CS 465 Computer Security

Kent Seamons

Last update: Oct 31, 2005
Transport Layer Security
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

SSLv3 (1995)
Netscape

PCT (1995)
Microsoft

STLP (1996)
Microsoft

WTLS (1998)
WAP Forum

TLS (1997-1999)
IETF

Source: SSL and TLS, Rescorla
Figure 7.1 Relative Location of Security Facilities in the TCP/IP Protocol Stack
Figure 7.2  SSL Protocol Stack
Figure 7.3  SSL Record Protocol Operation

Application Data → Fragment → Compress → Add MAC → Encrypt → Append SSL Record Header
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.

Figure 7.6 Handshake Protocol Action
Review Questions

- How many shared keys are derived between the client and server that establish a TLS session?
- How does the client prove ownership of their private key?
- How does the server prove ownership of their private key?
- What is the pre-master secret? Who creates it? How is it securely transmitted?
- What is session resumption? How does it occur?
- When do the client and server start encrypting traffic using symmetric encryption?