Brief Report

Secure Socket Layer: Fundamentals and certificate verification

Mohammed Bilal Azhar-Ibrahim *

Posted Date: 13 June 2023

doi: 10.20944/preprints202306.0869.v1

Keywords: Secure Socket Layer (SSL); Security of Networks; Man in the Middle (MITM) Attacks; Transport Layer Security (TLS); Authentication; Confidentiality; Integrity; Encryption; Decryption; Private key; Public key; Rivest; Shamir and Adleman (RSA); Certification Authorities

Brief Report

Secure Socket Layer: Fundamentals and Certificate Verification

Bilal Azhar-Ibrahim

University of Bradford; Bradford, United Kingdom of Great Britain and Northern Ireland; mbazhari@bradford.ac.uk

Abstract: This paper intends to discuss SSLs, how they work, their advantages and drawbacks. It will end with the author's thoughts on the efficacy of the system and whether it is a viable solution for the majority of network security problems or if those drawbacks prevent that

Keywords: Secure Socket Layer (SSL); security of networks; Man in the Middle (MITM) Attacks; Transport Layer Security (TLS); Authentication; confidentiality; integrity; encryption; decryption; private key; public key; Rivest; Shamir and Adleman (RSA); Certification Authorities

I. Introduction

From 58 – 52 B.C, emperor of Rome, Julius Caesar wrote the book, Caesar's Commentary on the Gallic Wars, in which he talked of "[inducing] a certain man of the Gallic horse to convey a letter to [the camp of] Cicero" which was written in Greek characters [7]. The emperors reasoning was such that the enemy Gallic warriors would be unable to understand the Greek language, thus preventing them from understanding the meaning of such military orders in the eventuality where they did manage to procure such messages. Historian Gaius Suetonius Tranquillus wrote, "if [Caesar] had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out." If any interceptor were to have received these messages, to decrypt the encoded memoranda they "must substitute the fourth letter of the alphabet with, namely D, for A, and so with the others" [6].

Cryptography has been imperative since even before the Roman era; with personal information being digitised and more easily accessible, it is important now, more than ever, to maintain the security of networks tasked with protecting this. Authentication of sender and receiver identities is a commonly used technique to prevent any malicious attacks from outsiders. One particular method that can be implemented is through the use of a Secure Socket Layer (SSL). Widely used, it has become commonplace in interactions between internet browsers and mail clients such as Outlook [1].

In this paper, the SSL method is broken down and explained, giving the reader a much broader understanding of its functionality and why it works this way. Due to its ever-growing presence in the security of networks, it is important to advance one's own knowledge and investigate the drawbacks and advantages to such systems. Section II will discuss all sources of information used in this paper. Sections III and IV will discuss the functionality and potential attacks used on SSLs respectively. The conclusion of the paper is contained within section V, with further acknowledgements and a list of references used being listed after that.

II. Discussion of sources used

References [1], [3] and [13] were used in this paper to research the workings of an SSL. Regarding the workings of cryptography and certificates, [2], [5], [6], [10] , [11] and [14] were used to varying degrees. Regarding the potential attacks posed, references [4] and [12] provided examples and techniques to consider. References [7] and [9] were pivotal in setting up the introductory paragraphs and allowed for prior examples of cryptography to be discussed and explored briefly. For modern regulations that must be followed, reference [8] was quoted.

III. SSL

With the constant improvements in technology, information is more readily transferred over the internet; this sector expanded dramatically, resulting in an impact in other sectors including leisure, health, and wellbeing. In each of these sectors, varying degrees of sensitivity is required to handle private information from being leaked unknowingly, meaning that security must also improve alongside the technology. This is backed by regulations detailed withing acts such as the General Data Protection Regulation (2018) which enforces proper handling and subsequent transfer of such personal data. For example, Article 32 of the GDPR dictates that any organisation which controls, or processes data must they complete the "pseudonymisation and encryption of personal data" in addition to "[ensuring] the ongoing confidentiality, integrity, availability and resilience of processing systems and services" [8]. One method of providing these conditions are met is by using a Secure Socket Layer to certify and authenticate information being transferred over a network.

Before understanding how the defence system works, it is imperative to discuss and interpret what an SSL is. The SSL resides lower than the Application layer on the OSI Model [1]. With embedded security features such as securing sensitive information that will be handled by the application layer protocols, it maintains many advantages over other methods. Varying examples of cryptography can be used in order to provide confidentiality in the transfer of messages. Furthermore, providing certificates ensures the identity of senders and receivers, which in turn justifies its use in the protection of confidential information. As mentioned before, cryptography is imperative to protecting classified data from unauthorised access. Secure Socket Layer does this through the use of many interesting features detailed below.

