Winning At HTTPS
WHY?
Why?
WHAT?
A prominent use of TLS is for securing World Wide Web traffic between a website and a web browser encoded with the HTTP protocol. This use of TLS to secure HTTP traffic constitutes the HTTPS protocol.[5]

### Website protocol support

<table>
<thead>
<tr>
<th>Protocol version</th>
<th>Website support[36]</th>
<th>Security[36][37]</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL 2.0</td>
<td>6.7% (-0.2%)</td>
<td>Insecure</td>
</tr>
<tr>
<td>SSL 3.0</td>
<td>20.7% (+0.0%)</td>
<td>Insecure[38]</td>
</tr>
<tr>
<td>TLS 1.0</td>
<td>96.1% (-0.1%)</td>
<td>Depends on cipher[1] and client mitigations[2]</td>
</tr>
<tr>
<td>TLS 1.1</td>
<td>78.3% (+0.7%)</td>
<td>Depends on cipher[1] and client mitigations[2]</td>
</tr>
<tr>
<td>TLS 1.2</td>
<td>80.7% (+0.7%)</td>
<td>Depends on cipher[1] and client mitigations[2]</td>
</tr>
<tr>
<td>TLS 1.3 (Draft)</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
SSL Client

(1) "client hello"
Cryptographic information

(2) "server hello"
CipherSuite
Server certificate
"client certificate request" (optional)

(3) Verify server certificate. Check cryptographic parameters

(4) Client key exchange
Send secret key information (encrypted with server public key)

(5) Send client certificate

(6) Verify client certificate (if required)

(7) Client "finished"

(8) Server "finished"

(9) Exchange messages (encrypted with shared secret key)
FAQ
Is HTTPS cached??
HTTPS hides metadata?
True or False
Are requests slower?
Longer connection times (yellow) with HTTPS
ONE DOES NOT SIMPLY HTTPS
Setup
Single name
mydomain.com
www.mydomain.com
Wildcard
*.bandcamp.com

$100-1000s
Multi-Domain SAN
mydomain.com
www.mydomain.com
random.com
www.random.com
sub.random.com

$100-1000s
Validation Types

- Self Signed
- Domain Validated
- Organisation Validated
- EV (Extended Validation)
openssl req \
    -newkey rsa:2048 -nodes -keyout domain.key \
    -out domain.csr

Generating a 2048 bit RSA private key
...........................................++++
.....................................++++
writing new private key to 'domain.key'
-----
You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank
For some fields there will be a default value, If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:NSW
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:My Company
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) [mydomain.com]:
Email Address []:james@crispdesign.net

Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password []:
An optional company name []:
Domain Validation

- Upload file
- cname / txt DNS record
- Email sent to contacts on domain
An SSL Certificate allows you to configure the HTTPS/SSL listeners of your Load Balancer. You may select a previously uploaded certificate below, or define a new SSL Certificate by supplying certificate name, a private key (pem encoded), and a public key certificate (pem encoded). You may also provide an optional public key certificate chain (pem encoded). Learn more about setting up HTTPS load balancer listeners and certificate management.

<table>
<thead>
<tr>
<th>Choose from your existing SSL Certificates</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Upload a new SSL Certificate</th>
</tr>
</thead>
</table>

| Certificate Name:* | example_cert  
(e.g., myServerCert) |
|--------------------|
| Private Key:*      | MIICITCCAfCCQD6m7oRw0uXojANBkgkhiG9w0BAQUFADCBiDELMAkGA1UE  
BhMCVVMxCzABgNVBAQTAldBMRAwDgYDVQQHEwdTZWFW0dGxlMQ8wDQYD  
(pem encoded) |
| Public Key Certificate:* | MIICITCCAfCCQD6m7oRw0uXojANBkgkhiG9w0BAQUFADCBiDELMAkGA1UE  
BhMCVVMxCzABgNVBAQTAldBMRAwDgYDVQQHEwdTZWFW0dGxlMQ8wDQYD  
(pem encoded) |
| Certificate Chain: |  
(pem encoded. Optional field) |  

* Required field

Click **Save** to save the changes.
Apache

SSLEngine On
SSLCertificateFile /etc/apache2/ssl/server.crt
SSLCertificateKeyFile /etc/apache2/ssl/server.key
SSLCertificateChainFile /etc/apache2/ssl/server.ca-bundle
web.config

<rule name="Force WWW and SSL" enabled="true" stopProcessing="true">
  <match url="(.*)" />
  <conditions logicalGrouping="MatchAny">
    <add input="{HTTP_HOST}" pattern="^[^www]" />
    <add input="{HTTPS}" pattern="off" />
  </conditions>
  <action type="Redirect" url="https://www.zzz.com/{R:1}" appendQueryString="true" redirectType="Permanent" />
</rule>

