JAICT

ISSN 2355 1771
E-ISSN 2723-4827

JOURNAL OF APPLIED INFORMATION, COMMUNICATION AND TECHNOLOGY

Published by:
Research Center of Technology and Innovation
Directorate of Academic Research and Community Services
Swiss German University

Leak in OpenSSL

Jason Yapri, Rinkel Hananto

Department of Information Technology, Swiss German University, Tangerang 15143, Indonesia

Article Information

Received: 17 December 2019
Accepted: 15 January 2020
Published: 18 March 2021
DOI: 10.33555/ejaict.v7i1.70

Corresponding Author:

Jason Yapri
Email: Jason.yapri@student.sgu.ac.id

ISSN 2355-1771
eISSN 2723-4827

ABSTRACT

The term "hacker" has been spread around the world and has always been considered as a threat when we use the internet. We often hear hackers deface websites' contents and break into system to steal private and confidential information, such as account's username and password, credit card numbers and others. This is definitely an unethical behavior of irresponsible people who mostly aims to gain profit. However, the term hacker, on the contrary actually originates from an expert computer technician who tries to access the system to debug and fix security problems of the system.

Nowadays there are dozens of websites out there and some of those websites have low level of security. Hacker can easily break through their system and steal their private confidential data but just because these websites have low level security, that doesn't mean that it is ethical to break into someone's system and read their data. It goes the same when someone entering other people's house because the door was left open by the owner.

As web development grows rapidly, security has become an essential part to make the website more secure and reliable. This is when a group of people decided to make a collaborative project on the implementation of SSL (Secure Socket Layer) and TLS (Transport Layer Security) that is available to be used by everyone. This project is called as OpenSSl and has been used by most of the websites in the internet today. What if this OpenSSL, which has been trusted and implemented by 2/3rd of the websites all around the world can be breached? Definitely it will attract dozens of hackers all around the world to do something unimaginably dangerous.

Keywords: *Ethics, Hacking, Heartbeat, Heartbleed, OpenSSL, Security*

1. Introduction

1.1. Reasons for Hacking

Every hacker has different reasons for hacking a computer system. It can be either for good purposes, bad purposes or merely for some pranks. The purpose of hacking has always be for good purposes to fix and debug the system to create a more secure and reliable computer system. Yet today there are more hackers that do it for a bad purpose.

Theft of services can sometimes be the case why they hack through the system. It is when they want to use the service provided by a computer system without paying for it. For instance, many websites provide a premium service other than that of the regular services that can be used by everyone. Surely this premium service is meant only to some people who pay an amount of money to use it. In this case, hackers hack into the system to get these premium services for free. The second reason a hacker hacks is to take valuable private and confidential data. E.g. credit card numbers, account’s username and password, etc. They usually do this for financial motives.

Another reasons a hacker hacks is either for a thrill and excitement or for a vengeance. They can do it on purpose just to cause harm to other people or for the sake of their own enjoyment. Some people may even do it for experiment purposes. By doing so, they can learn a great deal of knowledge every time they break into the system.

In our opinion, whatever the reason why hackers hack into a system, if it is for bad purposes (theft of services, data theft) or to fulfill their own pleasure and hatred, then it shall be considered as an unethical behavior that must not be followed by others.

1.2. Heart Bleed Bug

Heartbleed bug is a bug on the OpenSSL technology which implements both SSL (Secure Socket Layer) and TLS (Transport Layer Security). The bug located in the heartbeat extension of the OpenSSL. RFC6520 defines SSL Heartbeats extensions that are used to keep a connection alive without the need to constantly renegotiate the SSL session. When it is exploited it cause memory leak in the contents from the client to the server and vice versa. That is why it is called as the Heartbleed bug.

Heartbleed bug has affected countless websites using OpenSSL v1.0.1 – v1.0.1f including large organization’s websites. Fortunately, after the announcement of heartbleed bug, the developer fixes the OpenSSL by distributing a new version of OpenSSL v1.0.1g. It is however three days after the bug is publicize.

