Study on Cipher Suit to Secure the Data on Cloud Web Server

[1]Sushmita Narayan Gaonkar, [2]Ms Uma N
[1]Student, [2]Asst.Prof,
[1]CSE,
[1]New Horizon college of Engineering, Bengaluru, India

Abstract: Cloud server usually stores public data such as product information, technical information contact information, Server also contains confidential business data, which is very crucial. Since the Web Servers are accessible for the public, there is a high chance of data getting compromised by the malicious users. So securing such type of data is very important. We make use of cipher suite to ensure that the servers are not hacked or information is not leaked by the malicious users. We can prevent some attacks by disabling lower version of TLS and SSL and enabling higher versions of TLS and SSL

Index Terms **- Cloud server, Cipher suite, TLS, SSL, Malicious, Crucial data**

I. INTRODUCTION

A set of algorithms that can be used to secure a connection which uses the Transport Layer Security or SSL is called as the cipher suite. The components of the algorithms include an encryption algorithm, key exchange and MAC algorithm.

The basic function of the key exchange algorithm is to exchange the key between two devices. The main purpose of the key is encryption and decryption at both the ends. The encryption algorithm performs the task of encryption and decryption of the data that has to be transferred. The MAC ensures that the data integrity is preserved and no alteration have been taken place over the transfer of the message. In addition to this, the cipher suite can use digital signature and digital certificates to preserve the authenticity. A number of combination and permutation could be made to attend utmost security.[12]

Cipher suite is used while exchanging messages, before exchanging the message client and server has to agree on specific cipher suite which goanna be used in process. If either client or server don't agree on specific cipher suite, then there won't be any connection. Selection of cipher suite is done during the TLS Handshake Protocol. Server and client still has the ability to modify the cipher by "change Cipher Spec" protocol either in current handshake or in new handshake.
SSL/TLS Scanner can be used to know which TLS cipher is supported by server.

TLS 1.0–1.2 handshake

The client begins the procedure by sending a ClientHello message to the server that incorporates the adaptation of TLS being utilized and a rundown of cipher suites in the request of the customer's inclination. Accordingly, the server sends a ServerHello message that incorporates the picked cipher suite and the session ID. Next the server sends an advanced testament to check its personality to the customer. The server may likewise ask for a customer's advanced confirmation if necessary. If pre-shared keys are not used by client and server, then client will send the encrypted message to server. Which will help both client and server to know which secret key they should use during the process. Once the authentication of sever is verified, then client will send the finished message that will conform to the server that it has finished with the handshake process. Once sever receives this message from the client it sends back the finished message to complete the handshake. Now both client and server agree on which cipher suite to use for further commination. [31]

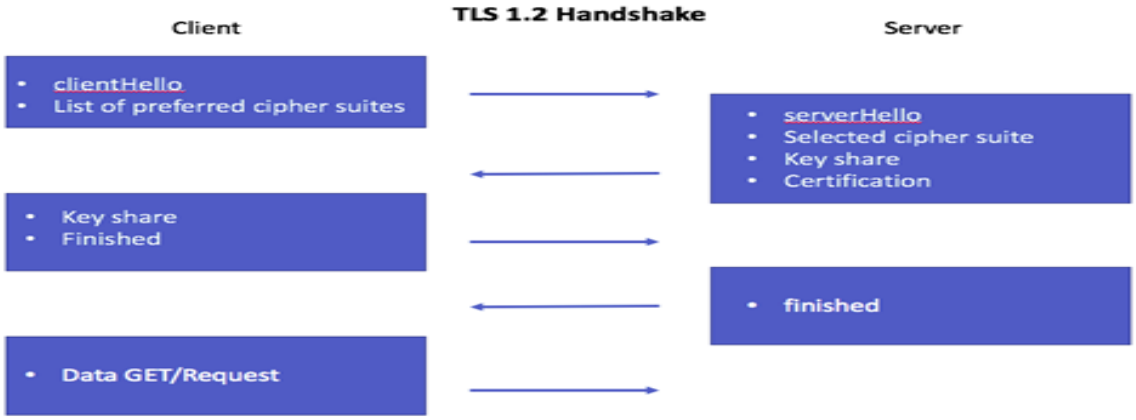

Fig.1 TLS 1.2 Handshake

TLS 1.3 handshake

Here in TLS 1.3 handshake only one round trip compared to other previous version of TLS/SSL.
At first client will send a ClientHello message to server which contains list of client preferred chippers and also if secret key has to be shared then which algorithm should be used. Once the message is received by the server, then server will send the ServerHello message along with the key, certificate, cipher suite which has been chosen and also finished message. After receiving the finished message from server by client, client and server coordinate on which cipher suite they should use.

