International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

The Heartbleed Bug: An Open Secure Sockets Layer Vulnerability

Thabiso Peter Mpofu[1], Noe Elisa[2], Nicholaus Gati[3]

[1]M. Tech. Student, Department of Computer Science, School of IT, Jawaharlal Nehru Technological University Hyderabad, India

[2, 3]M. Tech. Student, Department of Computer Networks and Information Security, School of IT, Jawaharlal Nehru Technological University Hyderabad, India

[3]M. Tech Student, Department of Computer Networks and Information Security, School of IT, Jawaharlal Nehru Technological University Hyderabad, India,

Abstract: ***The Open Secure Sockets Layer (OpenSSL) is used to provide a secure platform for transactions that happen over the internet. About two thirds of the servers on the internet use the OpenSSL platform to provide secure transaction over the internet. The OpenSSL is a widely used open source implementation of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS). Transactions such as online shopping, emails and online banking are carried out on the internet through the OpenSSL and other platforms which provide a security. Vulnerabilities have however been found in the OpenSSL that has resulted in a wide public outcry all over the world. A vulnerability referred to as the Heartbleed Bug has sent shockwaves all over the internet. From the study we conducted, the scope of the data that has been potentially compromised is astronomical and includes usernames, passwords, bank account and credit card numbers, medical data, documents in online cloud storage. Not only has all of this user data been directly compromised, but, what are worse, the private keys of the servers running the vulnerable versions of OpenSSL were also almost certainly compromised. We recommend patching of affected applications or/and upgrade to versions that are not vulnerable in order to mitigate the risks identified.***

Keywords: OpenSSL, Heartbleed bug, secure, Transport Layer Security, Secure Sockets Layer, vulnerability**.**

1. Introduction

Security of transactions happening on the internet has become of the essence in this digital era that we are now living in. As more and more transactions from financial transactions to daily human interactions go online, the need for a secure platform is now a prerequisite. Valuable and sensitive information such as credit card details and passwords is transferred from computer to computer every split second. If data is sent as plain text it could easily be accessed or tempered with. The information being transferred should not fall into the wrong hands. Secure platforms such as the OpenSSL were developed specifically for that purpose. The OpenSSL is an open source implementation of the Secure Sockets Layer (SSL) and the Transport Layer Security (TLS) [7].The OpenSSL platform provides security when data is transferred from one point of the internet to another part [1]. The Secure socket layer (SSL) is the most popular protocol used on the Internet for secure transfer of data [4]. The OpenSSL protocol is used in two-thirds of all websites to prevent hackers from stealing sensitive information like passwords or credit card data[9],[16].If the data being transferred is edited along the way, data integrity is compromised and if the data is accessed and falls into the wrong hands, confidentiality of data is lost. Confidentiality is achieved through the use of encryption. Encryption algorithms such as RSA algorithm are used [5]. Data Integrity and confidentiality should be maintained as data moves from point to point. The OpenSSL protocol works by authenticating the server to the client and client to server through the use of digital certificates signed by a trusted third party. Private and public keys are also used in the OpenSSL to provide security. The OpenSSL protocol is however subject to vulnerabilities [2], [3] whether directly or indirectly. This can be seen by the trusted third parties who authenticate the identities of transacting individuals have been coming under attack [6]. Various other vulnerabilities have been found within the OpenSSL protocol and the most notable has been the Heartbleed bug.

2. OpenSSL

OpenSSL protocol is an open-source implementation of the SSL and TLS protocols [15]. Most sites use simple SSL or TLS to secure Hyper Text Transfer Protocol (HTTP) to provide HTTP over SSL (HTTPS). HTTPS refers to secure HTTP. The SSL/TLS provides three important functions

a) Authentication

Authentication is provided through the use of digital certificates and the RSA cryptographic algorithm. A Certificate Authority is used to validate the clients/servers authenticity in the use of digital certificates [14]. However most people's certificates are outdated and can be subject to man in the middle attacks [2]. The RSA is a public key cryptographic algorithm used in authentication and it is used to facilitate digital signatures.

b) Confidentiality

Access to the data being exchanged should only be granted only to the authenticated participants. Symmetric key encryption is used where one key is shared between client

and server. RC4 symmetric cipher is used to encrypt the exchange of the messages

c) Integrity

Messages being exchanged should not be altered interfered with. Messages digests such as MD5 and SHA-1 are used to ensure the integrity of the messages being exchanged is not compromised.The internet is based on the TCP/IP architecture as shown by figure 1 below.

