INTERNATIONAL CRYPTOGRAPHIC MODULE CONFERENCE 2017

May 16-19 | Westin Arlington Gateway | Washington, DC

Inside the OpenSSL 1.1 FIPS Module Project

Tim Hudson

tjh@openssl.org / tjh@cryptsoft.com

Mark J. Minnoch

mark@safelogic.com

S21A 18-May-2017 10:00am

Session Overview

- In July 2016, OpenSSL announced the commencement of a particularly difficult project – the development and validation of a FIPS 140-2 module for OpenSSL 1.1.
- This session will provide an inside look at the progress and hurdles faced by the unprecedented partnership between OpenSSL and SafeLogic.

OpenSSL & FIPS140-2

Strategic Overview

Strategic Overview – Why is it important

- OpenSSL is very widely used
- OpenSSL forms the core of a large number of FIPS140-2 validated products (>244)
- OpenSSL itself is the FIPS140-2 solution directly for a much larger pool of applications
- OpenSSL ships pre-installed on a wide range of operating systems

Strategic Overview – Why is it so hard

- OpenSSL validations have always been complex
  - Multiple competitors (commercial vendors)
  - Everything out in the open and subject to review
  - Unique challenges of being open source
  - Multiple stakeholders

Strategic Overview – Why is it so hard

- Stakeholder goals and project goals often do not align
- Project Goals
  - Goal is broad platform support
  - Broad algorithm support
  - Widespread availability
  - Building block for subsequent updates (change letters)
- Stakeholder Goals
  - Minimal platforms (often 1 or 2)
  - Specific set of algorithms
  - Time is of the essence

OpenSSL & FIPS140-2

Historical Information

FIPS140

- FIPS140 related work effectively entirely funded the OpenSSL project from 2009-2014
- No long term / major sponsor during this time
- Selling into USA Government where FIPS140-2 support is mandatory is important to most large vendors
- The validation process is time consuming and subject to changed requirements
- Coordinating multiple sponsors on a multi-year journey with no guarantee of successful outcome is in itself challenging

FIPS140 – OpenSSL Validation History

- June 2002: initial research and correspondence
- October 2002: selected DOMUS as accredited test lab
- April 2003: secured initial funding from DMLSS & HP
- August 2003: major software mods complete
- May 2004: algorithm validations
- January 2005: new I.G. document, first CMVP feedback
- February 2005: face-to-face meeting with NIST
- January 2006: NIST “done deal” announcement
- March 2006: final award of first open source validation

FIPS140 – OpenSSL Validation History

- #642 1.0 22-Mar-2006
- #733 1.1 06-Feb-2007
- #918 1.1.2 29-Feb-2008
- #1051 1.2 17-Nov-2008
- #1111 1.2 03-Apr-2009 (OpenSSL FIPS Runtime Module)
- #1747 2.0 27-Jun-2012
- #2398 2.0.9+ 24-Jun-2015
- #2437 2.0.9/10 13-Nov-2015

FIPS140 – OpenSSL Validation History

Vendor Open Source Software Institute - 5
1111 140-2 Software 1 2009 Aspect Open Source Software Institute OpenSSL FIPS Runtime Module Software Version: 1.2
1051 140-2 Software 1 2008 DOMUS Open Source Software Institute OpenSSL FIPS Object Module Software Versions: 1.2, 1.2.1, 1.2.2, 1.2.3 or 1.2.4
918 140-2 Software 1 2008 DOMUS Open Source Software Institute OpenSSL FIPS Object Module Source Content Version: 1.1.2; Resultant Compiled Software Version: 1.1.2
733 140-2 Software 1 2007 DOMUS Open Source Software Institute OpenSSL FIPS Object Module Source Content Version: opensslfips1.1.1.tar.gz; Resultant Compiled Software Version: 1.1.1
642 140-2 Software 1 2006 DOMUS Open Source Software Institute OpenSSL FIPS Object Module Source Content Version: OpenSSLfips1.0.tar.gz; Resultant Compiled Software Version: 1.0

FIPS140 – OpenSSL Validation History

Vendor OpenSSL Software Foundation - 3
2473
140-2 Software 1 2015 InfoGard OpenSSL Software Foundation
OpenSSL FIPS Object Module RE
Software Version: 2.0.9 or 2.0.10
2398
140-2 Software 1 2015 InfoGard OpenSSL Software Foundation
OpenSSL FIPS Object Module SE
Software Versions: 2.0.9, 2.0.10, 2.0.11, 2.0.12 or 2.0.13
1747
140-2 Software 1 2012 InfoGard OpenSSL Software Foundation
OpenSSL FIPS Object Module
Software Versions: 2.0, 2.0.1, 2.0.2, 2.0.3, 2.0.4, 2.0.5, 2.0.6, 2.0.7, 2.0.8, 2.0.9 or 2.0.10

