OpenSSL after HeartBleed

Tim Hudson
Cryptsoft, OpenSSL Team
Rich Salz
Akamai Technologies, OpenSSL Team

OpenSSL
Cryptography and SSL/TLS Toolkit

The most important date

- April 3, 2014

The most important date

- April 3, 2014

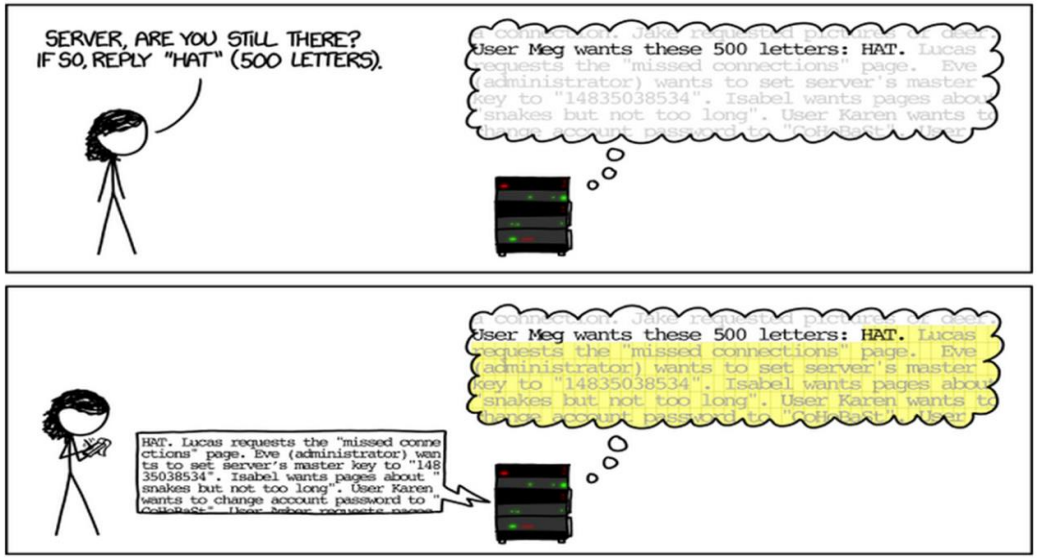
- HeartBleed
- Re-key the Internet

So what was HeartBleed?

- Massive mainstream press coverage

So what was HeartBleed?

- A very simple bug, the code didn't check a buffer length.



Source: http://xkcd.com/1354/ courtesy Randall Munroe

So what was HeartBleed?

To the best of our knowledge, Heartbleed is the first computer systems bug to have both its own website and its own logo, the cute bleeding heart. As such, Heartbleed sets a precedent that will have both positive and negative ramifications for future vulnerabilities and malware.

…

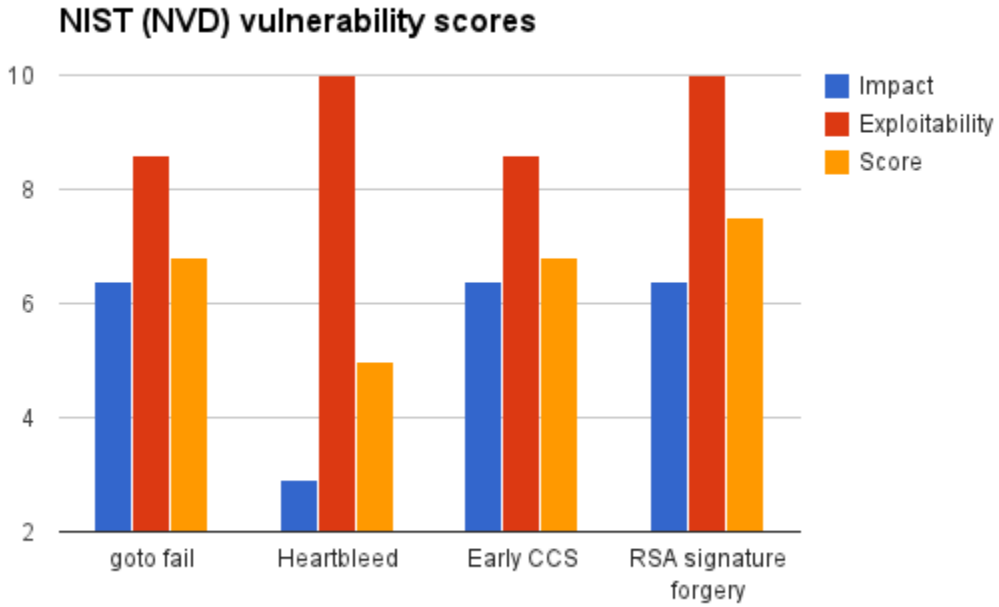
Even among the vast majority of the population who have no idea what OpenSSL is, people everywhere quickly found out that a major bug could compromise their Internet security.

