Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 4, April 2015, pg.401 – 405

RESEARCH ARTICLE

SSL/TLS SECURITY POSTURE IDENTIFIER

Pavithra S, Sheeba Pari

M. Tech (CSE), New Horizon College of Engineering, Bangalore, India
Asst. Professor, Department of Computer Science & Engineering, New Horizon College of Engineering, Bangalore, India
pavithrashivakumarg1@gmail.com, sheba.pn@gmail.com

Abstract:

SSL/TLS (Secure socket layer) is a cryptographic protocol that provides secure communication over internet. Any parties when they want to perform secure communication over internet. They can use SSL/TLS and be sure of their data not been disclosed over the network. There has been lot of security issues already identified and patches have been released for it. Still companies fail to implement all the patches because they lack knowledge required to understand SSL/TLS security and its implementation. We will develop a scanner for SSL/TLS which identifies well know existing issues in SSL/TLS security and provide report with SSL/TLS implementation issues. This will help any person without the knowledge of SSL/TLS security to identify weakness in their SSL/TLS secure implementation.

This paper particularly tests the server against vulnerabilities such as SSLv2 is supported, weak ciphers enabled, OPENSSL/TLS is vulnerable to heart bleed, certificate validity, poodle attack is possible. The resources to those who are new to the information assurance field can provide an insight to two common protocols used in Internet security. Though SSL and TLS are not the only secure protocols currently in use, they are very common for sites dealing with transactions that could involve sensitive data (eg: personal and financial information, passwords etc).

Keywords: Cipher Suites (CS), InetSocketAddress (ISA), Server Certificate (SC), Heart Bleed (HB).

I. INTRODUCTION

The Transport Layer Security (TLS) protocol evolved from SSL protocol and SSL is often used to refer to what is actually TLS. The combination of SSL/TLS is the most widely deployed security protocol used today and is found in applications such as Web browsers, email and basically any situation where data needs to be securely exchanged over a network, like file transfers, VPN connections, instant messaging and voice over IP.

SSL is designed to establish encryption and identity assurance. It enables encrypted communication between a web server and a web browser. SSL ensures that all data passed between the web server and browser remains private and secure. The developed scanner takes in IP address of a system/server and generate a report stating which of the security issues existing as per this paper like SSLv2 is supported, weak ciphers enabled, OPENSSL/TLS is vulnerable to heart bleed, certificate validity, poodle attack is possible. The report will be in the form of a notepad with existing issues in particular tested server with description regarding the issue.

SSL/TLS security is an every changing landscape. There has been lot of security issues already identified and patches have been released for it. Still companies fail to implement all the patches because they lack knowledge required to understand SSL/TLS security and its implementation. Hence we are developing a scanner for SSL/TLS which identifies well known existing issues in SSL/TLS security and provide report with SSL/TLS implementation issues. This will help any person without the knowledge of SSL/TLS security to identify weakness in their SSL/TLS secure implementation.

II. RELATED WORK AND SYSTEM DESIGN

There has been lot of security issues already identified and patches have been released for it. Still companies fail to implement all the patches. All patches are not applied even though patches are available. Because of lack of knowledge required to understand SSL/TLS security and its implementation.

The http clear-text protocol is normally secured via an SSL or TLS tunnel, resulting in https traffic. In addition to providing encryption of data in transit, https allows the identification of servers by means of certificates validity. Historically, there have been limitations set in place by the U.S. government to allow cryptosystems to be exported only for key sizes of at most 40 bits of key length which could be broken and would allow the decryption of communications. Since then, cryptographic export regulations have been relaxed..

Vulnerability scanners include checks regarding certificate validity, including name mismatch and time expiration. They usually report other information as well, such as the CA(Certificate Authority) which issued the certificate. Remember that there is no unified notion of a “trusted CA”; what is (trusted depends on the configuration of the software and on the human assumptions made beforehand. Browsers come with a preloaded list of trusted CAs. If your web application relies on a CA which is not in this list you should take into account the process of configuring user browsers to recognize the CA.

SYSTEM DESIGN

There has been lot of security issues already identified and patches have been released for it. Still companies fail to implement all the patches. All patches are not applied even though patches are available. Because of lack of knowledge required to understand SSL/TLS security and its implementation.

III. PROPOSED FRAMEWORK

The design includes the developing of a scanner for SSL/TLS. The developed scanner identifies the issues in any SSL/TLS security implementation. Provide report with SSL/TLS implementation issues after testing a particular server against vulnerabilities. The SSL/TLS security testing is done to identify weaknesses in the SSL/TLS secure implementation.