Apache Rewrite Rule

RewriteCond %{HTTPS} off
RewriteCond %{HTTP_HOST} ^(www.)*([a-z.]+)$ [NC]
RewriteRule ^/(.*)$ https://www.%2/$1 [R=301,L]
HTTPS
HTTPS
HSTS

```
Strict-Transport-Security: max-age=31536000; includeSubDomains
```

chrome://net-internals/#hsts

IE11+, Edge, FF, Chrome, Safari
Engineering a Reversible HTTPS Migration

- 302 “temporary” redirect in rewrite rules
- Don’t set HSTS!
- Change to 301 and set HSTS once it’s all OK
OH NOES
WAI U DO DIS
Tips & Gotchas

• Mixed mode sites HTTP/HTTPS

• With invalid certificate, Chrome only caches images, not JS or CSS
KeepAlive

Short KeepAlive can cause IE problems on slow connections
<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>211</td>
<td>21.956</td>
<td>10.90</td>
<td>173.129</td>
<td>TCP</td>
<td>66</td>
<td>59560-80 [SYN] Seq=0 Win=8192 Len=0 MSS=1260 WS=4 SACK_PERM=1</td>
</tr>
<tr>
<td>213</td>
<td>22.017</td>
<td>10.90</td>
<td>173.129</td>
<td>TCP</td>
<td>66</td>
<td>80-59560 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1380 WS=128</td>
</tr>
<tr>
<td>214</td>
<td>22.017</td>
<td>10.90</td>
<td>173.129</td>
<td>TCP</td>
<td>54</td>
<td>59560-80 [ACK] Seq=1 Ack=1 Win=66780 Len=0</td>
</tr>
<tr>
<td>215</td>
<td>22.018</td>
<td>10.90</td>
<td>173.129</td>
<td>HTTP</td>
<td>990</td>
<td>GET /LocationCodesServlet?fromLocCode=SanFrancisco%2CUS(SFO)&amp;toLocCode=Chennai%2CIN(MAA)</td>
</tr>
<tr>
<td>218</td>
<td>22.079</td>
<td>10.90</td>
<td>173.129</td>
<td>TCP</td>
<td>60</td>
<td>80-59560 [ACK] Seq=1 Ack=16512 Win=16512 Len=0</td>
</tr>
<tr>
<td>219</td>
<td>22.093</td>
<td>10.90</td>
<td>173.129</td>
<td>TCP</td>
<td>347</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>220</td>
<td>22.094</td>
<td>10.90</td>
<td>173.129</td>
<td>HTTP</td>
<td>60</td>
<td>HTTP/1.1 200 OK (application/json)</td>
</tr>
<tr>
<td>221</td>
<td>22.094</td>
<td>10.90</td>
<td>173.129</td>
<td>HTTP</td>
<td>60</td>
<td>HTTP/1.1 200 OK (application/json)</td>
</tr>
<tr>
<td>222</td>
<td>22.094</td>
<td>10.90</td>
<td>173.129</td>
<td>TCP</td>
<td>54</td>
<td>59560-80 [ACK] Seq=937 Ack=294 Win=66484 Len=0</td>
</tr>
<tr>
<td>223</td>
<td>22.119</td>
<td>10.90</td>
<td>173.129</td>
<td>TCP</td>
<td>54</td>
<td>59560-80 [ACK] Seq=937 Ack=299 Win=66480 Len=0</td>
</tr>
<tr>
<td>224</td>
<td>22.119</td>
<td>10.90</td>
<td>173.129</td>
<td>HTTP</td>
<td>678</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>225</td>
<td>22.182</td>
<td>10.90</td>
<td>173.129</td>
<td>HTTP</td>
<td>447</td>
<td>POST /servlet/APIEmulatorServlet HTTP/1.1 (application/x-www-form-urlencoded)</td>
</tr>
<tr>
<td>231</td>
<td>22.539</td>
<td>10.90</td>
<td>173.129</td>
<td>TCP</td>
<td>60</td>
<td>59560-80 [ACK] Seq=954 Ack=655 Win=66124 Len=0</td>
</tr>
<tr>
<td>232</td>
<td>22.540</td>
<td>10.90</td>
<td>173.129</td>
<td>HTTP</td>
<td>60</td>
<td>HTTP/1.1 200 OK (application/json)</td>
</tr>
<tr>
<td>233</td>
<td>22.540</td>
<td>10.90</td>
<td>173.129</td>
<td>TCP</td>
<td>54</td>
<td>59560-80 [ACK] Seq=954 Ack=660 Win=66120 Len=0</td>
</tr>
<tr>
<td>263</td>
<td>23.305</td>
<td>10.90</td>
<td>173.129</td>
<td>TCP</td>
<td>54</td>
<td>59560-80 [ACK] Seq=954 Ack=660 Win=66120 Len=0</td>
</tr>
<tr>
<td>264</td>
<td>23.508</td>
<td>10.90</td>
<td>173.129</td>
<td>HTTP</td>
<td>153</td>
<td>POST /servlet/APIEmulatorServlet HTTP/1.1 (application/x-www-form-urlencoded)</td>
</tr>
<tr>
<td>265</td>
<td>23.541</td>
<td>10.90</td>
<td>173.129</td>
<td>TCP</td>
<td>60</td>
<td>80-59560 [FIN, ACK] Seq=660 Ack=1954 Win=20224 Len=0</td>
</tr>
<tr>
<td>266</td>
<td>23.541</td>
<td>10.90</td>
<td>173.129</td>
<td>TCP</td>
<td>54</td>
<td>59560-80 [ACK] Seq=2676 Ack=661 Win=66120 Len=0</td>
</tr>
<tr>
<td>267</td>
<td>23.541</td>
<td>10.90</td>
<td>173.129</td>
<td>TCP</td>
<td>54</td>
<td>59560-80 [FIN, ACK] Seq=2676 Ack=661 Win=66120 Len=0</td>
</tr>
<tr>
<td>270</td>
<td>23.567</td>
<td>10.90</td>
<td>173.129</td>
<td>TCP</td>
<td>60</td>
<td>80-59560 [ACK] Seq=661 Ack=2676 Win=22144 Len=0</td>
</tr>
<tr>
<td>271</td>
<td>23.602</td>
<td>10.90</td>
<td>173.129</td>
<td>TCP</td>
<td>60</td>
<td>80-59560 [ACK] Seq=661 Ack=2677 Win=22144 Len=0</td>
</tr>
</tbody>
</table>
HTTPS links/ assets

