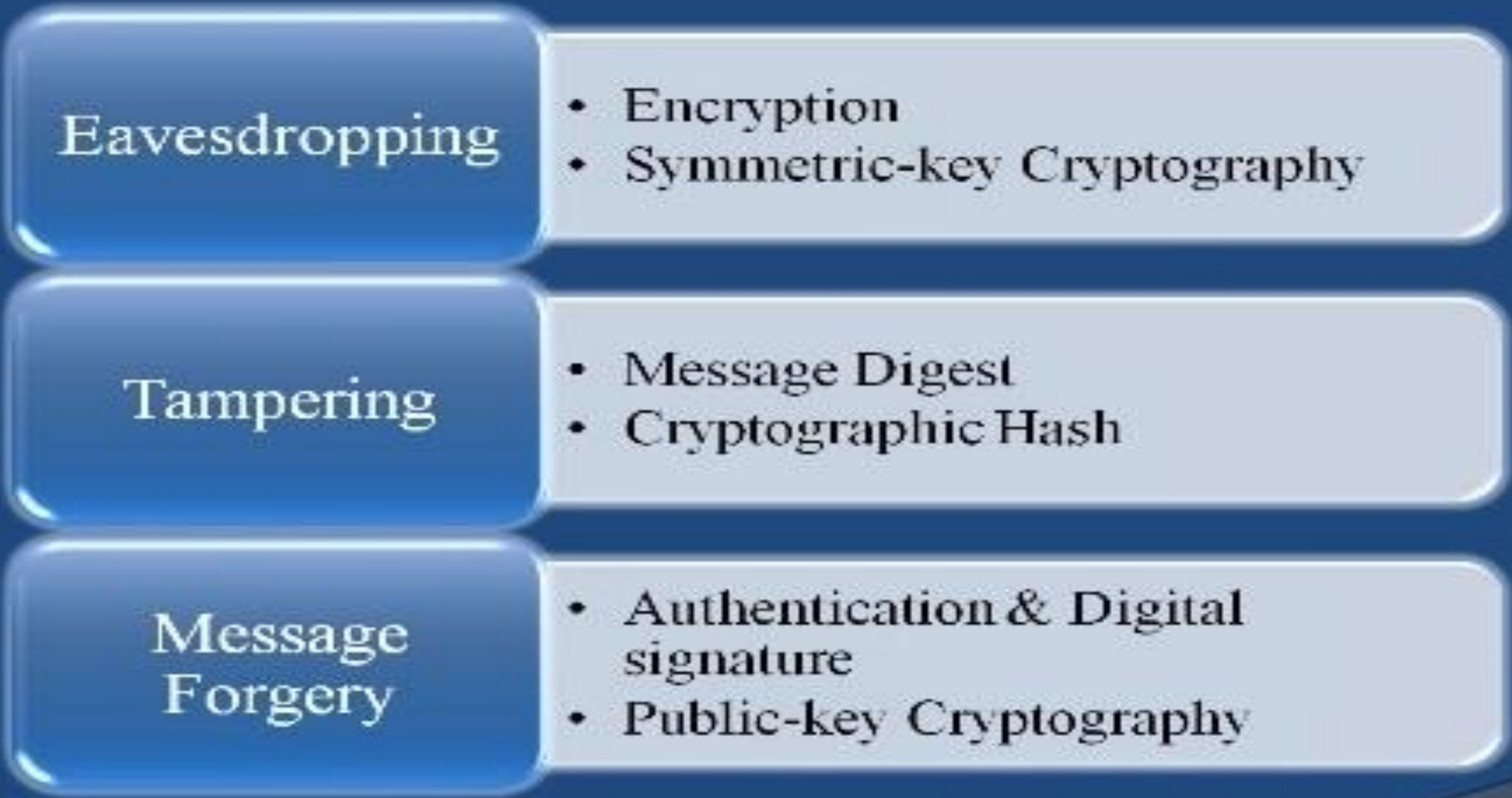
Where SSL fits?



What security is provided?

- **By providing:**
  - Endpoint Authentication
  - Unilateral or Bilateral
  - Communication Confidentiality
- **For preventing:**
  - Eavesdropping
  - Tampering
  - Message Forgery

How security is provided?



