2016 2nd International Conference on Next Generation Computing Technologies (NGCT-2016)
Dehradun, India 14-16 October 2016

A comprehensive study on security attacks on SSL/TLS Protocol

Preeti Sirohi
Institute of Mangement studies
preeti.sirohi@imsgzb.com

Amit Agarwal
UPES Dehradun
coer.info@gmail.com

Sapna Tyagi
Institute of Mangement studies
sapna.tyagi@imsgzb.com

Abstract: Secure Socket Layer (SSL) protocol was introduced in 1994 and was later renamed as transport layer security (TLS) protocol for securing transport layer. SSL/TLS protocol is used for securing communication on the network by ensuring data confidentiality, data integrity and authenticity between the communicating party. Authentication of the communicating party and securing transfer of data is done through certificates, key exchange and cipher suites. Security issues were found during evolutionary development of SSL/TLS protocol. The paper gives a detailed chronological order of attacks of past 22 years on SSL/TLS protocol.

Index Term - *Security, Attacks, TLS/SSL, Cipher suites*

I INTRODUCTION

SSL/TLS protocol provides security at Transport layer providing security related to authentication and transfer of data. The SSL/TLS protocol suite is chosen for providing confidentiality, authenticity, integrity, privacy in network communication. Overall the SSL/TLS protocol suite has gone through the revisions that is from SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1 and TLS 1.2, the new versions released each time improved the flexibility and removes the weakness of the previous version[1]. SSL/TLS Protocol is divided into two protocols handshake protocol and record protocol. Both the sub protocols use key exchange, establishment of master secret, certificates and cryptographic techniques to provide authentication, data privacy and integrity. Both the client and the server are negotiated with same cryptographic parameters for communication in the network. SSL/TLS is prone to various security attacks which occur at various level of communication in the network [2]. Attacks have been witnessed on the handshake protocol, record protocol, application data protocol and PKI infrastructure etc

II SECURITY ATTACKS IN CHRONOLOGICAL ORDER

This section will briefly summarize the security attacks on SSL/TLS protocol. The timeline of all of the attacks on SSL and TLS are mentioned in the table below.

Table 1: Timeline of the attacks on SSL/TLS protocol

S.No.	Year	Attacks
1.	1994-1996	Random Number Prediction ChangeCipherSpec Message Drop
2.	1997-1998	Cipher suite Rollback Attack on Handshake Protocol Key Exchange Algorithm Confusion Version Rollback
3.	1999-2001	Bleichenbacher's Attack
4.	2002–2004	Rise of Padding Attack Dangers related to compression Chosen Plaintext attack on SSL
5.	2005-2007	MD5 Collision attack on PKI Chosen Plaintext attack on SSL Reloaded
6.	2008- 2010	Denial of Service Renegotiation Attack
7.	2011- 2013	ECC based Timings attack BEAST Attack, DLTS Attack , C.R.I.M.E Attack, Breach Attack, RC4 Biases
8.	2014–2016	Triple handshake Attack FREAK Attack--- Logjam Attack

Random Number Prediction

Goldberg and Wagner [3] in 1996 did an analysis on the generation of random number which is used in SSL protocol to provide security. The author identified discovered the problem in the algorithm which is used in Random number generation. If the attacker can substitute pseudo random bits in such a way that he can predict, security is compromised. The algorithm is dependent on values such as current time, current process id and process id of parent process therefore the scope of random number generation is very limited.

ChangeCipherSpec Message Drop

Wagner and Schneier in [4] discovered ChangeCipherSpec Message Drop attack on SSL2.0. ChangeCipherSpec message is used for communication between the parties. For securing cryptographic primitives are identified and shared between the communicating parties .The man in middle can drop this message and this message will not be shared as a result the communicating parties will never activate their pending state leading to security issue.

Cipher suite Rollback Attack on Handshake Protocol

Wagner and Schneier in [4] discussed about Cipher suite Rollback attack, the intruder alters or replace the cipher suites send in the Client Hello message. Man in the middle attacker by replace whole of cipher-suites list to the weaker ciphers or the Null ciphers and passes the manipulated message to the server. The server can either reject or accept the weak ciphers. In case of acceptance of the weaker cipher suite leads to the security issues.

