Software Engineering and OpenSSL is not an oxymoron

Rich Salz
Akamai Technologies
OpenSSL Dev Team
rsalz@{akamai.com,openssl.org}

Main lesson

It’s not the crypto that kills you (or your open source project)

Historical Era’s

- SSLeay
- OpenSSL
- The CVE that Must Not Be Named
- Recovery
- Today and tomorrow

SSLeay

- Various creation legends:
  - Let’s put on a show (Eric: “I’ve got DES and a BIGNUM package” Tim: “Let’s do SSL”)
  - Two guys in a garage
- Small set of folks sending patches
- Handful of tests; minimal functionality

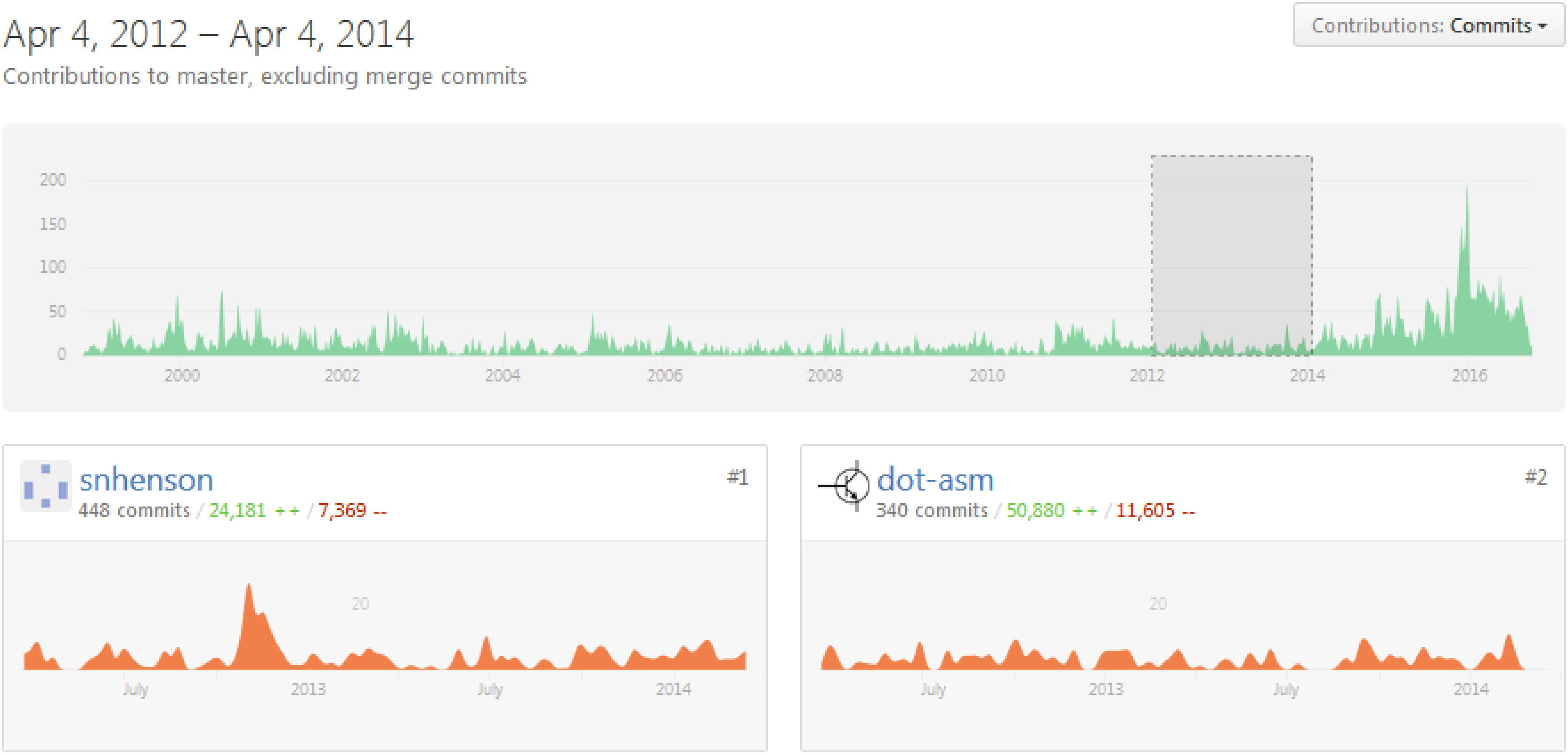
The Rise of OpenSSL

- Started off big; as many as a dozen members
- Export control: stay away from the US
- Active mailing lists, still took patches
- “Interop with OpenSSL more important than what the RFC says”