FIPS140 – OpenSSL Validation History

- 07/09/12: Added SW 2.0.1, Alg Certs AES 2116, DRBG 229, DSA 661, HMAC 1288, RNG 1087, RSA 1086, SHS 1840, TDES 1346, ECDSA 315, and CVL 24. Replaced Cascade Server with CascadeOS. Added OEs Apple iOS 5.1 (gcc Compiler Version 4.2.1); Microsoft Windows CE 6.0 (Microsoft C/C++ Optimizing Compiler Version 15.00 for ARM); Microsoft Windows CE 5.0 (Microsoft C/C++ Optimizing Compiler Version 13.10 for ARM); Linux 2.6 (gcc Compiler Version 4.1.0); DSP Media Framework 1.4 (TMS320C6x C/C++ Compiler v6.0.13); Android 4.0 running on TI OMAP 3 (ARMv7) with NEON (gcc Compiler Version 4.4.3), updated security policy.
- 07/18/12: Updated security policy.
- 10/23/12: Added SW 2.0.2, Alg Certs AES 2234, DRBG 264, DSA 693, HMAC 1363, RNG 119, RSA 1145, SHS 1923, TDES 1398, ECDSA 347 and CVL 36 and updated security policy plus added OE NetBSD 5.1 (gcc Compiler Version 4.1.3).
- 01/22/13: Updated contact phone number and added Microsoft Windows 2008 running on Intel Xeon E3-1220v2 (32-bit) (Microsoft 32-bit C/C++ Optimizing Compiler Version 16.00 for 80x86); Microsoft Windows 2008 running on Intel Xeon E3-1220v2 (64-bit) (Microsoft C/C++ Optimizing Compiler Version 16.00 for x64); RHEL 6 running on Intel Xeon E3-1220v2 (32-bit) (gcc Compiler Version 4.4.6); RHEL 6 running on Intel Xeon E3-1220v2 (64-bit) (gcc Complier Version 4.4.6); Microsoft Windows 7 running on Intel Core i5-2430M (64-bit) with AES-NI (Microsoft C/C++ Optimizing Compiler Version 16.00 for x64) and updated security policy.
- 02/06/13: added ""under vSphere"" for some OE and updated security policy.
- 02/22/13: added algorithm ECDSA 378 and CVL 49 also OS Android 4.1 and 4.2 and updated security policy.
- 02/28/13: Added SW 2.0.3, Alg Certs AES 2342, DRBG 292, DSA 734, HMAC 1451, RNG 1166, RSA 1205, SHS 2019, TDES 1465, ECDSA 383 and CVL 53 and updated security policy plus added OE Windows Embedded Compact 7 running on Freescale i.MX53xA (ARMv7) with NEON (Microsoft C/C++ Optimizing Compiler Version 15.00.20720); Windows Embedded Compact 7 running on Freescale i.MX53xD (ARMv7) with NEON (Microsoft C/C++ Optimizing Compiler Version 15.00.20720); Android 4.0 running on Qualcomm Snapdragon APQ8060 (ARMv7) with NEON (gcc compiler Version 4.4.3)
- 03/28/13: Added OS and OE VMware Horizon Mobile 1.3 under VMware running on Qualcomm MSM8X60 (ARMv7) with NEON (gcc Compiler Version 4.4.6); Apple OS X 10.7 running on Intel Core i7-3615QM (Apple LLVM version 4.2); Apple iOS 5.0 running on ARM Cortex A8 (ARMv7) with NEON (gcc Compiler Version 4.2.1) and updated security policy.
- 05/16/13: added SW 2.0.4, added Algorithm certs AES 2394, DRBG 316, DSA 748, HMAC 1485, RNG 1186, RSA 1237, SHS 2056, Triple-DES 1492, ECDSA 394 and CVL 71. added OpenWRT 2.6 running on MIPS 24Kc (gcc Compiler Version 4.6.3) and updated security policy.
- 06/14/13: added SW 2.0.5, added Algorithm certs AES 2484, DRBG 342, DSA 764, HMAC 1526, RNG 1202, RSA 1273, SHS 2102, Triple-DES 1522, ECDSA 413 and CVL 85. added QNX 6.4 running on Freescale i.MX25 (ARMv4) (gcc Compiler Version 4.3.3); Apple iOS 6.1 running on Apple A6X SoC (ARMv7s) (gcc Compiler Version 4.2.1); eCos 3 running on Freescale i.MX27 926ejs (ARMv5TEJ) (gcc Compiler Version 4.3.2) and updated security policy.
- 08/16/13: add new OE: Vmware Horizon Workspace 1.5 under vSphere running on Intel Xeon E3-1220 (gcc Compiler Version 4.5.1); Vmware Horizon Workspace 1.5 under vSphere running on Intel Xeon E3-1220 with AES-NI (gcc Compiler Version 4.5.1) and updated security policy.
- 08/23/13: added new OE: Ubuntu 13.04 running on AM335x Cortex-A8 (ARMv7) (gcc Compiler Version 4.7.3); Ubuntu 13.04 running on AM335x Cortex-A8 (ARMv7) with NEON (gcc Compiler Version 4.7.3); Linux 3.8 running on ARM926 (ARMv5TEJ) (gcc Compiler Version 4.7.3) and updated security policy.
- 09/16/13: Updated security policy adding a logo of a sponsor.
- 11/08/13: added new OE: Linux 3.4 64-bit under Citrix XenServer running on Intel Xeon E5-2430L (x86) without AES-NI (gcc Compiler Version 4.8.0); Linux 3.4 64-bit under Citrix XenServer running on Intel Xeon E5-2430L (x86) with AES-NI(gcc Compiler Version 4.8.0); Linux 3.4 64-bit under Vmware ESX running on Intel Xeon E5-2430L (x86) without AES-NI (gcc Compiler Version 4.8.0); Linux 3.4 64-bit under Vmware ESX running on Intel Xeon E5-2430L (x86) with AES-NI (gcc Compiler Version 4.8.0); Linux 3.4 64-bit under Microsoft Hyper-V running on Intel Xeon E5-2430L (x86) without AES-NI (gcc Compiler Version 4.8.0); Linux 3.4 64-bit under Microsoft Hyper-V running on Intel Xeon E5-2430L (x86) with AES-NI (gcc Compiler Version 4.8.0); iOS 6.0 running on Apple A5 / ARM Cortex-A9 (ARMv7) without NEON (gcc Compiler Version 4.2.1); iOS 6.0 running on Apple A5 / ARM Cortex-A9 (ARMv7) with NEON (gcc Compiler Version 4.2.1)
- 12/20/13: added new OE: PexOS 1.0 under vSphere running on Intel Xeon E5-2430L (x86) without AES-NI (gcc Compiler Version 4.6.3); PexOS 1.0 under vSphere running on Intel Xeon E5-2430L (x86) with AES-NI (gcc Compiler Version 4.6.3) and updated security policy.
- 06/27/14: Added SW 2.0.6 and updated the security policy.
- 07/03/14: Added SW 2.0.7, AES 2824, DRBG 485, DSA 853, HMAC 1768, RNG 1278, RSA 1477, SHS 2368, Triple-DES 1695, ECDSA 496, CVL 260, OE Linux 2.6 running on Freescale e500v2 (PPC) (gcc Compiler Version 4.4.1); AcanOS 1.0 running on Intel Core i7-3612QE (x86) without AES-NI (gcc Compiler Version 4.6.2); AcanOS 1.0 running on Intel Core i7-3612QE (x86) with AES-NI (gcc Compiler Version 4.6.2); AcanOS 1.0 running on Feroceon 88FR131 (ARMv5) (gcc Compiler Version 4.5.3); FreeBSD 8.4 running on Intel Xeon E5440 (x86) without AES-NI (gcc Compiler Version 4.2.1); FreeBSD 9.1 running on Xeon E5-2430L (x86) without AES-NI (gcc Compiler Version 4.2.1); FreeBSD 9.1 running on Xeon E5-2430L (x86) with AES-NI (gcc Compiler Version 4.2.1); ArbOS 5.3 running on Xeon E5645 (x86) without AES-NI (gcc Compiler Version 4.1.2); Linux ORACLESP 2.6 running on ASPEED AST2100 (ARMv5) (gcc Compiler Version 4.4.5); Linux ORACLESP 2.6 running on ServerEngines PILOT3 (ARMv5) (gcc Compiler Version 4.4.5) and updated the security policy.
- 09/02/14: Added OE ArbOS 5.3 running on Xeon E5645 (x86) with AES-NI (gcc Compiler Version 4.1.2); FreeBSD 9.2 running on Xeon E5-2430L (x86) without AES-NI (gcc Compiler Version 4.2.1); FreeBSD 9.2 running on Xeon E5-2430L (x86) with AES-NI (gcc Compiler Version 4.2.1) and updated the security policy.
- 09/12/14: Added SW 2.0.8, AES 2929, DRBG 540, DSA 870, HMAC 1856, RNG 1292, RSA 1535, SHS 2465, Triple-DES 1742, ECDSA 528, CVL 331, OE FreeBSD 10.0 running on Xeon E5-2430L (x86) without AES-NI (clang Compiler Version 3.3); FreeBSD 10.0 running on Xeon E5-2430L (x86) with AES-NI (clang Compiler Version 3.3) and updated the security policy.
- 10/16/14: Added OE FreeBSD 8.4 running on Intel Xeon E5440 (x86) 32-bit (gcc Compiler Version 4.2.1) and updated the security policy.
- 12/31/14: Added SW 2.0.9, AES 3090, DRBG 607, DSA 896, HMAC 1937, RNG 1314, RSA 1581, SHS 2553, Triple-DES 1780, ECDSA 558, CVL 372, OE Vmware Horizon Workspace 2.1 under vSphere ESXi 5.5 running on Intel Xeon E3-1220 (x86) without AES-NI (gcc Compiler Version 4.5.1); Vmware Horizon Workspace 2.1 under vSphere ESXi 5.5 running on Intel Xeon E3-1220 (x86) with AESNI (gcc Compiler Version 4.5.1); QNX 6.5 running on Freescale i.MX25 (ARMv4) (gcc Compiler Version 4.3.3); Apple iOS 7.1 64-bit running on Apple A7 (ARMv8) without NEON (clang Compiler Version 5.1); Apple iOS 7.1 64-bit running on Apple A7 (ARMv8) with NEON (clang Compiler Version 5.1) and updated the security policy.
- 06/15/15: Removed incomplete platforms listings from OE.
- 09/04/15: Added SW 2.0.10, AES 3264, DRBG 723, DSA 933, HMAC 2063, RNG 1349, RSA 1664, SHS 2702, Triple-DES 1853, ECDSA 620, CVL 472, updated several OE and updated the security policy.
- Deprecated use of the non-approved RNG.
- Updated vendor name.

