Alex Hesselgrave
CS35L Lab 4
5/7/2014

# Heartburn from Heartbleed Review

This article covers more of the aftermath of Heartbleed and what will and should ensue from it rather than the bug itself. The author claims that although it was not the worst bug to happen to OpenSSL, it was still incredibly significant because of its widespread media coverage.

According to the article, OpenSSL is an internet encryption tool used by many websites and companies to transfer important private data such as "usernames, passwords, Social Security numbers, and credit card numbers" (Rosenblatt). Heartbleed allowed hackers and other people with malicious intent to breach OpenSSL encrypted servers and retrieve valuable information by exploiting a bug in the recent heartbeat feature.

The author claims that Heartbleed is not the worst of OpenSSL's bugs, but how come we have never heard of those previous bugs if OpenSSL dominates in internet security? One of the main reasons was media coverage. Heartbleed was discovered on April 1st by a security company called Codenomicon. They were doing routine tests on their software and noticed how significant the problem with the current version of OpenSSL was. Only 6 days later, two other independent research teams also independently found the Heartbleed bug, further emphasizing the severity of the issue. OpenSSL made an announcement that same day regarding the bug, and Codenomicon coined the term and created the logo for Heartbleed for media ease. Soon, tech media and even news media were flooded with reports about the bug.

Heartbleed's popularity was an incredibly important step in the right direction for open source projects. It's widespread knowledge allowed users and companies to quickly apply the patch before any exploits could occur on their server(s). Additionally, it led to the debate about funding open source projects. Currently, the premise of open source security is the hope that "across the entire userbase, somebody has spent the time to make sure their investment is protected" (Rosenblatt). Even though the heartbeat feature went under code review, the researcher reviewing the code ended up missing the bug. Having just one person doing a code review is nowhere near enough, and the author agrees on this point. Since open source projects are used so much by major corporations and organizations that control much of what we do, it is important to ensure that what is being used is working correctly and will have no possibility of exploits.

There is already a step in the right direction with the infamy of Heartbleed. Companies such as Google, Facebook, and Microsoft, just to name a few, pooled together over $1 million to help review the security of open source projects. Chris Wysopal, the chief of technology officer for Veracode, believes that that funding is not enough, but it's a start. He believes that "any project that requires cryptography should have extra scrutiny", and I agree wholeheartedly (Wysopal).

Open source projects do not nearly get enough support financially compared to how frequently they are used. Linux and OpenSSL are used by practically every major company for their ease, availability, and lack of cost. However, as Heartbleed and other bugs demonstrate, code is always buggy and can be vulnerable; it is crucial to review and keep an eye on the libraries being used. Now more than ever, with open source becoming ever popular and major bugs being portrayed on mass media, it is imperative to start funding and giving back to open source projects to ensure the security of all internet users. Chances are something like this will happen again, but with the enough programmers contributing to the project, we can drastically reduce the frequency of major bugs being introduced into the internet infrastructure.