Homework 5

sdh140430 **Swapnil Hasabe**

Heartbleed bug in OpenSSL

What is Heartbleed Bug in OpenSSL? (Causes)

1. The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.
2. Also it is programming mistake in popular OpenSSL library that provides cryptographic services such as SSL/TLS to the applications and services.
3. It results from improper input validation (due to a missing bounds check) in the implementation of the TLS heartbeat extension

How does Hearbleed Bug affect (work)? (Consequence)

1. The Heartbleed bug allows anyone on the Internet to read the memory of the systems (leak of memory content from server to client and vice versa) protected by the vulnerable versions of the OpenSSL software.

2. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

Impact of Heartbleed bug (What leaks)?

1. In practice, attacker steals secret keys used for X.509 certificates, user names and passwords, emails, business critical documents and communications without using any privileged information or credentials

2. Cisco Systems has identified 78 of its products as vulnerable, including IP phone systems and telepresence (video conferencing) systems.

3. Several GNU/Linux distributions were affected e.g. Debian, Linux Mint , CentOS, Oracle Linux and Amazon Linux

How to fix it?

1. Do not use vulnerable version of OpenSSL. Instead deploy Fixed OpenSSL which has been released already. Service providers and users have to install the fix as it becomes available for the operating systems, networked appliances and software they use.

2. To regain confidentiality and authenticity, compromised servers must regenerate all compromised private key-public key pairs and must revoke and replace all certificates linked to these.

3. According to Wheeler, the most efficient technique which could have prevented Heartbleed is an atypical test suite thoroughly performing what he calls "negative testing". Wheeler highlights that a single general-purpose test suite could serve as a base for all TLS implementation.
4. The Nmap security scanner includes a Heartbleed detection script from version 6.45