Eavesdropping

- Encryption
- Symmetric-key Cryptography

Tampering

- Message Digest
- Cryptographic Hash

Message Forgery

- Authentication & Digital signature
- Public-key Cryptography

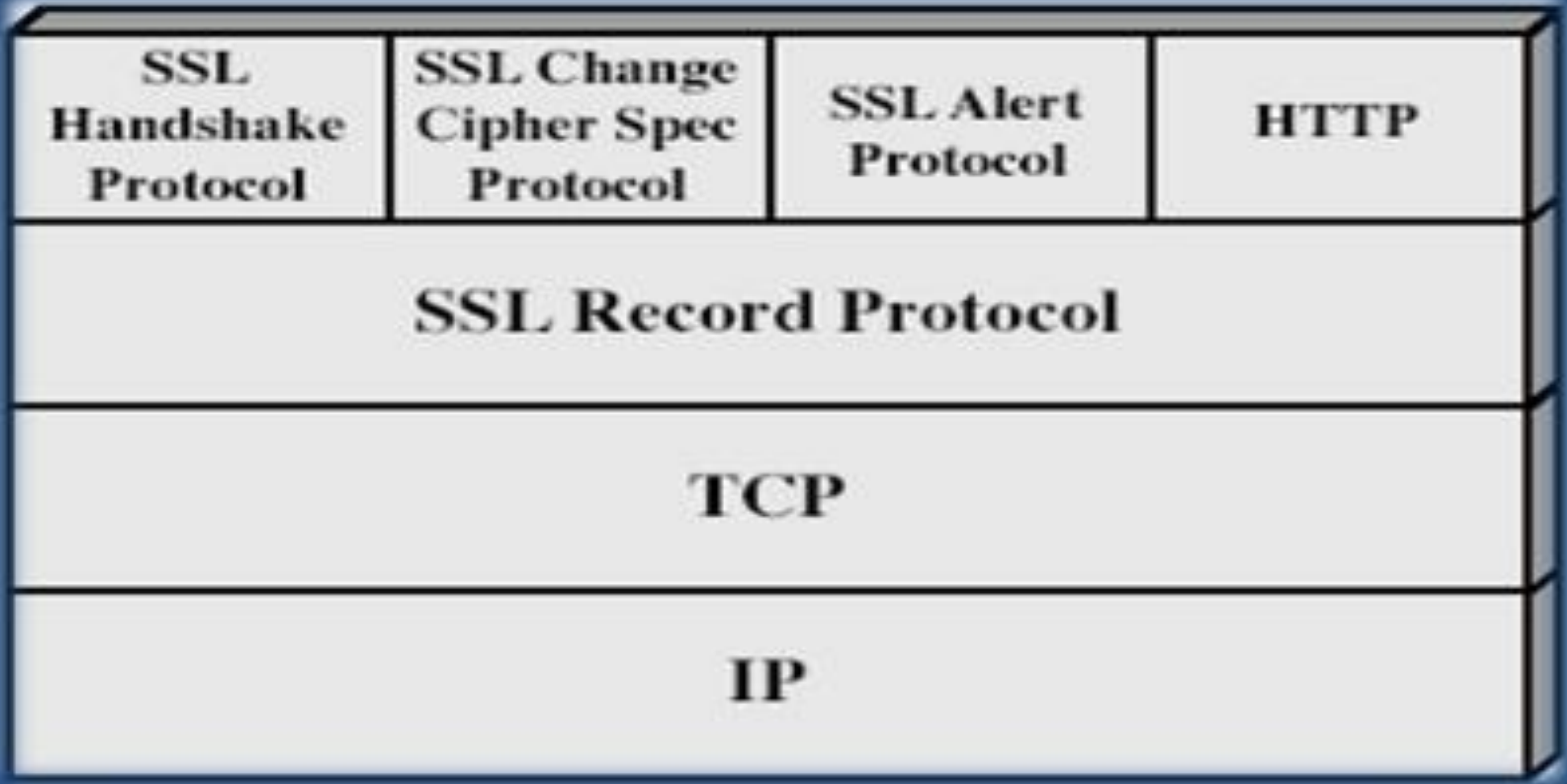
Uses public key scheme

- Each client-server pair uses
  - 2 public keys
    - one for client (browser)
      - created when browser is installed on client machine
    - one for server (http server)
      - created when server is installed on server hardware
  - 2 private keys
    - one for client browser
    - one for server (http server)

Cipher Suite

- **Common Cipher Suite algorithms:**
  - Encryption algorithm
    - RC4,Triple DES,AES, IDEA, DES, Camellia
  - Message authentication code (MAC) algorithm
    - Authentication by RSA, DSA, ECDSA
    - Hashing by MD5, SHA
  - Key exchange algorithm
    - RSA, Diffie-Hellman, ECDH, SRP, PSK
  - Pseudorandom function (PRF)

