Vulnerabilities in SSL/TLS: Analysis And Enhancement in IBE System

Kanwar Azlan
Department of Computer Networks and security
FAST NU
Karachi, Pakistan
k237709@nu.edu.pk

***Abstract*— SSL/TLS are the two different methods or Certifications that must be acquire for any particular organization or enterprise which represents their authority of using HTTPS protocol to meet the industry standards. HTTPS (Hyper Text Transfer protocol Security) is a network protocol used for the securely transferring of data between the web browser and the website. Apart from the HTTPS, HTTP is the same but lower level version of HTTPS that transfer the data between the browser and the website but not have that much security of the data in between. But there are maybe some loop holes in HTTPS as well. The technologies of symmetric cryptography and public encryption have been combined to create (Secure Sockets Layer) and TLS (Transport Layer Security), which seek to offer confidentiality and integrity of data in transit across untrusted networks. However, a number of major flaws in SSL/TLS protocols have been found over the past couple of years. This article refers to analyzing the loop holes and vulnerabilities that HTTPS have and how we can conduct a survey and response exercise to mitigate the issues occur. Sensitive data communication over the Internet has increased dramatically in recent years due to the quick adoption of apps like online banking, stock trading, and corporate remote access. The majority of Internet security protocols, such as SSL and IPSec, use rapid symmetric key algorithms to guarantee the secrecy, integrity, and source authentication of large amounts of data after generating symmetric keys using a public key cryptosystem.**

Keywords—SSL, TLS, Vulnerabilities, loop holes, mitigate, IBE, MD5, Hashing.

I. Introduction

The most well-known and extensively used method for protecting web browser sessions is SSL/TLS. In order to establish a VPN, TLS can also be used to tunnel the full network stack to offer session initiation authentication and encryption (SIP), as well as any client-server transaction (abeer, 2015) [1]. The SSL protocol has two layers: the SSL Record Protocol is at the lower layer, and the SSL Handshake Protocol, SSL Alert Protocol, and SSL Change Cypher Spec Protocol are in the upper layer. Data compression, encryption, authentication, and fragmentation are all features of the SSL Record Protocol. The SSL Handshake Protocol enables the negotiation of encryption and Message Authentication Code (MAC) methods as well as cryptographic keys between the two parties (server and client). Alert messages are sent using the SSL Record Protocol and the SSL Alert Protocol. To switch between cypher specifications, utilize the Change Cypher Spec Protocol. Researchers have found a few flaws in the design and execution of SSL during the previous few years (abeer, 2015) [1]. However, the SSL/TLS protocol is not foolproof Because the security state of the terminal is not included, this secure connection is not complete. If malicious software gains access to the communication end, it will result in an embarrassing situation: despite successful terminal authentication, connection formation, and secure transmission, the malicious program will still steal user data (YU, 2010) [2] In computer networking there are some protocols to be followed in order to share the data between the two parties. Likewise networking protocol like HTTP and HTTPS are two main protocols that transfer the data between the web browser and the website. Identity based encryption (IBE), as opposed to the RSA used in PKI, can offer the same security with less processing overhead and do away with the requirement for certificates. Even said, there are still a lot of issues with IBE from its hurried launch, and there are now very few viable commercial alternatives available (SUN, 2009) [6].

In the Section 2, we proposed the problems and limitations of the HTTPS (SSL/TLS), then Section 3, Describes the problem description in detail, Section 4 is the total literature review of the HTTPS, SSL/TLS, IBE system and it's enhancement. Section 5 proposed the solution to the enhanced version of the ID's of users and servers from MD5 hash.

II. Research Gap

They transfer data between the browser and the website by the help of Encryption. SSL/TLS still have some vulnerabilities that we could be possibly see and make the best use of them to mitigate the risks and challenges faced by them. Attackers can steal or breach the sensitive data if any enhanced attempt will not be made. The most well-known and extensively used method for protecting web browser sessions is SSL/TLS. In order to establish a VPN, TLS can also be used to tunnel the full network stack to offer session initiation authentication and encryption (SIP), as well as any client-server transaction (abeer, 2015) [1]. TLS (Transport Layer Security) was first used in Navigator web browser for HTTPs protocols and was standardized by Internet Engineering Task Force (IETF) based on the earlier SSL specifications. SSL and TLS are cryptographic protocols designed to provide communication security over a computer network. SSL (Secure Sockets Layer) is the most well-known and widely used application of practical cryptography in the world. Data from the application protocol and handshake protocol are combined in the record protocol. To ensure messages are carried precisely and safely, Record Protocol will complete a number of functions, such as packet fragmentation and reassembly, compression and decompression, authentication, and encryption. Numerous flaws in the SSL/TLS protocol have been found during the last few years:

- Padding oracle attacks
- BEAST
- CRIME
- BREACH
- Lucky 13
- RC4 BIASES

These cryptographic operations requires strong mitigation against the threats as these are the vital and important aspects to encounter (Jing, 2015) [3].

