Secure Socket Layer: Fundamentals and Certificate Verification

By Amir Ibrahim

***Abstract*— In the ever-changing realm of cyber security, adversaries are finding ways to compromise businesses and organisations for those that require online communications. They target those that do not have SSL (Secure Socket Layer) on their websites. This report analyses the method of encryption and decryption fundamentals by exploring the different types of SSL, understanding the definition of SSL and Cryptography protocols. This study dives deeper into Certificate validation and the different methods used to enhance the security of online communications. The primary aim of this report is to revise the importance of a secure socket layer, the methods for certification validation and the fundamentals of SSL (Secure Socket Layer). This report will also address the different types of asymmetric and symmetric key algorithms while discussing the benefits of each key cryptography to protect organizations.**

Keywords—SSL, Certification Verification, Encryption, Decryption, Symmetric, Asymmetric, Cryptography, Data encryption standard (DES), Elliptic Curve Cryptography (ECC), RSA; Rivest, Shamir and Adleman, Diffie-Hellman, Benefits

I. Introduction (What is SSL?)

The requirement for secure communication has never been more vital in a world dominated by electronic transactions and data exchange. SSL, a protocol designed to offer a secure route for transmitting information over the internet, satisfies this requirement through encryption and authentication procedures. The secured hypertext transfer protocol (HTTPS) is a method of communication protocol which enables computers to send and receive encrypted data over the World Wide Web also known as WWW. HTTPS corresponds to HTTP with a Secure Socket Layer (SSL). A secure socket layer (SSL) is a method of encryption utilised on a Web server capable of supporting HTTPS.

The core goal of SSL is to maintain data integrity. With SSL replacing the old protocol TLS (Transport Layer Socket), attackers find it difficult to get in the path of a secure channel between a user and a web interface. SSL is one of the most essential and well-known protocols that achieve data confidentiality, integrity and authentication in web transactions [1]. This is commonly known as the CIA triad. This protocol operates between the OSI application and Transport layers explicitly built to provide client and server suitable connection oriented systems to establish an encrypted communication channel. While there are many ways in which attackers would like to disturb companies websites, a method in which an attacker may disrupt a web face is denial of service attacks also known as (DoS). DoS attacks, in terms of the web interface, are when an attacker commences by obtaining messages exchanged between the client and the server. Following the completion of this process, the client requests are either rejected or replied to via the server, with particular error messages causing the handshake authentication stage to be unsuccessful.
Furthermore, SSL is built upon a straightforward but unique method to keep data secure. SSL works purely on the base of cryptography. Cryptography is a method of encrypting data, such as symmetric and asymmetric encryption. If a specific recipient is to decode the ciphertext, the sender and receiver must employ the same cryptographic technique while maintaining a secret, such as a randomly generated number (called a key) in the case of symmetric key cryptography. Also, this may apply to the private key of a public/private key pair in the case of public key cryptography.

II. Background OF SSL

A. Background

SSL is divided into two levels, each utilising lower-layer services and delivering functionality to upper layers. Over a connection oriented dependable transport protocol such as TCP, the SSL record layer protects confidentiality, authenticity, and replay. The SSL handshake protocol, which is layered atop the record layer, is a key exchange protocol that initialises and synchronises the cryptographic state at the two endpoints. After completing the key exchange protocol, sensitive application data can be transmitted using the SSL record layer. Secure Socket Layer aims to establish a secure connection between two parties [2]. This means that if a customer visits an online shopping website, places an order, and enters their credit card information on the shopping website, the credit card credentials will travel across the internet while being accessible to attackers. SSL was created to prevent such secure socket layer attacks on a website and to utilise encryption to protect a customer's or consumer's identity and credentials online. SSL ensures that anyone who intercepts data between a user and a web server sees just a scrambled mess of characters by encrypting it [21]. The consumer's credit card information is now secure, viewable only to the shopping website where it was input.