• Relative urls “/users/edit” “/public/img.svg”

• HTTPS urls

• Protocol relative urls
  eg, `<script src="//ajax.microsoft.com/ajax/jquery/jquery-1.3.2.min.js">`

Assessed on: Mon, 10 Oct 2016 11:28:08 UTC | Hide Clear cache

Summary

Overall Rating

Certificate
Protocol Support
Key Exchange
Cipher Strength

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

Intermediate certificate has a weak signature. Upgrade to SHA2 as soon as possible to avoid browser warnings. MORE INFO

This server uses RC4 with modern protocols. Grade capped to C.

The server does not support Forward Secrecy with the reference browsers. MORE INFO

Authentication

Server Key and Certificate #1

- Subject: www.hsbc.com.au
- Fingerprint SHA1: 8d86b9247515ed85a29335b7138941f9b7512
- Fingerprint SHA256: df5f90f56bd07d934f407bfa468ab4faa456bcb7

- Common names: www.hsbc.com.au
- Alternative names: www.hsbc.com.au
- Valid from: Mon, 25 Jul 2016 00:00:00 UTC
- Valid until: Thu, 26 Jul 2018 23:59:59 UTC (expires in 1 year and 9 months)
- Key: RSA 2048 bits (e 65537)
- Weak key (Debian): No
- Issuer: Symantec Class 3 EV SSL CA - G3
- Signature algorithm: SHA256withRSA
- Extended Validation: Yes
SSL Report: google.com (2607:f8b0:4005:805:0:0:0:200e)
Assessed on: Tue, 18 Oct 2016 23:05:19 UTC | HIDDEN | Clear cache

Summary

Overall Rating

Certificate
Protocol Support
Key Exchange
Cipher Strength

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

Intermediate certificate has a weak signature. Upgrade to SHA2 as soon as possible to avoid browser warnings. MORE INFO »

Authentication

Server Key and Certificate #1

<table>
<thead>
<tr>
<th>Subject</th>
<th>*.google.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common names</td>
<td>*.google.com</td>
</tr>
<tr>
<td>Valid from</td>
<td>Fri, 14 Oct 2016 00:26:00 UTC</td>
</tr>
<tr>
<td>Valid until</td>
<td>Fri, 06 Jan 2017 00:26:00 UTC (expires in 2 months and 18 days)</td>
</tr>
<tr>
<td>Key</td>
<td>EC 256 bits</td>
</tr>
<tr>
<td>Weak key (Debian)</td>
<td>No</td>
</tr>
<tr>
<td>Issuer</td>
<td>Google Internet Authority G2</td>
</tr>
<tr>
<td>Signature algorithm</td>
<td>SHA256withRSA</td>
</tr>
</tbody>
</table>
Questions?