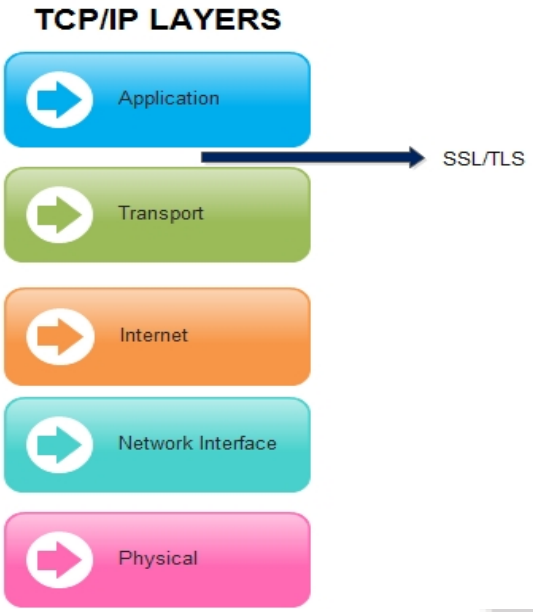

Figure 1: TCP/IP layers

The SSL is located between TCP (Transport layer) and HTTP protocols (application layer) as shown in figure 1.

The SSL can be divided into three protocols

i. Handshake Protocol
Used to facilitate Authentication of server and client

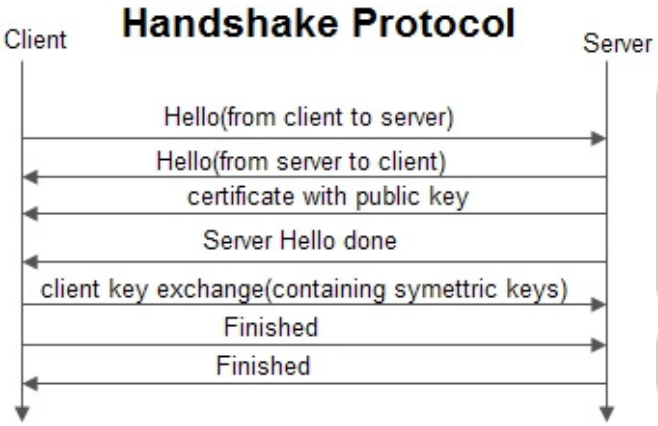

Figure 2: Handshake Protocol

As shown in figure 2, a series of handshakes are carried out. Parameter negotiation, secret key exchange and digital certificates are used to authenticate the identities of the transacting parties.

ii. Record Protocol
The Record protocol facilitates the exchange of encrypted messages

iii. Alert protocol
If an error is encountered, it is dealt with by the Alert Protocol.

3. The Heartbleed Bug

The Heartbleed bug has been described as one of the biggest security threats the Internet has ever seen to date [10]. The Heartbleed bug is a flaw found in the OpenSSL protocol and OpenSSL is the core cryptographic library used by most servers on the internet [7]. The logo representing the Heartbleed bug is shown in figure 3. Heartbleed bug was as a result of a lack of input validation as there was no bounds check that was carried out in the TLS heartbeat extension. The name Heartbleed came about from this flaw found in the heartbeat extension. This flaw could result in an attacker accessing up to 64kb with every heartbeat [13].

Figure 3: The Heartbleed bug Logo

The Heatbleed bug in the OpenSSL was as a result of a lack of bounds check, a Heartbeat request consisting of a payload whose payload length was also specified is sent from client to server, on receiving the request the server then must send the exact same payload back to the sender. This is illustrated in figure 4 below. However due to a lack of validation in bounds checking, client can send a small payload and specify a bigger payload length.

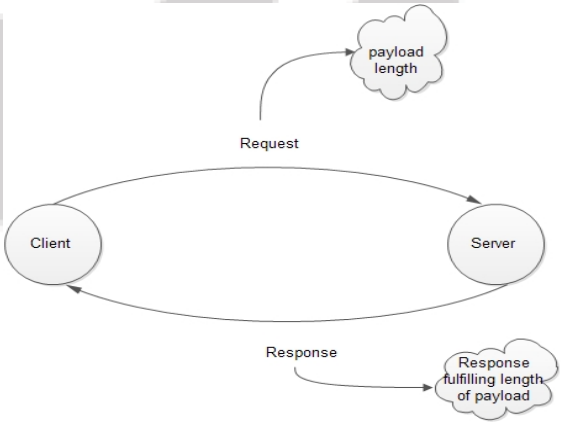

Figure 4: The Heartbleed Bug Vulnerability

If the payload length specified in the request is bigger than the actual payload, it would result in a return of the payload followed by whatever contents are currently contained in the active memory buffer.