The Fall of OpenSSL

- Project had become 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)

The Picture of Stasis



Apr 4, 2012 – Apr 4, 2014

Contributions to master, excluding merge commits

Contributions: Commits ▾

snhenson #1

448 commits / 24,181 ++ / 7,369 --

dot-asm #2

340 commits / 50,880 ++ / 11,605 --

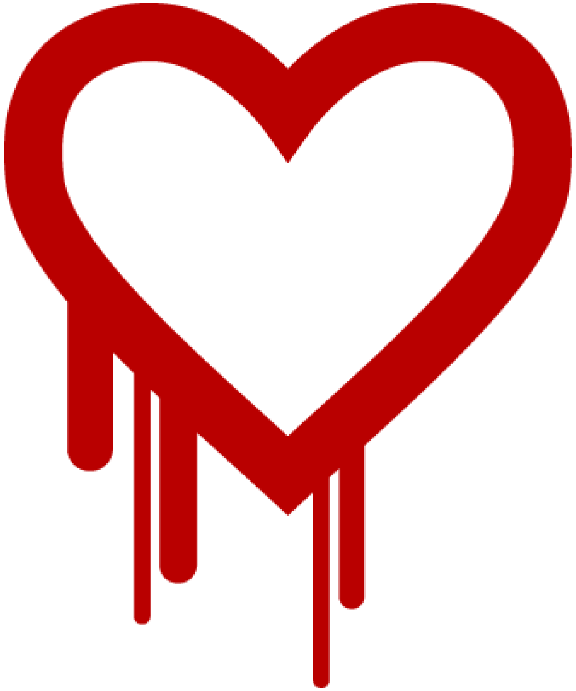
Why the fall?

- Long learning cycle to understand code
- Need to get consulting dollars (FIPS) to keep project alive
- Very little time spent on building community
- No ability to make, announce, and keep to plans

- … all added up to “stay dark” attitude

The CVE That Must Not Be Named

- CVE-2014-0160, April 3



DAILY Mirror

By George he looks like dad...

WORLD EXCLUSIVE

Why I sit in that court every day

BY REEVA'S MUM

CHANGE ALL YOUR PASSWORDS

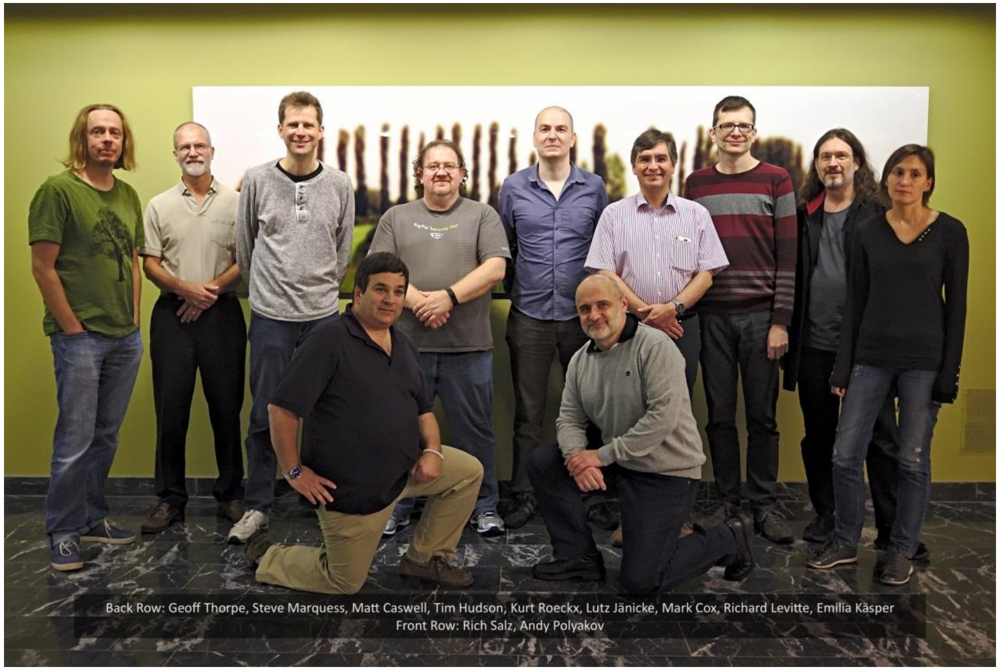
Warning as millions hit by Heartbleed computer bug targeting online details

