SESSION ID: OST-W09

OpenSSL and FIPS... They Are Back Together!

Matt Caswell
OpenSSL - OMC/OTC/Committer

Ashit Vora
Vice President
Acumen Security
@aavora
Agenda

- History of OpenSSL and FIPS
- OpenSSL 3.0 Design
- OpenSSL 3.0 FIPS Module
- Current Status
History

The Story so far...
History of OpenSSL and FIPS

- OpenSSL FIPS Object Module 1.0/1.1/1.2
  - Project work: June 2002 to March 2006
  - OpenSSL release: OpenSSL-0.9.7 (last update early 2007)
  - Status: Historical

- OpenSSL FIPS Object Module 2.0
  - Project work: April 2009 to June 2012
  - OpenSSL release: OpenSSL-1.0.2 (end-of-life 31-Dec-2019)
  - Status: Sunset Date 21-Jan-2022
History of OpenSSL and FIPS

- OpenSSL Versions
  - OpenSSL 0.9.8 – EOL 31-Dec-2015
  - OpenSSL 1.0.0 – EOL 31-Dec-2015
  - OpenSSL 1.0.1 – EOL 31-Dec-2016
  - OpenSSL 1.0.2 – EOL 31-Dec-2019 (Extended Support option)
  - OpenSSL 1.1.1 – EOL 11-Sep-2023
  - OpenSSL 3.0.0 – currently in-development release
History of OpenSSL and FIPS

- OpenSSL FIPS validations always “special”
- Substantial resources invested in revalidation and porting work
- OpenSSL FIPS Object Module 2.0
  - 46 validation updates from 2012
  - 209 platforms (excluding private label validations)
- Over 250 other FIPS modules use OpenSSL
# FIPS Validations to date

<table>
<thead>
<tr>
<th>Cert #</th>
<th>Version</th>
<th>Validation Date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>642</td>
<td>1.0</td>
<td>22-Mar-2006</td>
<td>Historical</td>
</tr>
<tr>
<td>733</td>
<td>1.1</td>
<td>06-Feb-2007</td>
<td>Historical</td>
</tr>
<tr>
<td>918</td>
<td>1.1.2</td>
<td>29-Feb-2008</td>
<td>Historical</td>
</tr>
<tr>
<td>1051</td>
<td>1.2</td>
<td>17-Nov-2008</td>
<td>Historical</td>
</tr>
<tr>
<td>1111</td>
<td>1.2</td>
<td>03-Apr-2009</td>
<td>Historical</td>
</tr>
<tr>
<td>1747</td>
<td>2.0</td>
<td>27-Jun-2012</td>
<td>21-Jan-22</td>
</tr>
<tr>
<td>2398</td>
<td>2.0.9+</td>
<td>24-Jun-2015</td>
<td>21-Jan-22</td>
</tr>
<tr>
<td>2437</td>
<td>2.0.9/10</td>
<td>13-Nov-2015</td>
<td>21-Jan-22</td>
</tr>
</tbody>
</table>
FIPS Validations to date

- Low-level FIPS approved crypto algorithms
- Source was separately maintained and versioned
- Re-certifications were ad-hoc
- Validated crypto “module” was a statically linked object
  - Either for statically linked applications; or
  - Inserted into a shared library for dynamically linked applications
FIPS140 Boundary – OpenSSL with STATLIB 2.0

Application

Application Programming Interfaces

Non-Security  Non-FIPS ALGS  FIPS ALGS

C Runtime

Operating System

Non-FIPS ALGS

EXE

STATLIB

SHLIB/DLL

Integrity check

FIPS Canister
FIPS140 Boundary – OpenSSL with SHLIB 2.0
FIPS Validations to date

• Common challenges
  – Code effectively forked long ago
  – Orphaned unmaintained code base
  – Too many platforms
  – Too few people involved in the coding and testing

• This was not the original plan ...

• Note: over 250 other FIPS modules use OpenSSL
OpenSSL 3.0 Design
OpenSSL 1.1.1 Recap

- TLS v1.3
- New unified build system
- Data structures opaque
- Automatic cleanup
- Thread handling routines
- Changed cipher suite handling and defaults
- X25519, ChaCha20, Poly1305 support
- Cleaned up IPv6 handling
- DANE TLSA peer authentication
- Removed export (insecure) cipher suites

- ASYNC support
- SSL/TLS state machine rewrite
- Reworked “apps” command line parsing, help strings, option consistency
- OCB mode support
- Many bug fixes
- More test cases and new testing framework
- More documentation
- Obsolete/dead/unsupported code removed
OpenSSL 3.0 Design Meeting

OMC+SPONSORS+ACUMEN MEETING IN BRISBANE, AUGUST 2018
OpenSSL 3.0 Overview

- OpenSSL 3.0 is the next version after OpenSSL 1.1.1
- Removal of unsupportable code in OpenSSL 1.1.1 provides cleaner base for future work
- Major reworking of OpenSSL internals
- Algorithm selection challenges
- Published documents on design
- Published future design objectives
OpenSSL 3.0 – Conceptual Component View
OpenSSL 3.0 – Packaging View

- Applications
  - Common Services
    - Protocols
      - TLS Protocols
      - Other Protocols
    - Supporting Services
  - Legacy APIs