Source: VDC Research - http://blog.vdcresearch.com/embedded_sw/2014/04/exploiting-the-exploit-the-marketing-of-heartbleed.html

The sky is falling …

- CVE-2011-0014 - infoleak, true impact unknown
- CVE-2012-2110 - possibly arbitrary code execution on reading certificates
- CVE-2012-2333 - buffer over-read, true impact unknown
- CVE-2014-1266 - “goto fail” server spoofing (Apple)
- CVE-2014-0160 – Heartbleed
- CVE-2014-0224 - “early CCS” disables encryption
- CVE-2014-1568 - RSA signature forgery (NSS)

Or is it …


NIST (NVD) vulnerability scores
10
8
6
4
2
Impact
Exploitability
Score
goto fail
Heartbleed
Early CCS
RSA signature forgery

So what was HeartBleed?

- Basically missed validating a variable containing a length
- Contributed code had a bug – bug was in code base for **three years**!
- Project team member review missed the bug
- Other team members either didn't review or also simply missed the bug
- Multiple external security reviewers and auditors missed the bug
- OpenSSL external developers and users missed the bug
- Security review teams in major OpenSSL using organisations missed the bug
- **All** existing code analysis tools missed the bug
- Bug allowed clients to attack servers **and** servers to attack clients

So what was HeartBleed?

Add support for TLS/DTLS heartbeats.

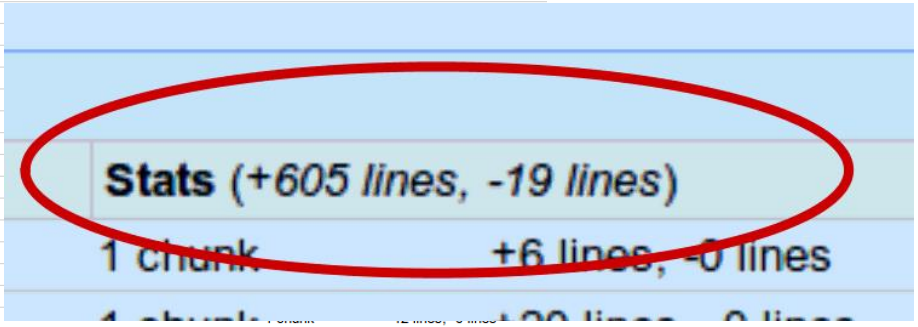
Description

```
Add support for TLS/DTLS heartbeats.
```

Patch Set 1 (edit)