Recovery

- New blood (enthusiasm) on the team
  - – CII created, funds two
  - – Donations jump, funds two
- We met in Oct 2014:
  - – Wrote release, security policies
  - – Coding Style (!!!)
  - – Socialized; POODLE helped

Going to Meetings is part of Recovery

- We also met in Oct 2016:
  - CVE notification process
  - CII/LF discussions (about and with)
  - How to grow the team
  - How to get more testing
  - Update roadmap and platform doc
  - Regular release cadence



Back Row: Geoff Thorpe, Steve Marquess, Matt Caswell, Tim Hudson, Kurt Roeckx, Lutz Jänicke, Mark Cox, Richard Levitte, Emilia Käsper
Front Row: Rich Salz, Andy Polyakov

Recovery: Transparency

- *Building community is job 1*
  - Documented what we want to do, and how.
  - Website overhauled (still too wordy)
  - Mailing lists moved
  - RT sped up (multiple moderators), and then removed
- Virtuous cycle: when a project isn’t a black hole, people contribute

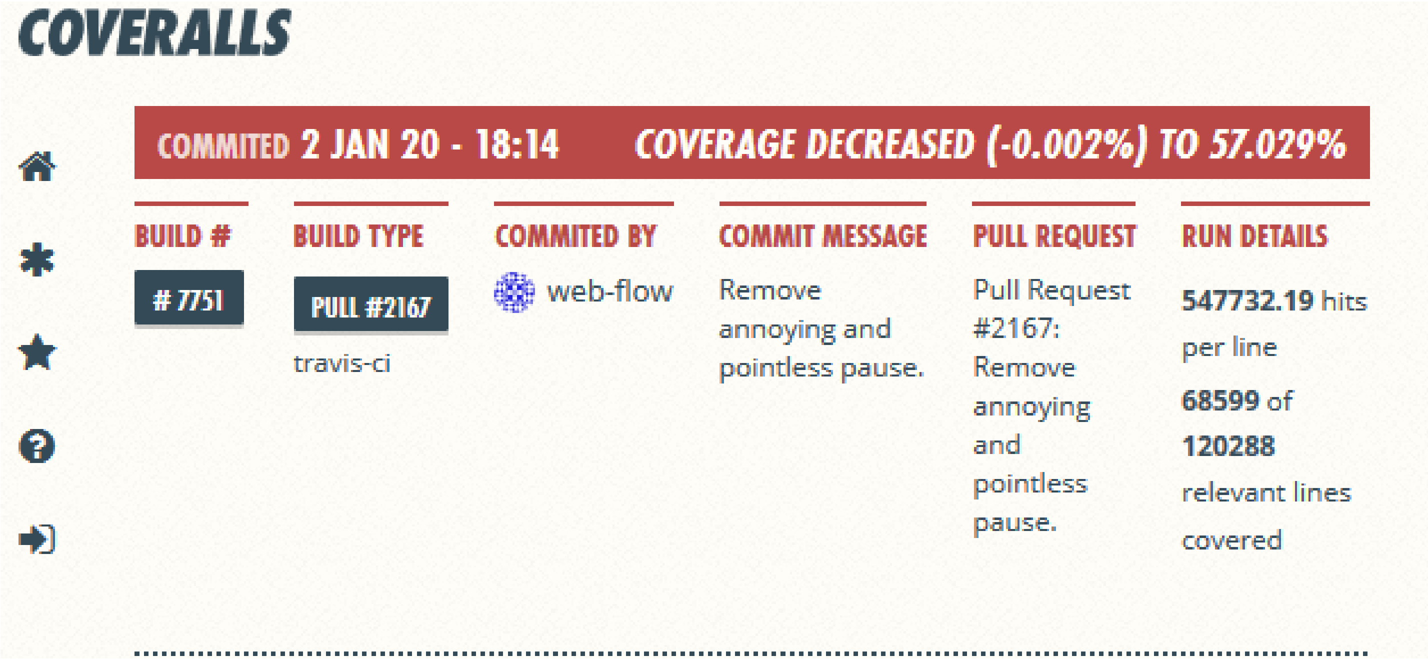
Recovery: Code Quality

- Appearances count
  - Almost-repeatable code reformatting
- Mandatory review by a second team member
  - We're still improving this
- More tests: Coveralls reports 57% of lines
- Modern practices: fuzzing, CI, etc.
  - Remember, OpenSSL is *old*

No longer a dumping ground

- Removed dozens of old platforms we could not test (Duo-culture is useful)
- Removed old and/or weak cipher suites
- GOST moved to external ENGINE
- Related: most structures are opaque, for future-proof (API/ABI compatibility; did hamper us before)