Within the field of network security, there are three major concepts to consider when evaluating the success of a system protection for users' private information. Confidentiality refers to ensuring the contents of any and all messages are able to be viewed solely by the receiver and sender [3]. Any potential interceptors of this message would breach the confidence of both innocent parties on this network. Another key concept surrounds the authenticity of both a sender and receiver. Of course, it is essential to ensure the source and recipient of any message is indeed who they claim to be. In regards to SSLs, this is discussed in more detail at a later stage in this report. The final key idea is that if integrity. Similar to as is mentioned before, potential Man in the Middle attackers having the ability to not only intercept but edit the contents of messages is devastating for the trust that clients entrust within a system and thus that scenario must be prevented.

One simple way of ensuring some form of confidentiality during the transfer of sensitive information is through the use of Symmetric Key Encryption. In this method, both parties have access to a common symmetric key. This means that a sender can encrypt a plaintext message, m, using this key, K_S, and a recipient would in turn use the same key to decrypt it. This is displayed in the following formula: $m = K_S(K_s(m))$ [2]. An obvious example if this is the aforementioned Caesar Cipher, in which the sender and receiver agree upon a key shift that will take place, mapping one letter onto another, giving a ciphertext which contains the encoded version of a plaintext message. Due to its simplicity, however, it does open certain vulnerabilities that can be exploited by potential attackers. For example, the number of possible key mappings is finite, and thus brute force attacks can provide accurate results of what the cipher was originally intended to display [4]. With constant improvements to computational power in all sectors, the time taken for these attacks to take place shortens dramatically, leaving this Symmetric Key Encryption as an unfavoured option for modern cryptography. More recently, block ciphers, such as AES (Advanced Encryption Standard), DES (Data Encryption standard), and 3DES are used in conjunction with Symmetric Key Encryption. [12]

To combat the predictable predetermined key mapping, block ciphers use repeated functions to encrypt classified records. By layering this with multiple uses of the function and key, it increases the amount of time it would take for a brute force attack to penetrate the system, whilst also increasing the complexity of the cipher significantly. These attacks require the observation that there are 2^n possible keys where n is the length of the key. "NIST [NIST 2001] estimates that a machine that could crack 56-bit DES in one second (that is, try all 256 keys in one second) would take approximately 149 trillion years to crack a 128-bit AES key" [11].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 June 2023 doi:10.20944/preprints202306.0869.v1

Certification is vital in the inner workings of the SSL. By using a combination of public and private keys to encrypt data in what is known as Public Key Cryptography, it's possible to prevent an attacker from understanding a message even if they do manage to intercept it in transmission; by creating a virtual signature which acts similarly to a physical. If it is only replicable by one user, it becomes a unique identifier for them providing authenticity that can be trusted.

Both the public and private key work exactly as is implied by their names; the public key is openly available for all users on a network to access and use. Typically, one user would use the public key of a receiving party to encrypt a message that is going to be sent over a network. The reason for this is as follows: the private keys assigned to a user are only visible to their owner and they act as a decryption key to any message that is encrypted with the corresponding public key. Typically, the example of Alice and Bob sending messages over a network is used, and it will be shown here through some upcoming examples. If Alice is the sender of a message, and Bob is the receiver, she will use Bob's public key, K_B^+, to encrypt the message, m. As the indented recipient of the message, Bob will use his private key, K_B^-, to revert what is sent to him to the original plaintext message. This can be denoted in the formula $m = K_B^-(K_B^+(m))$.

Figure 1. A figure showing the process of sending, encrypting, receiving, and decrypting a message.

By enforcing the use of this, confidential information can be easily hidden from potential attackers, thus decreasing the likely hood of potential data breaches with harmful and serious consequences. The private and public keys can encrypt and decrypt these messages in multiple different ways, but one of the most widely algorithms in public key encryption is the RSA (named after its creators Rivest, Shamir and Adleman) algorithm [11].

This system follows the implication that any messages is built up of binary patterns, which can all me converted to integers of base 10 which can be unique for each character. For instance, 0001 would correspond to the denary number 1, which in turn could perhaps refer to letter 'a'. In reality, the system would take the 32-bit pattern that is encrypted from the corresponding integers in an 8-bit ASCII table.