FIPS140

- The OpenSSL FIPS 2.0 module (#1747, #2389, #2437) works with OpenSSL-1.0.x
- The previous OpenSSL FIPS 1.0 module for OpenSSL-0.9.x is **no longer usable**
- A major update is required for a new OpenSSL FIPS module to work with OpenSSL-1.1.x
- Objective is to make the FIPS140 related changes “less intrusive”

FIPS140-2 Operational Environments (1 of 9)

AcanOS 1.0 running on Feroceon 88FR131 (ARMv5) (gcc Compiler Version 4.5.3)
AcanOS 1.0 running on Intel Core i7-3612QE (x86) with AES-NI (gcc Compiler Version 4.6.2)
AcanOS 1.0 running on Intel Core i7-3612QE (x86) without AES-NI (gcc Compiler Version 4.6.2)
AIX 6.1 32-bit running on IBM POWER 7 (PPC) (IBM XL C/C++ for AIX Compiler Version V13.1)
AIX 6.1 32-bit running on IBM POWER 7 (PPC) with optimizations (IBM XL C/C++ for AIX Compiler Version V10.1)
AIX 6.1 64-bit running on IBM POWER 7 (PPC) (IBM XL C/C++ for AIX Compiler Version V13.1)
AIX 6.1 64-bit running on IBM POWER 7 (PPC) with optimizations (IBM XL C/C++ for AIX Compiler Version V10.1)
AIX 7.1 32-bit running on IBM POWER 7 (PPC) (IBM XL C/C++ for AIX Compiler Version V13.1)
AIX 7.1 32-bit running on IBM Power8 (PPC) without PAA (IBM XL Compiler V13.1)
AIX 7.1 32-bit running on IBM Power8 (PPC) with PAA (IBM XL Compiler V13.1)
AIX 7.1 64-bit running on IBM POWER 7 (PPC) (IBM XL C/C++ for AIX Compiler Version V13.1)
AIX 7.1 64-bit running on IBM Power8 (PPC) without PAA (IBM XL Compiler V13.1)
AIX 7.1 64-bit running on IBM Power8 (PPC) with PAA (IBM XL Compiler V13.1)
AIX 7.2 32-bit running on IBM Power7 (PPC) without PAA (IBM XL Compiler V13.1)
AIX 7.2 32-bit running on IBM Power8 (PPC) without PAA (IBM XL Compiler V13.1)
AIX 7.2 32-bit running on IBM Power8 (PPC) with PAA (IBM XL Compiler V13.1)
AIX 7.2 64-bit running on IBM Power7 (PPC) without PAA (IBM XL Compiler V13.1)
AIX 7.2 64-bit running on IBM Power8 (PPC) without PAA (IBM XL Compiler V13.1)
AIX 7.2 64-bit running on IBM Power8 (PPC) with PAA (IBM XL Compiler V13.1)
Android 2.2 (gcc Compiler Version 4.4.0)
Android 2.2 running on OMAP 3530 (ARMv7) with NEON (gcc Compiler Version 4.1.0)
Android 2.2 running on Qualcomm QSD8250 (ARMv7) with NEON (gcc Compiler Version 4.4.0)
Android 2.2 running on Qualcomm QSD8250 (ARMv7) without NEON (gcc Compiler Version 4.4.0)
Android 3.0 (gcc Compiler Version 4.4.0)
Android 3.0 running on NVIDIA Tegra 250 T20 (ARMv7) (gcc Compiler Version 4.4.0)