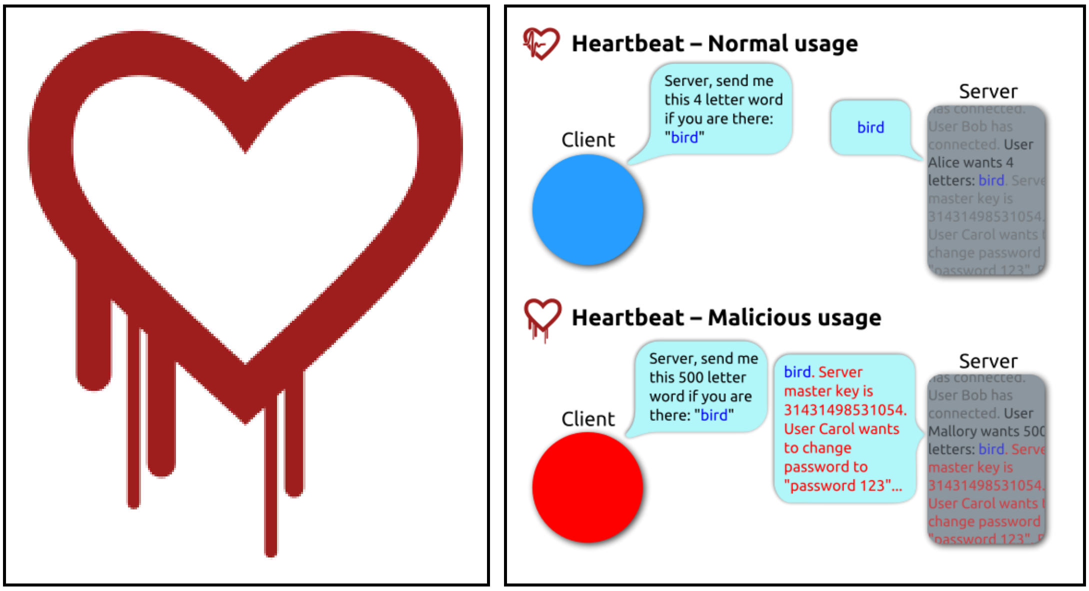
Heartbeat – Normal usage
Client
Server, send me this 4 letter word if you are there: "bird"
bird
Server
has connected. User Bob has connected. User Alice wants 4 letters: bird. Serve master key is 31431498531054. User Carol wants t change password "password 123". P
Heartbeat – Malicious usage
Client
Server, send me this 500 letter word if you are there: "bird"
bird. Server master key is 31431498531054. User Carol wants to change password to "password 123"...
Server
has connected. User Bob has connected. User Mallory wants 500 letters: bird. Serve master key is 31431498531054. User Carol wants t change password "password 123". P

Figure. 1. (a) Heartbleed Logo (b) Heartbeat Extensions Usage

To explain more about how heartbleed bug works, the following is an illustration from Fig 1 b of the uses of the bug to steal private information from a server:

During the normal usage of the OpenSSL’s heartbeat extensions, the client sends a request for 4 letter word which is “bird”. The server will response the request from the client, so in other words the server will send the 4-letter word back to the client.

During the malicious usage of the OpenSSL’s heartbeat extensions, the client sends a request for 4 letters which is “bird”, but stated in the file that it consists of 500 letters instead of 4. The server didn’t double-check the length of the word from the file that the client sent, instead it just sends all the 500 letters from the server to the client that is requested from the file. In this way, the client can see all the information sent from the server including private and confidential data inside the server.

2. Case Study

Case 1:

“A 19-year-old Canadian became the first person to be arrested in relation to the Heartbleed security breach.”

Stephen Arthuro Solis-Reyes from London, Ontario was accused of hacking into the Canadian Revenue Agency (CRA)'s website last Friday by the Royal Canadian Mounted Police.

The RCMP say Mr Solis-Reyes then stole 900 social insurance numbers.

