Volume 4, Issue 11, November 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Recent Attacks on SSL

Anjula Madhuri Burgula, Dasari A Rachana S, D S V Lakshmi
Dept of CSE,Sri Indu Institute of Engg &Technology,
Hyderabad, India

Abstract*— Secure Socket Layer, known as SSL is a security protocol. SSL is used to establish a secure connection between Server and Client. Recently in 2014, few attacks were identified by Security Researchers on SSL. We are going to focus on what are the recent Attacks on SSL, What is the impact on the web applications, and how we can mitigate them for our web applications in real time usage.

***Keywords*— Secure Socket layer, SSL, Heartbleed, Poodle Bug, Open SSL, Attacks on SSL**

I. INTRODUCTION

Normally, the data is transmitted in plain text between a server and client. That means the data sent between a web server and browser is transmitted in plain text which is vulnerable to eavesdropping. If any attacker intrude/intercept the network, he may see and use the data .To prevent that, data should be transmitted in a protected manner. SSL fulfils this requirement .SSL is the security technology for establishing an encrypted link between a web server and a browser. This link ensures that data passed between a web server and browser remain private and integral. SSL is an industry standard and is implemented by millions of websites in the protection of their online transactions with their customers.Transport Layer Security (TLS), the successor of SSL, is the most popular and widely used.

SSL Protocols:

- **SSL 1.0, 2.0 and 3.0**
- **TLS 1.0**(or SSL 3.1, Released in 1999)
- **TLS 1.1** (or SSL 3.2, Released in 2006)
- **TLS 1.2** (or SSL 3.3, Released in 2008)

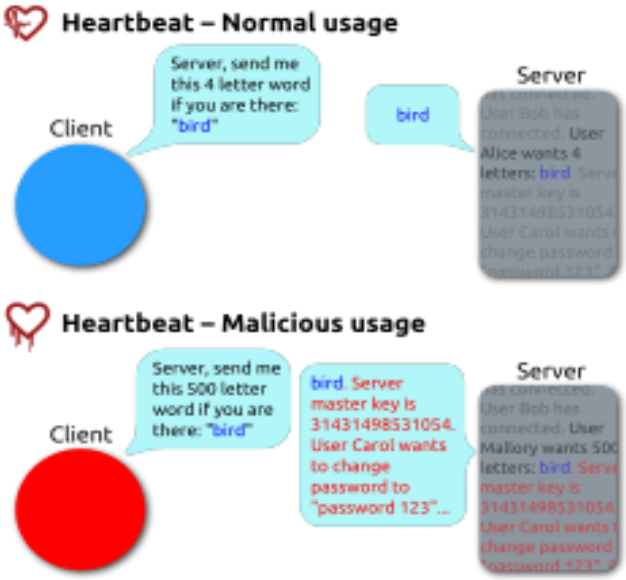
TLS/SSL provides numerous benefits to clients and servers over other methods of authentication, including:

- Strong authentication, message privacy, and integrity
- Interoperability
- Algorithm flexibility
- Ease of deployment
- Ease of use

Researchers have discovered a number of vulnerabilities in the Transport Layer Security Protocol, the widely used encryption scheme used to secure sensitive information like credit card numbers, social security numbers, and login credentials and e-commerce transactions etc. on the internet. Recently in 2014, two attacks were discovered on SSL/TLS. 1. Heartbleed bug and 2.Poodle attack on SSL

Heartbleed Bug:

Heartbleed is a security vulnerability in OpenSSL software that lets a hacker access the memory of data servers. The Heartbleed bug allows an attacker to steal a server's digital keys that are used to encrypt communications and get access to a company's secret internal documents. OpenSSL is an open Source software for SSL implementation across the web. The versions with vulnerabilities are 1.0.1 through 1.0.1f.