Recovery: Test Coverage

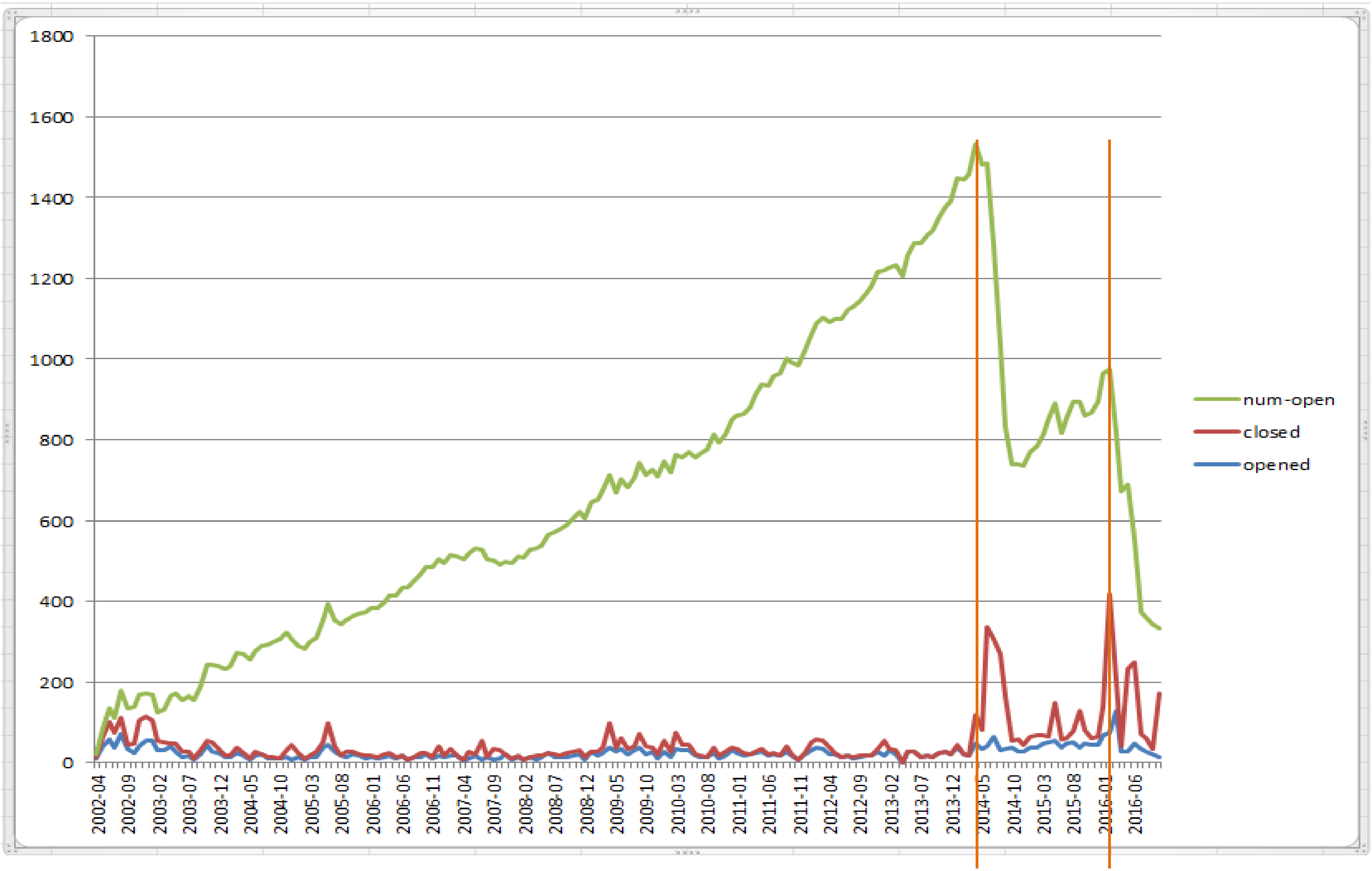


COVERALLS