Created: 0 minutes ago

	Unified diffs	Side-by-side diffs	Delta from patch set	Stats (*+605 lines, -19 lines*)	
M	CHANGES	View		1 chunk	+6 lines, -0 lines
M	apps/s_cb.c	View		1 chunk	+20 lines, -0 lines
M	apps/s_client.c	View		1 chunk	+8 lines, -0 lines
M	apps/s_server.c	View		1 chunk	+10 lines, -0 lines
M	crypto/objects/obj_dat.h	View			
M	crypto/objects/obj_mac.h	View			
M	crypto/objects/obj_mac.num	View			
M	crypto/objects/objects.txt	View			
M	crypto/rsa/rsa_pmeth.c	View			
M	ssl/d1_both.c	View			
M	ssl/d1_clnt.c	View			
M	ssl/d1_lib.c	View			
M	ssl/d1_pkt.c	View			
M	ssl/d1_srvr.c	View			
M	ssl/dtls1.h	View			
M	ssl/s3_clnt.c	View			
M	ssl/s3_lib.c	View			
M	ssl/s3_pkt.c	View			
M	ssl/s3_srvr.c	View			
M	ssl/ssl.h	View		6 chunks	+24 lines, -2 lines
M	ssl/ssl3.h	View		2 chunks	+4 lines, -0 lines
M	ssl/ssl_err.c	View		3 chunks	+4 lines, -0 lines
M	ssl/ssl_locl.h	View		1 chunk	+7 lines, -0 lines
M	ssl/t1_lib.c	View		8 chunks	+211 lines, -0 lines
M	ssl/tls1.h	View		2 chunks	+13 lines, -0 lines
M	util/mkdef.pl	View		1 chunk	+1 line, -1 line



Life before HeartBleed

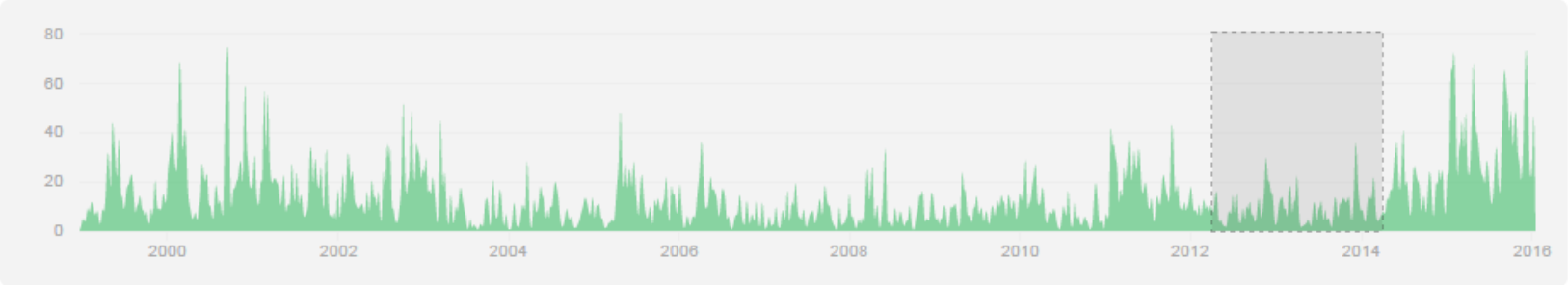
- Project had effectively become somewhat moribund
- Releases were not pre-announced, no documented policies
- Source code was complex and arcane
- Hard to maintain; harder to contribute
- Main developers were overworked and overcommitted
- Project donations minimal (sub USD$2000 per annum)

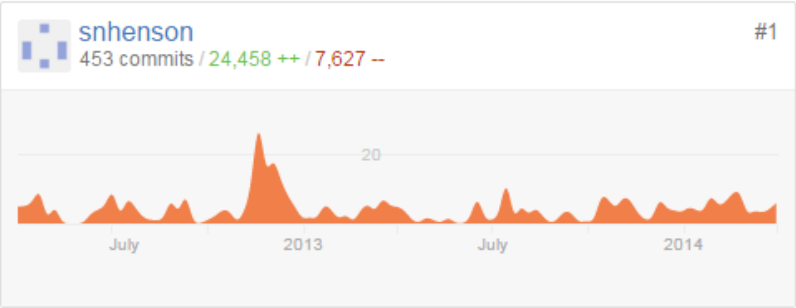
Repo activity, 2012 - 2014

Apr 1, 2012 – Apr 1, 2014

Contributions to master, excluding merge commits

Contributions: **Commits**





How did we let this happen?