SSL Architecture



SSL Handshake Protocol

SSL Change Cipher Spec Protocol

SSL Alert Protocol

HTTP

SSL Record Protocol

TCP

IP

The Four Upper Layer Protocols

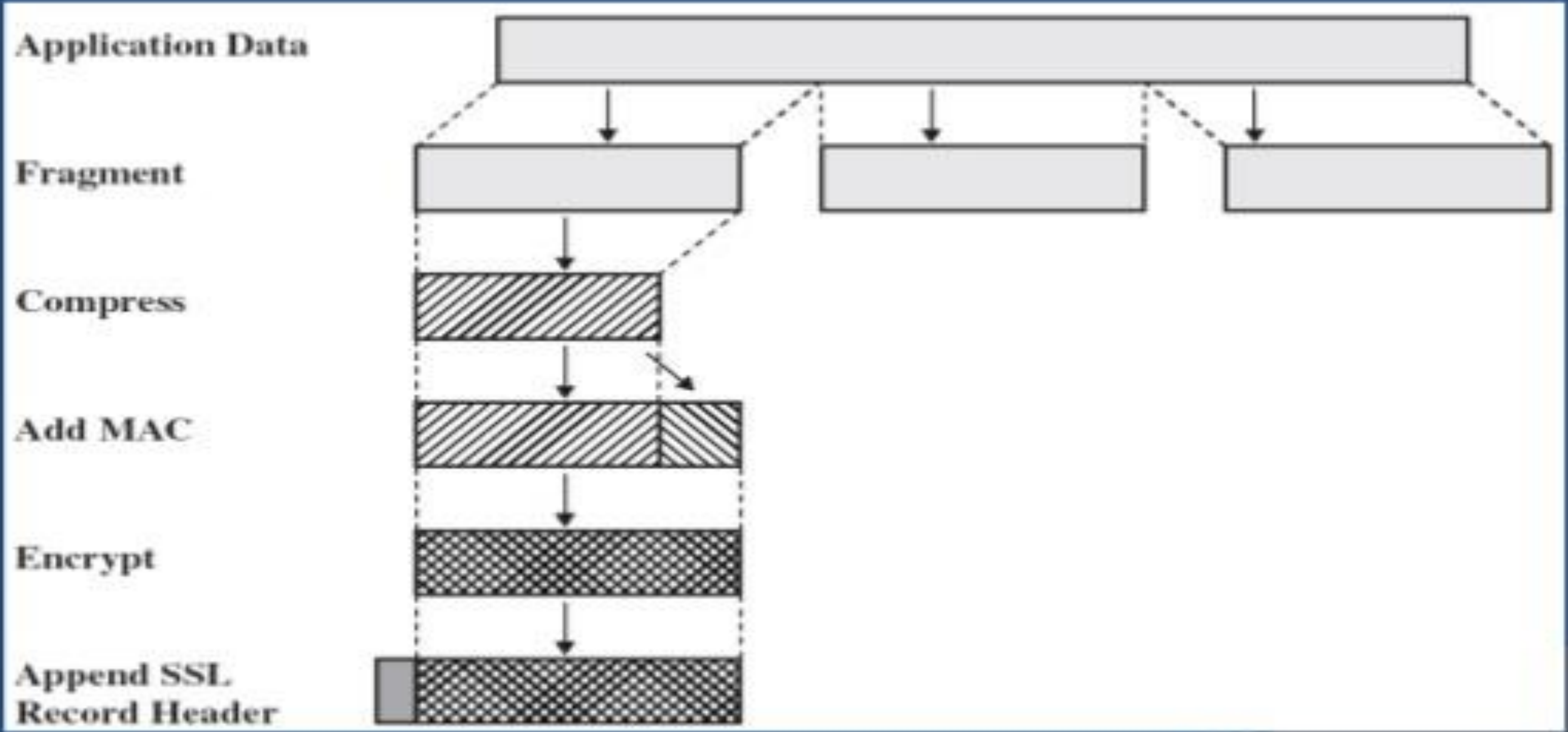
- Application Encryption Protocol
  - Encrypt/Decrypt application data
- Change Cipher Spec Protocol
  - Alert to a change in communication variables
- Alert Protocol
  - Messages important to SSL connections
- Handshaking Protocol
  - Establish communication variables

SSL Record Protocol

Services provided are :

- **Confidentiality**
  - using symmetric encryption with a shared secret key defined by Handshake Protocol
  - IDEA, RC2-40, DES-40, DES, 3DES, Fortezza, RC4-40, RC4-128
  - message is compressed before encryption
- **Message integrity**
  - using a MAC (Message Authentication Code) created using a shared secret key and a short message

SSL Record Protocol (Contd.)



SSL Change Cipher Spec Protocol

- one of 3 SSL specific protocols which use the SSL Record protocol
- a single message
- Purpose of message
  - Cause copy of pending state to current state.
  - Updates cipher suite to be used on the current connection .

SSL Alert Protocol

- conveys SSL-related alerts to peer entity
- Consists of two bytes
  - 1st byte : warning or fatal
  - 2nd byte: code for specific alerts
- specific alert types
  - unexpected message, bad record mac, decompression failure, handshake failure, illegal parameter
  - close notify, no certificate, bad certificate, unsupported certificate, certificate revoked, certificate expired, certificate unknown
- compressed & encrypted like all SSL data

SSL Handshake Protocol (1/10)

- The most complex part of SSL.
- allows server & client to:
  - authenticate each other
  - to negotiate encryption & MAC algorithms
  - to negotiate cryptographic keys to be used
- comprises a series of messages in phases
  - Establish Security Capabilities
  - Server Authentication and Key Exchange
  - Client Authentication and Key Exchange
  - Finish

Simple Handshake process (2/10)

- The client(Alice) and server(Bob) must agree on various parameters to establish the connection
  - Alice request a secure connections and presents a list of Cipher Suites
  - Bob picks the strongest supported Cipher Suite
  - Bob sends back his digital certificate
    - Including the certificate authority and his public key
  - By encrypting using the server's public key, Alice send a random number to Bob securely
  - Alice and Bob generate key material from the random number
  - Secure connection established