Key Exchange Algorithm Confusion

Wagner and Schneier in [4] discussed temporary key exchange method. SSL 3.0 supports RSA and DH as temporary key exchange algorithms which are signed by long term key during handshake. The security issue arises when the key during the transfer of key exchange material has missing information which creates confusion to each party which is dependent on the context which key material is expected and decodes accordingly. The attacker fool the client in establishing RSA based key agreement while at the same time performing DHE with the server.

Version Rollback

Wagner and Schneier discussed an attack in [4] , The intruder downgrades the version from the highest version to the lowest version for negotiation on the security parameters in SSL/TLS.

BLEICHENBACHER's Attack

Daniel Bleichenbacher [5] described this attack on SSL RSA based cipher suite for key exchange in [5]. PKCS#1 v1.5 format is used for the attack and showed that it is possible to decrypt the premastersecret (a random value generated by the client and server for key exchange) in an acceptable amount of time. The attacker can steal te encrypted message and decrypt it later.

Rise of Padding Attack

Serge Vaudenay [6] introduced the attack which rely on the fact that the block encryption schemes operates on the fixed length of blocks but generally plain text do not accurately fit the requested length and therefore it is necessary to do padding in the plain text to make block size equal to the block cipher as requested. The attacker can add an invalid message to make the size of the block. Such an additional message leads to vulnerability in the data sent.

Dangers related to compression

Kelsey [7] observed an information leakage based on compression which reveals that information on the plain text is encrypted through cryptosystems. Kelsey analysed that by using compression a new side channel arises which could be used to gain hints on the plain text. Compression algorithms which are used for encoding patterns in the input data to shorter representations and substitutes each occurrence with new representations. Different input strings of the same length compress to string of different lengths, kesley exploit this observation to gain knowledge on the plain text.

Chosen Plaintext attack on SSL

Gregory Brad [8] discovered that in cipher block cryptography , the initialization vector is chosen randomly in the first plain text. All the subsequent initialization vector use the last block of the previously encrypted plaintext. An attacker can easily find which block of the plain text has the random value and which one is the used value.

MD5 Collision attack on PKI

Lenstra, Wang and de Weger [1] described the attack in which an attacker create two certificates which are valid and have equal hash values. These colliding hash values makes possible to impersonate servers, since a valid signature in the certificate can be exploit to create fraud certificate.

Chosen Plaintext attack on SSL Reloaded

Gregory Brad [10] discussed the plain text attack on SSL , the necessary condition for the attack is to be able to access SSL connection. An attacker uses a Java applet which is executed on the victim's machine to rise the attack.

Denial of Service

Qijun Gu, Peng Liu et.al in [11] talked about attack on TLS protocol in which the machine and network resources are made unavailable to the intended user and in some cases can even shutdown the connection. The attacker sent the spoofed messages which lead to the denial of service security attack.

Renegotiation Attack

Ray and Dispensa in [12] showed that man in middle attack on the renegotiation function of

TLS Protocol. The attacker use the renegotiation flaw to inject data into the running connection without destroying the session and when server ask for authentication , the attacker could then splice on a real connection with an authorized

client by simply forwarding a new handshake message to the legitimate client. This lead to exploitation of established sessions.

ECC based Timing Attack

Brumley and Tuveri [13] showed an ECDSA based TLS connections is vulnerable to the attack. The algorithm contains the weakness of the timing side- channel. The author combined this side-channel with the lattice attack of Howgrave-Graham and Smart [14] to recover the secret keys. ECDHE_ECDSA cipher suites rely on scalar multiplication to increase speed, to exploit the algorithm the author measured the timing difference between the Client Hello message and Server Key Exchange message and measure runtime of scalar multiplication function and get an idea of the input parameters.

BEAST Attack

Rizzo and Duong in [15] presented BEAST attack that is able to decrypt HTTPS traffic .TLS uses two common mechanisms one is an initialization vector (IV) and a cipher block chaining mode (CBC). The author uses an IV is a random string that is XoRed with the plain text message prior to encryption. even if you encrypt the message twice the cipher text will be different because the message were each encrypted with different random IV. The initialization vector is not secret. It would be difficult to track a new IV for every encryption block so for longer messages CBC mode simply use the previous ciphertext block as the IV for

the following plaintext block. The use of IVs and CBC is not perfect a chosen-plaintext attack can occur if the attacker is able to predict the IV that will be used for encryption of a message under their control and the attacker knows the IV that

was used for the relevant message they are trying to guess.

