Browser Security Using Secure Socket Layer

Vandana jaswal

M.Tech student (CSE)

Bahra University, Shimla Hills

Himachal pradesh

***Abstract*: Browser security is a term which is very essential in today's world because of the threats of the internet. For safe browsing, different internet sites have launched HTTPS and SSL secure certification point so that the user does not affected from the malwares of the different internet sites. Generally we see that the browsers do not bother about the SSL certification or HTTPS verification of the site. Our basic problem is to design a browser which can identify the secure sites at run time and if they are not secure in terms of contents and SSL certification, the user should get a notification that the surfing site is not secure enough to be browsed. This kind of approach will lead to an enhancement in the internet security.**

***Index terms:* Https, cryptography, secure socket layer, transport layer security**

I. INTRODUCTION

A. DEFINITION OF SSL:

Transport Layer Security or TLS, widely known also as Secure Sockets Layer or SSL, is the most popular application of public key cryptography in the world. It is most famous for securing web browser sessions, but it has widespread application to other tasks. TLS/SSL can be used to provide strong authentication of both parties in a communication session, strong encryption of data in transit between them, and verification of the integrity of that data in transit. TLS/SSL can be used to secure a broad range of critical business functions such as web browsing, server-to-

server communications, e-mail client-to-server communications, software updating, database access, virtual private networking and others. However, when used improperly, TLS can give the illusion of security where the communications have been compromised. It is important to keep certificates up to date and check rigorously for error conditions. In many, but not all applications of TLS, the integrity of the process is enhanced by using a certificate issued by an outside trusted certificate authority.

1.TLS provides 3 basic benefits:

• It provides authentication of the communicating parties, either one-way or in both directions.

• It encrypts the communication session "on the wire".

• It ensures the integrity of the data transferred.

2.Authentication and Verification:

Public key cryptography allows two parties to authenticate each other. Each party has two keys, which are large numeric values. A message exchanged between the parties is run through a hashing algorithm. A hash function takes a block of data and creates a value from it, known as a hash or digest. Make even a small change in the data and the hash changes significantly. At the same time there is no way to recreate the data from the hash.

3.Key Security

There are some absolute rules which need to be followed in order for the public key infrastructure to work properly.

4.Private keys must be private: The signer of a message needs to keep their private key absolutely confidential. Anyone who has it can effectively impersonate the sender.

5.Public keys must be public: Well, not necessarily public, but they have to be accessible to anyone who might have a valid reason to read the message or encrypt a message to the entity named in the certificate.

6.Hash algorithms must not collide: A collision is when the hash algorithm generates the same digest from two different data blocks. At some point this is inevitable, but the ability to generate collisions intentionally compromises all functions of public key cryptography. This is why new and better hash algorithms have been developed over time and put into public use. [1]

B. SSL Encryption:

Application encryption (also called SSL or TLS) over the Internet protects the confidentiality of sensitive information while in transit. SSL also prevents people who can see your traffic (for example at a public Wi-Fi hotspot) from being able to impersonate you when logging into web based applications (webmail, social networking sites, etc.). Whenever possible, web-based applications such as browsers should be set to force the use of SSL. Financial institutions rely heavily on the use of SSL to protect financial transactions while in transit. Many popular applications such as Face book and Gmail have options to force all

Communication to use SSL by default. Most web browsers provide some indication that SSL is enabled, typically a lock symbol either next to the URL for the web page or within the status bar along the bottom of the browser. [2]

C.Identity Information

Identity information is the key to successfully committing identity theft. The object of identity theft is to commit fraud using the credit profile of the victim. Identity theft victims may find fraudulent bank withdrawals, new accounts opened in their names, and even bankruptcy filed in their names. Specialized forms of identity theft can wreak even more havoc on victims. Medical identity theft, for example, occurs when someone uses another person's identity to receive payment for medical treatment or provide medical goods. In addition to the usual credit problems that follow for identity theft, these victims may have to correct inaccurate medical records. The ripple effects of identity theft can include complications wit taxpayer records that need to be resolved with the Internal Revenue Service (IRS). [3]

D.ADC: Many ADC vendors actually use the same SSL processors. Therefore, aside from speed and the number of chips, SSL performance is dependent on how tightly coupled and intelligently the software is designed to extract maximum performance and utilization from those chips. Leading ADC vendors, like Citrix with Net Scalar, have developed advanced technologies to optimize SSL performance for 2048-bit keys. These include:

Intelligent load balancing of SSL chips – SSL sessions are load balanced across SSL chips to provide the best processing performance and lowest latency.

Multiple queues per SSL chip – Multiple SSL operations can be queued per chip to optimize utilization of a chip's processing capabilities.

