YAHOO!

State of the SSL Onion

Susan Hinrichs – ATS Summit Spring 2016

From Last Summit's discussion

- A desire to normalize SSL configuration
  - Tickets (not just domain specific)
  - Client sessions (not just global)
  - ALPN protocol strings
  - Notes http://network-geographics.com/assets/docs/PostFall2015SummitSSLnotes.pdf
- I had no time to work on any of this. Leif has worked on the ticket configuration cleanup.

TS-4180: Multiple certificate chains

- Fixed logic to load multiple CA's if there is a comma separated list in ssl_multicert.config
- If openssl 1.0.2 is used, the protocol specific intermediate chain will be returned
- For earlier versions of openssl, all intermediate certificates will be returned.

Testing and openssl version specification

- Testing TS-4180 brought up the issue of testing features that depend on specific library versions.
- With TSQA can we specify the open ssl library version to use?
- Do we just always test with openssl 1.0.2? Do we want to test against 1.0.1, 1.0.2, and 1.1 for different tests?
  - Thomas mentioned if-skip option for TSQA

TS-4179: OCSP stapling broken

- Still to be fixed

TS-4357: Remove SSLv2 and reduce SSLv3 for 7.0

- SSLv2 is gone
- SSLv3
  - Gone for client/proxy
  - Still allow configuration for SSLv3 to origin

TS-4373: SSLContext API

- Proposed by Matthias and David
- TSSslServerContextCreate returns a new SSL Context that's configured according to the settings in records.config. This is useful if an extension wants to use the TS_SSL_CERT_HOOK to control loading of SNI certificates, and still want to respect the cipher suite and related SSL settings.
- Add TSSslContextDestroy method.
- Committed April 2016
- https://docs.trafficserver.apache.org/en/latest/developer-guide/api/functions/TSSslServerContextCreate.en.html

SSL Handshake threads

- Introducing off-box elements to the SSL handshake (CryptoProxy) will cause idle blocking during SSLAccept
  - Even if socket is non-blocking
  - Greatly harms performance
- I have a branch that spawns a thread for each SSLAccept call
  - Need to duplicate Ethread environment to allow for stats calls
  - Reasonably low impact code-change
  - But not completely happy with runtime/performance implications
  - Currently have freelists turned off because synching back was very expensive

SSL Asynchronous Handshake

- Thomas Jackson mentioned recent openssl changes introduced to support Intel encryption hardware assists.
- Merged to openssl main in November 2015
- Matt Caswell's email introducing the feature
  - https://mta.openssl.org/pipermail/openssl-dev/2015-October/002984.html

TS-3527: Hooks to allow state sharing

- I would really like to get back to this this quarter
- Allow people to implement their own cross box state communication without completely overriding the SSL hooks directly.

Dynamic Certificate Loader

- Reveler
- Getting there. Nearly ready to start testing in production.

TS-3216: Add HPKP

- Masaori

TLS 1.3

- Bryan
- Demos are showing up, but unstable.
- Let it ride for another 6 months or 1 year before trying out.

Engine configuration file support

- TS-3249
- TS-2984

Any more experience with non-openssl implentations?

- Primarily BoringSSL.
  - Avoids some of the locking performance problems of openssl