DLTS Attack

AlFardan and Paterson [16] applied Vaudenay's oracle padding attack to DTLS, which works on UDP protocol (Unreliable transmission). DTLS protocol has two limitations firstly it do not support Alert message and the second states that the messages which cause error are automatically dropped. Vaudenay's attack on DTLS does not cause session validation, lack of error message does not give a feedback that if the modified message contains the valid padding. The work of author discovered the attack which allow them to recover a plain text from a DTLS which is implemented on the OpenSSL and GnuTLS

C.R.I.M.E Attack

Pratik Guha Sarkar and Shawn Fitzgerald in [17] discussed the CRIME attack discovered by Juliano Rizzo and Thai Duong [15] on SSL/TLs protocol**.** The attacks targets HTTPS request by enabling cookie stealing and other secret information. The attack exploits web sessions of SSL/TLS protocol when they use DEFLATE and gzip data compression schemes. The attacker prefix the secret with guessed sub sequences and observes if it leads to compression, a decreased cipher text length implies redundancy which shows that prefixed subsequence caused redundancy in the plaintext. This implies that a guess has something in common with the secret leading to security flaw.

Breach Attack

Pratik Guha Sarkar and Shawn Fitzgerald in [17] showed BREACH attack defined by Yoel Gluck, Neal Harris and Angelo Prado. The attack

Occurs an application of a side channel style of attack on HTTP responses. The attacker injects a guess in HTTP requests and measures the size of the compressed and encrypted responses. The

Smaller the response size indicates more close matching secret value which is later repeated on a character by character bases. the attacker should have the ability to Monitor the encrypted traffic which is travelling between the victim and website and this can be achieved by ARP spoofing which force the victim to visit attacker-controlled website in order to leverage the advantage of compression of response body for ex-filtration of the secret

RC4 Biases
Isobe, Ohigashi, Watanabe and Morrii in [18] already found weakness in initial key stream bytes of RC4 that is used to perform plaintext recovery of encrypted cipher texts and thus break SSL/TLS encryption.

Triple Handshake Attack
Triple handshake attack is discussed in [19]. The intruder establish two connections which have same encryption keys and interested in handshake, the intruder insert the data in one connection and renegotiate so that the connections may be forwarded to another.

FREAK Attack

K Bhargavan [19] talked about Factoring RSA Export keys attack which is a cryptographic limitation of SSL/TLS, the attacker decrypt the secure communications between vulnerable client and server and force them to use the weakened encryption which the attacker can easily enter and steal the important information.

LOGJAM ATTACK
Logjam attack [20] is the novel TLS protocol flaw. This attack is done by manipulating both server and client into using weak and deprecated export crypto and sub sequentially breaking the
Diffie-Hellman key exchange. The cryptographic algorithm generate the shared secret (symmetric key) between the communicating parties. The attacker intercepts their communication between the parties and compute discrete logarithm to obtain the secret exponents a or b. The Discrete Log problem for large numbers can be done using the number field sieve algorithm. When the attacker has built the a log db for the given prime he can decrypt the communication between the client and the server.

III Conclusion and Future Work

SSL/TLS is the protocol used for secure communication on the internet. The protocol has several weakness and limitations which leads to various vulnerabilities in the form of attacks. The cryptographic algorithms are designed and are helpful in making the SSL/TLS protocol secure for communication but still various flaws are observed. Countermeasures are suggested for the attacks but still the recent attacks like logjam , Freak attack, SSL stripping remains opened challenged. Novel algorithms and frameworks need to be designed to overcome the challenges related to the security issue on SSL/TLS protocol.