B. Types of SSL

The secure Socket layer protocol was introduced by Netscape in 1994. Although most of the internet was growing, many implementations and designs for transport security for web browsers and multiple TCP protocols existed. Having said this, SSL version 1.0 was never released due to the rising security flaws [3]. The reason for this was due to weak Cipher keys that were used, which attackers were still able to intercept. With this in mind, Netscape took this idea,

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

redesigned and implemented this new SSL version 2.0, which was an official release in 1995. However, version 2.0 had many drawbacks, including security and usability issues. One of the issues was using duplicate cryptographic keys for message authentication and encryption. It has weak MAC construction that uses MD5 hash functions with a secret prefix, making it vulnerable to length expansion attacks [4]. However, due to multiple security flaws in SSL 2.0, it was deprecated by the Internet Engineering Task Force, also known as IETF. Following on from this, SSL version 3.0 was introduced in 1996. SSL v3.0 aimed to provide privacy and reliability between 2 communicating applications [25]. However, once SSL v3.0 was released to the public, many security issues regarding cipher-block chaining (CBC) ciphers were vulnerable [22]. Attacks such as the POODLE attack cause devastation towards the public. SSL v3.0, in terms of Poodle attack, uses encryption such as RC4 stream cipher or block Cipher in CBC mode. RC4 is known to be a weakness for many SSL v3.0 as this cipher has the same password sent over many connections and is also encrypted with many rc4 streams, information will be leaked out and attackers can read plain text passwords [5].

III. Fundamentals of SSL

A. Cryptography

SSL uses cryptography to safeguard confidential information to achieve a high level of confidentiality; sensitive data is encrypted across public networks. PKI primarily uses asymmetric cryptography, which is seen as more secure than symmetric encryption. Asymmetric algorithms, to put it simply, encrypt data using one key and then decrypt it using a different key. Because the third party continues to require the other key in addition to decrypting the message in the opposite direction, asymmetric algorithms are more potent than symmetric ones, even if the encryption key is learned in one direction.

B. Symmetric Cryptography

Symmetric cryptography is a cryptography system that uses a shared key to convert plaintext into cypher text. Both the sender and the receiver possess the same secret key. The symmetric cryptography schemes are as follows:

The Data Encryption Standard acronym for DES was introduced in early 1970 at IBM. Horst Feistel inspired the early design of DES. DES is a symmetric cryptographic method used for message encryption and decryption. DES uses one secret key for both the encryption and decryption stages. The critical size of the data encryption standard is 56 bits. For the encryption and decryption process to work, the sender and receiver must have the same key [6]. The approach employs the self-certification method, meaning the key is self-certified [23]. The key must be shared through encrypted communication. The attacker can quickly decipher the encrypted message if the sender key has been compromised. The symmetric technique can be unique as it provides a faster service without requiring many resources. However, there have been several types of developments while employing symmetric cryptography. Four of them are DES, blowfish, AES, and 3Des [7].

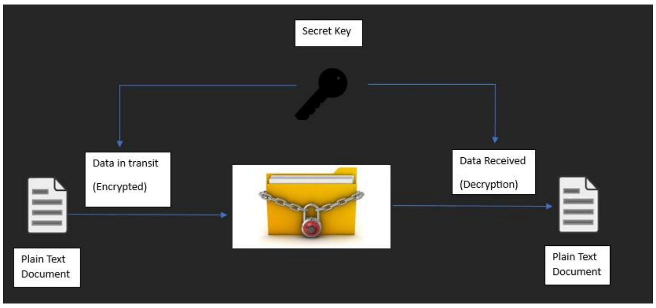

Fig 1. Symmetric Key Cryptography

C. Asymmetric Key Cryptography

The use of public keys also refers to asymmetric key cryptography. With this technique, the sender encrypts the message using the receiver's public key, and the recipient decrypts it using their private key. So, with this technique, there are two keys used; one is public, and the second key is private key [8]. This method only requires a few keys to encrypt and decrypt; however, this can be an issue regarding long messages. Additionally, there are a few algorithms which Asymmetric uses. There are three of them: RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC).

- RSA, the acronym for Rivest, Shamir and Adleman, was introduced for an essential public key cryptosystem built around modular exponential computing. Although RSA uses a public key cryptosystem, it also uses digital signatures. RSA algorithm depends on the difficulty of decomposition of large numbers [9]. The algorithm generates the public and private keys by employing two huge prime numbers. The complexity of predicting the plaintext from the signal key plus the cypher text is comparable to the decomposition of the sum of a pair of large prime numbers.