III. PROBLEM DESCRIPTION

In computer networking there are some protocols to be followed in order to share the data between the two parties. Likewise networking protocol like HTTP and HTTPS are two main protocols that transfer the data between the web browser and Server. TLS and SSL in the Internet Protocol stack work on behalf of the underlying transport layer, whose payload carries encrypted data, by encrypting data from the application layer. Record protocol and handshake protocol are both components of the SSL/TLS protocol (handshake protocol is the top layer of record protocol). Data from the application protocol and handshake protocol are combined in the record protocol. To ensure messages are carried precisely and safely, Record Protocol will complete a number of functions, such as packet fragmentation and reassembly, compression and decompression, authentication, and encryption (Jing, 2015) [3]. Security doesn't become a top concern for anyone unless there has been a breach. By definition, a proactive and defensive strategy for IT security is necessary. By definition, a proactive and defensive strategy must be used to combat web security threats. We hope to inspire a security attitude in order to achieve that. There are many known vulnerabilities that can cause harm or destroy our IT systems and can effect in devastating results. HTTP and HTTPS can lead us to many unknown and unfortunate circumstances (Kalman, n.d.) [4]. HTTPS is gradually becoming the most popular application protocol on the Internet as a result of people' growing need for security and privacy when they browse the Web. The Internet. This shift to HTTPS to provide a secure Web presents significant difficulties with regard to the administration of HTTPS traffic to ensure fundamental network characteristics (Shbair, 2020) [5].
Here are some of them listed below:

- Authentication and Authorization

IT specialists and programmers frequently express misunderstanding about the difference between authorization and authentication. Both terms are referred to using the acronym auth, which adds to the confusion around them. Let's define and explain the difference:

Authentication: is the process of confirming that a user is (or at least seems to be) who they claim to be.
Authorization: Giving a user permission to access a particular resource or carry out a specific action.

- Injection Flaws

A classic inability to filter untrusted input leads to injection problems. When we send unfiltered data to the LDAP server (LDAP injection), the browser (through Cross Site Scripting), the SQL server (SQL injection), or any other location, injection problems may occur. The issue here is that the attacker can include commands to take over clients' browsers and lose data as a result.

- Broken Authentication

Broken authentication can cause a variety of issues, not all of which have the same basic cause. It is not advised to roll your own authentication code because it can be challenging to get it right. Many potential problems exist.

- Cross Site Scripting

Your web application receives JavaScript tags from an attacker. The user's browser would run this input when it was returned to them unclean. This is a pretty common instance of input sanitization failure, which is essentially an injection fault.

- Insecure direct object reference

This is a classic example of trusting user input at the expense of acquiring a security vulnerability as a result. A direct object reference exposes an internal object to the user, making us vulnerable to attack (for example, a file or a database key). If authorization is either not enforced or violated, the attacker gains access by providing this reference.

