THE HEARTBLEED BUG CASE

Case Study Report Submitted

to

MANIPAL ACADEMY OF HIGHER EDUCATION

For Partial Fulfillment of the Requirement for the

Award of the Degree

Of

Bachelor of Technology

in

Information Technology

by

Sriyans K	Harshitha Gupta	Chitrap Shrivastava	Sasikiran
210911228	210911224	210911198	200911146

Under the guidance of

Mr. K Krishna Prakasha
Associate Professor
Department of I&CT
Manipal Institute of Technology
Manipal, Karnataka, India

Subject: ICT 3156- CYBER SECURITY

MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
A Constituent Unit of MAHE, Manipal

November 2023

2

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

The exploitation of the OpenSSL cryptographic library which was a key implementation in Transport Layer Security (TLS) is the Heartbleed Bug. TLS secures the HTTPS protocol which ensures secure communication. Several users lost their passwords, credit card details, numbers and other personal information to the heartbleed bug as it exploited the vulnerable implementation of the OpenSSL library.

The Heartbleed bug was made public on April 7, 2014. Even though the bug was disclosed in April 2014, it was present for well over 2 years before that.

Attackers stole information from several well-reputed and high-profile websites like Yahoo, Facebook, GitHub, Google etc. Even America's National Security Agency (NSA) exploited the bug.

The Heartbleed bug was a huge thing as it showed that even the most trusted and assumed secure software was not immune to attack.

1.1 KEY FINDINGS AND SIGNIFICANCE

The Heartbleed bug was a significant security incident because it allowed attackers to steal sensitive information from a wide range of websites and organisations. The bug was also significant because it was easy to exploit and because it had been present in OpenSSL for over two years before it was disclosed.

The Heartbleed bug highlighted the importance of security and the need to be constantly vigilant against cyber threats. It also showed the importance of open-source software, as the Heartbleed bug was discovered and patched by open-source software developers.

2. INTRODUCTION

The Heartbleed bug cybersecurity case study is a significant case study because it highlights a number of important cybersecurity issues. The case study shows how a single security vulnerability can be exploited by attackers to steal sensitive information from a wide range of organizations. It also shows the importance of open-source software in discovering and patching security vulnerabilities.

The Heartbleed bug case study is relevant and important because it provides valuable lessons learned that can help organizations improve their cybersecurity posture. The case study also highlights the need for individuals to be aware of the risks associated with using online services and to take steps to protect their personal information.

3. CASE STUDY DETAILS

3.1 BACKGROUND

The Heartbleed bug was discovered in April 2014 by a team of security researchers from Codenomicon and Google. The bug was present in OpenSSL, a widely used cryptography library. OpenSSL is used to secure HTTPS connections, which are used by most websites to protect user data.

3.2 CYBERSECURITY ISSUE

The Heartbleed bug allowed attackers to steal sensitive information, such as usernames, passwords, and credit card numbers, from websites and other online services that were using vulnerable versions of OpenSSL.

4. SECURITY VULNERABILITIES

The Heartbleed bug was caused by a flaw in the implementation of the TLS heartbeat extension. The heartbeat extension is a TLS feature that allows servers and clients to verify that they are still connected to each other.

The Heartbleed bug allowed attackers to send specially crafted heartbeat requests to vulnerable servers. These requests would trick the server into revealing its memory contents. The memory contents could contain sensitive information, such as usernames, passwords, and credit card numbers.

5. IMPACT AND CONSEQUENCES

The Heartbleed bug had a significant impact on a wide range of organisations. The bug was exploited by attackers to steal sensitive information from several high-profile websites and organizations, including Yahoo, Google, Facebook, and GitHub. The bug was also exploited by government agencies, such as the National Security Agency (NSA) in the United States.

The consequences of the Heartbleed bug for affected organizations included financial losses, reputational damage, and regulatory compliance issues.

6. LESSONS LEARNED

The Heartbleed bug case study provides several valuable lessons learned for organizations and individuals.

6.1 LESSONS LEARNED FOR ORGANISATIONS

Organisations should regularly audit their software systems for security vulnerabilities.

Organizations should implement security policies and procedures to mitigate the risk of cyberattacks. Organisations should educate their employees about cybersecurity best practices.

6.2 LESSONS LEARNED FOR INDIVIDUALS

Individuals should use strong passwords and enable two-factor authentication on all their online accounts. Individuals should be careful about what links they click on and what attachments they open in emails. Individuals should keep their software up to date.

7. CONCLUSION

The Heartbleed bug marked a critical flaw within the OpenSSL cryptography library, enabling attackers to illicitly access sensitive data from numerous websites and entities. Exploited by hackers, it led to the theft of user credentials, payment details, and other confidential information from prominent platforms such as Yahoo, Google, Facebook, and GitHub.

This case study significantly underscores key cybersecurity challenges. It highlights how a single vulnerability can be manipulated to compromise various organizations, emphasizing the crucial role of open-source software in identifying and addressing security flaws.

The Heartbleed bug case study offers pivotal lessons for both entities and individuals. Organisations must routinely scrutinize their software systems for vulnerabilities, enforce robust security protocols to curb cyber threats, and educate their staff on cybersecurity practices. Meanwhile, individuals should employ robust passwords, activate two-factor authentication across their online accounts, practice caution with email links and attachments, and consistently update their software for enhanced security.