- Whitefield Diffi and Martin Hellman founded Diffie-Hellman. The algorithm allows two parties, Alice and Bob, who are connected by an authenticaton but otherwise insecure channel, to produce a secret key that is (believed to be) difficult to compute for eavesdropping Alice [10].

- ECC, short for Elliptic Curve Cryptography, produced its first documentation by Certicom and NIST in 2000 [11]. Elliptic curve cryptography is the process of transforming a mathematical issue into a computer technique. This type of encryption method is a key which utilises and executes crucial security activities such as encryption, authentication, and digital signatures. The core of elliptic curve arithmetic is an operation called scalar point multiplication, which computes Q = kP (a point P multiplied k times, resulting in another point Q on the curve) [12]. What is meant by this is that Scalar multiplication is achieved by combining point-additions (which merge two distinct points) and point-doublings (which integrate two separate instances of a point). Point addition is calculated by taking two points along an elliptic curve and adding them together (R=P+Q). It must always be a prime number, and the value returns x, considering that p - x is also determined by root.

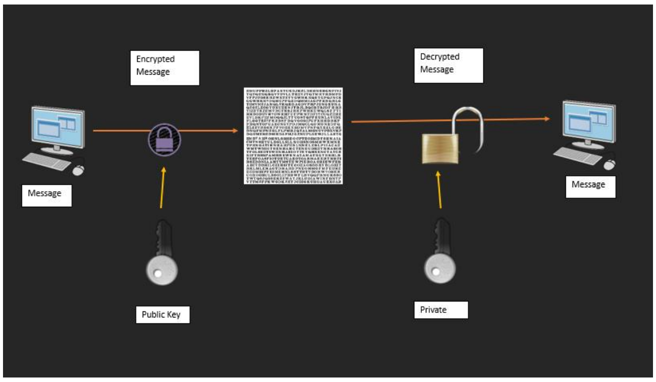

Fig 2. Asymmetric Key Cryptography

III. Certificate Validation

The validation of certificates in the Secure Socket Layer is crucial to Internet security. As a result, it is essential to ensure that certificate validation in SSL is executed correctly. During the handshake process, SSL authenticates a server or client by authenticating its certificate. Certificate verification goals is to securely connect a specific public-key to the key holder's name. A trusted CA issues a certificate in a PKI to ensure the integrity of a user's public key. Since the issuing CA digitally signs the certificate, it can be easily transferred among users without requiring a central distribution point. Each certificate has a set validity period, usually around 3 and 5 years. However, a certificate may need to be revoked before its expiration date due to security events. Some digital signatures will be exploited or need to be invalidated in any extensive system. Like passports and other kinds of physical identification, a compromised private key can be copied, so secure revocation checking is critical.

A. *Handshake*

In an SSL enabled application, the client first sends a "hello" message to the server, and the server, in turn, then returns the server's hello message along with the server's digital certificate to the client upon confirming the agreed credentials. The digital certificate for the server contains information on the server's public key, certificate validation term, and ownership and issuer information. Once the client authorises the server with the server's certificate, the client and server generate the session keys, known as symmetric keys, to encrypt and decrypt information transmitted during the SSL session and checks message integrity [26]. As a result, the SSL enabled application uses an ordinary symmetric key encryption algorithm to provide digital certificate based server authentication, public key based key exchange, and session key based data secrecy.

B. *X.509 Certificates*

An X.509 certificate authenticates a person's identity and public key. RFC 5280 primarily defines the structure in which the certification information is stored [13]. X.509 presents two types of authentications: simple authentication, using a password to verify a claimed identity, and strong authentication, using cryptographic techniques to form credentials. X.509 focuses on developing a system for securely rendering information available to a third party. X.509, on the other hand, does not seek to address the level of work required to validate the information in a certificate, nor does it establish a global meaning for that information outside of the CA's management acts. The primary function of a CA is to bind a public key to the name provided in the certificate, thereby assuring third parties that some care was taken to guarantee that this binding is valid for both the name and key. However, whether a user's DN corresponds to identity credentials related to a person or just to an e-mail address and how such linkage was validated falls outside the scope of X.509 and is determined by each CA's self-defined CPS.