- Very little time spent on building community
- Long lead time to understand code
- Static project team membership
- Need to focus on consulting dollars (FIPS140) to keep project alive
- No ability to make, announce, and keep to plans

- … all added up to “ultra cautious” to any change attitude

The usual questions …

- How could the project let this happen?
- How could the project members be so stupid?
- What other nasty break-the-internet bugs are yet to be found?
- Why didn't the project fix this sooner?
- Why didn't all those companies making money off OpenSSL contribute?
- How could we possibly trust the team to not make the same mistake in future?
- Why shouldn't I simply switch over to one of the forks?

After-affects

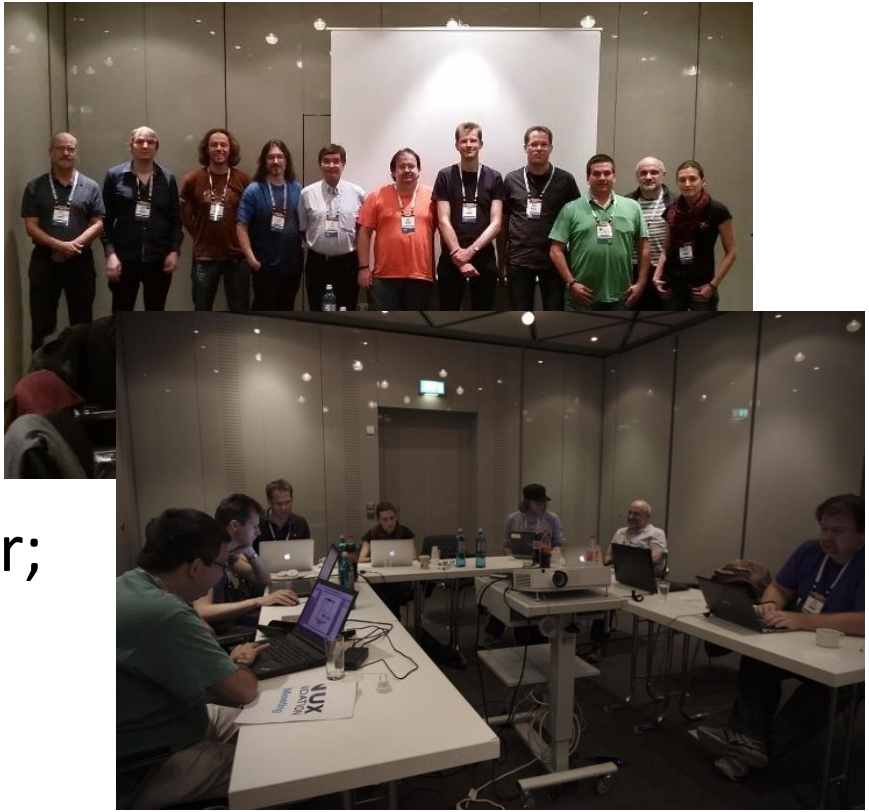
- Wider recognition of dependency on critical under-funded projects
- Creation of the Core Infrastructure Initiative, a multi-million dollar effort to add effective resources to the open source projects that make the Internet work

Growing the Team

- Prior to April 2014
  - Two main developers (one primary committer) entirely on volunteer basis; all other team members focused on other areas; main developer basically funded by paid OpenSSL consulting work
  - No formal decision making process
- As of December 2014
  - Fifteen project team members; a couple inactives
  - Two full time funded by CII; two full time funded by donations
  - Formal decision making process

After-affects

- We had the first-ever F2F
- Drafted major policies:
  - Release strategy
  - Security policy
  - Coding style
- Socialized with each other; POODLE helped



