NEWSANALYSIS

The Linux Voice view on what's going on in the world of Free Software.

Opinion

Lessons for Open Source from Heartbleed

The armageddon has been and gone – let's not waste a good crisis

Simon Phipps is president of the Open Source Initiative and a board member of the Open Rights Group and of Open Source for America.

We've had a while for the shock of the Heartbleed announcement to sink in and there's a lot to consider. While the first impressions might be about the serious, exploitable bug and the repercussions of its abuse, the incident casts light on both the value and risks of open source. All programmers make mistakes, so there's no huge surprise that it happened in OpenSSL. But why did it go undetected for so long? There are several contributing factors.

It's hard to spot error in complex code: First, the OpenSSL code is huge, years old and implements a set of algorithms that need specialist cryptographic knowledge to understand them. Reading someone else's code in this context is difficult, dull and time consuming. That's not a recipe for scrutiny even with a large paid team.

Community too small: There is no large, paid team. The whole community developing and maintaining OpenSSL was no larger than 11 people before Heartbleed, with only one of them working full-time on the code. Despite being widely deployed, the community did not receive regular participation from developers using OpenSSL in other projects. There's been speculation why. An obvious explanation is that the cryptographic complexity of the code meant that non-specialists were not effective as community participants, but US government open source specialist David A Wheeler has speculated that the unusual licensing arrangement for OpenSSL – a custom open source licence with non-GPL-compatible copyleft effects and potentially challenging advertising clauses – also discouraged community involvement.

Exploit detection turned off: What can a small community do to spot uninitialised memory and buffer over-run errors? String handling libraries today often include detection at compile-time or even run-time for such errors, and the OpenBSD code used by OpenSSL for this purpose is no exception. But according to Theo de Raadt, leader of the OpenSSH project, these detection capabilities had been turned off at compile time in the OpenSSL build for performance reasons long ago and had never been turned on again, despite the performance issues being addressed in the code.

Would proprietary be better?

Doing this with proprietary code would be unlikely to make things better. Hiding a development team behind NDAs and corporate secrecy, having their priorities driven by unseen managers and keeping code invisible to potential users all constitute an anti-pattern for security software. In addition, the ability of open source to bring all the best hands to the problem once it's identified would simply not exist with a proprietary solution. Engaging would need permission and bureaucracy, and many contributors would just say no.

Should I make donations?

So what's the right way to react? Fork the code? No, that's been done, and probably just increases the problem by removing potential expert participants from the OpenSSL pool. Re-implement it? That's been tried as well. Even with various forks and re-implementations, OpenSSL remains widely used, because the problem is complex and the experts are few. Those new projects are unlikely to surpass in a few months what OpenSSL has largely succeeded at doing over a decade. Donate money? While cash donations to a project can be a short-term fix, in the long term it is unlikely to help unless it leads to more developers both writing and testing the code. The best fix would be for the companies most dependent on OpenSSL to hire experts and pay them to join the community and work on the code.

This, after all, is the key to open source. It's not about free stuff; rather, open source delivers the liberties that enable developers with differing motivations and origins to collaborate on a codebase without needing to ask permission from anyone other than each other, and even then only out of social effectiveness. Throwing money at an open source project doesn't automatically make anything better; that takes people with actual skills.

Heartbleed has shown us that open source is no guarantee of invulnerability. Fortunately, the crisis has highlighted a set of needs that are being met in a way no other approach would have allowed. Looking past the crisis, it's possible Heartbleed is actually making things become better, faster.

"Throwing money at an open source project doesn't automatically make anything better."

CATCHUP **Summarised:** the eight biggest news stories from the last month

1 OpenSSL has been forked: say hello to LibreSSL

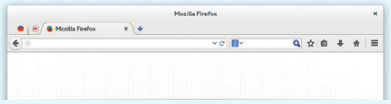
After all the fun and games of the OpenSSL Heartbleed vulnerability, which made vast swathes of the internet open to cracking, the OpenBSD team (see news item 8) has had enough. A bunch of developers has forked OpenSSL into LibreSSL, and they're going through the code discovering some truly horrendous holes and coding errors. Right now the website is in Comic Sans with blink tags, but donations should fix that: **www.libressl.org**

2 Linus Torvalds wins yet another award

Not content with having won the Technology Academy of Finland's Millennium Technology Prize, NEC's C&C Prize, the Takeda Award for Social/Economic Well-Being, the British Computer Society's Lovelace Medal and the Electronic Frontier Foundation Pioneer Award, everyone's favourite narky kernel hacker has another to add to the list: the 2014 IEEE Computer Society Computer Pioneer Award. For his contributions to computing, Linus can expect a bronze medal in the post.

3 Firefox 29 sports a redesigned interface

This has been massively controversial, but then any major UI update for a well-used app always is. Firefox 29 features a trimmed-down interface that "makes it easy to focus on web content". In addition the redesigned tab bar is "sleek and smooth to help you navigate the web faster". Sounds a bit buzzwordy to us... **www.mozilla.org**



4 Canonical puts Ubuntu for Android project in limbo

Ubuntu maker Canonical is ambitious with its plans to have the Unity interface everywhere: on phones, tablets, TVs and desktops. One part of this convergence strategy has been kicked into the long grass though: Ubuntu on Android. This was supposed to provide a regular Android experience on your mobile devices, but when you plugged them into a TV or monitor, you'd get the full Unity experience. Canonical has said it isn't dead, but they'll focus on Ubuntu phones for now.

5 Band releases album as a Linux kernel module

This is charmingly silly. Netcat, a Seattle-based band that "explores the intersection between technology, complexity and free improvisation" has just kicked out a new album. But listening to it is a challenge: you have to build a custom kernel module that creates a **/dev/netcat** device node that you can then pipe into an audio player. But be warned: if you decide to go this far, you'll need "several gigabytes of memory" to build it. See: **http://tinyurl.com/netcatmod**

6 It's official: Edward Snowden is a Linux user

Many people suspected this all along, but now it has been confirmed that leaker extraordinaire Edward Snowden used Linux in his data gathering antics. Specifically, he used the Tails distribution, a highly paranoid flavour of Linux that routes all of its internet traffic through Tor and stores everything in RAM (thereby leaving no trace of activity on a computer's hard drive). We still don't know if he prefers Vim over Emacs though. Tails' site: **https://tails.boum.org**

7 New consortium that includes Microsoft to fund core FOSS projects

More fall-out after the Heartbleed fiasco: a bunch of big-name companies including Amazon, Dell, Facebook, Google, IBM, Intel and Microsoft have teamed up with the Linux Foundation to offer financial support for "critical open source projects". And guess which project will receive funds first? Yes, OpenSSL. Finally, the big companies that use FOSS realise it doesn't grow on trees. **http://tinyurl.com/lrlmzh4**

8 Ultra-secure Unix flavour OpenBSD 5.5 released

Hang on – this isn't Linux! True, but we like to support our other FOSS brethren in the operating system world too. OpenBSD is a lot like Linux, offering oodles of advanced security features but not so much desktop hardware compatibility. It's superb for small servers and routers though. The 5.5 release brings about a 64-bit **time_t**, which means that the operating system's clock won't overflow until Sunday, 4 December in the year. 292,277,026,596. **www.openbsd.org**