Exercise 5: Software Security in Practise

Heartbleed security bug exploit & impact:

Heartbleed bug is a serious vulnerability found in the OpenSLL library of version 1.0.1 or below. OpenSLL is an open source code library that implements the cryptographic protocols - Transport Layer Security (TLS) and Secure Socket Layer (SSL) protocols. It is a security bug that allows an attacker to download and obtain a random chunk of memory (RAM) from the server to the client and vice-versa. Through this memory, the attacker can get access to sensitive data, passwords, private encryption keys that protects users' accounts. This vulnerability is registered in Common Vulnerabilities and Exposures (CVE) database as CVE-20140160.

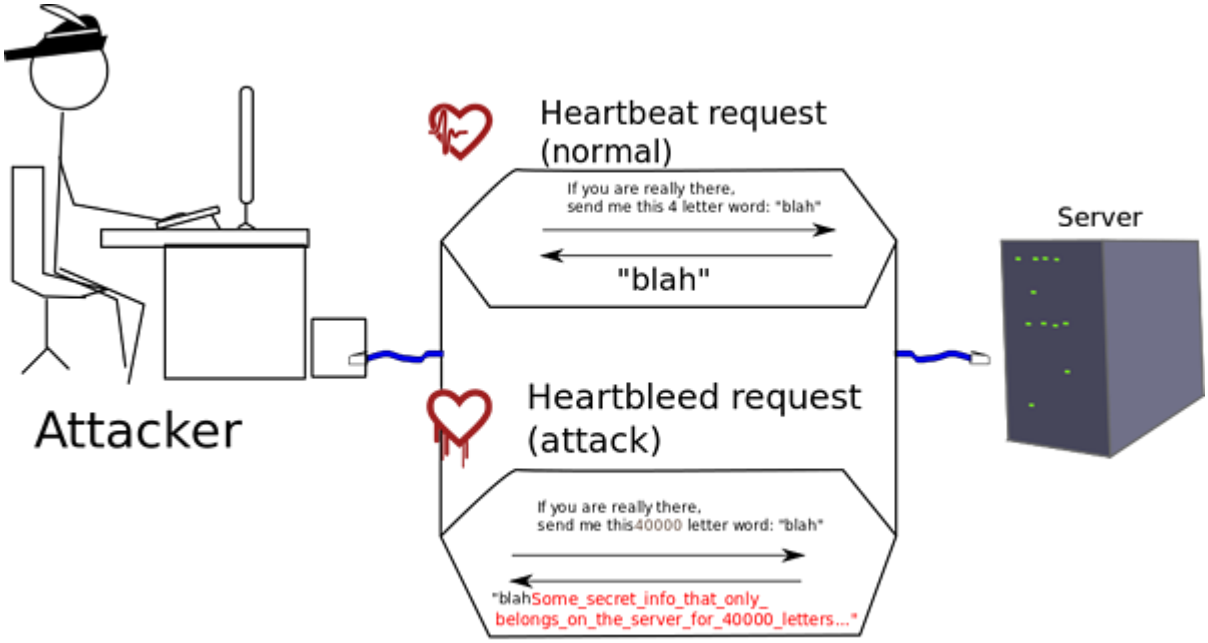

Fig:1 Pictorial explanation of Heartbleed bug

This flaw was in the TLS Protocol heartbeat extension, which when exploited can expose memory content to the Internet. For instance, if the client sent a heartbeat request of 40kb long to the server but the actual request is only 20kb long. Then the server would set 40kb of memory buffer, trusting the client request. The server will store this actual request of 20kb along-with the extra 20kb memory buffer. And, send the requested 40kb back to the client. In this communication, the server blindly trust the 40kb request from the client instead of cross-checking with the actual required 20kb request. In this way, extra 20kb of data is the sensitive information that the attacker was now able to extract from the server. Hence, this bug name Heartbleed is derived from Heartbeat vulnerability. The impact of Heartbleed bug was very large. One paper stated that "Heartbleed's severe risks, widespread impact, and costly global cleanup qualify it as a security disaster". Most of the software using vulnerable OpenSSL were badly affected. These included:

- Web-servers like Apache & nginx,
- Email-servers like SMTP, POP and IMAP Protocols,
- Chat-servers XMPP protocol,
- SSL Virtual Private Networks (VPN),

- Various client side software and,
- Network appliances.

Reasons for why it was undetectable since long & it's fixes:

It was difficult to detect the exploitation of Heartbleed bug in a system because it does not leave any trace in the logs in order to recognize any abnormal activity. Besides, this bug contains lots of complicated and obscured code that most tools like static analysis tool and Dynamic analysis tool failed to find the Heartbleed bug. Also, one of the reasons were less funds for OpenSSL. At the time of Heartbleed bug, only one person was working on complete OpenSSL.

The way to fix the Heartbleed vulnerability can be either by:

- Upgrading to fixed and latest version of OpenSSL, or
- Re-compiling OpenSSL with removed TLS handshake code (by compile time option).