SSL/TLS - Attacks and It's Fixes

KiranRaj KG[1], Shahikant Khot[2], Sneha Ambhore[3]
Ajeenkya DY Patil University – Pune

Abstract **-** The boom of the internet, web technologies brings the whole world under a single roof. Transferring information through e-ways leads security to be an important aspect to deal with the IP network. A security flaws which makes these protocols vulnerable to be eavesdropped and modified information later. This paper discusses attacks which happen against Secure Socket Layer/ Transport Layer Security.

Keywords **-** Phishing, Secure Socket Layer, Transport Layer Security, Spoofing

I. INTRODUCTION

Securing communication streams demands encryption. Most e-Commerce web applications which is used now has the Secure Sockets Layer and it's also known as Transport Layer Security protocol, and it is used to encrypt and establish a secure communication between client and the server. The Secure Socket Layer protocol allows authentication between a client and server and to establish an encrypted connection.

SSL/TLS allows users to authenticate with public key certificates. But in working environment, user authentication occurs on application layer which includes personal identification number, passwords as well as strong authentication mechanisms, such as one-time password, Kerberos and Two-factor Authentications. But Secure Socket Layer protocol is assumed to be secure. In working environment, however, the majority of SSL/TLS based web applications uses user authentication at the application layer will be victim for attacks.

SSL works upper side of TCP/IP layer and lower side of HTTP, LDAP and other network protocols. For the SSL v3.0 in plain text form, SSL, the RSA public-key cryptographic operations usually used to exchange the session key at the start of the connection and is computationally intensive. It takes more CPU time to establish an SSL/TLS connection than normal connections.

II. TYPES OF ATTACKS

The biggest threats to transport-level security is due to flaws of SSL/ TLS, which is been used to secure the communication between client and server. Flaws in SSL triggers both active and passive attacks such as BEAST, CRIME, TIME, BREACH, LUCKY 13, SSL Renegotiation, POODLE, etc.

A. Beast Attack - It is a short variety of Browser Exploit of SSL attack happens by exploiting TLS 1.0 it was made by T. Duong and J. Rizzo. It takes the benefits of symmetric encryption and cipher block chaining, technique to guess the secret key that is employed to encrypt the plaintext. In TLS 1.0, the last ciphertext block is the initialization vector for current plaintext. XOR operation between the initialization vector and plaintext is encrypted by the symmetric key to produce the corresponding ciphertext. If the hacker can guess a plaintext block, there is a chance he will find the symmetric key and check ciphertext is matched or not. It is one variety of brute force attack and it will be happened against TLS 1.1 and TLS 1.2 versions.

B. Crime Attack - It's the short of Compression Ratio Info-Leak Mass Exploitation attacks that happens by hijacking the session and decrypting session cookies and it was made by J. Riazo [6]. It uses the advantages of TLS and SPDY header compressions. SPDY is an open networking protocol which is developed by Google. The key is obtained by cheating the browser and sending an encrypted compressed request to the real web site, watching for the HTTP response [7] size and increase attack with respect to HTTP responses. Hacker repeats the techniques with completely different values until the key is going to be obtained.

C. Time Attack - Timing Info-Leak created straightforward (TIME) attack by that attacker extracts secret info while not getting into network and it was made by T. Beery and A. Shulman of Imperva. To conduct this attack, hacker desires to understand the cookies location, and site to insert plaintext. Info regarding the session cookies is captured by time taken to urge the response from client/server [8]. Because of noise over the network, one method is going to be recurrent for a particular integral of time and minimal response time is taken as the final response time for that particular request. If in the second iteration for arbitrary user input is "secret element = a" and the response size is 1008 bytes. So it is taken less time compare to the primary iteration. With many requests, the shortest time for each character for each and every position within the payload is computed that is happened to be the right guess and specific value of the secret element.

D. Breach Attack - The full form of BREACH is Browser Reconnaissance and Exfiltration via Adaptive Compression of machine-readable text are that the criminal attack against the response body and it absolutely was developed by A. Prado, N. Harris, and Y. Gluck [9]. Attacker will exploit HTTP compression technique by guess character and symbol while not downgrading SSL/TLS to launch this attack and will be reflected in the response body [8]. It's taken less than thirty seconds for fairly stable pages to get the secret like CSRF token, view state etc... It is vulnerable to any version of SSL or TLS.