- openssl executable
- libssl
- libcrypt0
OpenSSL 3.0 Design Overview

- All development is public
- Issues raised
- Pull requests
- Incremental changes of components
- Comments welcome
OpenSSL 3.0 Design Overview

- Minimal impact on majority of existing applications
- Only recompilation will be necessary for the majority of existing applications working with OpenSSL 1.1.1
- No marked deprecated API will be removed
- Many low-level functions will be marked as deprecated but remain for this release
- Packaging changes – component / provider based
OpenSSL 3.0 FIPS Design
None of these modules work with OpenSSL v1.1 or OpenSSL v3.0.
History of OpenSSL and FIPS

- OpenSSL FIPS Object Module 3.0
  - Project started seeking sponsors from 2012
  - Initial planning work with potential sponsors in 2015
  - Sponsors finally confirmed mid 2018
  - Project kick off was in late 2018
  - Currently in-development release
  - Everything is public
    - [www.openssl.org](http://www.openssl.org)
    - [github.com.openssl/openssl](https://github.com.openssl/openssl)
    - [https://www.openssl.org/docs/OpenSSL300Design.html](https://www.openssl.org/docs/OpenSSL300Design.html)
OpenSSL 3.0 and FIPS

- **Sponsors**
  - Akamai Technologies
  - Blue Cedar
  - NetApp
  - Oracle
  - VMware

- **FIPS Validation Laboratory**
  - Acumen Security

- **OpenSSL Project Roadmap**
  - Core feature is a FIPS module for validation
OpenSSL 3.0 and FIPS

- Goals for this validation are
  - Small set of operational environments (OEs) tested
  - Core set of algorithms
  - Enable others parties to perform their own validations
  - Maintaining validation made easier
  - Cross-release validation compatibility

- Core restructuring in 3.0 to support these goals
OpenSSL 3.0 FIPS Design – High Level

- New concept of Providers
- Validated FIPS module will be a Provider
- FIPS module is integrated into main line OpenSSL
  - No need for a separate download
  - FIPS module version aligned with main OpenSSL
- The old “fips canister” approach will not be used
- Module boundary will be a dynamically loaded Provider
FIPS140 Boundary – OpenSSL with SHLIB 3.0
OpenSSL 3.0 FIPS Design

- Total of 12 OEs to be tested
  - Various Linux distributions
  - Windows, FreeBSD, Solaris
  - iOS, Android

- Typical set of crypto algorithms

- Highlights: AES KW, SHA-3, HMAC-SHA-3, SP 800-56A (DH and ECC), SP 800-132 (PBKDF2), TLS 1.2 and 1.3 PRF

- Reduction of self-tests overhead using IGs 9.1, 9.2, 9.3, 9.4 and 9.11

- Integrity test for image on disk
Current Status
Current Status – OpenSSL 3.0 Schedule

- Alpha1, 2020-03-31: Basic functionality plus basic FIPS module
- Alpha2, 2020-04-21: Complete external provider support (serialization, support for new algs, support for providers which only include operations in a class)
- Alpha3, 2020-05-21: Aiming to test the API completeness before beta1 freezes it)
- Beta1, 2020-06-02: Code complete (API stable, feature freeze)
- BetaN: Other beta releases TBD
- Final: 2020 early Q4
Progress to date ...
https://github.com/openssl/openssl/projects/2
Latest Status

https://github.com/openssl/openssl/projects/2

- 12 – To do
- 15 – In progress
- 8 – Needs review
- 4 – Reviewer approved
- 301 – Done
Current Status - Development

- Default, Legacy and FIPS provider are present and most of the crypto algorithms have been migrated
- Tremendous work has gone into making OpenSSL 3.0 a reality, however much is to be done
- Code completion: End of Q2 2020
- Final release: End of Q4 2020
Acumen has started developing the ACVP test tool. In parallel, they will begin work on the operational test tool. The goal is to have test tools ready by code complete. Acumen is working closely with OMC in order to finish testing as close to final release as possible. The current expectation is validation report submission code complete + 4-6 weeks. Validation by report submission + 6 months.
Post Certification - Rebranding

- Current validation is limited in OEs
- OMC is not going to be involved in rebranding/addition of OEs
- Interested parties are free to rebrand and add OEs
  - Work directly with Acumen
  - Work directly with lab of your choice
Post Certification – Certificate Maintenance

- OMC plans to keep certification current as opposed to point in time
- Re-certification will be driven based on requirements changes and/or addition of functionality
- Will try and leverage 1SUB and 3SUB re-certification scenarios
Important Links

- OpenSSL: [https://www.openssl.org/](https://www.openssl.org/)
- OpenSSL Blog: [https://www.openssl.org/blog/](https://www.openssl.org/blog/)
- OpenSSL Github: [https://github.com/openssl/openssl](https://github.com/openssl/openssl)
- Acumen Security: [https://www.acumensecurity.net/](https://www.acumensecurity.net/)
Apply what you have learned today

- **Next week you should:**
  - Review development on Git
  - Follow OpenSSL blog for latest developments

- **End of year:**
  - Prepare for final release
  - Ensure your applications work with v1.1.1 and v3.0 (when available)
  - Determine what additional OEs/Rebrands will be required for your business

- **Q1-Q2 2021:**
  - Execute on plans for additional OEs/Rebrands