A client can send a heartbeat request to the server for ten character word but specify the payload length as one hundred letters. The server will respond with a payload of ten characters and the remaining 90 characters will be what is contained in the active memory buffer. The active memory can contain critical data such as digital certificates, private keys and passwords thus compromising security. An attacker can get up to60kb of data. An attacker does not choose what they get they only have access to what is contained within the active memory at that particular time.

4. Effects of the Heartbleed bug

The bug has affected many popular websites and services Gmail, Yahoo and Facebook [10]. Sensitive account information such as passwords and credit card numbers could have been exposed over the past two years because the version containing the vulnerability was affected in December 2012[16]. By reading the memory of the web server, attackers could access sensitive data, including the server's private key. This could lead to man in the middle attacks [8]

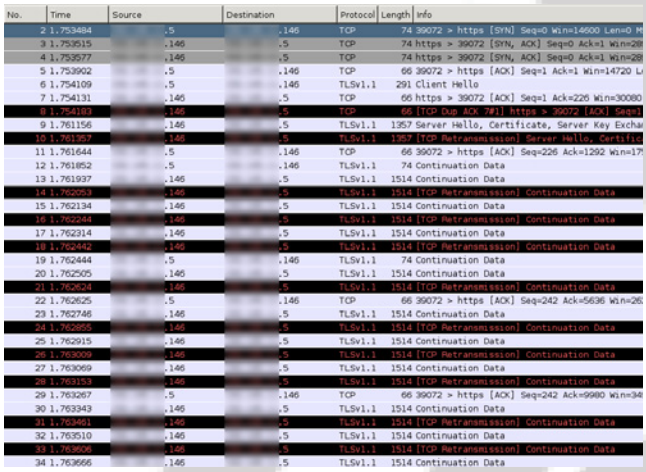

Figure 5: Network Traffic during Heartbleed attack

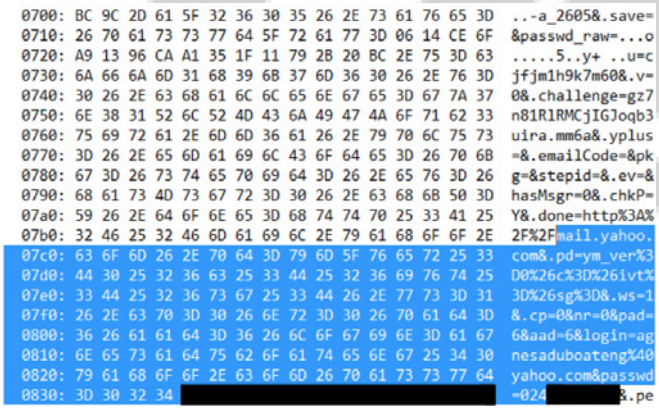

Figure 6: Login Data Retrieved Through an Heartbleed Bug Exploitation

5. Future work

Because of the heartbleed bug a new vulnerability was found. The latest vulnerability was introduced in 1998 and went undetected for all these years [8], [12]. The new flaw is more difficult for hackers to exploit as it requires them to intercept traffic between two computers [9]. The OpenSSL team issued an advisory advising people to update their OpenSSL versions [11]. Other vulnerabilities which have affected the OpenSSL such as Timing attacks on RSA Keys;

OCSP stapling vulnerability; SSL, TLS and DTLS Plaintext Recovery Attack to mention but a few have also been found [14]. The vulnerabilities have been dealt with in their own capacities. The fight against these vulnerabilities therefore remains an ongoing process. Vulnerabilities will continue to be dealt with as we go on.

6. Conclusion and Recommendations

OpenSSL version 1.0.1 is susceptible to the heartbleed flaw. Web masters and other users are encouraged to update the OpenSSL versions and patch to version 1.0.1g. Version 1.0.1g has bounds checking included to prevent buffer over-read. Internet users running vulnerable versions have been urged to install the patches. Companies such as Facebook, Google, Microsoft, Amazon and IBM, have joined forces to try to prevent another Heartbleed-like security breach. The companies have combined to fund open source projects which are critical such as the OpenSSL. With 66% of the internets' servers running on the OpenSSL platform, an awareness of this vulnerability is of the essence, most of the major service providers have however updated their versions of OpenSSL but there remains some which remain vulnerable.