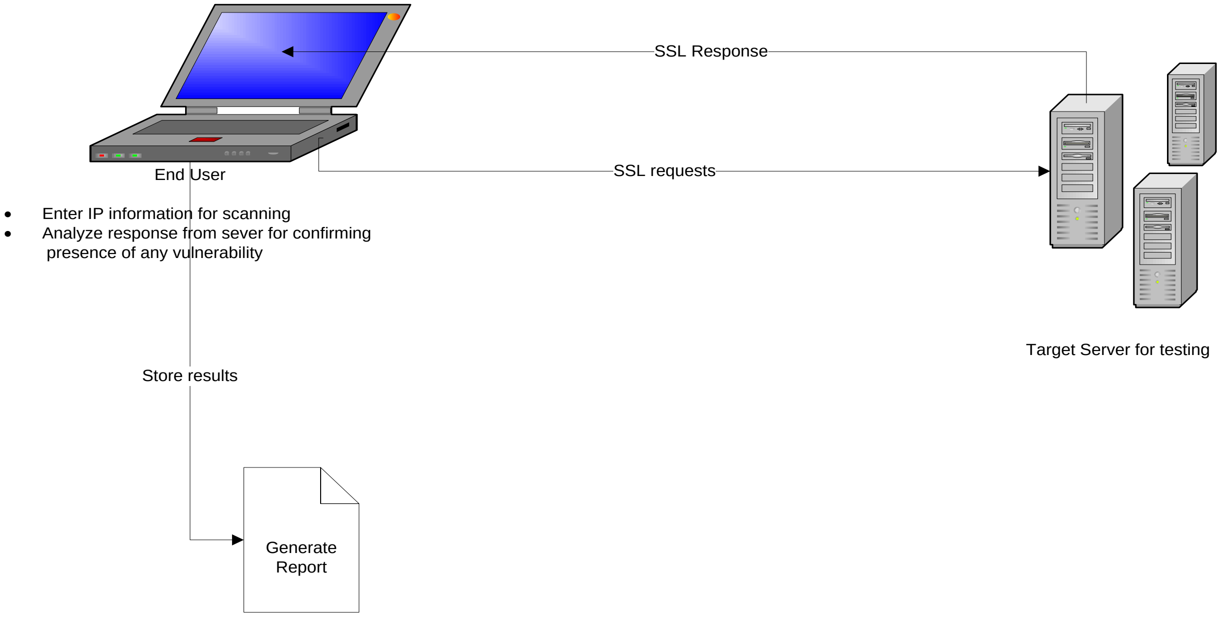

SSL Response
SSL requests
End User
Enter IP information for scanning
Analyze response from sever for confirming presence of any vulnerability
Target Server for testing
Store results
Generate Report

Figure 1: Design and data flow of SSL scanner

The developed scanner works by taking the IP address entered by the user of any system to be tested. Developed scanner will send request to target server. Analyze the response from server for confirming the presence of vulnerability. Finally the result will be stored in a report. Generated report will be very helpful for reference to find out which ever issues are associated in their SSL/TLS implementation.

This tool will be a GUI based. It will take in IP address of a system and generate a report stating which of the below security issues exists.

SSLV2 is supported: It is an older implementation of SSL protocols. Then the attacker can capture and alter information when transmitting information from client to server. SSLv2 has many security flaws, but I am going to focus on the ability to downgrade the encryption used to establish SSL connections. SSLv2 is already broken for any number of key lengths. So if any server/system supports SSLv2, then it will leads to vulnerability.

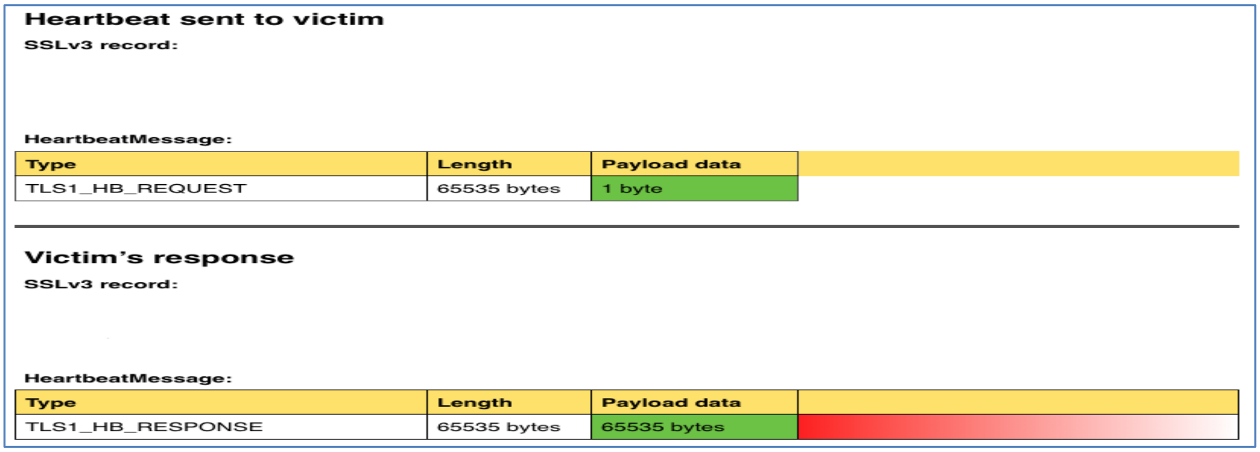
Weak ciphers are enabled: Due to this attack, attackers can easily access the information while transmission. If a user's browser negotiates such a weak protocol, the whole communication can potentially be compromised by a cryptanalytic attack. Keys less than 128-bits are not approved by the cryptographic standards.