FIPS140-2 Operational Environments (2 of 9)

Android 4.0 (gcc Compiler Version 4.4.3)
Android 4.0 running on NVIDIA Tegra 250 T20 (ARMv7) (gcc Compiler Version 4.4.3)
Android 4.0 running on Qualcomm Snapdragon APQ8060 (ARMv7) with NEON (gcc compiler Version 4.4.3)
Android 4.0 running on TI OMAP 3 (ARMv7) with NEON (gcc Compiler Version 4.4.3)
Android 4.1 running on TI DM3730 (ARMv7) (gcc Compiler Version 4.6)
Android 4.1 running on TI DM3730 (ARMv7) with NEON (gcc Complier Version 4.6)
Android 4.1 running on TI DM3730 (ARMv7) without NEON (gcc Compiler Version 4.6)
Android 4.2 running on Nvidia Tegra 3 (ARMv7) (gcc Compiler Version 4.6)
Android 4.2 running on Nvidia Tegra 3 (ARMv7) with Neon (gcc Compiler Version 4.6)
Android 4.2 running on Nvidia Tegra 3 (ARMv7) with NEON (gcc Compiler Version 4.6)
Android 4.2 running on Nvidia Tegra 3 (ARMv7) without NEON (gcc Compiler Version 4.6)
Android 4.4 32-bit running on Intel Atom Z3735F (x86) (gcc Compiler Version 4.8)
Android 5.0 32-bit running on Qualcomm APQ8084 (ARMv7) with NEON (gcc Compiler Version 4.9)
Android 5.0 32-bit running on Qualcomm APQ8084 (ARMv7) without NEON (gcc Compiler Version 4.9)
Android 5.0 64-bit running on SAMSUNG Exynos7420 (ARMv8) with NEON and Crypto Extensions (gcc Compiler Version 4.9)
Android 5.0 64-bit running on SAMSUNG Exynos7420 (ARMv8) without NEON and Crypto Extensions (gcc Compiler Version 4.9)
Apple iOS 5.0 running on ARM Cortex A8 (ARMv7) with NEON (gcc Compiler Version 4.2.1)
Apple iOS 5.1 (gcc Compiler Version 4.2.1)
Apple iOS 5.1 running on ARMv7 (gcc Compiler Version 4.2.1)
Apple iOS 6.1 running on Apple A6X SoC (ARMv7s) (gcc Compiler Version 4.2.1)
Apple iOS 7.1 64-bit running on Apple A7 (ARMv8) with NEON (clang Compiler Version 5.1)
Apple iOS 7.1 64- bit running on Apple A7 (ARMv8) without NEON (clang Compiler Version 5.1)
Apple OS X 10.7 running on Intel Core i7-3615QM (Apple LLVM version 4.2)
ArbOS 5.3 running on Xeon E5645 (x86) with AES-NI (gcc Compiler Version 4.1.2)
ArbOS 5.3 running on Xeon E5645 (x86) without AES-NI (gcc Compiler Version 4.1.2)

FIPS140-2 Operational Environments (3 of 9)

CascadeOS 6.1 (32 bit) (gcc Compiler Version 4.4.5)
CascadeOS 6.1 (32 bit) running on Intel Pentium T4200 (gcc Compiler Version 4.4.5)
CascadeOS 6.1 (64 bit) (gcc Compiler Version 4.4.5)
CascadeOS 6.1 (64 bit) running on Intel Pentium T4200 (gcc Compiler Version 4.4.5)
CentOS 5.6 64-bit running on Intel Xeon E5-2620v3 (gcc Compiler Version 4.1.2)
CentOS 5.6 64-bit running on Intel Xeon E5-2690v3 (gcc Compiler Version 4.1.2)
DataGravity Discovery Series OS V2.0 running on Intel Xeon E5-2420 (x86) with AES-NI (gcc Compiler Version 4.7.2)
DataGravity Discovery Series OS V2.0 running on Intel Xeon E5-2420 (x86) without AES-NI (gcc Compiler Version 4.7.2)
Debian 7.9 running on Marvell Mohawk (ARMv5TE) (gcc Compiler Version 4.4.5)
DSP Media Framework 1.4 running on TI C64x+ (TMS320C6x C/C++ Compiler v6.0.13)
DSP Media Framework 1.4 (TMS320C6x C/C++ Compiler v6.0.13)
eCos 3 running on Freescale i.MX27 926ejs (ARMv5TEJ) (gcc Compiler Version 4.3.2)
ExtremeXOS-Linux 3.1 running on Cavium Octeon II (MIPS)(gcc Compiler Version 4.9.2)
Fedora 14 running on Intel Core i5 with AES-NI (gcc Compiler Version 4.5.1)
FreeBSD 10.0 running on Xeon E5- 2430L (x86) with AES-NI (clang Compiler Version 3.3)
FreeBSD 10.0 running on Xeon E5-2430L (x86) with AES-NI (clang Compiler Version 3.3)
FreeBSD 10.0 running on Xeon E5-2430L (x86) without AES-NI (clang Compiler Version 3.3)
FreeBSD 10.2 running on Intel Xeon E5-2430L (x86) with AES-NI (clang Compiler Version 3.4.1)
FreeBSD 10.2 running on Intel Xeon E5-2430L (x86) without AES-NI (clang Compiler Version 3.4.1)
FreeBSD 8.4 running on Intel Xeon E5440 (x86) 32-bit (gcc Compiler Version 4.2.1)
FreeBSD 8.4 running on Intel Xeon E5440 (x86) without AES-NI (gcc Compiler Version 4.2.1)
FreeBSD 8.4 running on Intel Xeon E5440 (x86) without AESNI (gcc Compiler Version 4.2.1)
FreeBSD 9.1 running on Xeon E5-2430L (x86) with AES-NI (gcc Compiler Version 4.2.1)
FreeBSD 9.1 running on Xeon E5-2430L (x86) without AES-NI (gcc Compiler Version 4.2.1)
FreeBSD 9.1 running on Xeon E5-2430L (x86) without AESNI (gcc Compiler Version 4.2.1)