To launch a breach attack, both attacker and victim must be in the same network. The command and control center have web server driver called iframe streamer which is going to inject HTTP request within the victim, recall listener whose work is to call back when response comes to victim and the

traffic monitor captures and shows the length of ciphertext coming back. Basic Oracle logic is that the assortment of algorithms is employed to guess the secrets. For fighting against Huffman coding, character set pool and random padding are employed and for fighting against block cipher, window technique is employed.

E. Lucky 13 Attack - It's one among the foremost attacks that happens on SSL till now and it was developed by N. A. Fardan and K. Paterson at Royal Holloway, the University of London in February 2013. It uses a padding oracle technique is a side channel attack which is affected only on the padding of ciphertext. An attacker exploits TLS's cipher block chaining by replacing the last some bytes with chosen bytes and watch the amount of time taken by the server to respond to a request. TLS packets that have contain true padding responses takes less time to process.

If TLS generates a transaction to fail, it will produce a response message that will carries errors which helps an attacker to send malicious packets in a new session repeatedly backing each and every foregoing failure [6]. The result shows that 223 sessions required extracting information about cookies and 219 sessions required if 64-bit encoding scheme is used by TLS. Overall LUCKY 13 attack requires 213 sessions if information regarding MAC padding is already known.

F. RC4 Biases Attack - It is also known as ARC4 attack and it had been discovered by Alfardan, Bernstein, Paterson, Pottering, and Schuldt by exploiting all versions of SSL/ TLS. The RC4 128 bit encryption is used to encrypt the payload. It takes 128 keys and it will generate a string of keys randomly. The output keys are XORed with a different plaintext to produce ciphertexts, problem is random keys which is generated by RC4 are not random which makes attacker helpful to recover some part of plaintext with large number of TLS encryptions.

As keys are not quite random or there are tiny biases, the ciphertexts will be not quite random or very small biases exist. Attackers tally up these deviations from random by doing a statistical analysis of individual locations of the ciphertexts. Experimental results show that approximately 232 ciphertexts give nearly all plaintexts. Around 230 sessions required to extract plain texts from ciphertexts.

G. SSL Renegotiation Attack - It's happened by exploit of SSL 3.0 and it's all versions of TLS. Attacker will hijacks HTTPS connections to add plaintext upon conversions [9]. He doesn't decrypt the client-server communications. During secure online transaction, the client requests for SSL handshaking process. Hacker blocks that requests he will capture those transmitted packets. Then the attacker will start a new session and complete the process of handshake. Then, the attacker informs the server to credit money to his bank account during a transaction. Server asks for renegotiation. Those block packets of the victim will be sent to the server which will be the new SSL handshake over the session that previously established. Two sessions are enough to lunch attacks against the victim.

H. Poodle Attack - This is the one of men in the middle attack where attacker exploit SSL 3.0 vulnerabilities to decrypt HTTP cookies. The attacker will be sitting between client and server on TLS version 1.0 or later version handshake started between them for secure transmission to SSL version 3.0. Padding technique is used in SSL v3.0 which is random in nature

The last byte of padding indicates a number of padding bytes are used which is helpful for a hacker to trigger the attack. Attackers will copy intermediate bytes to last bytes and try to exploit them. If the modified last byte is accurate same as previous byte then after decryption correct number of padding will be trunked without affecting any MAC bytes. Now these messages will take by the server which will be helpful for the hacker to recover plaintext byte to byte but one byte at a time. 1 out of 256 times the message will be accepted, and 255 times out of 256 shows error message and these sessions will be aborted but last, it will be normal.

I. Freak Attack - FREAK is one of the best TLS flaws found in many web browsers It is mostly called server spoof attack against Internet browsers. A group of weak exported ciphers are used by TLS and is targeted by the hacker. These algorithms are implemented on several TLS client libraries such as Open SSL. The Implementation of above libraries in the Internet browsers use cipher suite incorrectly even if not cipher suite has been negotiated between server and client for data exchange.

Negotiation of these exported cipher suite between server and client allows hackers to confuse the client's browser to use weak export key by performing a Man in attack. The FREAK attack will downgrade the cipher suite that uses RSA key exchange algorithms and key size is lesser than 512 bits. So, factorization will take less than 12 hours. Like FREAK, flaws on SSL/TLS allows an hacker to downgrade the export cipher suite that uses the Diffie-Hellman key exchange algorithm.