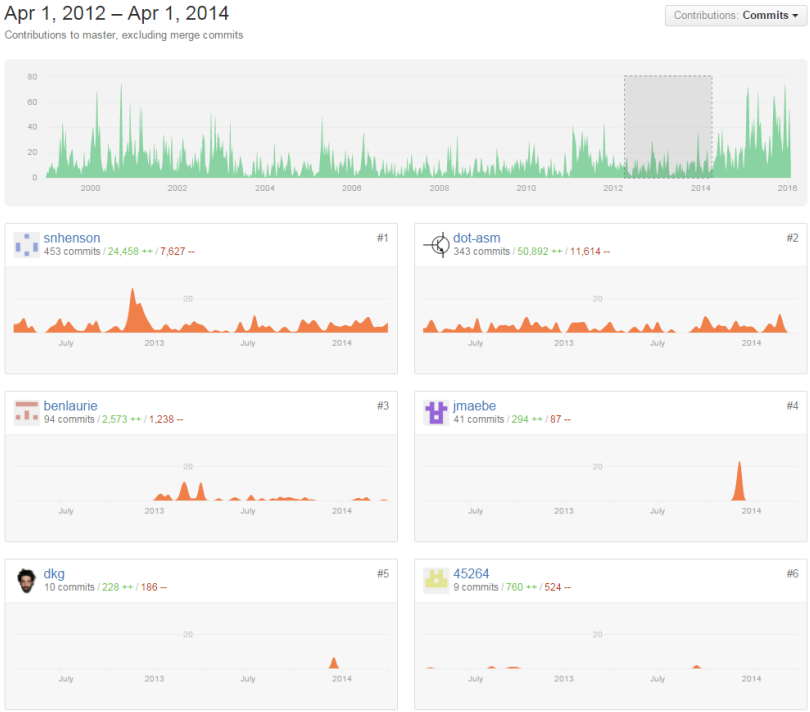
Transparency

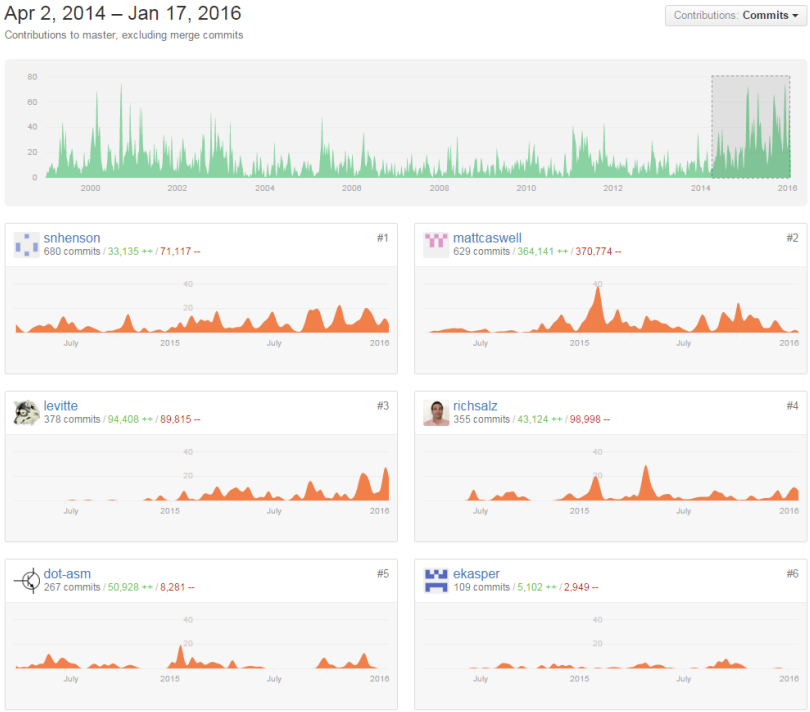
- We use GitHub for many things.
- We have public policies for security fixes, a release schedule and high-level content, code of conduct, and so on.
- Email traffic increased, and (seems) more useful

