International Journal of Life Science and Engineering
Vol. 1, No. 2, 2015, pp. 45-49
http://www.publicscienceframework.org/journal/ijlse

# A Perfunctory Negligence on the Undying Capabilities Resulted in the Heart Bleed Vulnerability in Open SSL

**Edward Danso Ansong[1, *], Dominic Damoah[1], J. B. Hayfron-Acquah[2]**

[1]Department of Computer Science & Information Technology, Valley View University, Oyibi, Ghana
[2]Department of Computer Science, Kwame Nkrumah University of Science & Technology, Kumasi, Ghana

## Abstract

The denunciation on Open SSL tool caused total devastation and trust concerns with modern security technologies purported to be secured. A careful relook at the Heart bleed vulnerability provides insights with lessons that should inform how cryptographic software libraries are built and implemented. This article outlines the antecedents of a retinue of security vulnerabilities with the Open SSL solution. The evidence adduced is that Open SSL is indeed not entirely secure after all until subjected to rigorous testing.

## Keywords

Cryptography, Open SSL, Heart Bleed, SSL and TLS

Received: February 24, 2015 / Accepted: April 9, 2015 / Published online: April 17, 2015



## 1. Introduction

Communication via the internet has not been entirely secure but some measures have been taken to ensure that at least the data transferred and communicated via the internet is secure. Some measures adopted for implementation of cryptography in communication are tools such as SSL (Secure Sockets Layer) and TLS (Transport Layer Security) that allow for encryption modules to be developed in order to secure data and information via the internet. As the technology advances the means to sustain and maintain security are of paramount concern.

One such implementation of SSL and TLS is the Open SSL cryptographic library which aids secured communication of data via the internet. This popular tool for securing data transmission had serious inherent flaws furtively explored by attackers to dupe unsuspecting users. Put differently, this cryptographic library and toolkit used globally by almost two thirds of the world's webservers' has been proven vulnerable due to a bug known as "Heart bleed". The purpose of this article is to identify what went wrong and the negative effects on users directly affected by the bug. On the other hand after the Heart bleed vulnerabilities were fixed, other exploiter surfaced and this questioned the security of the Open SSL software library.

The article has been structured in two main sections namely: the basic section and the extended section. The basic section focuses on the technology and utilities of Open SSL whereas the extended section discusses implementation, milestones, vulnerabilities, security values, challenges, and further works.

## 2. Background

Due to its wide use Open SSL is the most successful open source project and it is recognized as very important because most internet security infrastructure depend on it. This project has both command-line toolkit and extensive

* Corresponding author:
E-mail address: edkan20002002@yahoo.com (E. D. Ansong)

performance implementation of key cryptographic algorithms (Ristic, 2013). The undying capabilities of Open SSL in terms of security has been proven flawed since March 2012 till the affected version was patched in April 2014(Julian, 2014). Thus, the discussion in this article to express concern on how secure Open SSL is after every patch and how devastating a bug is to users(Mcree, 2012)(Canada Tax Agency Hacked Using Heartbleed, 2014)(Experts, 2014) as there are new vulnerabilities with the Open SSL library discovered every now and then.

## 2.1. Open SSL

Open SSL is a popular and effective open-source version of SSL and TLS, most widely used protocol for secure communications(Pravir Chandra, 2002). Open SSL evolved from the earlier work from SSLeay in 1995(Ristic, 2013). This was discontinued when the first version of Open SSL was developed with two components namely cryptography library and an SSL toolkit(Pravir Chandra, 2002). According to Ristic [1] the Open SSL project was founded to aid in the development of commercial-grade, full-featured and open source implementation of SSL and TLS protocols. It is also dual-licensed under Open SSL and SSLeay licenses.

## 2.2. Utilities of Open SSL

As stated above, Open SSL consists of a cryptographic library and an SSL toolkit. Open SSL can be implemented in a website to protect data transactions on that website. This software is used in servers that host websites; most web developers may have a fair idea what cryptographic module their websites use because they solicit hosting features from web hosts who directly use cryptographic libraries on their servers for hosting. Open SSL is an implementation of SSL (Secure Socket layer) and TLS (Transport Layer Security) protocols which is open source. Therefore most web hosts make use of Open SSL's openness by modifying code to suit the purpose of securing information via the internet (Ristic, 2013).

## 2.3. Open SSL Implementation

This is required when a certificate signing request is needed (websense, 2014). Vendors could acquire a signed certificate using Open SSL alone or in combination with another Certification Authority. Basically, Open SSL is to secure applications and according to (Pravir Chandra, 2002), many applications are built to support Open SSL. An example is the Open SSH which requires the library to be present before it can compile. Technically its implementation is unlimited because of the constant modification by its developers and users (i.e. modify to suit their purpose).