FIPS140-2 Operational Environments (4 of 9)

FreeBSD 9.2 running on Xeon E5-2430L (x86) with AES-NI (gcc Compiler Version 4.2.1)
FreeBSD 9.2 running on Xeon E5-2430L (x86) without AES-NI (gcc Compiler Version 4.2.1)
HP-UX 11i (32 bit) (HP C/aC++ B3910B)
HP-UX 11i (32 bit) running on Intel Itanium 2 (HP C/aC++ B3910B)
HP-UX 11i (64 bit) (HP C/aC++ B3910B)
HP-UX 11i (64 bit) running on Intel Itanium 2 (HP C/aC++ B3910B)
iOS 6.0 running on Apple A5 / ARM Cortex-A9 (ARMv7) with NEON (gcc Compiler Version 4.2.1)
iOS 6.0 running on Apple A5 / ARM Cortex-A9 (ARMv7) without NEON (gcc Compiler Version 4.2.1)
iOS 8.1 32-bit running on Apple A7 (ARMv8) with NEON (clang Compiler Version 600.0.56)
iOS 8.1 32-bit running on Apple A7 (ARMv8) with NEON (clang Compiler Version 600.0.56)
iOS 8.1 32-bit running on Apple A7 (ARMv8) without NEON (clang Compiler Version 600.0.56)
iOS 8.1 32-bit running on Apple A7 (ARMv8) without NEON (clang Compiler Version 600.0.56)
iOS 8.1 64-bit running on Apple A7 (ARMv8) with NEON and Crypto Extensions (clang Compiler Version 600.0.56)
iOS 8.1 64-bit running on Apple A7 (ARMv8) with NEON and Crypto Extensions (clang Compiler Version 600.0.56)
iOS 8.1 64-bit running on Apple A7 (ARMv8) without NEON and Crypto Extensions (clang Compiler Version 600.0.56)
iOS 8.1 64-bit running on Apple A7 (ARMv8) without NEON and Crypto Extensions (clang Compiler Version 600.0.56)
iOS 8.1 64-bit running on Apple A7 (ARMv8) without NEON and Crypto Extensions (clang Compilerv Version 600.0.56)
Linux 2.6.27 (gcc Compiler Version 4.2.4)
Linux 2.6.27 running on PowerPC e300c3 (gcc Compiler Version 4.2.4)
Linux 2.6.32 (gcc Compiler Version 4.3.2)
Linux 2.6.32 running on TI AM3703CBP (ARMv7) (gcc Compiler Version 4.3.2)
Linux 2.6.33 (gcc Compiler Version 4.1.0)
Linux 2.6.33 running on PowerPC32 e300 (gcc Compiler Version 4.1.0)
Linux 2.6 (gcc Compiler Version 4.1.0)
Linux 2.6 (gcc Compiler Version 4.3.2)

FIPS140-2 Operational Environments (5 of 9)

Linux 2.6 running on a Nimble Storage CS300 with AES-NI
Linux 2.6 running on a Nimble Storage CS500 with AES-NI
Linux 2.6 running on a Nimble Storage CS700 with AES-NI
Linux 2.6 running on Broadcom BCM11107 (ARMv6) (gcc Compiler Version 4.3.2)
Linux 2.6 running on Freescale e500v2 (PPC) (gcc Compiler Version 4.4.1)
Linux 2.6 running on Freescale PowerPCe500 (gcc Compiler Version 4.1.0)
Linux 2.6 running on TI TMS320DM6446 (ARMv4) (gcc Compiler Version 4.3.2)
Linux 3.10 32-bit running on Intel Atom E3845 (x86) with AES-NI (gcc Compiler Version 4.8.1)
Linux 3.10 32-bit running on Intel Atom E3845 (x86) without AES-NI (gcc Compiler Version 4.8.1)
Linux 3.10 on VMware ESXi 6.00 running on Intel Xeon with AES-NI (gcc Compiler Version 4.8.3)
Linux 3.10 on Vmware ESXi 6.00 running on Intel Xeon without AES-NI (gcc Compiler Version 4.8.3)
Linux 3.10 running on Intel Xeon with AES-NI (gcc Compiler Version 4.8.3)
Linux 3.10 running on Intel Xeon without AES-NI (gcc Compiler Version 4.8.3)
Linux 3.14 running on ARM Cortex A9 (ARMv7) with NEON (gcc Compiler Version 4.8.2)
Linux 3.14 running on ARM Cortex A9 (ARMv7) without NEON (gcc Compiler Version 4.8.2)
Linux 3.16 running on Atmel ATSAM9G45 (ARMv5TEJ) (gcc Compiler Version 4.8.3)
Linux 3.16 running on Atmel ATSAMA5D35 (ARMv7) (gcc Compiler Version 4.8.3)
Linux 3.4 64-bit under Citrix XenServer running on Intel Xeon E5-2430L (x86) without AES-NI
Linux 3.4 under Citrix XenServer 6.2 running on Intel Xeon E5-2430L with AES-NI (gcc Compiler Version 4.8.0)
Linux 3.4 under Citrix XenServer 6.2 running on Intel Xeon E5-2430L without AES-NI (gcc Compiler Version 4.8.0)
Linux 3.4 under Microsoft Windows 2012 Hyper-V running on Intel Xeon E5-2430L with AES-NI (gcc Compiler Version 4.8.0)
Linux 3.4 under Microsoft Windows 2012 Hyper-V running on Intel Xeon E5-2430L with AES-NI (gcc Compiler Version 4.8.0)2
Linux 3.4 under Microsoft Windows 2012 Hyper-V running on Intel Xeon E5-2430L without AES-NI (gcc Compiler Version 4.8.0)
Linux 3.4 under Vmware ESXi 5.1 running on Intel Xeon E5-2430L with AES-NI (gcc Compiler Version 4.8.0)
Linux 3.4 under Vmware ESXi 5.1 running on Intel Xeon E5-2430L without AES-NI (gcc Compiler Version 4.8.0)