2016 Activity (so far)

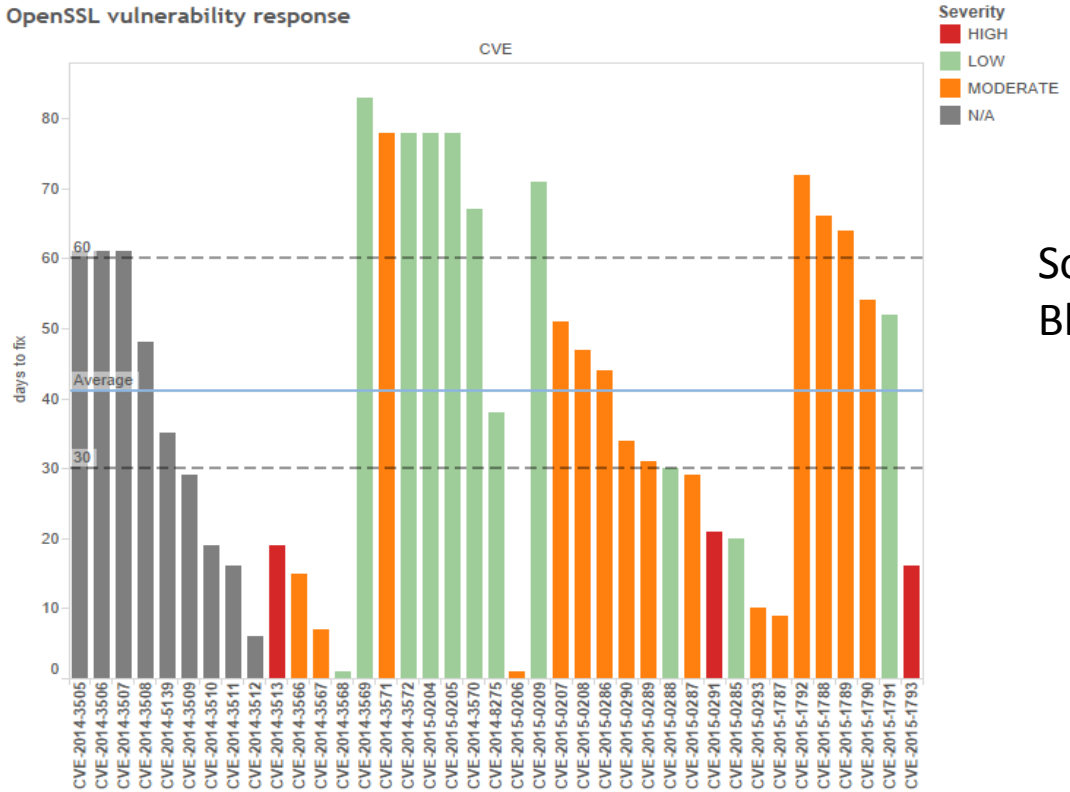
- 3246 commits
- One major release, 15 bugfix releases; 29 CVE's
- GitHub:
  - 281 users created 122 issues, 63 PR's.
  - Team closed 972 issues; 733 PR's (usually merged)