This approach requires the use of the arithmetic operation, modulo, in which *a mod b* would return r, where r is the integer remainder of a divided by b. To follow this process, one must primarily decide upon two prime values which will be assigned to p and q. Whilst it is possible to choose smaller prime numbers such as 2 and 5, this leads to vulnerabilities in the system due to a lack of complication. Prime numbers on the order of 1024 bits are recommended to ensure the utmost difficulty in intercepting and decrypting messages when it is not intended. However, an increase in these values' size understandably also increases the time taken in both encrypting and decrypting messages for transmitters and recipients, thus slowing down the process of data transfer. After selecting p and q, it is imperative to calculate the values of n and z, where $n = p * q$ and $z = (p-1) * (q-1)$. An encryption key, e, is now required and it must be both smaller than n and share only 1 as a common factor with z. Correspondingly, a decryption key is needed, which must follow the rule that $e * d \bmod z = 1$. For context, these encryption keys can be linked closely to public and private keys that were discussed in prior paragraphs, where $K_B^+ = (n, e)$ and $K_B^- = (n, d)$. The encrypted ciphertext after all of this is completed can be denoted by the equation $m^e \bmod n$ and the decrypted plaintext by $c^d \bmod n$.

Reference [11] provides the example in which Alice would like to send a message to Bob, in which the bit pattern of one character is 00001100. This converts directly to the denary integer 12. If Bob were to select 5 and 7 to represent p and q respectively, then the values of n and z would understandably become 35 and 24. To maintain prime relativity in this, Bob could allow e = 5, and d = 29, to allow $e * d \bmod z = 1$ to remain as a true statement.

To tackle the case of authenticity, a digital signature can be created which would verify the identity of a user. In terms of cryptography, both $K_B^+(K_B^-(m))$ and $K_B^-(K_B^+(m))$ are identical in value. In other words, encrypting a plaintext message with a private key and then decrypting its corresponding public key would yield the same result as encrypting a plaintext message with a public key and

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 June 2023 doi:10.20944/preprints202306.0869.v1

then decrypting its corresponding private key. This can be used to prove the identity of a sender and receiver in what is known as a handshake. This occurs when, prior to transmitting data, an initial set up conversation begins. Since private keys are only visible to the user they are associated with, they can also only be decrypted with the public key provided. This is a many-to-one function meaning there is only one way of completing this successfully, proving the identity of the users in a system before any sensitive files can be intercepted by an imposter.

IV. Attacks used on SSL

Whilst many security measures can be put in place, there is always the threat of attackers using whatever methods possible to intercept a message for personal gain or to cause disruption to a system. On such method, which happens to be highly favourable, is a Man in the Middle attack. By intercepting information in transit, the attacker can act as a hidden intermediary between the intended recipient and transmitter. Without knowledge of any intruder in a network, the conversation could play out normally, with both intentionally included parties receiving valid certification and messages.

If Bob and Alice were once again communicating and an intruder, Trudy, were attempting to gain access to their private conference she would only need to relay the messages between Bob and Alice, replacing the requested private and public keys with her own, thus tricking the others with false senses of confidentiality and integrity. Of course, this can be combatted through the use of the aforementioned handshake method, due to Trudy being unable to access either Alice's or Bob's private keys. Whilst this should ensure that the correct digital signatures are used to verify the integrity of a user, Trudy can simply provide her own private key with a plaintext message encoded by it; any user who may receive this would be non-the-wiser to the fact that they have not set up a connection with their intended target and may unknowingly send over private information they would not have done so otherwise.

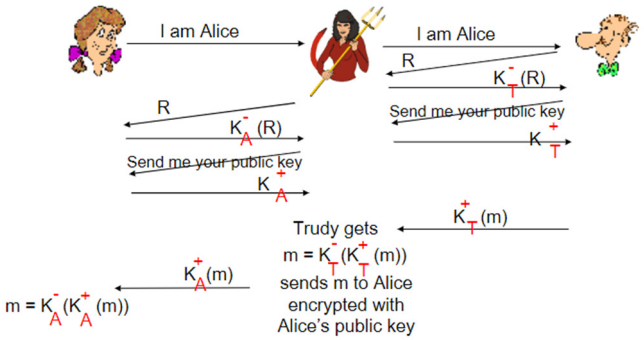

Figure 2. A figure displaying how an intruder may act as the Man in the Middle, and relay messages between other users.

To counteract this, some networks use Certification Authorities to provide improved data integrity. Usually, public keys are stored with the user they represent individually, so every user holds both of their own keys. However, CAs act as a central structure that maintain a record of all of the public keys on a network. This eliminates one user asking another for their public key, meaning the difficulty for Trudy to attack will dramatically increase. If the public key in the CA can not revert the ciphertext to the original plaintext, they must not match up as intended. This makes spotting an intruder considerably easier as Trudy would no longer be able to simply relay any information from a transmitter to a receiver.