In a separate development, UK parenting site Mumsnet has provided fresh details about how it fell victim to the bug.

The site has published a post explaining how a hacker hijacked several accounts last week - including one belonging to Mumsnet's founder Justine Roberts - after exploiting the cryptology flaw to expose the owners' credentials.

"I hope the actions of hijacking Justine's account help draw attention to how big a deal this is," the hacker wrote on the social network.

"I suspect a lot of people would not have taken it seriously otherwise. Be thankful that the person who got access to the server information was kind enough to let you all know (and at least try and be funny with it) instead of simply sitting on the information."

Source: http://www.bbc.com/news/technology-27058143

Case 2:

Millions of Android devices remain vulnerable to the Heartbleed bug a week after the flaw was made public.

Google announced last week that handsets and tablets running version 4.1.1 of its mobile operating system were at risk.

The search giant has since created a fix, but it has yet to be pushed out to many of the devices that cannot run higher versions of the OS.

It potentially places owners at risk of having sensitive data stolen.

In addition, security firms warn that hundreds of apps available across multiple platforms still need to be fixed.

These include Blackberry's popular BBM instant messaging software for iOS and Android.

The Canadian firm has said that it will not issue a fix until Friday, but said there was only an "extremely small" risk of hackers exploiting the bug to steal its customers' data.

In the meantime, the program remains available for download from Apple's App Store and Google Play.

Source: http://www.bbc.com/news/technology-27020256

From the above cases, we know that this leak in openSSL is a serious problem for everyone that has online web account. OpenSSL is implemented in 60% of the websites in the internet. Thus, it attracts hackers to breach into computer system as Stephen Arthuro Solis-Reyes from London did. Even android devices running with version 4.1.1 are vulnerable to the attack. We do not know how many more unethical hackers that have successfully breach into computer systems all around the world and steal private and confidential data.

3. Law

Pasal 30

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

(3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Pasal 46

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah).

(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp 700.000.000,00 (tujuh ratus juta rupiah).

(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah).

4. Methodology

The recent bug on OpenSSL known as Heartbleed has been fixed using a patch by OpenSSL. However not all website owners follow the development of web technology. According to dailymail.co.uk, as of 9 May 2014 there are still 300,000 websites that is vulnerable to the heartbleed bug.

As for web owners, if you do not know whether your websites are vulnerable or not, we recommend you to patch the OpenSSL to the latest version and check your website’s vulnerability by visiting one of the following websites: https://lastpass.com/heartbleed/, http://tif.mcafee.com/heartbleedtest, https://filippo.io/Heartbleed/.

As for social media and other online services’ users, it is unclear which websites are attacked and which websites are not. As we can’t determine this, we recommended you to update your password with a strong combination of letters, alphabets and symbols if possible.

5. Conclusion

Since the rise of social media’s popularity, web technology development accelerates at a tremendous rate. As more people get connected with each other through social media, more personal and private information are stored in the web server. If this private information is not secured properly, users of these websites may become the victim of identity fraud and identity theft. There are some laws to prevent these abuses of private information. However, as the size of internet is enormous, there’s no definite way to control all abuse of internet.

“Heartbleed” is a recent bug infected in the most well-known and widely used open source implementation of SSL and TLS which has been used by 60% of all the websites worldwide. The bug has now been resolved by using a patch. However, most of the web owners and online web users seem not to care about this issue.

References

http://en.wikipedia.org/wiki/OpenSSL

http://en.wikipedia.org/wiki/Transport_Layer_Security

http://en.wikipedia.org/wiki/Secure_Sockets_Layer

http://en.wikipedia.org/wiki/Heartbleed

http://en.wikipedia.org/wiki/Hacker_(term)#Hacker_definition_controversy

https://filippo.io/Heartbleed/

http://heartbleed.com

https://lastpass.com/heartbleed/

http://www.bbc.com/news/technology-27058143

http://www.bbc.com/news/technology-27020256