## 2.4. Marks of Open SSL

The licensing terms to Open SSL allow for use of modified code commercially and the source code is available, which allow unlimited functionality and platform independence (14Ju).

## 2.5. Vulnerabilities of Open SSL

### 2.5.1. Timing Attacks on RSA Keys

This vulnerability was discovered on March 14, 2003 and was present in Open SSL versions 0.9.7a and 0.9.6. Because it is not possible to turn on RSA blinding when providing SSL or TLS using Open SSL, local and remote attackers were able to obtain private key of the server due to timing differences and the use of normal integer multiplication algorithms.

### 2.5.2. Denial of Service Asn.1 Parsing

In 2003 it was discovered that the ASN.1 (Abstract Syntax Notation One) bug affected Open SSL version 0.9.6k. Window machines generated large amounts of recursions and crash servers which were SSL/TLS enabled (Security Focus, 2002).

### 2.5.3. OCSP Stapling Vulnerability

Online certificate status protocol (OCSP) stapling vulnerability affected Open SSL versions 0.9.8h to 0.9.8q and Open SSL 1.0.0 to 1.0.0c. An attacker could cause a DDOS since the message parsing could lead to a reading of an incorrect memory address. This is normally caused by a client sending incorrect formatted Client "Hello" message that leads to Open SSL parsing more than the end of the message (Rapid7, 2011).

### 2.5.4. ASN1 Bio Vulnerability

This bug allowed for buffer overflow attacks and caused memory corruption which had other implications through DER (Distinguished Encoding Rules) data by an RSA public key (Rapid7, 2012). It affected version 0.9.8v and a few other patches except for 1.0.1i and 1.0.1a (Mcree, 2012).

### 2.5.5. SSL, TLS and DTLS Plaintext Recovery Attack

Plaintext could be recovered when timing differences are exploited during MAC (Message authentication code) processing due to a weakness in handling (Cipher Block Chaining) cipher suites in SSL, TLS and DTLS. All versions of Open SSL were affected with 1.0.1c, 1.0.0j and 0.9.8x all inclusive (IBM Security Bulletin, 2013).

### 2.5.6. Predictable Keys (Debian-Specific)

In the Debian implementation of the Open SSL suite, a patch

applied broke the random number generator and this version (0.9.8c to 1.0.0) was included in the Debian release in September, 17 2006. This compromised any key generated with the broken number generator as well as data encrypted with it. The error was fixed in later Debian distributed versions (Debian, 2008).

### 2.5.7. Heart Bleed Bug

This vulnerability is popular in Open SSL cryptographic software library; it affected versions 1.0.1 and 1.0.1f. This bug allowed information theft even in secured environments. The bug provided easy access to attackers on the internet to read system memory believed to be protected under the SSL/TLS encryption. This perceived security and privacy afforded in the use of the web, email, instant messaging (IM) and some virtual private networks (VPNs) were a facade(Julian, 2014).This vulnerability in Open SSL handles the SSL heartbeat that triggers a buffer over-read, resulting in confidential information being disclosed. The information the hacker acquires upon exploiting Heart bleed would be very damaging to the victim organization under attack. This bug was accidentally released due to a harmless update by a German programmer for the Open SSL project but apparently the code was faulty(Canada Tax Agency Hacked Using Heartbleed, 2014).

### 2.5.8. Heart Bleed Bug Fix

#### (i) Libre SSL

This is an open source implementation of the SSL and TLS, synonymous to the Open SSL software library but this was forked from it to fix the Heart Bleed vulnerability. Even though inApril 2014, Open BSD developers had introduced a new version starting from 1.0.1g branch (Seltzer, 2014),yet Google announced its own fork for Open SSL dubbed Boring SSL and it hopes to collaborate with Open SSL and Libre SSL developers (Goodin, 2014).

#### (ii) CCS Injection Vulnerability

This is a security bypass vulnerability affecting the Change Cipher Spec (CCS) processing in Open SSL it allows for a man-in-the-middle attack to be initiated to acquire decryption keys and modify traffic in transit that is by forcing SSL clients to use weak keys exposed to malicious nodes(lepidum, 2014). The CCS Injection vulnerability is as a result of a weakness in Open SSL method of keying materials. According to (Cyberoam, 2014) six new vulnerabilities have been discovered in Open SSL cryptographic library.

#### (iii) Parties Affected by Heart bleed

Most countries were affected by this bug, for example Ireland, Canada and a few more which did not make the news. On the other hand, with respect to Social Media and Email, we state the obvious that about half a million websites which amount to a high percentage of the internet community worldwide was affected as stated by(Mutton, 2014) and indicated in the pie chart labeled figure 1 below. Open SSL cryptographic library affected Over 17% of SSL web servers that used certificates issued by trusted certificate authorities. In a recent SSL survey by net craft it was realized that the heartbeat extension was enabled on 17.5% of SSL sites, accounting for around half a million certificates issued by trusted certificate authorities (Mutton, 2014). These certificates are susceptible to spoofing and the affected websites allow attackers copy them without raising browser warnings.