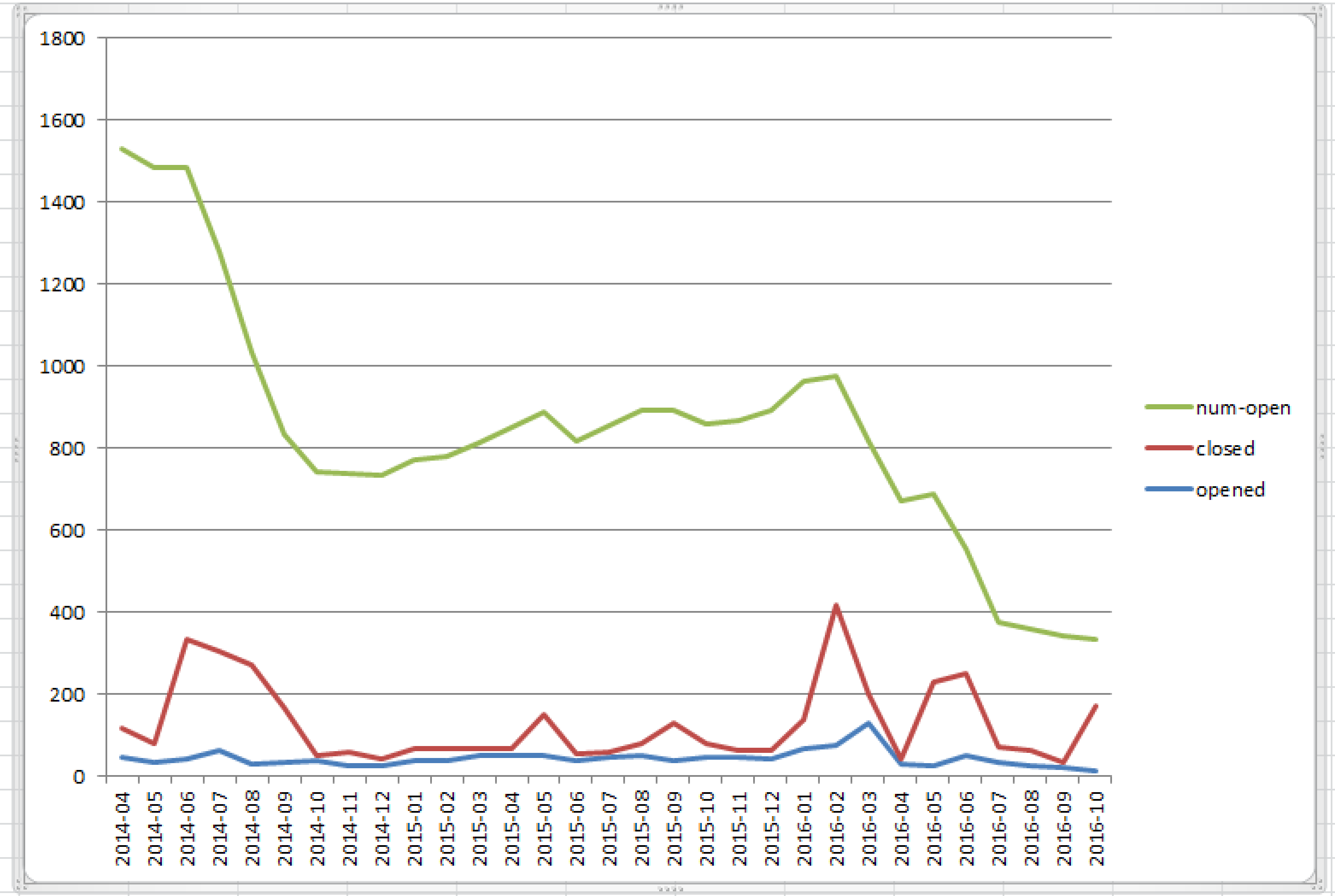
COMMITED 2 JAN 20 - 18:14 COVERAGE DECREASED (-0.002%) TO 57.029%

