TLS and HTTPS

CSE 461 Section
A joke about bad weather
TLS Fundamentals

- “Transport Layer Security” protocol
- Standard protocol for encrypting Internet traffic
- Previously known as SSL (Secure Sockets Layer), which has been around since 1994
- TLS replaced SSL in 1999
- Used for HTTPS (HTTP Secure) traffic
- Supported by nearly every web browser
When we don’t use TLS, web traffic goes over unencrypted
This includes HTTP payloads, but also HTTP headers
Why are headers a problem too?
Purposes for TLS (2)

- Data integrity
- Server (and client) authentication
### Defcon Wall of Sheep

![Wall of Sheep](image)

<table>
<thead>
<tr>
<th>login</th>
<th>pass</th>
<th>domain_ip</th>
<th>application</th>
</tr>
</thead>
<tbody>
<tr>
<td>h00p</td>
<td>tdc***</td>
<td>65.154.34.164</td>
<td>HTTP</td>
</tr>
<tr>
<td><a href="mailto:voltagespike@fastmail.fm">voltagespike@fastmail.fm</a></td>
<td>thab***</td>
<td>66.111.4.52</td>
<td>IMAP</td>
</tr>
<tr>
<td><a href="mailto:Jennifer.lee@post.harvard.edu">Jennifer.lee@post.harvard.edu</a></td>
<td>poc***</td>
<td>184.73.159.65</td>
<td>foursquare</td>
</tr>
<tr>
<td>demblew</td>
<td>MIC***</td>
<td>137.52.224.216</td>
<td>pop</td>
</tr>
<tr>
<td>wencevdn</td>
<td>Sla***</td>
<td>128.242.245.20</td>
<td>Twitter (on Android)</td>
</tr>
<tr>
<td>Nokia-osso-rx-49</td>
<td>JOS***</td>
<td>207.114.197.94</td>
<td>HTTP</td>
</tr>
<tr>
<td>computicu</td>
<td>1of***</td>
<td>128.242.245.116</td>
<td>Twitter</td>
</tr>
<tr>
<td>reuhelix</td>
<td>fay***</td>
<td>128.242.245.116</td>
<td>Twitter</td>
</tr>
<tr>
<td><a href="mailto:vishakn@yahoo.com">vishakn@yahoo.com</a></td>
<td>hea***</td>
<td>184.73.159.65</td>
<td>foursquare</td>
</tr>
<tr>
<td>em2827891836</td>
<td>622***</td>
<td>207.114.197.95</td>
<td>HTTP</td>
</tr>
<tr>
<td><a href="mailto:rossknapp@gmail.com">rossknapp@gmail.com</a></td>
<td>863***</td>
<td>184.73.159.65</td>
<td>foursquare</td>
</tr>
<tr>
<td>myylongs</td>
<td>tes***</td>
<td>128.242.245.43</td>
<td>TWITTER</td>
</tr>
<tr>
<td>crissti</td>
<td>int***</td>
<td>128.242.245.148</td>
<td>Twitter</td>
</tr>
<tr>
<td>6062191197</td>
<td>pre***</td>
<td>184.73.159.65</td>
<td>foursquare</td>
</tr>
<tr>
<td>ptkrisnan</td>
<td>4li***</td>
<td>128.242.245.20</td>
<td>twitter</td>
</tr>
<tr>
<td></td>
<td>fom***</td>
<td>184.73.159.65</td>
<td>4square</td>
</tr>
</tbody>
</table>
TLS and CONNECT

- HTTP CONNECT is used to establish a two-way connection “tunnel” between two parties
- After this, a “triple handshake” is performed over the tunnel
- After the handshake, the two parties can communicate securely
- We’ll take a closer look at this handshake
What do we need to do to communicate securely?
- Make sure we’re speaking the same language
- Prove who we are
- Establish a secret code
TLS Handshake Protocol (Rough Details)

- Client tells the server its protocol version and what cryptographic algorithms it can use
- Server responds with a protocol version and cryptographic algorithm to use
- Server sends its certificate to verify its identity
- Client verifies certificate and sends Pre-Master Secret, encrypted so only the server can read it
- Client and server both use that PMS to generate a Master Secret, which is used to generate encryption keys
- Communication commences
Heartbleed bug

- 2014 Bug in OpenSSL implementation of TLS
- Clients ask for a “heartbeat” message to test and keep alive communication links
- In OpenSSL, length checking wasn’t properly performed on the heartbeat data
How might data be intercepted by a MITM, even when encrypted over TLS?

- Implementation bugs (e.g., Heartbleed, 3Shake)
- Server/browser attacks (e.g., truncation attack)
  - “Truncate” logout packet from user
  - User’s browser tells them they’ve logged out
  - They haven’t
- Side-channel attacks
Side-channel TLS Attacks (1)

- Some data is leaked even with encryption
  - Packet send timing
  - Payload size
  - AJAX interfaces that load content dynamically provide insight into what the user is typing
Side-channel TLS Attacks (2)
Autocomplete Packet Sizes for "hackers"
Autocomplete Packet Sizes for "benaloh"
Autocomplete Packet Sizes for "xvwqxxzx"
Questions?