8. REFERENCES

1 Krebs, Brian. "The Heartbleed Bug: What You Need to Know." Krebs on Security, April 7, 2014. https://krebsonsecurity.com/

2 Greenberg, Andy. "Heartbleed: The Bug That Was Everywhere." Wired, April 8, 2014. https://www.wired.com/2014/04/heartbleedslesson/

3 Schneier, Bruce. "The Heartbleed Bug." Schneier on Security, April 7, 2014. https://www.bbc.com/news/technology-26969629

4 Codenomicon and Google. "Heartbleed: A Serious Vulnerability in OpenSSL." April 7, 2014. https://community.synopsys.com/s/topic/0TO34000000LiuoGAC/codenomicon

9. RELEVANT DIAGRAMS

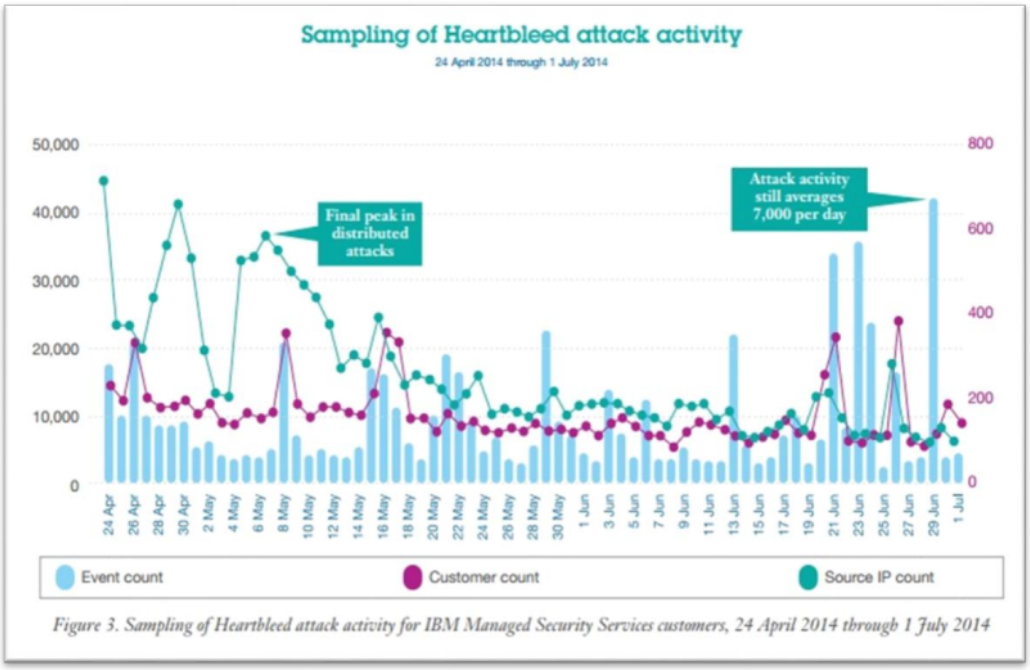

Fig 1. Number of Attacks vs Days (24 Apr 2014 – 1 Jul 2014)

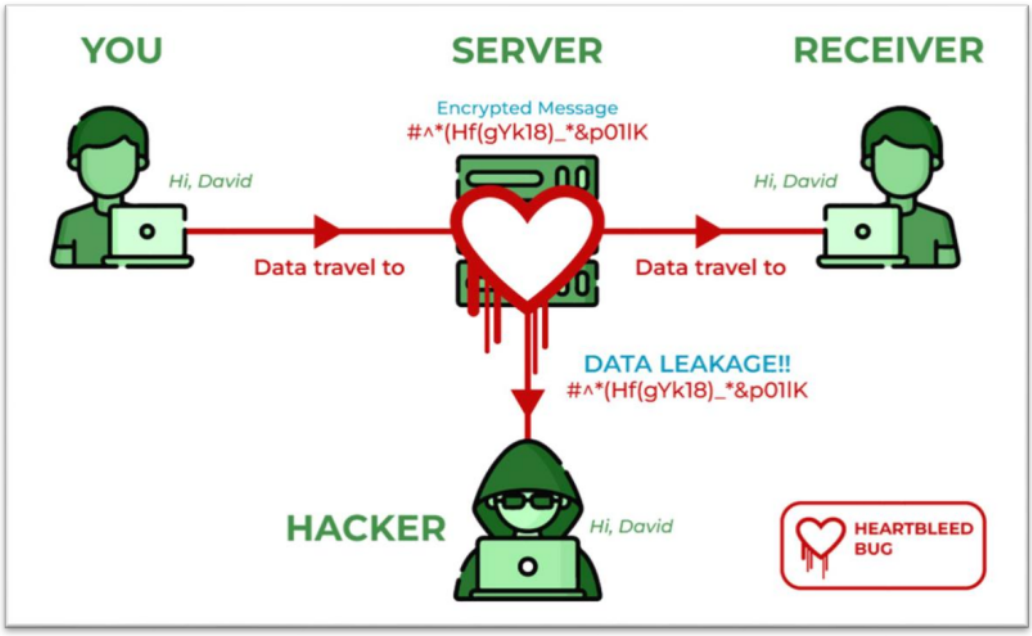

Fig2. Working of the Bug

10. INDIVIDUAL CONTRIBUTIONS

1 Sriyans 210911228: Conducted the plagiarism report, composed the Executive Summary and analysed Impact and Consequences.
2 Harshitha 20911224: Made Case Study Details and Security Vulnerabilities.
3 Chitrap 210911198: Wrote the Conclusion, Lessons Learned, and Recommendations and formatted the document.

4 Sasikiran 200911146: structured the Table of Contents, wrote the Introduction and created the Title Page.

CYS FISAC

ORIGINALITY REPORT

10%	10%	1%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	impressions.manipal.edu Internet Source	4%
2	www.coursehero.com Internet Source	2%
3	www.nstec.com Internet Source	1%
4	nlab.engr.uconn.edu Internet Source	1%
5	www.news18.com Internet Source	1%
6	inkwoodresearch.com Internet Source	1%

Exclude quotes	On	Exclude matches	< 3 words
Exclude bibliography	On		