IV. Benefits of SSL

A. *Symmetric Key Cryptography*

As we have discussed, the term Symmetric Key cryptography includes at least two independent issues: confidentiality protection; preventing information from being released to undesirable users and authentication; ensuring that messages received originate from the intended source and that they have not been altered in transit [14]. There are a couple of benefits of using Symmetric Key Cryptography to keep organisations safe and in business.

- As we have discussed, the term Symmetric Key cryptography includes at least two independent issues: confidentiality protection (preventing information from being released to undesirable users) and authentication (ensuring that messages received originate from the intended source and that they have not been altered in transit) [14]. This beneficial method will allow organisations to keep identity protect while ensure that authentication procedures are followed.

- Another Benefit of Symmetric Key Cryptography is that utilising Fernet Encryption in symmetric key cryptography has a more robust algorithm. It has much stronger algorithms than the RSA, which requires no communication [16]. This is due to the algorithm, which guarantees that the message is encrypted and ensures that the message cannot be manipulated or read without a specific key. Furthermore, this prevents attacks such as man-in-the-middle as the attackers intercept the message while it is delivered to the recipient. The attacker would need the decryption key in order to intercept the message.

B. *Asymmetric Key Cryptography*

As we have discussed, the definition of Asymmetric Key Cryptography is that the public key/private key pair encrypts the original message into cypher text. The associated private/public key is used at the receiver's end to decrypt the cypher text and restore plain text from it [17]. There are a couple of benefits when utilising Asymmetric Key

Algorithm, which can be used to keep organisations and businesses safe.

- A benefit of utilising the Asymmetric Key Algorithm is that RSA's encryption method uses a variable-size encryption block and variable-size key [18]. A block cipher is a randomised algorithm that works with fixed length groupings of bits, also known as blocks. Many cryptographic protocols rely on block ciphers as their fundamental building elements [24]. They are ubiquitous in data storage and exchange, where data is protected and validated through encryption. It has been utilised in hundreds of software applications for key exchange, digital signatures, and data encryption.

- Another benefit of utilising the Asymmetric Key Algorithm is using ECC, called Elliptic Curve Cryptography. ECC depends on the key's size, which depends on the curve strength [19]. The reasoning is that while ECC provides encryption and data security, it also uses fewer bits, increasing speed so that the encryption method can travel much faster than other algorithms. Furthermore, the ECC key size is 256 bits, equivalent to a 3072-bit RSA algorithm [20].

V. Conclusion

When considering most elements of secure socket layer encryption techniques, I agree with most authors on the necessity of a secure socket layer. Secure socket layers are crucial in cyber security and preserving sensitive data by maintaining data integrity. In this review, I endeavoured to cover the fundamentals of some advanced forms of secure socket layers, the method of certificate verification and the benefits of using symmetric and asymmetric key algorithms. This review serves as a starting point and offers intermediate-level knowledge to researchers interested in SSL in cyber security.

References

[1] El-Hajj, W., 2012. The most recent SSL security attacks: origins, implementation, evaluation, and suggested countermeasures. Security and Communication Networks, 5(1), pp.113-124.

[2] Al-Fantookh, A., Al-affendi, M., Al-mansour, H.M. and Al-qahtani, F.A., Secure Socket Layer (SSL).

[3] Prodromou , A. (2019). TLS Security 2: A Brief History of SSL/TLS. [online] Acunetix. Available at: https://www.acunetix.com/blog/articles/history-of-tls-ssl-part-2/.

[4] Diab, D. M., AsSadhan, B., Binsalleeh, H., Lambotharan, S., Kyriakopoulos, K. G., & Ghafir, I. (2019, August). Anomaly detection using dynamic time warping. In 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC) (pp. 193-198). IEEE.

[5] Wikipedia Contributors (2019). Transport Layer Security. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/Transport_Layer_Security.

[6] Möller, B., Duong, T. and Kotowicz, K. (2014). This POODLE Bites: Exploiting The SSL 3.0 Fallback Security Advisory. [online] Available at: https://wirelesspt.net/arquivos/docs/security/ssl_tls/ssl-poodle.pdf [Accessed 16 Dec. 2023].

[7] Maqsood, F., Ahmed, M., Ali, M.M. and Shah, M.A., 2017. Cryptography: A comparative analysis for modern techniques. International Journal of Advanced Computer Science and Applications, 8(6).

