Agenda

- HTTPS
- The HSTS Policy
- SSL Certificate
- Monthly Security News Review
HTTPS

- **HTTPS**: HTTP Over TLS, or HTTP Secure.
- **TLS**: Transport Layer Security.
- **SSL**: Secure Sockets Layer, predecessor of TLS.
- TLS and SSL are often used interchangeably.
Terms

- **Active attack**: attempts to alter system resources or affect their operation.
- **Passive attack**: attempts to learn or make use of information from the system but does not affect system resources.
- **Man-in-the-middle attack**: an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.
Why SSL/TLS exists?

- Encryption - Hiding what is sent from one computer to another.
- Identification - Making sure the computer you are speaking to is the one you trust.
Why SSL/TLS exists?

- **Encryption** - Hiding what is sent from one computer to another.
- **Identification** - Making sure the computer you are speaking to is the one you trust.
Many web sites support both HTTP and HTTPS.

The man-in-the-middle adversary may downgrade security to plain HTTP by rewriting URLs contained in an HTTP page to change the protocol from HTTPS to HTTP, this is called HTTPS stripping attack.
Browsers use graphic indicators to tell the user whether a connection is made over HTTP or HTTPS. Typically, this UI includes showing https in the browser’s address bar and a padlock icon.

However, user studies have indicated that the vast majority of users (upwards of 90%) do not notice if these security indicators are missing and are still willing to transmit sensitive data such as passwords and banking details.

It is insufficient to rely on users to detect if their connection to a normally secure server has been downgraded to HTTP by an attacker.
To counter the threat of HTTPS stripping, HSTS was proposed, which refers to HTTP strict transport security.

 Enables servers to request clients only communicate over HTTPS.

 Once set, the browser must refuse to send any traffic to the server over plain HTTP. Any request which would otherwise be transmitted over HTTP will be upgraded from HTTP to HTTPS.

 The primary means for a server to establish HSTS is by setting the HTTP header Strict-Transport-Security.
HSTS preloads

- To address the vulnerability of HTTPS stripping before the browser has visited a domain and observed an HSTS header, Chrome and Firefox both now ship with a hard-coded list of domains receiving a preloaded HSTS policy.
- Preloaded domains receive an automatic HSTS policy from the browser.
Why SSL/TLS exists?

- **Encryption** - Hiding what is sent from one computer to another.
- **Identification** - Making sure the computer you are speaking to is the one you trust.
Why SSL/TLS exists? - Identification

https://www.youtube.com/watch?v=AozNFKSj2uM
SSL Certificate

a.k.a. SSL server certificate. In SSL/TLS, a server is required to present a certificate as part of the initial connection setup. A client connecting to that server will verify at least two things:

- The subject of the certificate matches the hostname to which the client is trying to connect. (Hostnames are listed in the Subject Alternative Name field of the certificate)
- The certificate is signed by a trusted certificate authority.
SSL Certificate

- Previously we learned: public key: encryption; private key: decryption.
- Another usage of public/private key: private key: sign a certificate; public key: verify a certificate.
- Commonality: only one person/entity can have the private key, but everyone can have a public key.
Certificate Authority

- **Certificate Authority (CA)**: In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates. -wikipedia

- If a web site has a valid certificate, it means that a certificate authority has taken steps to verify that the web address actually belongs to that organization.
<table>
<thead>
<tr>
<th>Certificate Authority</th>
<th>Share</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comodo</td>
<td>34.8%</td>
</tr>
<tr>
<td>Symantec Group</td>
<td>30.0%</td>
</tr>
<tr>
<td>Go Daddy Group</td>
<td>17.8%</td>
</tr>
<tr>
<td>GlobalSign</td>
<td>10.3%</td>
</tr>
<tr>
<td>DigiCert</td>
<td>3.1%</td>
</tr>
<tr>
<td>StartCom</td>
<td>1.6%</td>
</tr>
<tr>
<td>Trustwave</td>
<td>0.7%</td>
</tr>
<tr>
<td>Entrust</td>
<td>0.7%</td>
</tr>
<tr>
<td>Verizon</td>
<td>0.6%</td>
</tr>
<tr>
<td>Secom Trust</td>
<td>0.3%</td>
</tr>
</tbody>
</table>

Percentages of websites using various SSL certificate authorities among the sites that use .com.

Hands-on: Find out the CAs for the following websites

- www.boisestate.edu
- www.google.com
- www.starbucks.com
- www.maroon5.com
- www.ashleymadison.com
- www.ups.com
- www.honest.com
- www.amazon.com
Certificates are not free

- Comodo: https://ssl.comodo.com/
- GoDaddy: https://www.godaddy.com/web-security/ssl-certificate
- Symantec: https://www.symantec.com/ssl-certificates/
Monthly Security News Review

Read the news and answer the following questions:

▸ Find out who issued the certificate used by www.google.com, who issued the certificate used by www.symantec.com.

▸ In the news you just read, which company is the certificate authority? Google or Symantec?

▸ If Google makes Chrome stop recognizing Symantec certificates, which of the following websites will be blocked?
  ▸ www.boisestate.edu
  ▸ www.maroon5.com
  ▸ www.honest.com
  ▸ www.amazon.com

▸ In the above scenario, if you still want to access that website anyway, let’s say www.amazon.com, what can you do?

▸ Let’s suppose you are the owner of a website that is using symantec-issued certificate, Google’s proposal may cause service disruption to your customers. As the owner of the website, what should you do?
A large portion of the material is adapted from:

- Internet Engineering Task Force RFC 2828, Internet Security Glossary
- How SSL works tutorial - with HTTPS example https://www.youtube.com/watch?v=iQsKdtjwtYI
- Public key certificate - wikipedia https://en.wikipedia.org/wiki/Public_key_certificate
Backup Slides
SSL Proxying

If you are using Burp Suite, or Paros Proxy, or ZAP, and you want to access a website (let’s say www.maroon5.com) over HTTPS; what would happen is,

- On the one hand, www.maroon5.com will send you its SSL certificate, but this certificate will be received/intercepted by your proxy, i.e., Burp Suite. Burp Suite will then act as you, and communicate with the server over HTTPS. In other words, the traffic between Burp Suite and the web server is encrypted.
SSL Proxying

▶ On the other hand, Burp Suite will create its own certificate and send it to you - i.e., the browser. If your browser does not trust Burp Suite (this is the default case), then it will show you a warning message or block you from accessing that maroon5.com. To address this problem, you have to install something called Burp’s CA certificate in your browser. After that, your browser will trust Burp Suite’s certificate, and then you browser will communicate with Burp Suite over HTTPS, and believes Burp Suite is the web server you want to access, i.e., it considers Burp Suite as https://www.maroon5.com. So the traffic between you (i.e., the browser) and Burp Suite is encrypted.

▶ Inside the proxy, it is where the traffic is not encrypted. That’s why using Burp Suite, you can see your own username and password on maroon5.com, or on any website you are accessing.
Discussion

1. Can a coffee shop (like Starbucks) monitor my HTTPS traffic over their network?
2. Can my company monitor my HTTPS traffic over their network?