Repo Activity, 2014-2016



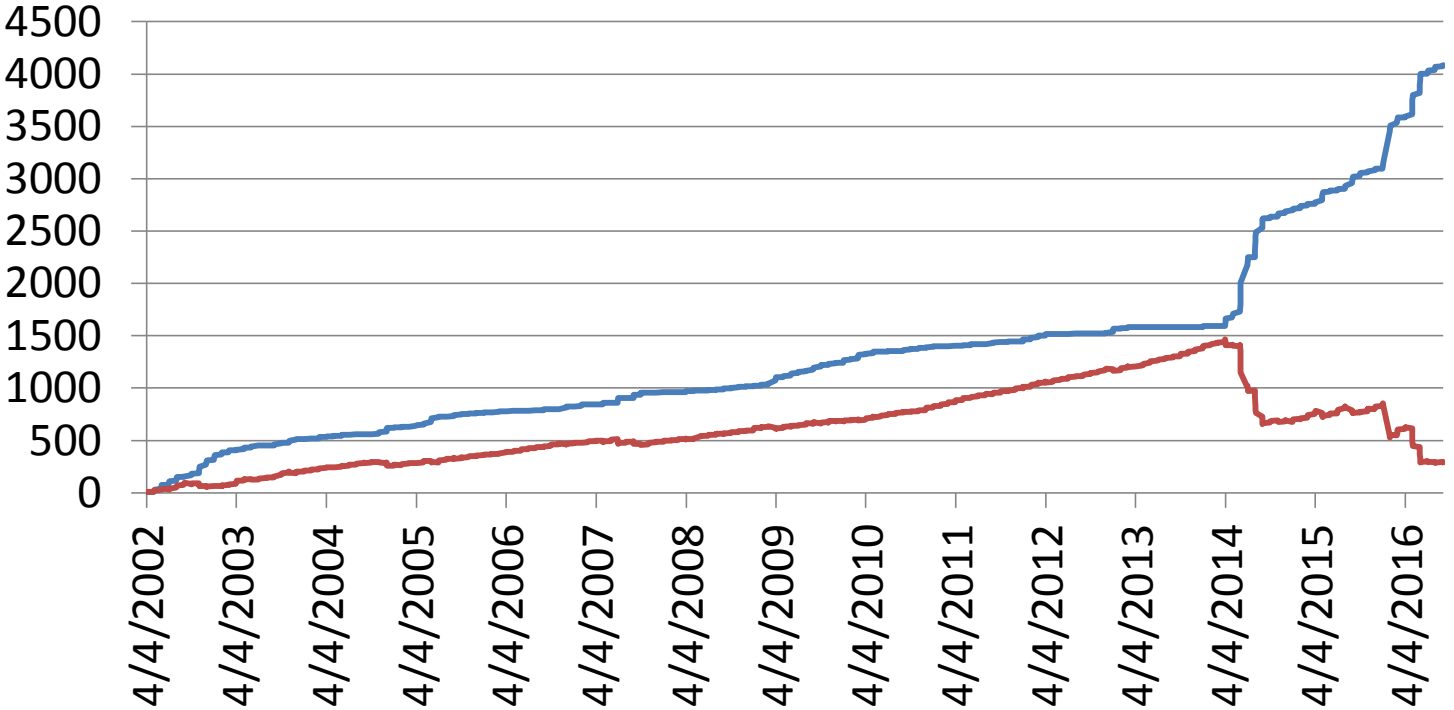


Transparency: security fixes



Source: OpenSSL Blog Entry

Bug tracking



Project Supported Releases

- Version 1.1.0 will be supported until 2018-04-30.
- Version 1.0.2 will be supported until 2019-12-31 (LTS).
- Support for version 1.0.1 will cease on 2016-12-31. No further releases of 1.0.1 will be made after that date. Security fixes only will be applied to 1.0.1 until then.
- Version 1.0.0 is no longer supported.
- Version 0.9.8 is no longer supported.

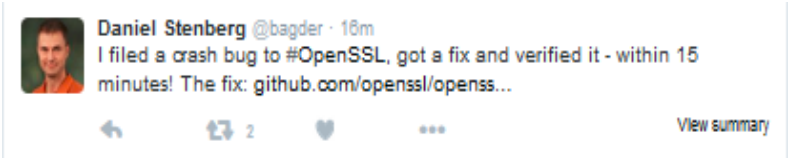
Renewed focus

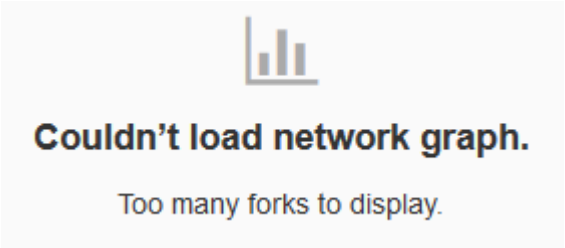
- Security researchers more actively looking for issues
- More fuzz testing going on
- Increased focus on automated testing
- Static code analysis tools rapidly updated
- Reported issues more quickly analyzed
- **Mandatory team member code reviews**

