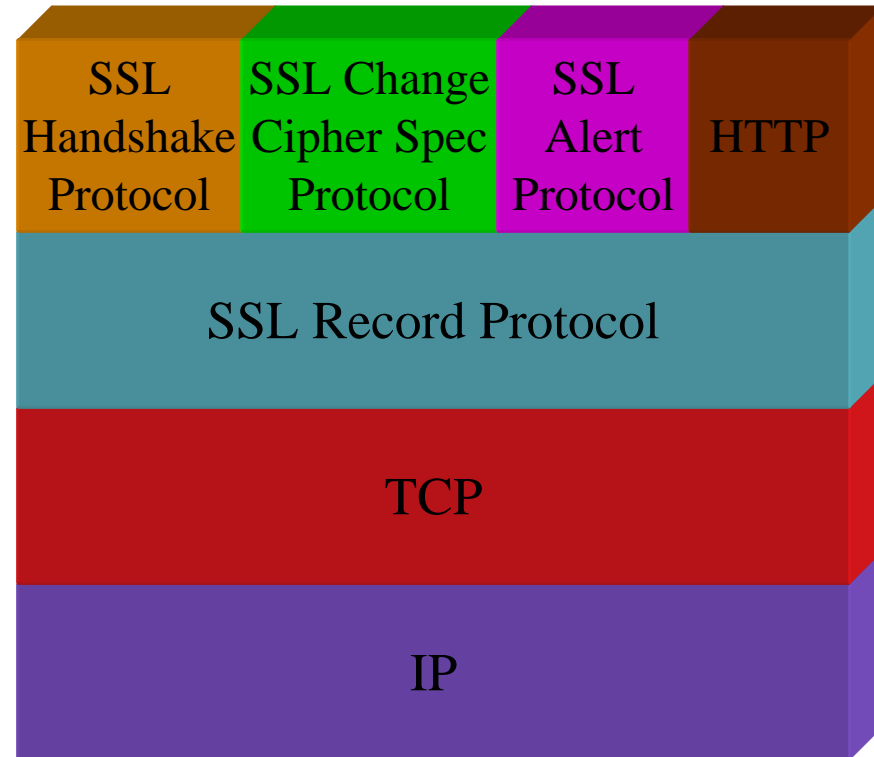


# More on SSL

---

# Secure Socket Layer (SSL)

- Makes use of TCP to provide reliable, secure end-to-end network service.
- Two layers of protocols:
  - SSL Record Protocol: transport.
  - Higher-layer protocols for connection negotiation & alerts.
- SSL connection: basically a secure stream within a session.
- SSL session: association between client and server.



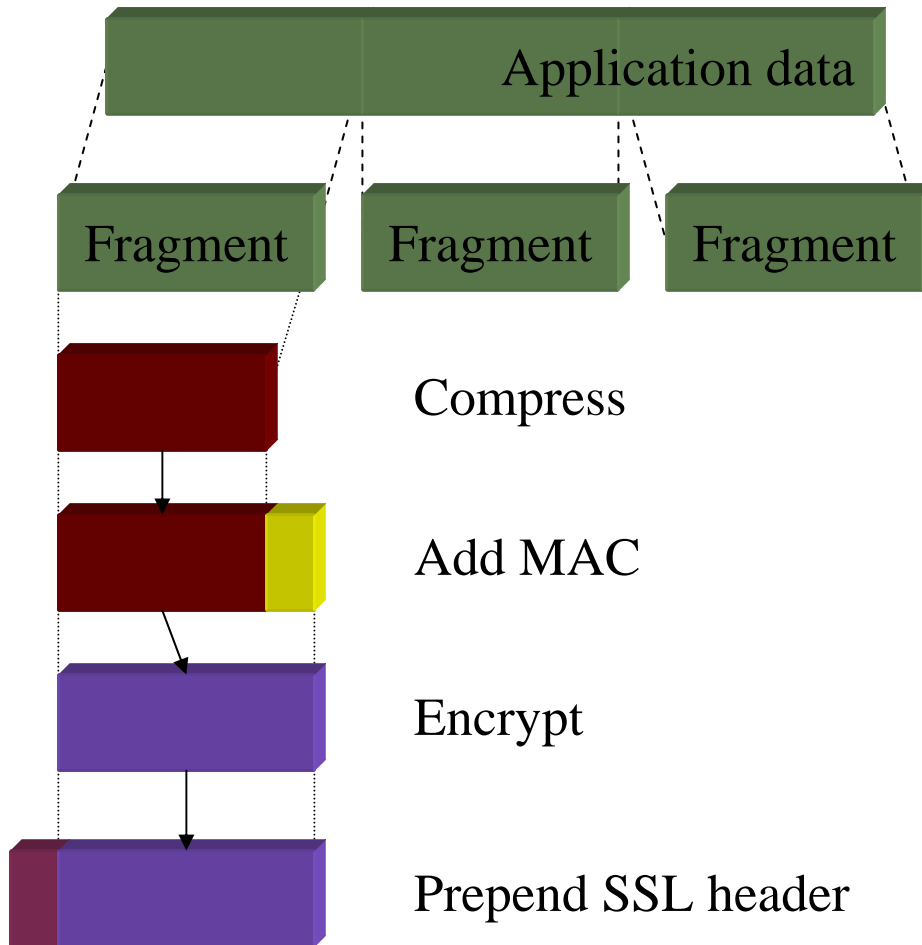
# SSL session state

Session identifier	Arbitrary byte sequence chosen by server to identify the session state.
Peer certificate	X509.v3 certificate of the peer (may be null).
Compression method	Algorithm used to compress data prior to encryption.
Cipher spec	Specifies the bulk data encryption algorithm (null, DES, etc.) and hash algorithm used for MAC calculation. Also includes other cryptographic attributes such as hash_size.
Master secret	48 byte secret shared between client and server.
Is resumable?	Flag indicating whether the session can be used to initiate new connections.

