Web Security and Enhancement Using SSL : A Review

Ajay Singh, Ramesh Loar
Department of Computer Science and Engineering, Rao Pahlad Singh Group of Institutions, Balana, Mohindergarh, Haryana, India

ABSTRACT

With the development of e-commerce, ssl protocol is more and more widely applied to various network services. It is one of key technologies to keep user's data in secure transmission via internet. This document majorly focuses on sslstrip which generates the most recent attack in the secure network connections. It strips out all the secure connections to unsecure plain connection. In this article we depict this attack and to nullify it, we have proposed a technique cum practical solution to strengthen data security by developing mozilla-firefox add-on and servlet code which will strengthen our defense against the https hijacking attacks. Internet users today depend daily on HTTPS for secure communication with sites they intend to visit. Over the years, many attacks on HTTPS and the certificate trust model it uses have been hypothesized, executed, and/or evolved. Meanwhile the number of browser-trusted (and thus, de facto, user-trusted) certificate authorities has proliferated, while the due diligence in baseline certificate issuance has declined. We survey and categorize prominent security issues with HTTPS and provide a systematic treatment of the history and on-going challenges, intending to provide context for future directions.

Keywords : HTTPS, SSL, SSLSTRIP

I. INTRODUCTION

Cyber security is very useful in every field of today’s world such as military, government and even in our daily lives. [1] Today, everything is connected to internet from simple shopping to defense secrets as a result there is huge need of cyber security. Billions of dollars of transactions happens every hour over the internet, this need to be protected. Even a small unnoticed vulnerability in a network can cause serious damage. In every field of Internet, whether it is financial, personal or business everyone wants to know whom they are communicating with, ensuring that their data can be sent securely, and whether it has reached the destination correctly. Cyber security is the continuing effort to protect electronic data and computer systems from unwanted intrusions. Transmission of data over a network implies a possible loss of confidentiality, message integrity or endpoint authentication.

In This chapter we define fist we use http protocol to make a secure connection but after some time we see it is not secure properly we have to need some new protocol it is not work on dedicated IP in which the algorithm use which is commonly use and hacker known about these algorithm so which can easily hack the all information it is use encryption method to established a connection between the client and server.

After that we use new protocol which is HTTPS which is make secure connection between the client and server it can be use SSL Certificate.

II. Literature Review

Er. Prabhjot Kaur, Er. Gurjeet Kaur, May 2017

In this paper, we focus on SSL because it can secure millions of peoples' data every second, during online transactions or when transmitting confidential information over Internet. With the data encryption up to 256-bits, SSL protocol converts data into virtually incomprehensible code that is safe from hackers and identity thieves and increases the confidence of users during transactions. It also provides confidence in the integrity and security in online business and network infrastructure. Thus, we can say that SSL is the backbone of secure Internet.

Ahmed Elnaggar, October 2015 (network engineer for the ministry of communication and information technology, Egypt)

The Secure Sockets Layer (SSL) protocol uses a combination of public-key and symmetric-key encryption. Symmetric-key encryption is much faster than public-key encryption; however, public-key encryption provides better authentication techniques. An SSL session always begins with an exchange of messages called the SSL handshake. The handshake allows the server to authenticate itself to the client by using public-key techniques, and then allows the client and the server to cooperate in the creation of symmetric keys used for rapid encryption, decryption, and tamper detection during the session that follows. Optionally, the handshake also allows the client to authenticate itself to the server.

Mohammed A. Alnatheer , Sept 2014

SSL is very computational intensive. The increase in total processing time, a result of decrypting a message that was encrypted with a public-key algorithm, is quite CPU intensive. Furthermore, SSL handshakes are performance-intensive operations because of the cryptographic operations using the public and private keys. So, Handshake processing takes up a lot of CPU time. The aforementioned are the most influential reasons for increasing the percentage of the total processing time.

Christopher Meyer, Fev 2014

SSL is the defintive foundation of secure communication over the internet at this time. The protocol suffers from some shortcomings leading to vulnerabilities, but provides – at least in the latest revision 1.2 – very good security with regards to the security goals confidentiality, integrity and optional authentication. Remaining challenges for the future are on the one hand reliable and future proof new algorithms with ideally proven security (with realistic and suitable assumptions) and on the other hand bug free and specification conform implementations. It remains questionable if both of these goals may ever be achieved by 100%. As seen in the previous chapters, security is not unbreakable and weaknesses can occur at various places, caused by various reasons. Confidentially, integrity and authentication are important security goals worth to be protected. These goals are essential for a reliable network that is used for various purposes.

III. CONCLUSION

Web clients today depend every day on HTTPS for secure correspondence with locales they plan to visit. Throughout the years, numerous assaults on HTTPS and the certificate trust show it utilizes have been guessed, executed, and additionally developed. In the mean time the quantity of program trusted (and in this way, true, client trusted) certificate experts has multiplied, while the due steadiness in gauge certificate issuance has declined. We review and arrange unmistakable security issues with HTTPS and give a methodical treatment of the history and on-going difficulties, meaning to give setting to future bearings.

IV. REFERENCES

1. Kartikey Agarwal and Dr. Sanjay Kumar Dubey," Network Security : Attacks and Defence." IJCSE 2016
2. Mr. Pradeep Kumar Panwar and Mr. Devendra Kumar," Security through SSL ." in International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 12, December 2012.
3. Confidentiality integrity and availability CIA http://whatis.techtarget.com/definition.
4. Encryption and secret key cryptography cryptography/www.wikipedia.org.
5. Network Security: History, Importance, and Future by University of Florida Department of Electrical and Computer Engineering Bhavya Daya.
6. Mohammed A. Alnatheer , "Secure Socket Layer (SSL) Impact on Web Server Performance ." in Journal of Advances in Computer Networks, Vol. 2, No. 3, Sept 2014.
7. K Kant, R. Iyer, and P. Mohapatra, "Architectural impact of secure socket layer on internet servers: A Retrospect" in Proc. International Conference on Computer Design.
8. K Kant, R. Iyer, and P. Mohapatra "Architectural impact of secure socket layer on internet servers" in Int. Conf. on Computer Design, pp. 7-14, 2000.
9. SSL Certificate Explained by Scion Solutions Ltd.
10. SSL Information Center/What is an SSL Certificatehttps://www.globalsign.com/en-in.
11. MS.Bhiogade Patni Computer Services, Secure Socket Layer InSITE - "Where Parallels Intersect" June 2002.
12. Yogesh Joshi, Debabrata Das, Subir Saha, International Institute of Information Technology Bangalore (IIIT B), Electronics City, Bangalore, India. "Mitigating Man in the Middle Attack over Secure Sockets Layer, 2009
13. What is SSL and how the SSL works http://docs.oracle.com/cd/E17904_01/core.1111/e10105/sslconfig.htm
14. A. J. Kenneth, P. C. Van Orshot and S. A. Vanstone, Handbook of applied Cryptography, CRC press, 1977.
15. IT security web site, The Secure Sockets Layer Protocol Enabling Secure Web Transactions http://www.verisign.com/ssl/ssl information center/how ssl security works/index.html
16. RSA website, 5.1 Security on the Internet, http://www.emc.com/security/rsasecurid/rsa-authentication-manager.htm
17. IT security web site, the risks of short RSA keys for secure communications using SSL, http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4259828&url=http%3A%2F%2Fieeexplor.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D425982
18. H. Otrok, Security testing and evaluation of Cryptographic Algorithms, M.S. Thesis, Lebanese American University, June 2003.