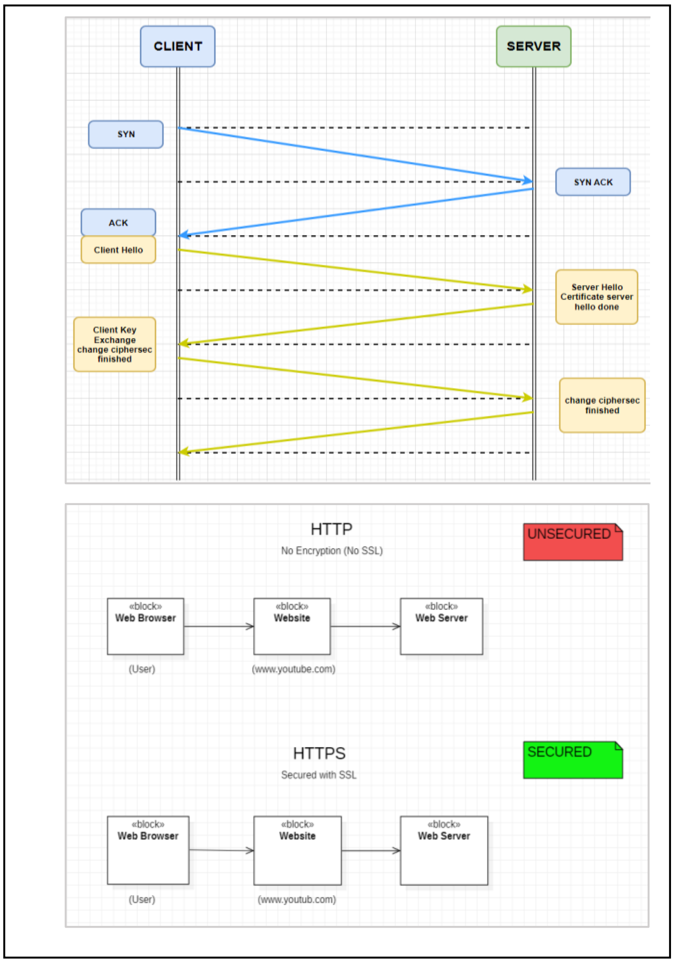
- Security misconfiguration

✓ running a production application with debug enabled
✓ enabling directory listing on the server, which discloses important information
✓ running older software (such as ancient PhpMyAdmin and WordPress plugins)
✓ Performing pointless services
✓ Using default passwords and keys (which happens more often than you'd think)

- Sensitive data exposure

Cryptography and resource protection are the focus of this web security flaw. Sensitive data should always be encrypted, both in transit and at rest. All rules apply. User passwords and credit card information should never be transmitted over the internet or kept in plain text, and passwords should always be hashed. It goes without saying that the cryptographic/hashing algorithm can't be weak.

- Missing function level access control



If appropriate authorization is not carried out when a server function is invoked, this failure occurs. Since the UI is generated by the server, it is a common misconception among developers that the client cannot access server-supplied functionality. It is not quite that easy because a request to the "hidden" functionality can always be forged by an attacker.

- Cross-site request forgery

In the event of CSRF, a third-party site issues a request to a target site (such as your bank) using your browser, cookies, and session. If your bank is susceptible to this kind of attack and you are signed into it on one browser tab, it is possible to manipulate another tab to cause your browser to utilize the attacker's credentials against you, leading to the confused deputy issue.

- Using components with known vulnerabilities

The name speaks for itself. This is more of a maintenance/deployment issue in my opinion. Research and perhaps audit should be done before adding new code. While it would be convenient to use code from a random user on GitHub, doing so carries a significant risk of online security vulnerability. When a web application accepts untrusted URL inputs, the URL redirection vulnerability can lead it to send an innocent user's request to a hostile site. Attackers can create a malicious URL within untrusted input that directs victims to the attacker's fake website, where they enter their login information into a login form.

IV. LITERATURE REVIEW

There are numerous security holes in the SSL/TLS protocol. This section analyses some theoretical and real-world SSL/TLS assaults as well as their defense mechanisms. The SSL Handshake and SSL Record protocols have been the targets of attacks on the presented attacks.

Attacks on handshake protocol are as follows:

- Cipher suite rollback
- Change cipher spec message drop
- Version rollback
- Bleichenbacher Attack on PKCS#l
- Remote timing attack on open SSL
- Key exchange algorithm confusion
- Denial of service
- Renegotiation flaw

Attacks on Record protocol are as follows:

- MAC does not cover padding length
- Attacks on CBC mode
- Attacks on compression algorithm
- Heartbleed attack
- Attack on RC4 algorithm