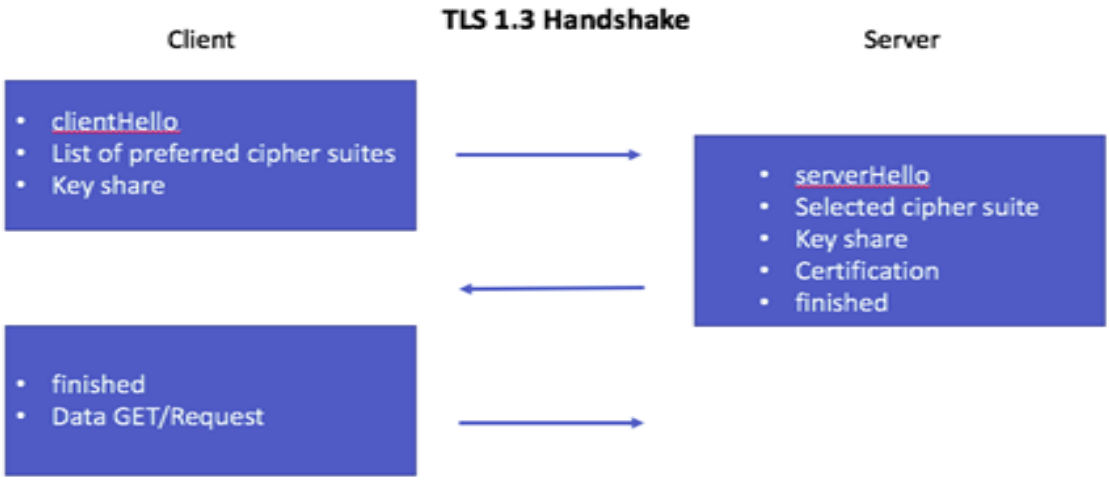

Fig. 2 TLS 1.3 Handshake

Vulnerabilities

A cipher suite is as secure as the algorithms that it contains. The cipher suite and the TLS connection are vulnerable only when encryption or authentication algorithm are of higher versions. Whenever an upgraded client request sever which are using lower version of TLS and SSL, then there are chances of occurring Downgrade attacks such as POODLE attack, BEAST.