# SSL connection state

Server & client random	Byte sequences chosen by server & client for each connection.
Server write MAC secret	Key used in MAC operations over data sent by the server.
Client write MAC secret	Key used in MAC operations over data sent by the client.
Server write key	Encryption key for data sent by server.
Client write key	Key for data sent by client.
Initialization vectors	Used to initialize encryption for data sent in CBC mode.
Sequence numbers	Maintained by each party for transmitted and received information. May not exceed $2^{64}-1$ .

# SSL Record Protocol



- Data fragmented into blocks of  $2^{14}$  bytes or less.
- Compression applied (optionally).
- MAC calculated.
- Payload & MAC encrypted.
- Header prepended:
  - content type,
  - major & minor version,
  - compressed length.

# Change Cipher Spec Protocol

---

- A single message that contains a single byte.
- A signal that the pending state should be copied into the current state:
  - Updates the cipher information used by this connection.
  - The state must have been set by the Handshake Protocol (more on this in a bit).

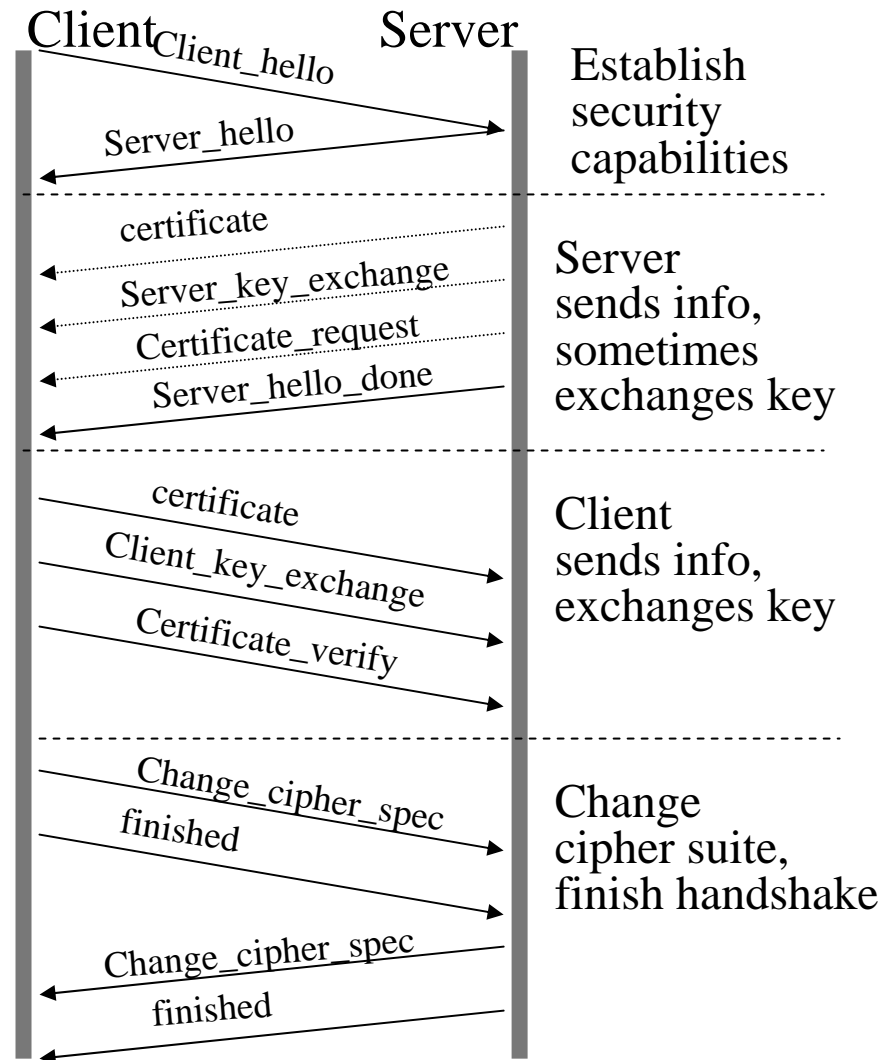
# SSL Alert Protocol

---

- Conveys SSL-related alerts (compressed and encrypted).
- Each message consists of exactly two bytes:
  - Level: severity of the alert (warning or fatal).
  - Alert code: what kind of alert is this?
    - unexpected message,
    - bad record MAC,
    - decompression failure,
    - handshake failure,
    - ...

# SSL Handshake Protocol

1. Establish security capabilities:
  1. Exchange information.
  2. Find common ground for secure message exchange.
2. Authenticate server.
3. Authenticate client.
4. Finish.



# Does it work?

---

- SSL has undergone lots of informal examination.
- There have also been systematic but informal analyses of SSL and some partial proofs.
- Now and then, some problematic issue is pointed out.
- It is just at the edge of what we can understand.
- It has no complete formal specification.

# Other issues

---

- SSL slows down servers.
- SSL “breaks” caching and complicates virtual hosting (multiple IP addresses for the same host).
- SSL protects data in transit, but not databases.
- SSL is a two-party protocol (unlike SET).