There are a number of publications for protocol designers and implementers that offer advice on the right selection and setup of the TLS protocol, such as NIST documents and SSL Labs publications, to help mitigate these attacks. According to protocol version support, cryptographic keys and algorithms, certificates, compression techniques, session resumption, and many other factors, these guidelines outline the specifications for TLS clients and servers (abeer, 2015) [1]. The system must first receive and keep the TPM's integrity report safe. The system should then extend the trust chain created by the TPM to the SSL/TLS Protocol each time the terminal establishes a connection to a server. As a result, in addition to the more common tasks, terminal integrity checking is carried out in the SSL/TLS handshake layer. Similar to the standard SSL/TLS protocol, client C sends Client Hello first, and server S responds with Server Hello. The updated message, which also includes Attestation Extension Data (Attest Ext) and a set of random numbers produced by the TPM's random generator, varies from the conventional one in this regard. The random number can withstand a replay attack, and the Attest Extension can specify the integrity information for the terminal, including the version number of the operating system and the process requirements (YU, 2010) [2]. Here, we use server S as an example because the following process is a symmetric one between client C and server S. Server S will then acquire a digital certificate with a Public Identity Key certificate after receiving the Supplemental Data from C. After S has confirmed the validity of the PIK certificate, it will then expand the integrity data and calculate the PCR to determine whether it matches the SML. Finally, S will utilize the C's public key to confirm that the integrity data is accurate and complete. The agreement is continued if the integrity of the C platform satisfies the requirements, and S ultimately decides whether the contents of the SML satisfy the credibility standards defined by S. On the other hand, if S cuts off communication with C, C will receive feedback regarding which configuration does not match criteria, the need for improvement, and so on. Other procedures are very similar to the standard SSL/TLS handshake (YU, 2010) [2]. Below given the comparison table of different research articles on the Survey of https:

Survey	Core Idea	Limitations	Year
Shbair[1]	HTTPS Traffic and Services Identification Approaches.	HTTPS Proxy: A solution with privacy concern.	2020
Yuji Suga[2]	SSL/TLS Renegotiation Vulnerabilities.	Disabling renegotiation feature but still server side problem exist.	2012
Tamara[3]	Decrypting network traffic for analysis.	IDS detects basic headers but not efficient in detecting payloads.	2018
Luo[4]	Analysis and comparison of algorithms in SSL/TLS Protocol.	Decryption Cost and need of hardware for the security Purpose.	2009
Tao Sun[5]	TLS protocol extension with identity based encryption (IBE).	key exchange method in IBE.	2009
Norazah[6]	Remote attestation mechanism in SSL/TLS Protocol.	Performance degradation of Web servers.	2014

- **Identity Based Encryption (IBE):**

Public key infrastructure (PKI) is the conventional architecture for public key authentication. It is most widely used in online applications. However, it still has a few unsolvable issues, like certificate administration costs. Instead of using a digital key, it offers a public key encryption approach where a public key is an arbitrary string like an IP address or email. credentials. The matching private key is produced by a reliable outside source known as Private Key Generator (PKG) which is aware of the master key. IBE can offer the same security with less computational overhead than RSA, which is used in PKI, and does away with the requirement for certificates. But in the race to market, IBE has several issues; for instance, key exchange rather than encryption is the true issue (SUN, 2009) [6].

- **SSL/TLS Handshake:**

The SSL/TLS protocol makes it possible for the client and server with SSL support to authenticate in both directions and creates an encrypted connection between them (SUN, 2009) [6].

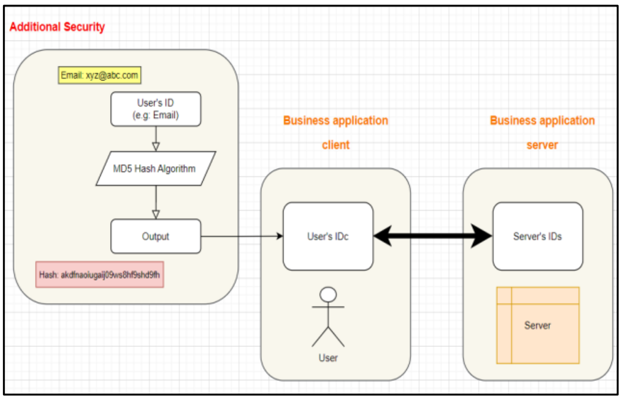
The purpose of the message exchange is to make the following actions easier to accomplish:

1) Verify the client's identity with the server.
2) Permit the cryptographic methods or cyphers that are supported by both the client and the server to be chosen.
3) Authenticate the client to the server if desired.
4) To create shared secrets, employ public key encryption techniques.
5) Create an SSL connection that is encrypted.

V. RELATED WORK

With only one PKG, it is an IBE application architecture. The private key SIDc and SIDs, which are used in place of a public key by the business client and server, can be obtained from the key management server (KMS) using the public parameters and PKG parameters. Examine how this IBE scheme eliminates the requirement for certificate management; nevertheless, since a user's identity serves as the public key, certificates are no longer required. It thereby does away with the need for PKI. We must create secure connections between the client and server, users, and PKG in order to guarantee the security of the scheme. As secure communication over the Internet is made possible by Secure Socket Layer or Transport Layer Security (SSL/TLS). Fortunately, authentication is possible with the identity based signcryption (IBS) approach. Establishing a secure SSL connection between the client and server—each of which is managed by a KMS—is beneficial. Moreover, a shared password can be amplified into a shared key through encrypted key exchange (EKE), which is useful for message authentication and encryption. Users and KMS must create a secure SSL connection in order for users to transmit encrypted communications without restriction (SUN, 2009) [6].