J. Bar Mitzvah Attack - Exploit RC4 stream cipher algorithm supported by SSL/TLS helps to extract information over encrypted communication. The hacker will extract weak keys by targeting the first 100 bytes of encrypted data's out of which 36 bytes belongs to SSL finished message. As finished message carries the most predictable information, these data are XORed with encrypted finished messages to extract part of Pseudo Random Number Generator Sequences. After Discarding PRNGS which do not follow the pattern of weak keys generated PRNGS, all the keys of selected PRNGS are used to decrypt ciphertext captured by an attacker using the RC4 algorithm. The Keys with has 0.5 probabilities are successfully determined and will minimize the number of trials taken by brute force attack as a difference of 211.2. This attack unable to extract full plaintexts from ciphertexts.

Table 1: Attacks and their fixes

Attacks	Fixes
BEAST ATTACK	Use RC4, 3DES, AES 256
TIME ATTACK	Encrypt the MAC, use AES-GCM ciphers
LUCKY 13 ATTACK	Add random time delays, use authenticated encryption, use RC4
BREACH ATTACK	Disable HTTP compression
RC4 BIASES ATTACK	Disable RC4 in SSL/TLS
SSL RENEGOTIATION ATTACK	Client and Server verify the previous handshake
POODLE ATTACK	Disable SSL 3.0 in a web browser
FREAK ATTACK	Configure SSL/TLS with a higher version of the cipher
BAR MITZVAH ATTACK	Disable RC4 in SSL/TLS

III. CONCLUSION

SSL/ TLS, the two protocols which are employed to secure communications between two ends by providing two layers of security such as authentication and encryption to user data. A logical or operational error in these protocols gives away to the attacker to exploit it. This paper outlines the architecture and operational flow of these protocols and summarizes different types of attacks and their fixes. Finally, more research on this field has to be done to increase the safety of SSL/ TLS by reducing bugs or vulnerabilities.

IV. REFERENCES

[1]. Homin, K., Lee. Malkin, T, and Nahum, E. "Cryptographic Strength of SSL/TLS Servers: Current and Recent Practices"; New York Software Industry Association, USA, ACM 978-1-59593-908, 2007.

[2]. Oppliger, R. Hauser, R. and Basin, D." SL/TLS Session-Aware User Authentication" Proceedings of the 15th GI/ITG Conference on "Kom-munikation in Verteilten System" (KiVS '07), Berne (Switzerland), Springer-Verlag, Berlin, LNCS, 2007, 225–236.

[3]. Zanin, G. Pietro, D, R. and Mancini, L.,"Robust RSA distributed signatures for large-scale long-lived ad hoc networks", Journal of Computer Security, 15, 1, 2007, 171-196

[4]. Shi-Qun Li. Dong, Y Wu. Zhou,Y and Chen, K. A,"Practical SSL server performance improvement algorithm based on batch RSA decryption", Journal of Shanghai Jiaotong University (Science), 13, 1, 2008, 67- 70.

[5]. Jung, W. Hong, S. Minkeun Ha and Kim, D., "SSL-based lightweight security of IP-based wireless sensor networks", Korea Science and Engineering Foundation (KOSEF), Korea, 2009.

[6]. Fang Qi. Tang, Z. Wang, G. and Wu, A.,"User Requirements aware Security Ranking in SSL Protocol" Mater Thesis, Department of Science and Engineering, Central South University, Changsha, China, 2009

[7]. Guha,P. S and Fitzgerald,S.,"Attacks on SSL A comprehensive study of beast, crime, time, breach, lucky" 13 & RC4 BIASES, iSEC Partners.

[8]. Akhawe, D. Amann, B. Vallentin, M. and Sommer, R., "Here's My Cert, So Trust Me, Maybe? Understanding TLS Errors on the Web" WWW 2013, May 13–17, 2013, Rio de Janeiro, Brazil.ACM 978-1-4503-2035-1/13/05, 2013

[9]. Zanin, G. Pietro, D, R. and Mancini, L.,"Robust RSA distributed signatures for large-scale long-lived ad hoc networks", Journal of Computer Security, 15, 1, 2007, 171-196.