SSL resource isolation – In a multi-tenant ADC deployment, each tenant is assigned dedicated SSL resources, preventing one ADC instance from consuming a disproportionate processing capacity and, thus, degrading the performance of other tenants. [4]

II. LITERATURE SURVEY AND RELATED WORK

[5]."Homin K. Lee,Tal Malkin and Erich Nahum""Cryptographic Strength of SSL/TLS Servers: Current and Recent Practices""October 24-26, 2007" says that the probing SSL security tool (PSST), and used it to analyze server security on the Internet, evaluating over 19,000 servers. Given the volume of sensitive Internet-based transactions which utilize SSL/TLS servers, understanding what security measures are in place today to protect confidential data, and to what degree, is extremely important. This is particularly true given the rapid pace at which our understanding of cryptography evolves, and vulnerabilities are discovered in protocols previously believed to be secure.

[6]."Protecting Your Website with Always On SSL""Updated May 1, 2012" says that In the past, many experts have advised website developers and operators to use SSL/TLS to protect user authentication, financial transactions, and other key activities, but many organizations were hesitant to encrypt their entire sites because of concerns about cost, performance and other issues. However, the Internet has reached a tipping point where it is clear that selective use of HTTPS is no longer adequate to protect today's mobile, always-online users. SSL/TLS itself is still fundamentally sound, but Fire sheep was a clarion call for website operators to protect the entire user experience, not just the login page or the shopping cart. Simply put, SSL is like a safety belt in an automobile: It should always be on in transit. Always On SSL is not a "silver bullet" for stopping hijackers, and must be implemented as part of an overall security strategy for protecting users when they interact with your website. Nevertheless, it is a proven approach to stopping side jacking and other man-in-the-middle attacks, and one that is no longer

computationally expensive for the vast majority of organizations. As Face book, Google, PayPal, Twitter and others have demonstrated, it is possible for even the largest and most complex websites to deliver a rich user experience over HTTPS. Issues such as latency and mixed content can present challenges, but the guidelines and best practices outlined in this white paper will help you manage these issues and optimize performance for your users.

[7]."Ivan Ristic" "SSL/TLS Deployment Best Practices""14 Feb 2012" says that this item is a reminder that SSL does not equal security. SSL is designed to address only one aspect of security confidentiality and integrity of the communication between you and your users—but there are many other threats that you need to deal with. In most cases, that means ensuring that your website does not have other weaknesses.

III. PROPOSED SYSTEM

Browser Security is one of the most challenging ongoing research area in computer networks. For safe browsing, different internet sites have launched HTTPS and SSL secure certification point so that the user does not affected from the malwares of the different internet sites. Our main goal is to create a browsing system which would consists a log files for the SSL certification and HTTPS content problem. When the user would surf through the browser, it would check the contrast from the log file and will confirm whether it is secured in terms of HTTPS and further on the same procedure would be followed for SSL certification error. A warning message will be issued if we get a negative feedback from the browser log file and the user will be warned for the same. By this manner we can increase the security for the browsing system and from the unauthorised access of the content which are phishing .

IV. OBJECTIVES

Our objectives will include the following:

- To identify the security risks of the browser.

- To create a dynamic database for SSL certification
- To work with URL REROUTING for safe and secure browsing.
- To check the dynamic database security against hacking threats.

V. RESEARCH METHODOLOGY

Methodology of constructing the proposed system will consists of various steps. Each step uses different techniques to perform its specific tasks. The research methodology includes the following steps given below:

- Start browsing
- Fetch url
- Database log file(Checking the log files according to the time frame set by admin)
- Check certifications from the council for HTTP AND SSL WEBSITES
- IF (SECURITY ==TRUE) then it proceed to browsing
- If not secure, issue a warning message to the use about the certification; update the log file for not secure websites in the database log files.

VI. REFERENCES

[1]."By Larry Seltzer""Best Practices and Applications of TLS/SSL""Vol 5 IJCSS".

[2]."The Information Assurance Mission at NSA""Best Practices for Keeping Your Home Network Secure""April 2011 Page 1".

[3]."Dan Sullivan""Business Security Measures Using SSL""Vol.5 IJCSS".

[4]."Best practices for implementing 2048-bit SSL""Vol.5 IJCSS".

[5]."Homin K. Lee, Tal Malkin and Erich Nahum""Cryptographic Strength of SSL/TLS Servers: Current and Recent Practices""October 24-26, 2007".

[6]."Protecting Your Website With Always On SSL""Updated May 1, 2012".

[7]."Ivan Ristic" "SSL/TLS Deployment Best Practices""14 Feb 2012".