FIPS140-2 Operational Environments (6 of 9)

Linux 4.4 running on ARM926EJS (ARMv5) (gcc Compiler Version 4.8.3)
Linux ORACLESP 2.6 running on ASPEED AST-Series (ARMv5) (gcc Compiler Version 4.4.5)
Linux ORACLESP 2.6 running on Emulex PILOT3 (ARMv5) (gcc Compiler Version 4.4.5)
LMOS 7.2 running on Intel Xeon E3-1231 (x86) with AES-NI (gcc Compiler Version 4.8.4)
LMOS 7.2 running on Intel Xeon E3-1231 (x86) without AES-NI (gcc Compiler Version 4.8.4)
LMOS 7.2 under VMware ESXi 6.5 running on Intel Xeon E5-2430L (x86) with AES-NI (gcc Compiler Version 4.8.4)
LMOS 7.2 under VMware ESXi 6.5 running on Intel Xeon E5-2430L (x86) without AES-NI (gcc Compiler Version 4.8.4)
Microsoft Windows 7 (32 bit) (Microsoft 32 bit C/C++ Optimizing Compiler Version 16.00)
Microsoft Windows 7 (32 bit) running on Intel Celeron (Microsoft 32 bit C/C++ Optimizing Compiler Version 16.00)
Microsoft Windows 7 (64 bit) (Microsoft C/C++ Optimizing Compiler Version 16.00)
Microsoft Windows 7 (64 bit) running on Intel Pentium 4 (Microsoft C/C++ Optimizing Compiler Version 16.00)
Microsoft Windows 7 running on Intel Core i5- 2430M (64-bit) with AES-NI (Microsoft ® C/C++ Optimizing Compiler Version 16.00 for x64)
Microsoft Windows 7 running on Intel Core i5-2430M (64-bit) with AES-NI (Microsoft « C/C++ Optimizing Compiler Version 16.00 for x64)
Microsoft Windows CE 5.0 (Microsoft C/C++ Optimizing Compiler Version 13.10 for ARM)
Microsoft Windows CE 5.0 running on ARMv7 (Microsoft C/C++ Optimizing Compiler Version 13.10 for ARM)
Microsoft Windows CE 6.0 (Microsoft C/C++ Optimizing Compiler Version 15.00 for ARM)
Microsoft Windows CE 6.0 running on ARMv5TEJ (Microsoft C/C++ Optimizing Compiler Version 15.00 for ARM)
Microsoft Windows Server 2008 R2 running on an Intel Xeon E5-2420 (x64) (Microsoft 32-bit C/C++ Optimizing Compiler Version 16.00.40219.01 for 80x86)
NetBSD 5.1 (gcc Compiler Version 4.1.3)
NetBSD 5.1 running on Intel Xeon 5500 (gcc Compiler Version 4.1.3)
NetBSD 5.1 running on PowerPCe500 (gcc Compiler Version 4.1.3)
OpenWRT 2.6 running on MIPS 24Kc (gcc Compiler Version 4.6.3)
Oracle Linux 5 (64 bit) (gcc Compiler Version 4.1.2)
Oracle Linux 5 (64 bit) running on Intel Xeon 5675 (gcc Compiler Version 4.1.2)
Oracle Linux 5 running on Intel Xeon 5675 with AES-NI (gcc Compiler Version 4.1.2)

FIPS140-2 Operational Environments (7 of 9)