References

[1] Deep Vardhan Bhatt, Stefan Schulze Gerhard P. Hancke "Secure Internet Access to Gateway Using Secure Socket Layer," IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, VOL. 55, NO. 3, pp 793-800, 2006

[2] Yogesh Joshi, Debabrata Das, Subir Saha, "Mitigating Man in the Middle Attack over Secure Sockets Layer," IEEE, pp 1-5, 2009

[3] Eman Salem Alashwali , "Cryptographic Vulnerabilities in Real-Life Web Servers," In Proceedings of the The 3rd International Conference on Communication and Information Technology(ICCIT-2013):Digital Information Management and Security Beirut, pp 6-11, 2013

[4] Krishna Kant and Ravishankar Iyer, Prasant Mohapatra, "Architectural Impact of Secure Socket Layer on Internet Servers: A Retrospect," IEEE pp 25-26, 2012

[5] H. Otrok, Montreal, R. Haraty, A. N. El-Kassar, "Improving the Secure Socket Layer Protocol by

[6] modifying its Authentication function," In Proceedings of the World Automation Congress (WAC) 2006, July 24-26, Budapest, Hungary, pp 1-6, 2006

[7] Neal Leavitt " Internet Security under Attack: The Undermining of Digital Certificates," IEEE Computer Society, pp 17-20, 2011
[8] CODENOMICON "The Heartbleed Bug," heartbleed.com , 29 April 2014 [Online]. Available: http://heartbleed.com/. [Accessed: June. 12, 2014]
[9] Tom Brewster, "Latest OpenSSL bug 'may be more dangerous than Heartbleed,"theguardian.com , 6 June 2014 [Online]. Available:http://www.theguardian.com/technology/2014/jun/06/heartbleed-openssl-bug-security-vulnerabilities [Accessed: June. 12, 2014]
[10] Gerald Smith "New Flaw Found in Software That Caused Heartbleed Bug," huffingtonpost.com 6 May 2014 [Online]. Available: http://www.huffingtonpost.com/2014/06/05/openssl-bug-heartbleed_n_5455613.html. [[Accessed: June. 12, 2014]
[11] Marshable Team " The Heartbleed Hit List: The Passwords You Need to Change Right Now," mashable.com, 10 April 2014 [Online]. Available: http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/ [Accessed: June. 12, 2014].
[12] OpenSSL.org "OpenSSL Security Advisory," openssl.org 05 June 2014 [Online]. Available: https://www.openssl.org/news/secadv_20140605.txt [Accessed: June. 12, 2014]
[13] Andrea Peterson "After the Heartbleed bug, researchers took a closer look at OpenSSL — and found more problems," washingtonpost.com, 6 June 2014 [Online]. Available: http://www.washingtonpost.com/blogs/the-switch/wp/2014/06/06/after-the-heartbleed-bug-researchers-took-a-closer-look-at-openssl-and-found-more-problems/ [Accessed: June. 12, 2014]
[14] Nick Sullivan "Staying ahead of OpenSSL vulnerabilities," blog.cloudflare.com, 7 April 2014 [Online]. Available: http://blog.cloudflare.com/staying-ahead-of-openssl-vulnerabilities [Accessed: June. 12, 2014]
[15] Wikepidia "OpenSSL," wikipedia.org, 8 June 2014 [Online]. Available: http://en.wikipedia.org/wiki/OpenSSL [Accessed: June. 12, 2014]
[16] OpenSSL Team" OpenSSL Project," openssl.org, 2014 [Online]. Available: https://www.openssl.org/ [Accessed: June. 12, 2014]
[17] Christina Warren, "Facebook, Google, Microsoft join forces to prevent another Heartbleed," mashable.com , 24 April 2014 [Online]. Available: http://mashable.com/2014/04/24/facebook-google-microsoft-join-forces-to-prevent-another-heartbleed/ [Accessed: June. 13, 2014]

Author Profile

Thabiso Peter Mpofu received B. Tech degree in Computer Science at Harare Institute of Technology (HIT), Zimbabwe in 2010. He is currently pursuing M. Tech Computer Science at JNTUH, India. He is a HIT staff development research fellow. His research interests are in the area of Electronic Commerce, Data Mining, Network Security and Mobile Computing.

Noe Elisa is currently pursuing M.Tech in computer networks and information security from JNTU Hyderabad, India. He completed his B.SC in Telecommunication engineering from university of dar es salaam, Tanzania in 2010. His research interests focus on security and privacy issues in distributed information systems, database systems, and communication networks. In particular Secure and privacy-preserving data sharing and data publishing, health informatics and Privacy and security in social networks.

Nicholaus Gati Received BSc degree in Computer Engineering and Information Technology from the University Of Dar Es Salaam, Tanzania. Pursuing M.Tech in Computer Networks and Information Security from School of Information Technology Jawaharlal Nehru Technological University, Hyderabad, India. His research interests include cloud computing security and storage, wireless network security, distributed systems and computing.