Module 2.3
SSL Architecture

Ravi Sandhu

Spring 2021
SSL

- layered on top of TCP
- SSL versions 1.0, 2.0, 3.0, 3.1
- Netscape protocol
- later refitted as IETF standard TLS (Transport Layer Security)
- TLS 1.0 very close to SSL 3.1
- Currently at TLS 1.3
SSL

- application protocol independent
- does not specify how application protocols add security with SSL
  - how to initiate SSL handshaking
  - how to interpret certificates
- left to designers of upper layer protocols to figure out
SSL vs TCP Ports

- https 443
- ssmtp 465
- snntp 563
- sldap 636
- spop3 995
- ftp-data 889
- ftps 990
- imaps 991
- telnets 992
- ircs 993
SSL Services

- peer entity authentication
- data confidentiality
- data authentication and integrity
- compression/decompression
- generation/distribution of session keys
  - integrated into protocol
- security parameter negotiation
# SSL Architecture

<table>
<thead>
<tr>
<th>SSL Handshake Protocol</th>
<th>SSL Change Cipher Spec Protocol</th>
<th>SSL Alert Protocol</th>
<th>HTTP</th>
<th>Other Application Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SSL Record Protocol</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# SSL Architecture

## SSL Record Protocol

- SSL Handshake Protocol
- SSL Change Cipher Spec Protocol
- SSL Alert Protocol
- HTTP
- Other Application Protocols

### Complex

Security dictates silent failure

### Straightforward

SSL Record Protocol

TCP

IP

© Ravi Sandhu

World-Leading Research with Real-World Impact!
Handshake protocol: complicated
- embodies key exchange & authentication
- runs in plaintext
- 10 message types

Change Cipher Spec protocol: straightforward
- single 1 byte message with value 1
- could be considered part of handshake protocol
- transitions from plaintext to encrypted and mac’ed

Record protocol: straightforward
- fragment, compress, MAC, encrypt
- uses 4 symmetric keys

Alert protocol: straightforward
- 2 byte messages
- 1 byte alert level- fatal or warning; 1 byte alert code
SSL Record Protocol

- 4 symmetric keys

Key 1 for MAC
Key 2 for encrypt

Key 3 for MAC
Key 4 for encrypt
SSL Record Protocol

- 4 steps by sender (reversed by receiver)
  - Fragmentation
  - Compression
  - MAC
  - Encryption
SSL Record Protocol

- each SSL record contains
  - content type: 8 bits, only 4 defined
    - change_cipher_spec
    - alert
    - handshake
    - application_data
  - protocol version number: 8 bits major, 8 bits minor
  - length: max 16K bytes (actually $2^{14} + 2048$)
  - data payload: optionally compressed and encrypted
  - message authentication code (MAC)