From the above it is observed that servers using Apache are the most vulnerable.

*Ireland*

After Heart bleed's discovery, nearly 11 percent of 600 Irish websites scanned by Trend Micro were vulnerable to attack by the Heart bleed bug. The bug evaded encryption that protected data sent between computers and servers, leaving sensitive and personal data vulnerable (Irish websites 'vulnerable' to Heartbleed bug - Technology Industry News _ Market & Trends , 2014).

*Canada*

Hackers managed to steal 900 taxpayers' social insurance numbers from the Canada Revenue Agency, just by exploiting Heart bleed. This caused the Canada Revenue Agency to shutdown access to its online services temporarily (Irish websites 'vulnerable' to Heartbleed bug - Technology Industry News _ Market & Trends , 2014)(Canada Tax Agency Hacked Using Heartbleed, 2014).

*Social Media*

The social networks affected by Heart bleed are as follows: Facebook and Instagram, twitter and vine, Pinterest, Google Plus and Youtube, Foursquare, Flickr and Tumblr. Personal information including name, address, phone number, personal contacts and other private information were exploitable. Slide share and LinkedIn were the only social media platforms (Experts, 2014) not affected.

*Email*

The users of Gmail, Yahoo mail, GoDaddy, Hotmail and Outlook were liable to have had their financial information such as credit cards, bank accounts, bill payments, tax information, and accounting information stolen by attackers(Experts, 2014).

*Other Popular Sites*

Amazon web services, Dropbox, OK Cupid, SoundCloud, and TurboTax also had a share of the "vulnerability cake" business information including proprietary documents and

also employee information, fax and accounting information as well as customer information(Experts, 2014).

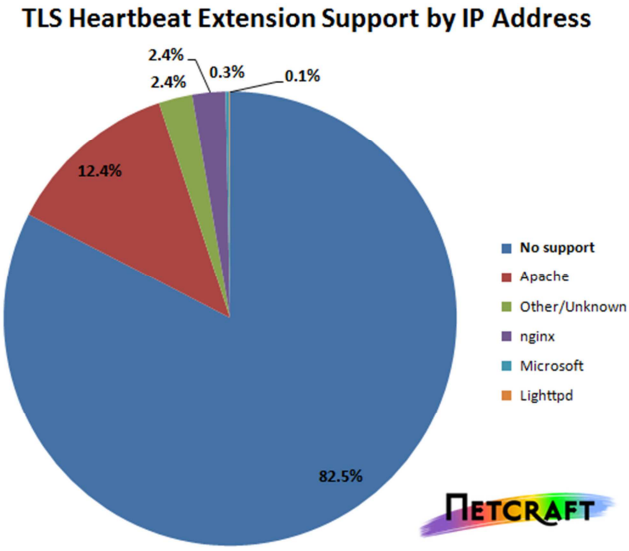


**Fig. 1.** TLS Heartbeat Extension Support by IP Address.

## 3. Security Value of Open SSL

Due to its open source nature, Open SSL's accessibility by the Information Technology industrialists for use, deemed it secured until recent events concerning whistle blower Edward Snowden, the term "secured" became questionable and then Heart bleed happened. Technically, the SSL library generates hash algorithms and powerful algorithms for private key and public key cryptography. It is responsible for all SSL protocols and could provide support for manipulating common certificate format and hardware (Pravir Chandra, 2002).

## 4. Open SSL Challenges

The obvious premise to the problem was the faulty update to the software library toolkit(14Ju) that proves the extent to which every update to the project is poorly scrutinized. According to (Pelletier, 2012) the problem with Open SSL is the poor documentation, and also there is no proper provision for implementing certain thread safety measures in the code for certain applications.

## 5. The Way Forward

Open SSL vulnerabilities now will cause a large number of people working on the project to adapt to more testing features upon an update's release. This means that updates will be tested extensively. This will affect the use of the Open SSL software library by end users (developers that modify code are inclusive), and it will make patching the affected version a lot less gruesome. Also documentation of the Open SSL software library must be considered a priority during development. This is likely to avert the implementation of several useless codes in operating systems that are out dated or not patronized by users as this was a major cause of the Heart bleed bug.

Forks that are newly implemented in the library should support code base with proper documentation in order for their adaptability to all affected versions. As a way of ensuring continuous efficiency with these forks it is best to support implementation with the required hardware that will ensure security depending on the amount of data load that is expected of a new fork because its functionality will remain the same and its users varying. Enterprises that implement Open SSL software library from now onwards should monitor the channels in every transaction and provide "first-aid" security measure with the help of a properly documented source code in case of bug discovery. Thus aiding in early reports of a bug and saving the massive user community of the version affected from cost burden when suppressing the damage that might have been caused and immediately patching up the error.