IV References

1. Meyer, C., & Schwenk, J. (2013). Lessons Learned From Previous SSL/TLS Attacks- A Brief Chronology Of Attacks And Weaknesses. IACR Cryptology ePrint Archive, 2013
2. Meyer, C., Somorovsky, J., Weiss, E., Schwenk, J., Schinzel, S., & Tews, E. (2014). Revisiting SSL/TLS implementations: New bleichenbacher side channels and attacks. In 23rd USENIX Security Symposium (USENIX 14) (pp. 733-748).
3. Goldberg, Ian, and David Wagner. "Randomness and the Netscape browser."Dr Dobb's Journal-Software Tools for the Professional Programmer 21.1 (1996): 66-71.
4. Wagner, D., & Schneier, B. (1996, November). Analysis of the SSL 3.0 protocol. In The Second USENIX Workshop on Electronic Commerce Proceedings (Vol. 1, No. 1, pp. 29-40)
5. Bleichenbacher, D. (1998, August). Chosen cip-hertext attacks against protocols based on the RSA encryption standard PKCS# 1. In Annual International Cryptology Conference (pp. 1-12). Springer Berlin Heidelberg.
6. Vaudenay, S. (2002, April). Security Flaws Induced by CBC Padding—Applications to SSL, IPSEC, WTLS... In International Conference on the Theory and Applications of Cryptographic Techniques (pp. 534-545).
7. Daemen, J., & Rijmen, V. (Eds.). (2003). Fast Software Encryption: 9th International Workshop, FSE 2002, Leuven, Belgium, February 4-6, 2002. Revised Papers (Vol. 2365). Springer
8. Bard, G. V. (2004). The Vulnerability of SSL to Chosen Plaintext Attack.IACR Cryptology ePrint Archive, 2004, 111.
9. Stevans M., Lenstra A. & Weger B. (2006). Collisions for MD5 and Colliding X.509 Certificates for Different Identities Cryptology ePrint Archive, Report 2005/067, Mar. 2005.
10. Bard, G. V. (2006, April). A Challenging but Feasible Blockwise-Adaptive Chosen-Plaintext Attack on SSL. In SECRYPT (pp. 99-109).

11. Aad, I., Hubaux, J. P., & Knightly, E. W. (2004, September). Denial Of service resilience in ad hoc networks. In Proceedings of the 10th annual international conference on Mobile computing and networking (pp. 202-215). ACM.
12. M. Ray and S. Dispensa, “Renegotiating TLS,” Inc., Tech. Rep., Nov. 2009
13. Brumley, B., Tuveri, N.: Remote Timing Attacks Are Still Practical. In Atluri,V., Diaz, C., eds.: Computer Security - ESORICS 2011. Volume 6879 of Lecture Notes in Computer Science. Springer Berlin / Heidelberg (September 2011)
14. Howgrave-Graham, N.A., Smart, N.P.: Lattice Attacks on Digital Signature Schemes. Designs, Codes and Cryptography 23 (2001)
15. Rizzo, J., Duong, T.: Here Come The XOR Ninjas (May 2011).
16. AlFardan, N., Paterson, K.: Plaintext-Recovery Attacks Against Datagram TLS. In: Network and
17. Distributed System Security Symposium (NDSS 2012). (February 2012)Sarkar, P. G., & Fitzgerald, S. (2013). Attacks on ssl a comprehensive study of beast, crime, time, breach, lucky 13 & rc4 biases. Internet: https://www. isecpartners. com/media/106031/ssl_attacks_survey. pdf [June, 2014].
18. Isobe, T., Ohigashi, T., Watanabe, Y., & Morii, M. (2013, March). Full plaintext recovery attack on broadcast RC4. In International Workshop on Fast Software Encryption (pp. 179-202). Springer Berlin Heidelberg.
19. Bhargavan, K., Lavaud, A. D., Fournet, C., Pironti, A., & Strub, P. Y. (2014, May). Triple handshakes and cookie cutters: Breaking and fixing authentication over TLS. In 2014 IEEE Symposium on Security and Privacy(pp. 98-113). IEEE.
20. Beurdouche, B., Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Kohlweiss, M., Pironti, A.& Zinzindohoue, J. K. (2015, May). A messy state of the union: Taming the composite state machines of TLS. In 2015 IEEE Symposium on Security and Privacy (pp. 535-552). IEEE.

.