Poodle Attack

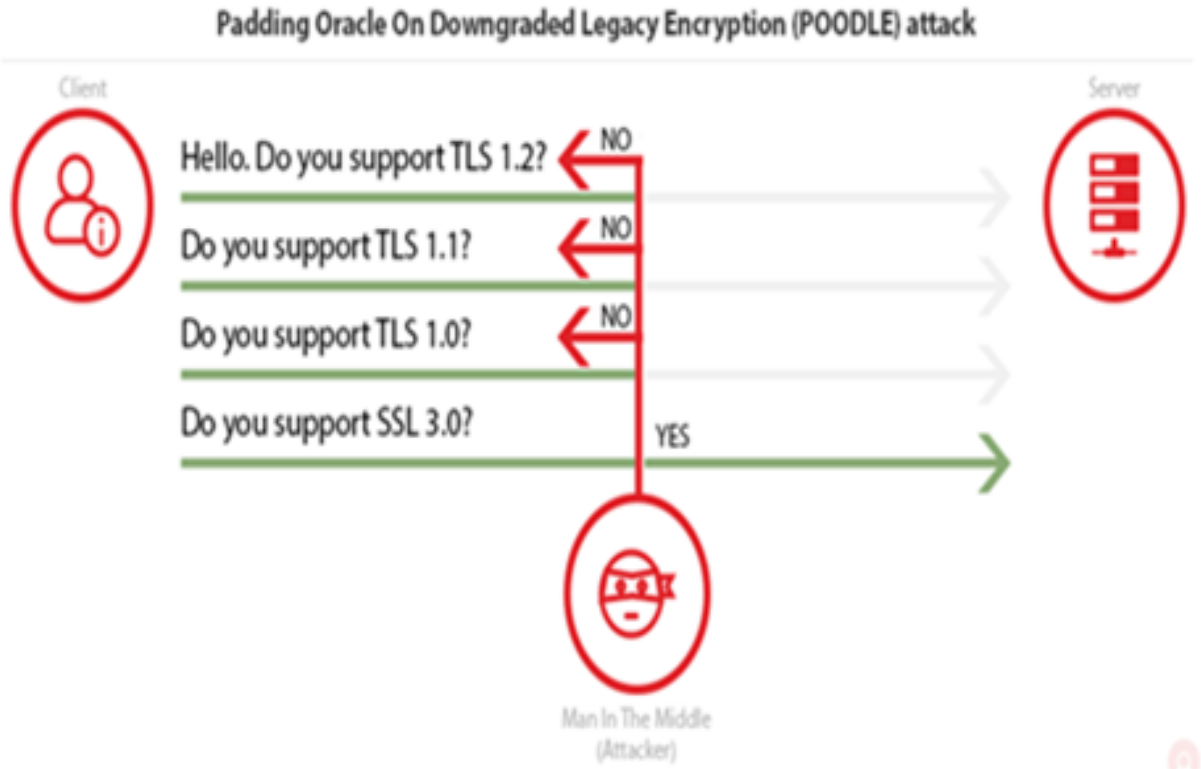

Fig. 3 TLS 1.3 POODLE Attack

When handshake is initiated by the modern client, it will offer highest protocol that it supports. If the connection is not successful, then it will automatically retry with lower protocol like TLS 1.0 / SSL 3.0 until connection is successful between client and the server. Due to this feature there can be attacks such as POODLE attack. Since lower version doesn't have the better security and vulnerabilities. We can avoid this attacks by disabling the ability of client and server to able to downgrade to lower versions.

BEAST Attack:

Hacker can decrypt the data which is exchanged between client and server by making the advantages of vulnerability in implementation of Cipher Block Chaining (CBC) mode in lower version of TLS (TLS 1.0) which permits them to execute chosen plaintext attack. Man-in-The-Middle technique is used to make this kind of attacks. We can prevent such attacks by disabling TLS 1.0 and updating to TLS 1.1 or TLS 1.2

II. EXISTING SYSTEM

As best practice, we should configure our servers to support the latest protocol versions to ensure that we are using the strongest algorithms and ciphers, and also it is equally important to disable older versions. If we continue to use the old versions of the protocols, then there might be some attacks such as downgrade, logjam, POODLE, FREAK, and BEAST attacks. To enable and disable such protocols there exits tools such as SSL LAB, SSL Server Security Test, SSL Analyzer.

SSL LAB: It's a testing tool to check the vulnerabilities

Tool features: Protocol details, cipher suites, handshake simulation.

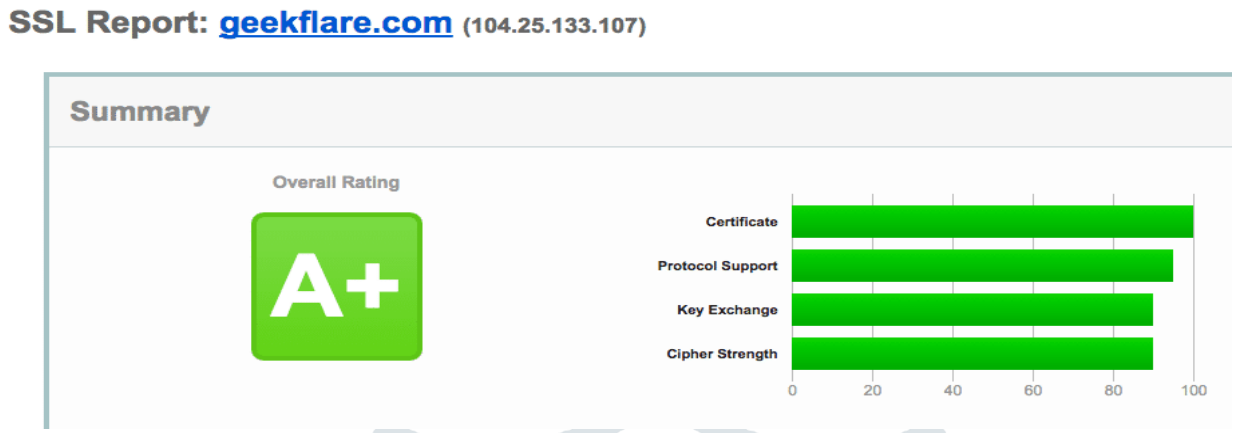

Fig. 4 SSL Lab

SSL Server Security Test**:** It scans against the URL and provides in-depth technical information.

