CS 465

TLS

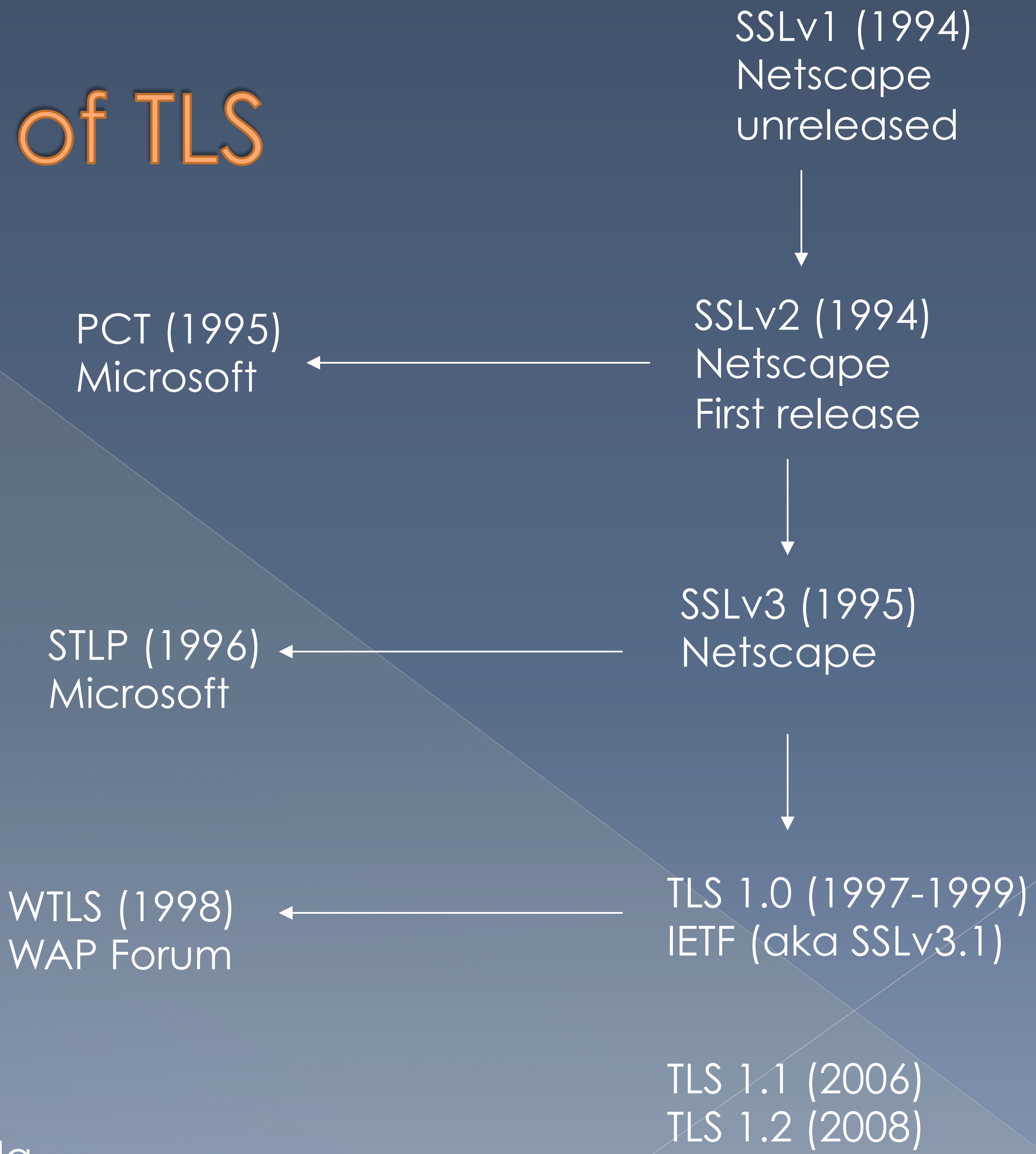
Slides by Kent Seamons and Tim van der Horst
Last Updated: Oct 8, 2012

TLS

Student Learning Goals

- Understand TLS handshake
- Understand client/server authentication in TLS
  - RSA key exchange
  - Explain ownership proofs in detail
  - What cryptographic primitives are used and why?
- Understand session resumption
- Understand the limitations of TLS

Genesis of TLS



SSLv1 (1994)
Netscape
unreleased

SSLv2 (1994)
Netscape
First release

PCT (1995)
Microsoft

SSLv3 (1995)
Netscape

STLP (1996)
Microsoft

TLS 1.0 (1997-1999)
IETF (aka SSLv3.1)

WTLS (1998)
WAP Forum

TLS 1.1 (2006)
TLS 1.2 (2008)