Weak Ciphers supported include:

- SSL_RSA_EXPORT_WITH_RC4_40_MD5
- SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_RSA_WITH_RC4_128_MD5
- SSL_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA

OPENSSL/TLS is vulnerable to Heartbleed: This vulnerability defines the implementation of TLS heart beat extension and the way an SSL server validates the heartbeat requests to provide a response. Vulnerability could allow an attacker that has heartbeat request with an improper length to receive responses that have private data stored in heap memory.



Heartbeat sent to victim

SSLv3 record:

HeartbeatMessage:

Type	Length	Payload data	
TLS1_HB_REQUEST	65535 bytes	1 byte	

Victim's response

SSLv3 record:

HeartbeatMessage:

Type	Length	Payload data	
TLS1_HB_RESPONSE	65535 bytes	65535 bytes	🟥

Figure 2: Heart Bleed Attack

The SSL standard includes a heartbleed option which allows a computer at one end of an SSL connection to send a short message to verify that the other computer is still online and get a response back. A vulnerable computer can trick into a transmitting contents of servers memory called as RAM. The SSL standard includes a "heartbeat" option which provides a way for a computer at one end of the SSL connection to check twice that there is still someone at the other end of the line.

SSL/TLS Certificate Validity: Certificate validity means to check if server is presenting a valid certificate. Otherwise application might be vulnerable to man in the middle attack. At least one of the statements below is the reason for an invalid digital certificate:

- An invalid CA signed the security certificate.
- The certificate has expired.
- The name on the certificate does not match the name of the site.
- The certificate is issued to multiple domains.

PODDLE attack is possible: The bug in SSL which intercept data that is supposed to be encrypted between computers and servers. So while decrypting the integrity of padding cannot be fully verified. Block cipher padding in CBC encryption used by SSL 3.0 is not deterministic and not protected by the MAC.

POODLE can be used to browser based communication that relies on the SSLv3 protocol for encryption and authentication. An attacker who wants to exploit POODLE takes the advantage of this by inserting himself into the communication session and forcing the browser to use SSL version 3. The Transport Layer Security protocol has replaced SSL for secure communication on Internet but many browsers will revert to SSL 3.0 when a TLS connection is unavailable.

The attacker is then free to a exploit design flaw in SSL 3.0 that allows the padding data at the end of a block cipher to be changed so that the encryption cipher become less secure each time it is passed. To prevent the attack that forces a browser to degrade to SSL version 3 and the administrators should check that their server software supports the latest versions of TLS.

CONCLUSION

The developed scanner for SSL/TLS identifies well know issues in SSL/TLS security and provide report with SSL/TLS implementation issues. This will help any person without the knowledge of SSL/TLS security to identify weakness in their SSL/TLS secure implementation by referring to the report generated.

REFERENCES

[1] [(2012). [Online]. Available: http://www.rapid7.com/db/vulnerabilities/sslv2-and-up-enabled
[2] 3GPP2 partners, [Online]. http://blog.securestate.com/ssl-vulnerabilities/
[3](2012). [Online]. Available: [Online]. https://www.owasp.org/index.php/Testing_for_Weak_SSL/TLS_Ciphers,_Insufficient_Transport_Layer_Protection_(OTG-CRYPST-001)
[4] (2014). [Online]. http://security.stackexchange.com/questions/55116/how-exactly-does-the-openssl-tls-heartbeat-heartbleed-exploit-work
[5] Data http://searchsecurity.techtarget.com/definition/Secure-Sockets-Layer-SSL
[6] http://info.ssl.com/article.aspx?id=10241
[7] (2012). [Online]. https://www.digitalocean.com/community/tutorials/how-to-protect-your-server-against-the-poodle-sslv3-vulnerability.
[8] http://www.shellhacks.com/en/HowTo-Check-SSL-Certificate-Expiration-Date-from-the-Linux-Shell
[9] http://blogs.iis.net/sakyad/enforcing-ssl-3-0-and-removing-weak-encryption-vulnerability-over-ssl-iis-6-0-and-isa
[10] http://superuser.com/questions/109213/how-do-i-list-the-ssl-tls-cipher-suites-a-particular-website-offers
[11][online] http://en.wikipedia.org/wiki/Stop_words
[12] (2013). [Online].http://www.start.umd.edu/gtd/dowloads/codebook.pdf