## 6. Conclusion

It is safe to conclude that in cryptography a perfunctory look at the technology believed to secure information concerning basic and extended transactions, later affects us negatively due to negligence and poor schematic definitions in documentation. Such cursory look at the technology will require governmental certification, scrutiny, verification and authentication if we are to avoid colossal losses and huge embarrassment.

## References

[1] (n.d.). Retrieved June 26, 2014, from https://minotaur.fi.muni.cz:8443/~xsvenda/docuwiki/lib/exe/fetch.php?media=public:pb173:openssl_en_v4.pdf

[2] *Canada Tax Agency Hacked Using Heartbleed*. (2014, April 15). (S. Mlot, Producer) Retrieved June 17, 2014, from http://www.pcmag.com/article2/0,2817,2456583,00.asp

[3] Cyberoam. (2014, June 12). (A Sophos Company) Retrieved June 27, 2014, from http://www.cyberoam.com/blog/openssl-continues-to-bleed-out-more-flaws-more-critical-vulnerabilities-found/

[4] Debian. (2008, May 13). *Debian Security Advisory*. (Debian) Retrieved June 27, 2014, from http://www.debian.org/security/2008/dsa-1571

[5] Experts, L. C. (2014). *LWG Consulting: Post Disaster Technical Experts*. (LWG Consulting) Retrieved June 26, 2014, from http://www.lwgconsulting.com/news/sites_affected_by_heartbleed_bug.aspx

[6] Goodin, D. (2014, June 20). *Risk Assessment and Hacktivism*. (ArsTechnica) Retrieved June 27, 2014, from http://arstechnica.com/security/2014/06/google-unveils-independent-fork-of-openssl-called-boringssl/

[7] *IBM Security Bulletin*. (2013, May 15). (IBM) Retrieved June 27, 2014, from http://www-01.ibm.com/support/docview.wss?uid=swg21637525

[8] *Irish websites 'vulnerable' to Heartbleed bug - Technology Industry News _ Market & Trends* . (2014, April 21). Retrieved June 17, 2014, from www.irishtimes.com

[9] Julian, S. (2014, April 12). *Cato*. Retrieved June 15, 2014, from http://www.cato.org/publications/commentary/nsas-heartbleed-problem-problem-nsa?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+CatoRecentOpeds+%28Cato+Recent+Op-eds%29

[10] *lepidum*. (2014, June 16). (lepidum) Retrieved July 11, 2014, from http://ccsinjection.lepidum.co.jp/

[11] Mcree, R. (2012, April 24). *InfoSec Handlers Diary Blog*. Retrieved June 26, 2014, from https://isc.sans.edu/diary/OpenSSL+reissues+fix+for+ASN1+BIO+vulnerability/13042

[12] Mutton, P. (2014, April 8). *Netcraft*. Retrieved June 27, 2014, from http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html

[13] Pelletier, P. (2012, October 27). *[Cryptography] Just How Bad is OpenSSL?* Retrieved June 26, 2014, from http://lists.randombit.net/pipermail/cryptography/2012-October/003388.html

[14] Pravir Chandra, M. M. (2002). *Network Security with OpenSSL*. O'Reilly.

[15] *Rapid7*. (2011, February 18). Retrieved June 25, 2014, from https://www.rapid7.com/db/vulnerabilities/http-openssl-cve-2011-0014 and http://www.openssl.org/news/secadv_20110208.txt

[16] *Rapid7*. (2012, April 19). Retrieved June 25, 2014, from https://www.rapid7.com/db/vulnerabilities/http-openssl-cve-2012-2110, http://www.openssl.org/news/secadv_20120419.txt, http://www.openssl.org/news/secadv_20120424.txt

[17] Ristic, I. (2013). *OPENSSL COOKBOOK; A Guide to the Most Frequently Used OpenSSL Features and Commands*. London: Feisty Duck Limited.

[18] *Security Focus*. (2002, July 20). Retrieved June 25, 2014, from http://www.securityfocus.com/bid/5366/discuss

[19] Seltzer, L. (2014, April 21). *ZDnet*. Retrieved June 27, 2014, from http://www.zdnet.com/openbsd-forks-prunes-fixes-openssl-7000028613/

[20] websense. (2014). *How to use OpenSSL and Microsoft Certificate Authority to create a websense manager SSL certificate*. Retrieved June 11, 2014, from http://www.websense.com/support/article/kbarticle/How-to-use-OpenSSL-and-Microsoft-Certification-Authority