Oracle Linux 6 (gcc Compiler Version 4.4.6)
Oracle Linux 6 running on Intel Xeon 5675 with AES-NI (gcc Compiler Version 4.4.6)
Oracle Linux 6 running on Intel Xeon 5675 without AES-NI (gcc Compiler Version 4.4.6)
Oracle Solaris 10 (32 bit) (gcc Compiler Version 3.4.3)
Oracle Solaris 10 (32 bit) running on SPARC-T3 (SPARCv9) (gcc Compiler Version3.4.3)
Oracle Solaris 10 (64 bit) (gcc Compiler Version 3.4.3)
Oracle Solaris 10 (64 bit) running on SPARC-T3 (SPARCv9) (gcc Compiler Version 3.4.3)
Oracle Solaris 11(32 bit) (gcc Compiler Version 4.5.2)
Oracle Solaris 11 (32 bit) running on Intel Xeon 5675 (gcc Compiler Version 4.5.2)
Oracle Solaris 11 (32 bit) running on SPARC-T3 (SPARCv9) (Sun C Version 5.12)
Oracle Solaris 11 (32 bit) (Sun C Version 5.12)
Oracle Solaris 11 (64 bit) (gcc Compiler Version 4.5.2)
Oracle Solaris 11 (64 bit) running on Intel Xeon 5675 (gcc Compiler Version 4.5.2)
Oracle Solaris 11 (64 bit) running on SPARC-T3 (SPARCv9) (Sun C Version 5.12)
Oracle Solaris 11 (64 bit) (Sun C Version 5.12)
Oracle Solaris 11 running on Intel Xeon 5675 with AES-NI (32 bit) (gcc Compiler Version 4.5.2)
Oracle Solaris 11 running on Intel Xeon 5675 with AESNI (32 bit) (gcc Compiler Version 4.5.2)
Oracle Solaris 11 running on Intel Xeon 5675 with AES-NI (64 bit) (gcc Compiler Version 4.5.2)
Oracle Solaris 11 running on Intel Xeon 5675 with AESNI (64 bit) (gcc Compiler Version 4.5.2)
PexOS 1.0 under vSphere ESXi 5.1 running on Intel Xeon E52430L with AES-NI (gcc Compiler Version 4.6.3)3
PexOS 1.0 under vSphere ESXi 5.1 running on Intel Xeon E52430L without AES-NI (gcc Compiler Version 4.6.3)
QNX 6.4 running on Freescale i.MX25 (ARMv4) (gcc Compiler Version 4.3.3)
QNX 6.5 running on Freescale i.MX25 (ARMv4) (gcc Compiler Version 4.3.3)
SurfWare 7.2 running on TI c64 DSP (TMS320C6x Compiler Version 6.0.19)
Timesys 2.6 running on PowerPC 440 (PPC) (gcc Compiler Version 4.6.3)

FIPS140-2 Operational Environments (8 of 9)

TS-Linux 2.4 running on Arm920Tid (ARMv4) (gcc Compiler Version 4.3.2)
TS-Linux 2.4 running on Arm920Tid (ARMv4) (gcc Compiler Version 4.3.2)4
Ubuntu 10.04 (32 bit) (gcc Compiler Version 4.1.3)
Ubuntu 10.04 (32 bit) running on Intel Pentium T4200 (gcc Compiler Version 4.1.3)
Ubuntu 10.04 (64 bit) (gcc Compiler Version 4.1.3)
Ubuntu 10.04 (64 bit) running on Intel Pentium T4200 (gcc Compiler Version 4.1.3)
Ubuntu 10.04 running on Intel Core i5 with AES-NI (32 bit) (gcc Compiler Version 4.1.3)
Ubuntu 10.04 running on Intel Pentium T4200 (gcc Compiler Version 4.1.3)
Ubuntu 12.04 running on Intel Xeon E5-2430L (x86) with AES-NI (gcc Compiler Version 4.6.3)
Ubuntu 12.04 running on Intel Xeon E5-2430L (x86) without AES-NI (gcc Compiler Version 4.6.3)
Ubuntu 13.04 running on AM335x Cortex-A8 (ARMv7) (gcc Compiler Version 4.7.3)
Ubuntu 13.04 running on AM335x Cortex-A8 (ARMv7) with NEON (gcc Compiler Version 4.7.3)
Ubuntu 13.04 running on AM335x Cortex-A8 (ARMv7) without NEON (gcc Compiler Version 4.7.3)
uClibc 0.9 running on ARM922T (ARMv4T) (gcc Compiler Version 4.8.1)
uClibc 0.9 running on ARM926EJS (ARMv5TEJ) (gcc Compiler Version 4.8.1)
uClibc 0.9 running on Marvell PJ4 (ARMv7) (gcc Compiler Version 4.8.1)
uCLinux 0.9.29 (gcc Compiler Version 4.2.1)
uCLinux 0.9.29 running on ARM 922T (ARMv4) (gcc Compiler Version 4.2.1)
uClinux-dist-5.0 running on Marvell Armada 370 (ARMv7) (gcc Compiler Version 4.8.3)
uClinux-dist-5.0 running on Marvell Feroceon 88FR131 (ARMv5TE) (gcc Compiler Version 4.8.3)
Vmware Horizon Workspace 1.5 under Vmware ESXi 5.0 running on Intel Xeon E3-1220 (x86) with AES-NI (gcc Compiler Version 4.5.1)1
Vmware Horizon Workspace 1.5 under Vmware ESXi 5.0 running on Intel Xeon E3-1220 (x86) without AES-NI (gcc Compiler Version 4.5.1)
Vmware Horizon Workspace 2.1 under vSphere ESXi 5.5 running on Intel Xeon E3-1220 (x86) with AES-NI (gcc Compiler Version 4.5.1)
Vmware Horizon Workspace 2.1 under vSphere ESXi 5.5 running on Intel Xeon E3-1220 (x86) with AESNI (gcc Compiler Version 4.5.1)
Vmware Horizon Workspace 2.1 under vSphere ESXi 5.5 running on Intel Xeon E3-1220 (x86) without AES-NI (gcc Compiler Version 4.5.1)

FIPS140-2 Operational Environments (9 of 9)

VxWorks 6.7 running on Intel Core 2 Duo (x86) (gcc Compiler Version 4.1.2)
VxWorks 6.8 (gcc Compiler Version 4.1.2)
VxWorks 6.8 running on TI TNETV1050 (MIPS) (gcc Compiler Version 4.1.2)
VxWorks 6.9 running on Freescale P2020 (PPC) (gcc Compiler Version 4.3.3)
Windows Embedded Compact 7 running on Freescale i.MX53xA (ARMv7) with NEON (Microsoft C/C++ Optimizing Compiler Version 15.00.20720)
Windows Embedded Compact 7 running on Freescale i.MX53xD (ARMv7) with NEON (Microsoft C/C++ Optimizing Compiler Version 15.00.20720)
Yocto Linux 3.10 running on Freescale i.MX6 (ARMv7) with NEON (gcc Compiler Version 4.8.1)
Yocto Linux 3.10 running on Freescale i.MX6 (ARMv7) without NEON (gcc Compiler Version 4.8.1)

OpenSSL & FIPS140-2

Current Sponsor Status

Current Status

- SafeLogic is the only Sponsor
- Additional Sponsors are needed to fund:
  - OpenSSL FIPS development
  - FIPS Lab testing
- Resources are available now

Challenges Ahead

- High risk validation – only the strong need apply
  - Many eyes on the validation
  - All parties are cautious
  - Caution creates longer timelines
- Critically important
  - 240+ FIPS modules reference OpenSSL
  - Countless others embed OpenSSL
  - TLS 1.3 only available in OpenSSL 1.1.x

Challenges Ahead (cont.)