As an attacker, performing a playback would be pertinent in retaliating against this. Playback occurs when an attacker intercepts a handshake request, and instead of interfering with the messages delivered, actively listens and records the next transmissions which would prove one another's integrity. By passively intercepting and recording the handshake of two members of a network, Trudy

would then be able to imitate either of these users accurately, by delivering the initial verification messages that would be encrypted with another user's private key.

V. Conclusion

In reflection, SSLs are incredibly important to network security due to their versatility and strength in encrypting data through tough-to-break encryption and prevention methods. Furthermore, the use of handshakes and certification strongly counters Man in the Middle and other potential attacks strongly, with many different methods of preventing unauthorized access. Since there is a lot of preliminary set up, there is an issue of time taken to verify the confidentiality, authenticity, and integrity of a system. However, following the process wholly ensures that these concepts are adhered too.

Acknowledgments: I would like to thank my lecturers, namely Amr Abdullatif and Ibrahim Ghafir who both contributed to my knowledge of SSLs and different methods of cryptography, as well as the potential attacks that take place. Additionally, I would like to thank Paul Trundle for assisting me in planning my usage of time and supporting me by listening to my personal issues.

References

1. Roza Dastres, Mohsen Soori. Secure Socket Layer (SSL) in the Network and Web Security. Unpublished. International Journal of Computer and Information Engineering, WASET, In press, 14 (10), pp.330-333. ffhal-03024764fJ. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
2. S. Duddu, A. Rishita sai, C. L. S. Sowjanya, G. R. Rao and K. Siddabattula, "Secure Socket Layer Stripping Attack Using Address Resolution Protocol Spoofing," 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), 2020, pp. 973-978, doi: 10.1109/ICICCS48265.2020.9120993.K. Elissa
3. O. Rama Devi et al 2020 IOP Conf. Ser.: Mater. Sci. Eng. 981 022015
4. M. A. Hussain, Z. Alaa Hussien, Z. A. Abduljabbar, S. Abdulridha Hussain and M. A. Al Sibahee, "Boost Secure Sockets Layer against Man-in-the-Middle Sniffing Attack via SCPK," 2018 International Conference on Advanced Science and Engineering (ICOASE), 2018, pp. 295-300, doi: 10.1109/ICOASE.2018.8548813.
5. Z. A. Alizai, H. Tahir, M. H. Murtaza, S. Tahir and K. Mcdonald-Maier, "Key-Based Cookie-Less Session Management Framework for Application Layer Security," in IEEE Access, vol. 7, pp. 128544-128554, 2019, doi: 10.1109/ACCESS.2019.2940331.
6. Chamila Wijayarathna, Nalin Asanka Gamagedara Arachchilage, Why Johnny can't develop a secure application? A usability analysis of Java Secure Socket Extension API, Computers & Security, Volume 80, 2019, Pages 54-73
7. *The Twelve Caesars*. Courier Dover Publications, 2018.
8. *GDPR 2018*
9. Dooley, J.F., 2018. *History of cryptography and cryptanalysis: Codes, Ciphers, and their algorithms*. Springer.
10. Alabduljabbar, A., Ma, R., Choi, S., Jang, R., Chen, S. and Mohaisen, D., 2022, May. Understanding the Security of Free Content Websites by Analyzing their SSL Certificates: A Comparative Study. In *Proceedings of the 1st Workshop on Cybersecurity and Social Sciences* (pp. 19-25).
11. Jim Kurose, Keith Ross, Addison-Wesley, 2013, Computer Networking: A Top Down Approach 6th edition
12. Ghafir, I., Hammoudeh, M., Prenosil, V., Han, L., Hegarty, R., Rabie, K. and Aparicio-Navarro, F.J., 2018. Detection of advanced persistent threat using machine-learning correlation analysis. *Future Generation Computer Systems*, *89*, pp.349-359
13. M.L. Das, N. Samdaria, "On the security of SSL/TLS-enabled applications" Appl. Comput. Inform. 2014, 10(1-2), pp.68-81.
14. J. Jonsson, B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1," RFC 3447, Feb. 2003.
15. Zhang, X.G., Yang, G.H. and Wasly, S., 2021. Man-in-the-middle attack against cyber-physical systems under random access protocol. *Information Sciences*, *576*, pp.708-724..