

# The State of TLS in httpd 2.4

The background of the slide is a photograph of the Texas State Capitol building in Austin, Texas, featuring its prominent dome. In the foreground, the Lone Star Monument is visible, which consists of three bronze statues on a stone pedestal: a soldier, a miner, and a settler. The scene is set outdoors with trees and a clear sky.

William A. Rowe Jr.  
wrowe@apache.org

# Getting Started

- Web references have grown stale
- Guidance is changing annually  
<https://www.ssllabs.com/ssltest/analyze.html?d=svn.apache.org>
- Plain http:// is nearing extinction  
<https://www.eff.org/encrypt-the-web-report>



# Follow Up-to-date Resources

- Several authors are doing a good job of explaining TLS issues in clear language.
- Ivan Ristić's blog  
<http://blog.ivanristic.com>
- Adam Langley's blog  
<https://www.imperialviolet.org/>

# Update to Modern Tools

- OpenSSL 1.0.1 provides the necessary TLSv1.2 facilities
- 1.0.2 is now the recommended version
- Apache HTTP Server 2.4 connects the dots for OpenSSL 1.0.1 features
- 2.4.16 revised the suggested `mod_ssl` configuration files



# More Reasons

- 2.4.17 introduces ALPN support for http/2
- Forward Secrecy, stronger hashes and ECC cryptography all require these updates

[http://httpd.apache.org/docs/2.4/new\\_features\\_2\\_4.html#module](http://httpd.apache.org/docs/2.4/new_features_2_4.html#module)

# Choose 2? (Or only one?)

- Confidentiality, performance or compatibility?
- Evaluate the scope of confidentiality:  
Value? RoI vs Bitcoin mining  
Trading off for performance  
Trading off for compatibility



# Protocols

- SSLv2 is long dead, SSLv3, and TLSv1.0 are also nearing death, by late 2016
- TLSv1.2 addresses a spectrum of weaknesses (OpenSSL 1.0.1p is needed to avoid new issues)
- OpenSSL 1.0.2 adds new API facilities, especially wildcard SNI handshakes

# Ciphers

- The Big List (Poor choices are present)  
openssl ciphers -v
- A simplified list (Efficient and Secure)  
openssl ciphers -v \  
**'HIGH:MEDIUM:!aNULL:!MD5'**



# Dictating Priority

- Teach your server to enforce -your- policy

[http://httpd.apache.org/docs/2.4/mod/mod\\_ssl.html#sslhonorcipherorder](http://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslhonorcipherorder)

# Disable SSLv3?

- The Protocol? The Cipher List?
- TLSv1.0 -is- SSLv3 in nearly every respect
- TLS\_FALLBACK\_SCSV is the bandaid
- TLSv1.2 -only- is coming soon



# Certs and Keys

- Hashes in MD5 / SHA1?
- A better RSA – SHA256 hashes
- ECDHE-RSA 'just works' with historical RSA certs
- ECDSA certificates offer an more efficient alternative

# (Perfect?) Forward Secrecy

- The Goal – discontinuity between sessions
  - `SSLSessionCacheTimeout [300]`
- ECDSA keys offer efficiency
- ECDH/RSA remains a compromise



# OCSP (and Stapling)

- Confirming continued validity – evolved from revocation lists
- OCSP Failure cases – overloaded providers and unroutable traffic
- Stapling can improve these issues
- Server is subject to the same issues

# Graceful Failure

SSLStaplingCache shmcb:ocsp(1048576)

SSLStaplingStandardCacheTimeout 86400

SSLStaplingErrorCacheTimeout 300

SSLStaplingReturnResponderErrors Off

SSLStaplingFakeTryLater off



# Sessions

- Cache and considerations
- Tickets and considerations
- Spanning the load balancer
  - A common SSLSessionCache
  - A common SSLSessionTicketKeyFile

# Renegotiation

- Server initiated
- Client initiated, pre-TLSv1.1
- Client initiated with TLSv1.1
- Inherent conflict with multiple streams (HTTP/2)



# Under Control

- The enterprise case; known user agents
- The operations case; peering application servers
- The forward proxy case; all bets are off?

# The Design Conundrums

- TLS compression – Do Not Use
- Encoding: gzip | deflate risks
- Client-supplied Input Reflection  
Buried into Cookies, HTTP headers, or  
form contents



# Broken Clients

- The perils of parallel consumers
- Sharing SSL Sessions between adversarial parties
- BREACH is a browser/application hosting defect

# Virtual Hosting

- SNI (Server Name Indication) in httpd 2.4 allows modern clients to share a single IP address for multiple certificates
- Presented based on the TLS SNI hostname indicated by the client.
- Old clients still need a wildcard certificate, or a list of AltSubjectNames



# CA Management

- Some tools for maintaining CA lists can be found in the openssl tools/ source directory (these are generally not installed by-default in vendor distributions).

# External Efforts

- EFF-led HTTPS Everywhere campaign
- Qualys SSL Labs Test  
<https://www.ssllabs.com/ssltest/index.html>
- Let's Encrypt – multiparty CA effort  
<https://letsencrypt.org/>



# Success stories

<https://github.com/blog/1727-introducing-forward-secrecy-and-authenticated-encryption-ciphers>

<https://blog.twitter.com/2013/forward-secrecy-at-twitter>

# A Never-ending Process

<http://www.openssl.org/news/vulnerabilities.html>

[http://httpd.apache.org/security/vulnerabilities\\_24.html](http://httpd.apache.org/security/vulnerabilities_24.html)

<http://httpd.apache.org/docs/2.4/>

<http://httpd.apache.org/docs/trunk/>  
(what is coming soon)



# Questions?

APACHE CON  
NORTH AMERICA

