State of the TLS Onion

Oath:

Rework SSL Handshake Hooks

- Calavera ran into problems with the SSL Handshake hooks not working reliably
  - They had evolved to more than two states controlled kind of by two booleans. Time to tidy up.
- Created a proper state machine and created a series of tls_hook autests to exercise different combinations of the SSL handshake hooks, so hopefully this part of the system doesn't degrade again.
- Updated TLS hook documentation
  - https://docs.trafficserver.apache.org/en/latest/developer-guide/plugins/hooks-and-transactions/ssl-hooks.en.html?highlight=servername

Session Ticket Fixes

- A variety of fixes to ensure that updates to session ticket files are handled correctly over ATS config reloads.
- On every config reload the ticket key files will be reloaded.

TLS Handshake Milestones

- Added TS_MILESTONE_TLS_HANDSHAKE_START and TLS_MILESTONE_TLS_HANDSHAKE_END
- Measuring these milestones from the server perspective.
  - In the Session Resume case the delta would be effectively 0
  - In the Full handshake the delta would be about 1 RTT

Limit ssl_read_from_net

- PDM was seeing stalls from large posts
- Adjusted the main SSL read loop to read at most a block's worth of data before giving up thread
- Speculation was that greedy SSL read loops were blocking other continuations.

Hook for Server Certificate Verification

- Added TLS_SSL_SERVER_VERIFY_HOOK
- Associated continuation called after openssl makes its decision on whether the origin server's certificate is valid (i.e. the certificate is signed by a trusted CA)
- The callback can override that decision.
  - E.g., check that certificate contains the expected name
- Documentation with Hook callback state machine.
  - https://docs.trafficserver.apache.org/en/latest/developer-guide/plugins/hooks-and-transactions/index.en.html?highlight=hooks
- Add option 2 for proxy.config.ssl.client.verify.server to enable "permissive" mode which logs verification result but doesn't enforce.
- Client certificate verification hooks have also been requested

Getting Ready for Openssl 1.1

- ATS compiles with Openssl 1.1 since around the beginning of 2017
  - Thanks to work from NotTheOilRig (Jack Bates)
- ABI Change from Openssl 1.0.x
  - You will crash if you link a combination of openssl 1.0.x and openssl 1.1
- Openssl 1.1 has less lock contention
  - In cached stress test of 23KB object, ats+1.1 scales to 90K rps. ats+1.0.2 scales to 11K rps
- Openssl 1.1.1 will provide TLS 1.3
- Openssl 1.1 has new ciphers like the stream cipher ChaCha20-Poly1305

Proposed Session API and hooks

- Enables cross POD session/ticket key sharing
- API Proposal
  - http://home.apache.org/~shinrich/docs/developer-guide/ssl-session-api.en.html
- PR
  - https://github.com/apache/trafficserver/pull/2663
- Working through making our cross POD session sharing plugin open source-able
  - Relies on Redis publish/subscribe for communication