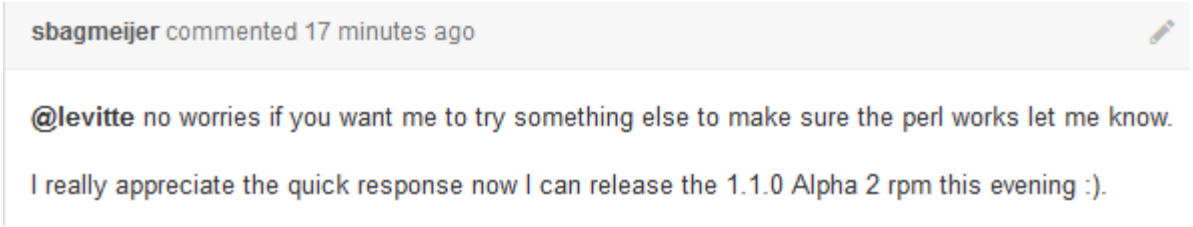
Project Roadmap

- Roadmap has been published and progress against roadmap updated - https://www.openssl.org/policies/roadmap.html
- Major items:
  - clear bug backlog
  - documentation
  - complexity
  - coding style
  - code reviews
  - release plan
  - platform strategy
  - security strategy

Vitality is its own reward







Future Plans

- TLS 1.3
- Apache v2 license
- More testing
- FIPS

- … what else is needed?

FIPS140

- FIPS140 related work effectively entirely funded the OpenSSL project for the last five years
- 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

- 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.

OpenSSL
Cryptography and SSL/TLS Toolkit

FIPS140 Plans

- The OpenSSL FIPS 2.0 module works with OpenSSL-1.0.x
- The previous OpenSSL FIPS 1.0 module for OpenSSL-0.9.x is no longer usable
- New FIPS module coming:
  - Thanks to SafeLogic for funding!
  - Will work with 1.1.0
  - Major goal is to make the FIPS changes “less intrusive”

Major Lessons

- Relying on any single individual to perform superhuman feats ultimately results in disappointment
- Code reviews actually require the reviewers to review the code in detail
- Assuming that users will review code is clearly a flawed strategy
- Assuming that automated code analysis tools by themselves can completely replace experienced code reviews is incorrect

How to Contribute

- Download the pre-releases and build your applications
- *Help is a two-way street*, join the virtuous circle. Or at least join the openssl-dev and/or openssl-users mailing lists
- Report bugs through RT, submit patches on GitHub. *Help close bugs.*
- If you are doing more than TLS for HTTP, *please let us* know
- More ideas on the Community page of www.openssl.org

The OpenSSL Development Team

- Matt Caswell (UK)*#
- Mark Cox (UK)*
- Viktor Dukhovni (US)
- Steve Henson (UK)#
- Tim Hudson (AU)*
- Lutz Jänicke (DE)*
- Emilia Käsper (CH)*
- Ben Laurie (UK)
- Richard Levitte (SE)*#
- Steve Marquess (US)*
- Bodo Möller (CH)
- Andy Polyakov (SE)*#
- Kurt Roeckx (BE)*
- Rich Salz (US)*
- Geoff Thorpe (CA)

Total: AU, BE, CA, CH(2), DE, SE(2), UK(4), US(3)
** means here at LinuxCon*
 # means funded (by OpenSSL or CII)

Questions?