This flaw allows a remote attacker to retrieve private memory of an application that uses the vulnerable OpenSSL library in chunks of 64k at a time.There is no total of 64 kilobytes limitation to the attack, that limit applies only to a single heartbeat. Attacker can either keep reconnecting or during an active TLS connection keep requesting arbitrary number of 64 kilobyte chunks of memory content until enough secrets are revealed.The sensitive information that may be retrieved using this vulnerability include:

- Primary key material (secret keys)
- Secondary key material (user names and passwords used by vulnerable services)
- Protected content (sensitive data used by vulnerable services)
- Collateral (memory addresses and content that can be leveraged to bypass exploit Mitigations.

II. HEARTBLEED BEHAVIOUR

For SSL to work, your computer needs to communicate to a server. To do this, it sends out what's called a "heartbeat." What a heartbeat does is send a specific signal to a server in order to see if that server is online. If the server is online, it sends that signal right back to your computer, allowing you to enjoy secure communications. Both your computer and the server send out heartbeats on regular intervals to make sure both you (the user) and the server (the service) aren't offline.
Heartbleed takes advantage of this "heartbeat" by sending a malicious heartbeat signal to servers. That malicious heartbeat essentially tricks the server into sending a random chunk of its memory back to the user who sent the malicious heartbeat. Contained in that memory can be a random collection of email addresses, usernames and passwords. Some of those credentials, worryingly, could belong to the company managing that server. This provides hackers with a way of accessing and exploiting information throughout the Internet.
We can test our websites weather they are effected with Heartbleed or not at below mentioned urls,

1) https://lastpass.com/heartbleed/
2) https://filippo.io/Heartbleed/

Solution for Heartbleed:

1) Upgrade the server to the latest version of OpenSSL (version 1.0.1g or later).
2) Rekey, reissue, and then revoke all certificates used with the vulnerable version of OpenSSL

III. POODLE ATTACK

Padding Oracle on Downgraded Legacy Encryption Attack, A CVE-2014-3566 vulnerability in SSLv3 protocol was identified by the Google security team in 15, October 2014.
A bug has been found in the Secure Sockets Layer (SSL) 3.0 cryptography protocol (SSLv3) which could be exploited to intercept data that's supposed to be encrypted between computers and servers. Three Google securityresearchers discovered the flaw and detailed how it could be exploited through what they called a Padding Oracle on Downgraded Legacy Encryption (POODLE) attack (CVE-2014-3566).Products which meet below criteria are vulnerable to POODLE attack, 1) Which support SSL 3.0, and 2) a block cipher in CBC mode is one of the transform sets being offered. Products that don't support SSL 3.0, and in which no block cipher in CBC mode is offered in the transform set are not affected.

As per Google, an attacker/Hacker that controls network between the computer and server could interfere with the handshake process used to verify which cryptography protocol the server can accept using a "protocol downgrade dance". This will force computers to use the older SSL 3.0 protocol to protect data that is being sent. Hackers can then exploit the bug by carrying out a man-in-the-middle (MITM) attack to decrypt secure HTTP cookies, which could let them steal information or take control of the victim's online accounts.

We can test our websites weather they are effected with POODLE or not at below mentioned urls,

1) http://poodlebleed.com/ and 2)https://www.tinfoilsecurity.com/poodle

The precautions for not affecting to POODLE attack is,

1) Check to see if SSL 3.0 is disabled on your browser (for example, in Internet Explorer it is under Internet Options, Advanced Settings)
2) Avoid MITM attacks by making sure "HTTPS" is always on the websites you visit.
3) Monitor any notices from the vendors you use regarding recommendations to update software or password
4) Avoid potential phishing emails from attackers asking you to update your password – to avoid going to an impersonated website, stick with the official site domain.

IV. CONCLUSION

Upgrade the Server to the latest version of OpenSSL to protect from Heartbleed and Disable SSL3.0 to be secure from POODLE attack.

REFERENCES

[1] http://en.wikipedia.org/wiki/Heartbleed
[2] http://poodlebleed.com/
[3] https://www.tinfoilsecurity.com/poodle
[4] http://safeweb.norton.com/heartbleed
[5] https://lastpass.com/heartbleed/
[6] http://safeweb.norton.com/heartbleed