Source: SSL and TLS, Rescorla

SSL RECORD PROTOCOL OPERATION

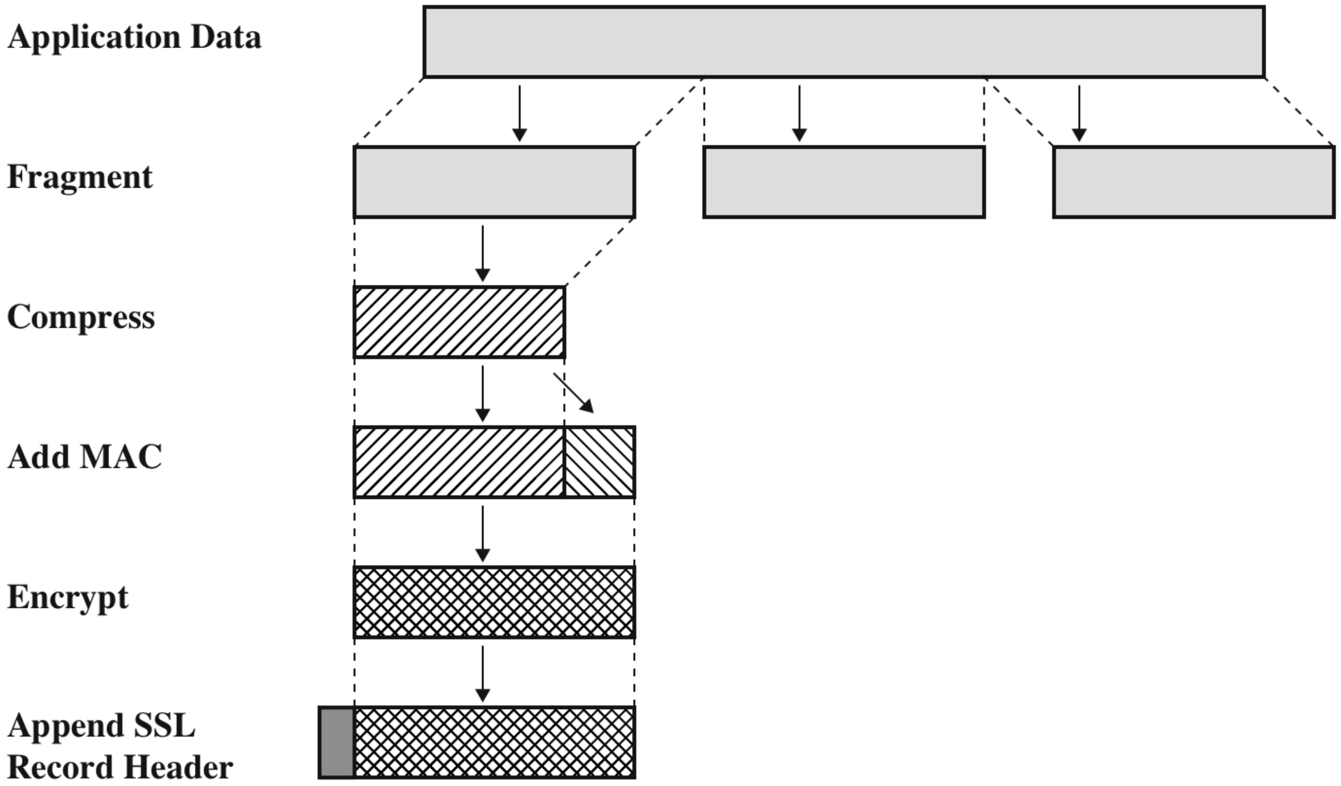


Figure 7.3 SSL Record Protocol Operation

SSL Record Protocol Operation

SSL RECORD FORMAT

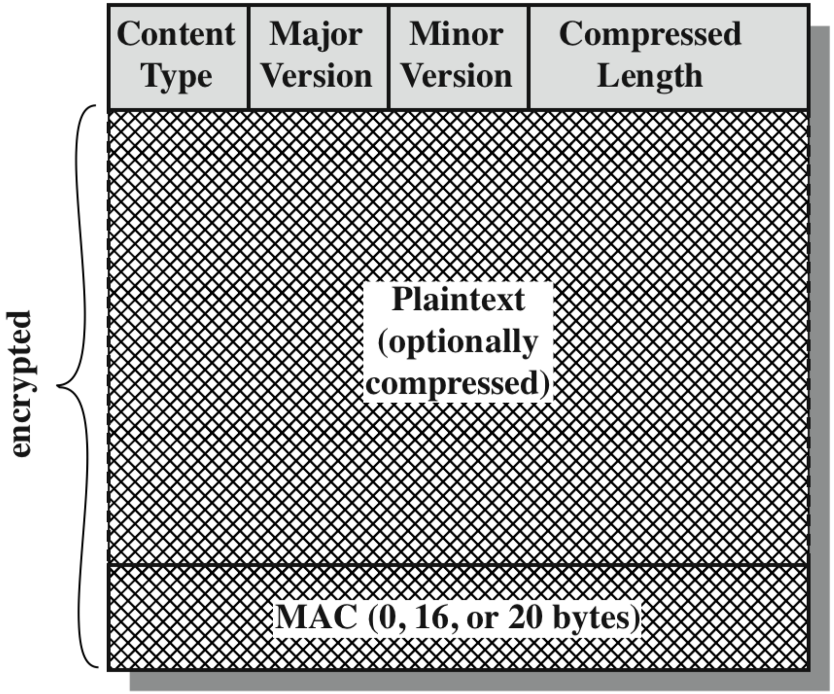
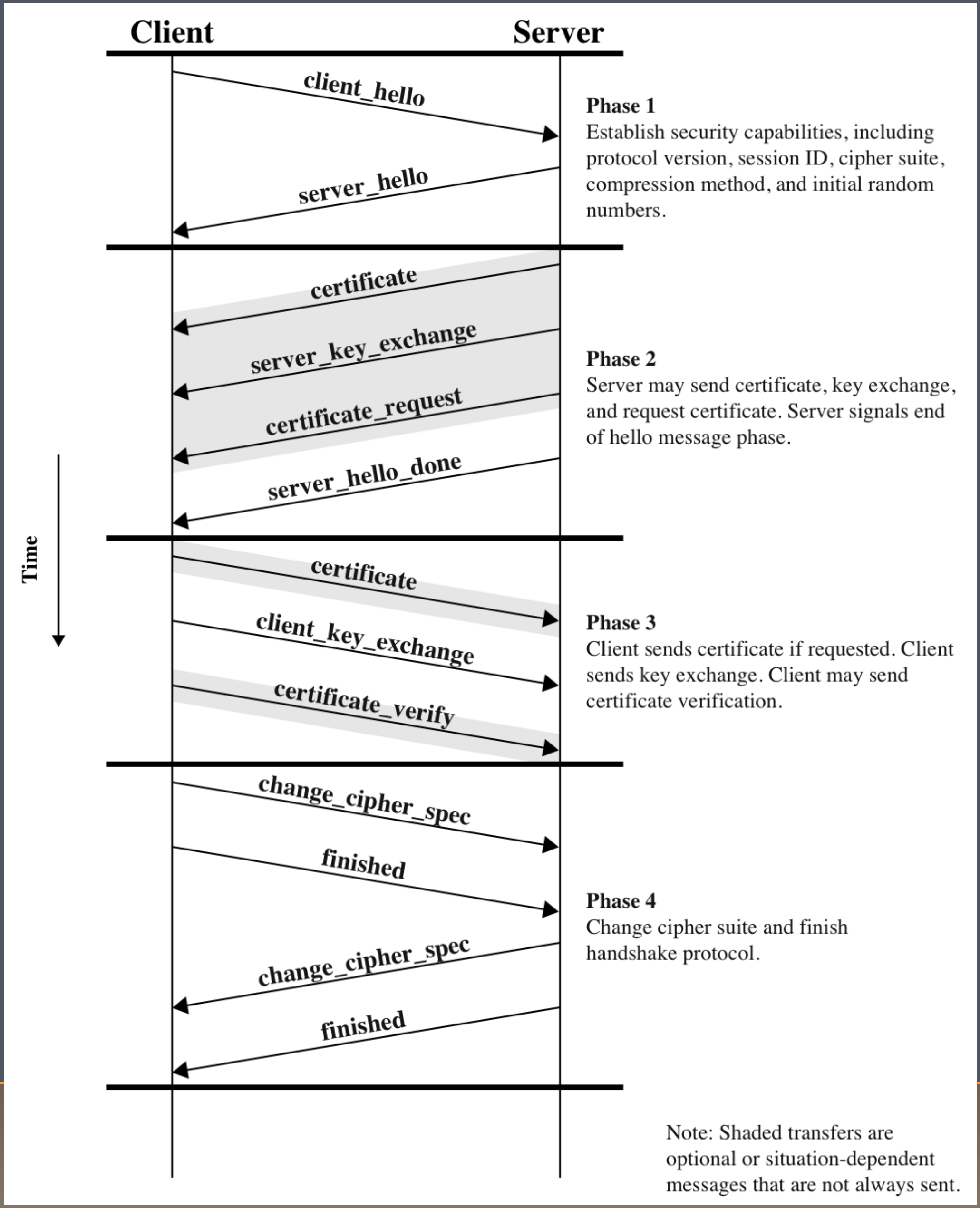


Figure 7.4 SSL Record Format

SSL Record Format

SSL HANDSHAKE



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.

Perfect Forward Secrecy

- In vanilla RSA, the premaster secret is encrypted with the server's public key
  - If the server's private key is compromised all past and future sessions are also compromised
  - Majority of TLS uses vanilla RSA
- Alternatives
  - Ephemeral RSA
  - Authenticated Ephemeral Diffie-Hellman

Review Questions

- How many shared keys are derived between a client and a server that establish a TLS session?
- How does the server prove ownership of its private key?
- How does the client prove ownership of its private key when client authentication is (rarely) used?
- What is the pre-master secret?
  - Who creates it?
  - How is it securely transmitted?
- What is session resumption?
  - How does it differ from a regular SSL handshake?
- When do the client and server start encrypting traffic using symmetric encryption?