BUILD #	BUILD TYPE	COMMITED BY	COMMIT MESSAGE	PULL REQUEST	RUN DETAILS
# 7751	PULL #2167 travis-ci	web-flow	Remove annoying and pointless pause.	Pull Request #2167: Remove annoying and pointless pause.	**547732.19** hits per line **68599** of **120288** relevant lines covered

Recovery: RT tickets, full history



Zooming in


1800
1600
1400
1200
1000
800
600
400
200
0
2014-04
2014-05
2014-06
2014-07
2014-08
2014-09
2014-10
2014-11
2014-12
2015-01
2015-02
2015-03
2015-04
2015-05
2015-06
2015-07
2015-08
2015-09
2015-10
2015-11
2015-12
2016-01
2016-02
2016-03
2016-04
2016-05
2016-06
2016-07
2016-08
2016-09
2016-10
🟩 num-open
🟥 closed
🟦 opened

2016 Project Activity

- 3889 commits
- 431 GitHub users; thousands of forks
- 250 new issues
- 107 new pull requests; 1052 PR’s closed
- Releases:
  - 1.1.0 a-c
  - 1.0.2 a-j
  - 1.0.1 h-u *EOL*

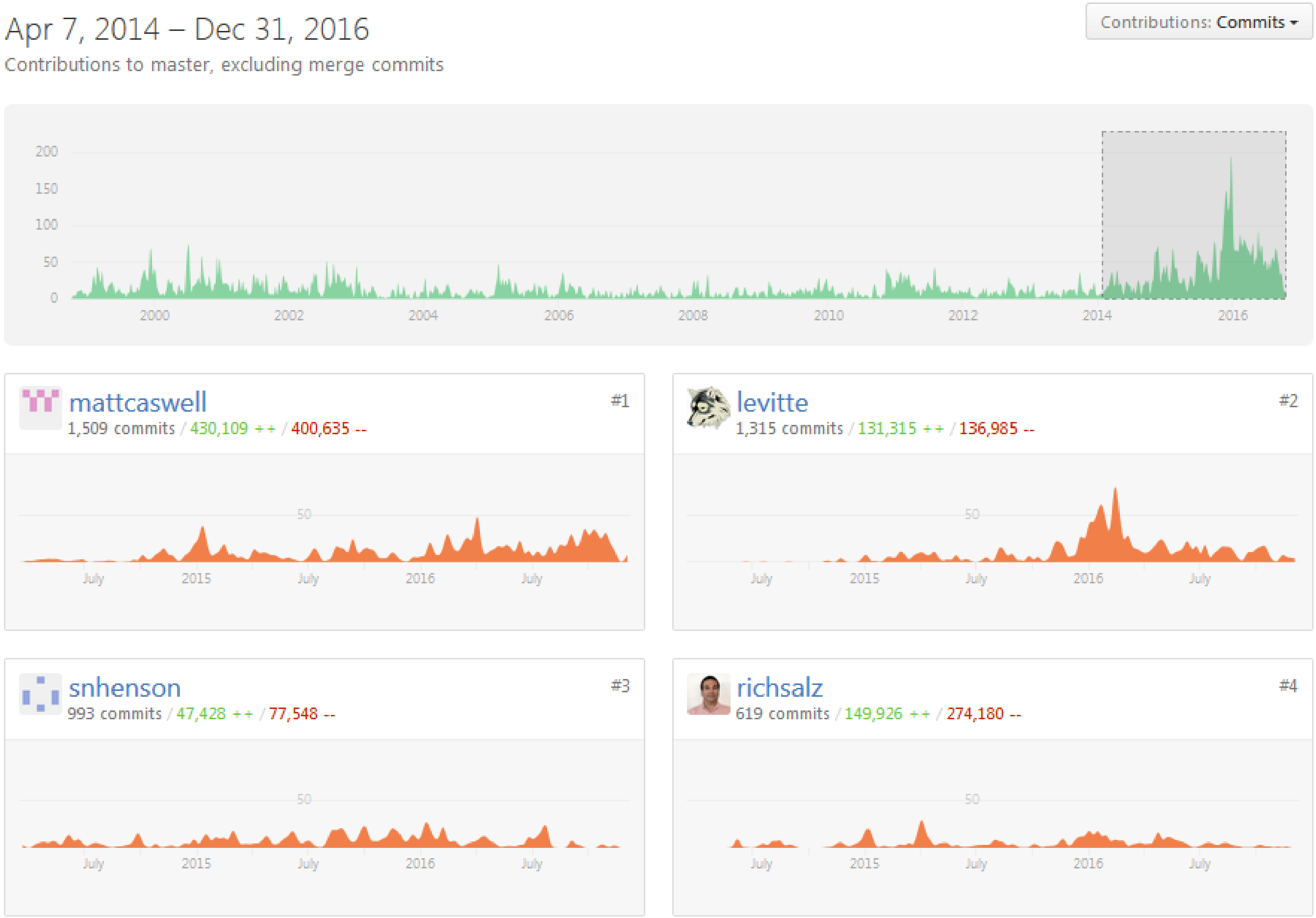
2016 CVE’s

- 9 high (force a release)
- 20 medium (might force a release)
- 28 low (just fix)

- Mostly met the disclosure/fix deadlines

- Thankfully no *critical* yet

GitHub: Current activity



Apr 7, 2014 – Dec 31, 2016

Contributions to master, excluding merge commits

Contributions: Commits ▾

mattcaswell #1

1,509 commits / 430,109 ++ / 400,635 --

levitte #2

1,315 commits / 131,315 ++ / 136,985 --

snhenson #3

993 commits / 47,428 ++ / 77,548 --

richsalz #4

619 commits / 149,926 ++ / 274,180 --

Today and Tomorrow: Excelsior

- Everything* is done on GitHub now
- Everyone has a CLA
- Major infrastructure components (technical debt) being addressed:
  - Threads, state machine, TLS packet formats
  - CLI flags, help improved
  - *All* docs are improved

What’s coming?

- FIPS work funded, but on-hold for TLS 1.3. Likely to mean ENGINE extensions.
  - might mean putting “old crypto” into an ENGINE
  - Tension between “safe” crypto and “everyone’s crypto”
- TLS 1.3
  - Contract in place with fixed delivery date and known interoperability
- Licensing
  - Moving to APLv2
- Testing
  - More and more and more and more
  - Can already run boringSSL test suite, e.g.

What Might/Should come

- All SSL public functions documented (101 missing out of 402)
- Need to fix the RNG, *portably*
- A generic STORE facility, for PKI objects.