ASYNC jobs and ATS

Susan Hinrichs

ATS Euro Tour

Cork

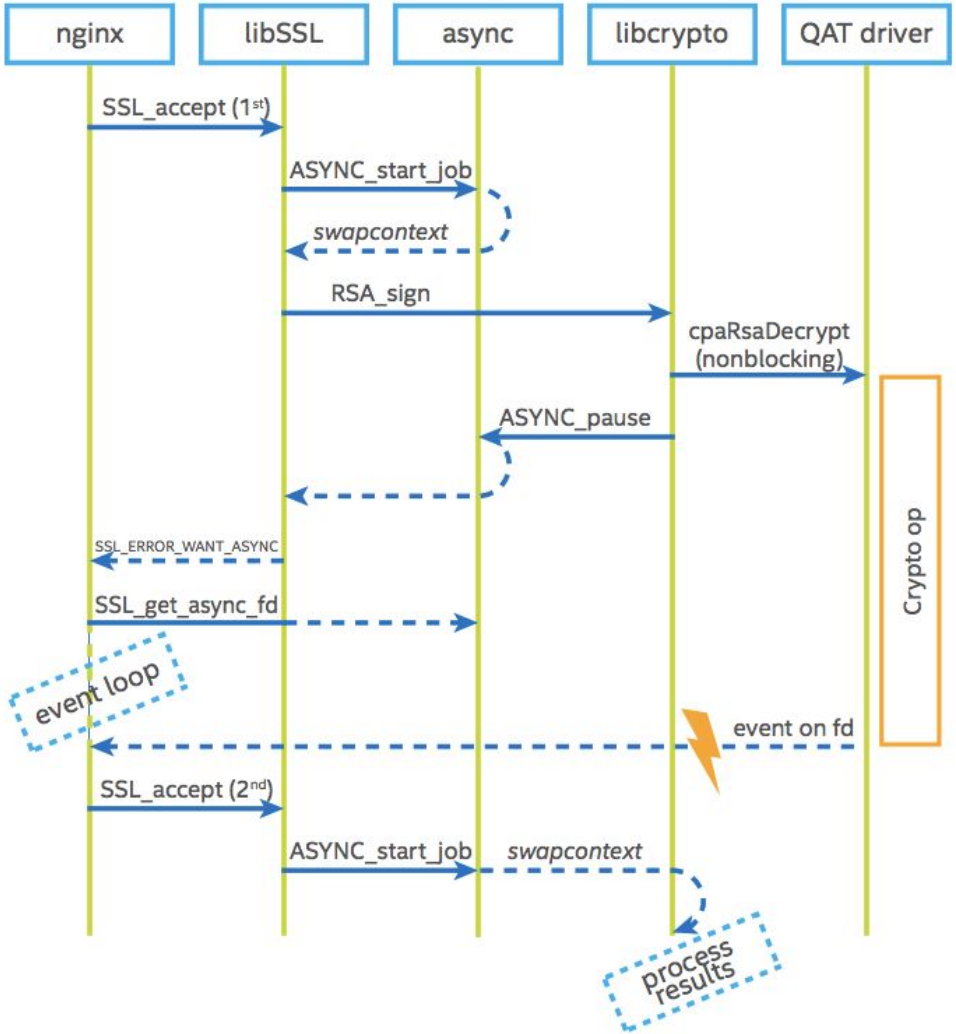
May 2018

The Problem: Time delays accessing crypto

- Off chip crypto resources introduce delay
  - Block chip thread for no reason
  - Bowels of Openssl will not release thread by default
- ASYNC_start_job / ASYNC_pause_job added in openssl 1.1
  - Allow RSA engine to pause job while waiting for off chip operation
  - Synchronizing file descriptor associated with job
  - Set event when operation complete
  - Signals caller to call SSL_accept again to continue
  - Using setcontext/getcontext under the covers to give application control of context switching
- ASYNC_*_job support integrated in ATS master January 2018

Example

Diagram from Intel write up
https://01.org/sites/default/files/downloads/intelr-quickassist-technology/intelquickassisttechnologyopensslperformance.pdf



Documentation

- Settings
  - `Proxy.config.ssl.async.handshake.enabled`
  - `proxy.config.ssl.engine.conf_file`
  - https://docs.trafficserver.apache.org/en/latest/admin-guide/files/records.config.en.html#proxy-config-ssl-async-handshake-enabled

Simple ATS use example

- Test crypto engine
  - Adds 5 second delay in RSA private key operations
  - https://github.com/apache/trafficserver/tree/master/contrib/openssl
- If we do ASYNC_*_job correctly in ATS, a single operation should only be delayed 5 seconds
- Without ASYNC_*_job the TLS requests will stack up with multiples of 10 second delays
- Exercise
  - ATS running with 1 exec thread
  - Batches of 100 curl requests are made

Use Cases

- Off chip encryption units
  - E.g., Trusted Platform Modules (TPM’s)
  - Hardware Security Modules (HSMs)
- Off box encryption

Links

- Test code
  - https://git.ouroath.com/shinrich/ssl-async-job-test
- ATS ASYNC_*_job commit
  - https://github.com/shinrich/trafficserver/commit/bdc88e62582aeaeb473677970caedb9180b00919
- Openssl ASYNC_*_job documentation
  - https://www.openssl.org/docs/man1.1.0/crypto/ASYNC_start_job.html