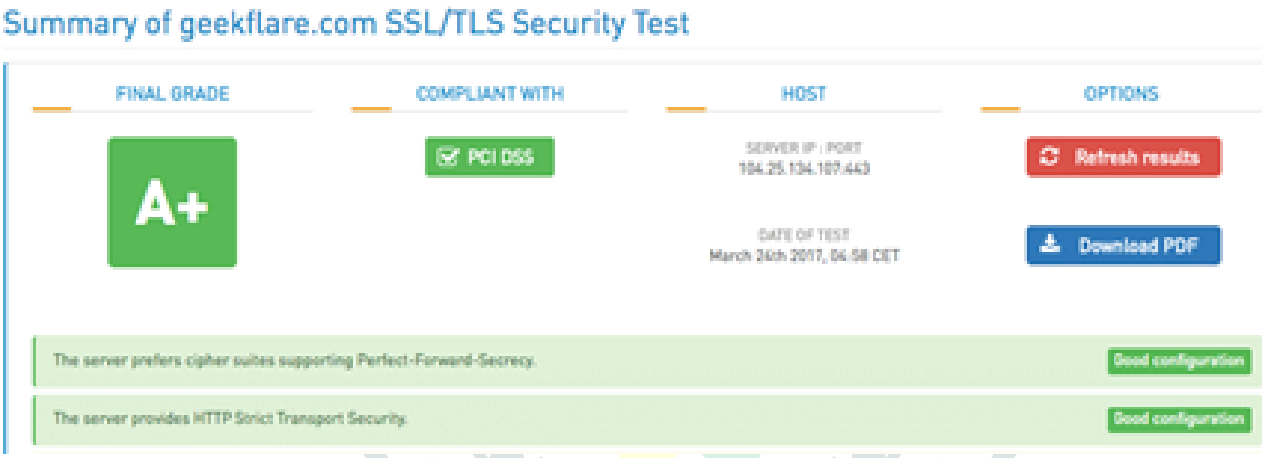

Fig. 5 SSL Lab

III. PROPOSED DESIGN

Now a days SSL /TLS has become integral part of secured communication. But many security experts or system admins doesn't have much experience on this particular field. Most security experts only concern about the certificate side of TLS /SSL handshake and neglect or fail to check whether connection strength is strong or not. To strengthen this connection expert should check the availability of cipher suite on both client and server applications.

The purpose of this research is to provide an implementation process to set up a strongly secured TLS/SSL system by inspecting the existing cipher suites which is present in a system. This can be done with the help of tool that gives ability to user to enable or disable protocols, hashes, key exchange algorithms on Linux, windows servers, user can also change the advanced settings and also can test the websites just by the single click.

Tool features:

- Stop DROWN, logjam, POODLE, FREAK, and BEAST attacks
- Enable TLS 1.1 and 1.2
- Enable forward secrecy Reorder cipher suites
- Disable weak protocols and ciphers such as SSL 2.0, 3.0, MD5 and 3DES
- Local users count
- Checking admins access

REFERENCES

[1]Robert Lin Symantec SSL/TLS Cipher Suite Analysis and strong Cipher Enablement, Senior Technical Engineer (14.01.2014)
[2] "Chosen cipher text attack on a chaotic stream cipher" College of Automation, Guangdong University of Technology, Guangzhou institute of science,
[3] Chandan Kumar Verify your SSL, TLS & Ciphers implementation
[4] R. Matthews, On the derivation of a "Chaotic"encryption algorithm. Cryptologia, Vol.13, No.1, 29-42, 1989.
[5] J. Yen, J. Guo, Efficient hierarchical chaotic image encryption algorithm and its VLSI realisation. IEE ProceedingsVision Image and Signal Processing, Vol.147, No.2, 167175, 2000
[6] S. Li, C. Li, G. Chen, et al, A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. Signal Processing Image Communication, Vol.23, No.3, 212-223, 2008
[7] Preeti Sirohi A comprehensive study on security attacks on SSL/TLS Protocol [2] Basu, S. 1997. The Investment Performance of Common Stocks in Relation to their Price to Earnings Ratio: A Test of the Efficient Markets Hypothesis. Journal of Finance, 33(3): 663-682.
[8] 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).
[9] Wagner, D., & Schneier, B. (1996, November). Analysis of the SSL 3.0 protocol
[10] AlFardan, N., Paterson, K.: Plaintext-Recovery Attacks Against Datagram TLS. In: Network