Heartbleed from OpenSSL viewpoint

A bit of pre-history:

- Originally OpenSSL is volunteer-driven project.
- It never sought for position it holds.
- Heartbleed pre-history goes back to 2008, when we get first bug reports from an aspiring German computer scientist.

Heartbleed from OpenSSL viewpoint

Open source development model is ultimately built on trust. It's only natural that trusted party has a little bit lower threshold for accepting submission. This is the mechanism that enabled Heartbleed.

But was it a breach of trust? Absolutely not.
Would we reject submission from the contributor in question? On the contrary, we would welcome it.

Heartbleed from OpenSSL viewpoint

Dark side of publicity:

- “custodians of internet” and “the team has been responsible for our credit card data”?
- We don't disclaim all responsibility, but we bear only small part of it.
- Enterprises should be accountable for knowing what they are using and how, personification was not justified.

Heartbleed from OpenSSL viewpoint

Light sight of publicity:

- Increased awareness that ensured swift patching.
- Existential conflict: can a volunteer-driven project provide de-facto infrastructure solution? In sustainable manner? Apparently it can get you rather far...

Heartbleed from OpenSSL viewpoint

Gray side of publicity:

- How many serious vulnerabilities go hardly noticed and as result linger unpatched?
- Are there any that are not as big deal?
- Erosion of terminology, what substitutes a remote exploit nowadays?

Heartbleed from OpenSSL viewpoint

What happened after?

- Team has effectively reorganized itself taking in new members, 14 now, several are working full-time.
- Review process is in place.
- Drafted future plans.
- Published security policy.

Heartbleed from OpenSSL viewpoint

http://www.openssl.org/about/secpolicy.html

- Formalization of prior experience.
- Security is not for sale.
- Advance notification of mere fact of security fix on <openssl-announce>.
- For high severity issues advance notification with more details and patches through 3rd party "distros" list at openwall.org.

Heartbleed from OpenSSL viewpoint

Random musings (from developer viewpoint)

- Can't formalize human ingenuity, can't tell somebody it's their turn to keep a critical eye.
- In pursue for cost effectiveness we seem to forget the value solution is supposed to protect.

Heartbleed from OpenSSL viewpoint

https://plus.google.com/+MarkJCox/posts/TmCbp3BhJma

http://www.openssl.org/about/roadmap.html

http://www.openssl.org/about/secpolicy.html

<appro@openssl.org>