One of the main concerns of this IBE system is of the key exchange. The public key used in this system is the ID's of the user's and server's ID as IDc and IDs respectively. The ID is like the email of the user that is being publicly exposed. This seems to be the major concern of the privacy. So to mitigate this, In this paper we have proposed a technique called 'hashing'. This technique is used to hide or encrypt the original message into the unreadable message. So If any intruder or hacker try to gain the access of the user's ID, they will get the hashed version of that ID. In this, we are using MD5 hash.



- **Advantages:**

1) Rapid Computation: MD5 is a good choice for applications that need to hash data quickly because it is reasonably rapid and computationally efficient.
2) Simple Implementation: The method is accessible to developers due to its simplicity and ease of use.
3) Widely Supported: MD5 was a popular option for a variety of applications because it was supported by numerous platforms and computer languages.
4) Fixed Size Output: MD5 generates a hash with a fixed size of 128 bits, or 32 hexadecimal characters, which gives checksums a standard length.
5) Checksum Verification: To guarantee the integrity of files, checksum verification was frequently performed using MD5 hashes. Two files are probably identical if their MD5 hashes match.

VI. CONCLUSION

The most well-known and extensively used method for protecting web browser sessions is SSL/TLS. In order to establish a VPN, TLS can also be used to tunnel the full network stack to offer session initiation authentication and encryption (SIP), as well as any client-server transaction (abeer, 2015) [1]. The SSL protocol has two layers: the SSL Record Protocol is at the lower layer, and the SSL Handshake Protocol, SSL Alert Protocol, and SSL Change Cypher Spec Protocol are in the upper layer. Data compression, encryption, authentication, and fragmentation are all features of the SSL Record Protocol. The SSL Handshake Protocol enables the negotiation of encryption and Message Authentication Code (MAC) methods as well as cryptographic keys between the two parties (server and client). In computer networking there are some protocols to be followed in order to share the data between the two parties. Likewise networking protocol like HTTP and HTTPS are two main protocols that transfer the data between the web browser and the website. Identity based encryption (IBE), as opposed to the RSA used in PKI, can offer the same security with less processing overhead and do away with the requirement for certificates. Even said, there are still a lot of issues with IBE from its hurried launch, and there are now very few viable commercial alternatives available (SUN, 2009) [6]. Public key infrastructure (PKI) is the conventional architecture for public key authentication. It is most widely used in online applications. However, it still has a few unsolvable issues, like certificate administration costs. Instead of using a digital key, it offers a public key encryption approach where a public key is an arbitrary string like an IP address or email. credentials. The matching private key is produced by a reliable outside source known as Private Key Generator (PKG) which is aware of the master key. IBE can offer the same security with less computational overhead than RSA, which is used in PKI, and does away with the requirement for certificates. Sensitive data communication over the Internet has increased dramatically in recent years due to the quick adoption of apps like online banking, stock trading, and corporate remote access. The majority of Internet security protocols, such as SSL and IPSec, use rapid symmetric key algorithms to guarantee the secrecy, integrity, and source authentication of large amounts of data after generating symmetric keys using a public key cryptosystem.

REFERENCES

[1] Abeer E, SSL/TLS Attacks: Analysis and Evaluation, International Conference on Computing, Control, Networking, Electronics and Embedded System Engineering, 2015.

[2] YU Yue, Expand the SSL/TLS Protocol on Trusted Platform Module, International Conference on Computer Application and System Modeling, 2010.

[3] Jing Wang, A Combination of Timing Attack and Statistical Method to Reduce Computational Complexities of SSL/TLS Side-Channel Attacks, 11th International Conference on Computational Intelligence and Security, 2015.

[4] Gergely Kalman, 10 common web security vulnerabilities, 2022.

[5] Wazen M. Shbair, A Survey of HTTPS Traffic and Services Identification Approaches, 2020.

[6] TAO, Proceedings of the Eighth International Conference on Machine Learning and Cybernetics, Baoding, SUN, “TLS PROTOCOL EXTENSIONS FOR WEB APPLICATIONS OF IDENTITY-BASED ENCRYPTION”, 2009.