[8] Aparicio-Navarro, F.J., Kyriakopoulos, K.G., Ghafir, I., Lambotharan, S. and Chambers, J.A., 2018, October. Multi-stage attack detection using contextual information. In MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM) (pp. 1-9). IEEE.

[9] Chandra, S., Paira, S., Alam, S.S. and Sanyal, G., 2014, November. A comparative survey of symmetric and asymmetric key cryptography. In 2014 international conference on electronics, communication and computational engineering (ICECCE) (pp. 83-93). IEEE.

[10] Bisht, N. and Singh, S., 2015. A comparative study of some symmetric and asymmetric key cryptography algorithms. International Journal of Innovative Research in Science, Engineering and Technology, 4(3), pp.1028-1031.

[11] Lefoane, M., Ghafir, I., Kabir, S. and Awan, I.U., 2021, December. Machine learning for botnet detection: An optimized feature selection approach. In The 5th International Conference on Future Networks & Distributed Systems (pp. 195-200).

[12] Zhou, X. and Tang, X., 2011, August. Research and implementation of RSA algorithm for encryption and decryption. In Proceedings of 2011 6th international forum on strategic technology (Vol. 2, pp. 1118-1121). IEEE.

[13] Maurer, U.M. and Wolf, S., 2000. The diffie–hellman protocol. Designs, Codes and Cryptography, 19(2-3), pp.147-171.

[14] Zhang, Y., Yang, Q., Lambotharan, S., Kyriakopoulos, K., Ghafir, I. and AsSadhan, B., 2019, October. Anomaly-based network intrusion detection using SVM. In 2019 11th International conference on wireless communications and signal processing (WCSP) (pp. 1-6). IEEE.

[15] Bos, J.W., Halderman, J.A., Heninger, N., Moore, J., Naehrig, M. and Wustrow, E., 2014. Elliptic curve cryptography in practice. In Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers 18 (pp. 157-175). Springer Berlin Heidelberg.

[16] Eltanani, S. and Ghafir, I., 2020, November. Coverage Optimisation for Aerial Wireless Networks. In 2020 14th International Conference on

Innovations in Information Technology (IIT) (pp. 233-238). IEEE.

[17] Gupta, V., Gupta, S., Chang, S. and Stebila, D., 2002, September. Performance analysis of elliptic curve cryptography for SSL. In Proceedings of the 1st ACM workshop on Wireless security (pp. 87-94).

[18] Tian, C., Chen, C., Duan, Z. and Zhao, L., 2019. Differential testing of certificate validation in SSL/TLS implementations: an RFC-guided approach. ACM Transactions on Software Engineering and Methodology (TOSEM), 28(4), pp.1-37.

[19] De Cannière, C., 2007. Analysis and design of symmetric encryption algorithms. Doctoral Dissertaion, KULeuven.

[20] Lefoane, M., Ghafir, I., Kabir, S. and Awan, I.U., 2022. Unsupervised learning for feature selection: A proposed solution for botnet detection in 5g networks. IEEE Transactions on Industrial Informatics, 19(1), pp.921-929.

[21] Bokhari, M.U. and Shallal, Q.M., 2016. A review on symmetric key encryption techniques in cryptography. International journal of computer applications, 147(10).

[22] Naik, P.G. and Naik, G.R., 2014. Asymmetric key encryption using genetic algorithm. International Journal of Latest Trends in Engineering and Technology (IJLTET), 3(3), pp.118-128.

[23] Gaithuru, J.N., Bakhtiari, M., Salleh, M. and Muteb, A.M., 2015, December. A comprehensive literature review of asymmetric key cryptography algorithms for establishment of the existing gap. In 2015 9th Malaysian Software Engineering Conference (MySEC) (pp. 236-244). IEEE.

[24] Eltanani, S. and Ghafir, I., 2021, May. Aerial Wireless Networks: Proposed Solution for Coverage Optimisation. In IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 1-6). IEEE.

[25] SenthilKumar, U.S.M.N. and Senthilkumaran, U., 2016. Review of asymmetric key cryptography in wireless sensor networks. International Journal of Engineering and Technology, 8(2), pp.859-862.

[26] Thayer, W. (2014). Benefits of Elliptic Curve Cryptography. [online] pkic.org. Available at: https://pkic.org/2014/06/10/benefits-of-elliptic-curve-cryptography/.