- Finding Sponsors is hard
- Sponsors would like:
  - Assurance of success
  - Other Sponsors to share costs
  - Schedule
  - Input on tested configurations

What lack of success looks like…

- …to technology vendors:
  - Fewer options for FIPS libraries
  - More FIPS work / less product development
- …to the CMVP and FIPS Labs
  - Multiple validations of the same base crypto library
- …to Federal agencies
  - Inconsistent implementations
  - Fewer FIPS validated products

What success looks like…

- …to technology vendors:
  - Smoother transition to OpenSSL 1.1.x
  - Less FIPS work / more product development
- …to the CMVP and FIPS Labs
  - Single validation of the crypto library
- …to Federal agencies
  - Consistent implementations
  - More FIPS validated products

T

OpenSSL & FIPS140-2

Current Technical Status

Current Technical Status

- Lessons Learned
  - Expect the unexpected
    - TLSv1.3 timing pushed FIPS140 work later
  - Many companies have expressed an interest in participating but to date only SafeLogic has committed to participation
- Challenges Remaining
  - Scope remains much larger than what is likely to be completed
  - Additional sponsor vendors will be required

Technical Details

- Keep the cryptographic module code minimal
  - no broader OpenSSL (non-crypto) dependencies
  - the cryptographic module should be fully usable entirely standalone
  - the module should contain the absolute minimum of code
- Keep the source distribution of the module minimal
  - only required source included
  - test suite and utility code separately packaged from the module source distribution

Technical Details

- Refactored algorithm testing approach
  - cleaner; more modular; benefits of having done previous validations is we know what we need to cover better than in the first validations
- Support easier embedded platform use
  - testing able to operate without file system support
    - Current testing for embedded platforms can be painful when there is limited “local” storage available
  - support building “out-of-tree”

Technical Details

- Default entropy gathering
  - remove this burden from the user of the module and gather sufficient entropy by default on all platforms
  - user will always be able to provide more but the module should function as-is on most platforms without additional user entropy having to be provided in order to pass the continuous runtime tests

Technical Details

- Improved integration with OpenSSL
  - should be able to be packaged as an OpenSSL engine
  - objective is to enable usage with a standard OpenSSL 1.1+ release (i.e. no need to build a special FIPS-capable OpenSSL in future)

Technical Details

- Specific FIPS 140-2 items
  - FIPS 186-4 Key Gen
  - NIST SP 800-56A Compliance (Self-tests as per I.G. 9.6)
    - Diffie-Hellman - Shared secret KAT, KDF KAT
  - NIST SP 800-56B vendor affirmation (as per I.G. D.4)
  - SHA-3 + SHAKE
  - Validation of “stitched” algorithms

Technical Details

- Power on Self-tests (POST)
  - incorporate any allowed efficiencies in self-tests
  - allow for specific “modes” where the POST executed list can be adjusted
  - allow for specific “modes” where the available algorithms can be “reduced”

Technical Details

- Items remaining resolution depending on CMVP viewpoint
  - Level of user control of POST
  - Validation of “stitched” algorithms
  - ChaCha20/Poly1305
  - New EC curves (e.g. curve 25519)

Technical Details

- Items requested by various stake holders that are **not committed** for delivery in any OpenSSL FIPS140 release
  - NIST SP 800-56B validation of RSA key wrapping (KTS validation)
  - AES-GMAC (I.G. A.5)
  - NIST SP 800-38F compliance for AES Key Wrap
  - PBKDF2
  - NIST SP 800-38G Format Preserving Encryption (FPE)
  - EC Curve 25519

Technical Details

- Items requested by various stake holders that are **not committed** for delivery in any OpenSSL FIPS140 release
  - NIST SP 800-153 KDFs
  - NIST SP 800-108 KDFs
  - AES XPN
  - AES XTS conformance to I.G. A.9

T

OpenSSL & FIPS140-2

Project Schedule

Current Draft Project Timeline

Target	Task
Month 0	SafeLogic + Other Sponsors commitments received
Month 1	Technical parameters locked in for development
Month 2	OpenSSL team begins development
Month 5	Development check point 1 – basic framework
Month 7	Development check point 2 – alpha level
Month 8	Development check point 3 – beta level
Month 9	Development check point 4 – final level
Month 10	FIPS 140-2 documentation finalized
Month 12	Lab submits FIPS 140-2 report to CMVP
Month **18+** ??	CMVP issues FIPS 140-2 certificate

Note: the timeline is a best guess – it is not a commitment as the review process is entirely unpredictable. Based on past experience this timeline is optimistic!

Current Project Challenges

- What is happening to the existing modules?
- When can I expect a validated module?
- When can I know which platforms are included?
- What about FIPS140-3?

OpenSSL & FIPS140-2

User Strategy

User Strategy

- Strategy for companies and individuals who hope to deploy the software
- How the community can assist

T

OpenSSL

Future Directions

OpenSSL – Future Directions

Contributing …

- Download the pre-releases and build your applications
- Join the openssl-dev and/or openssl-users mailing lists
- Report bugs, submit patches
- More ideas on the Community page of www.openssl.org

Questions

Tim Hudson

tjh@openssl.org / tjh@cryptsoft.com

Mark J. Minnoch

mark@safelogic.com

T

OpenSSL

Cryptography and SSL/TLS Toolkit