*Attacking SSL/TLS Implementations*

Shawn Philip Babu  
Information Systems Security  
Concordia UniversityMontreal, Canada  
shawn0111babu@gmail.com  
  
  
Sai Sandeep Vendra  
Information Systems Security  
Concordia UniversityMontreal, Canada  
sandeepvendra1404@gmail.com line 1: 3rd Given Name Surname  
line 2: *dept. name of organization (of Affiliation)*  
line 3: *name of organization (of Affiliation)*line 4: City, Country  
line 5: email address or ORCID  
  
line 1: 4th Given Name Surname  
line 2: *dept. name of organization (of Affiliation)*  
line 3: *name of organization (of Affiliation)*line 4: City, Country  
line 5: email address or ORCID

MANNAM VENKATESH  
INFORMATION SYSTEMS SECURITY  
CONCORDIA UNIVERSITYMONTREAL, CANADA  
venkateshmannam22@gmail,com

line 1: 6th Given Name Surname  
line 2: *dept. name of organization (of Affiliation)*  
line 3: *name of organization (of Affiliation)*line 4: City, Country  
line 5: email address or ORCID

*Abstract*—SSL stands for Secure Sockets Layer and, it's the standard technology for keeping an internet connection secure and safeguarding any sensitive data that is being sent between two systems, preventing criminals from reading and modifying any information transferred, including potential personal details. TLS (Transport Layer Security) is just an updated, more secure, version of SSL. We still refer to security certificates as SSL because it is a more commonly used term, but when you are [buying SSL](https://www.websecurity.digicert.com/ssl-certificate?inid=infoctr_buylink_sslhome) from DigiCert you are actually buying the most up to date TLS certificates with the option of [ECC, RSA or DSA encryption](https://www.websecurity.digicert.com/security-topics/how-ssl-works). However, there are undeniable differences between the libraries that implement SSL/TLS protocol and vulnerabilities in these libraries. Hence, the two main questions asked are: what’s the difference between TLS vs SSL? And is it something we need to worry about? In this report, we summarize some of the limitations by considering implementations of each along with review of past protocol-based and software-based vulnerabilities.

# Introduction

JEMY & EKASMEET

(Times new roman 10)

# Limitation of SSL/TLS Implementations

SHAWN & HARSHITHA

(Times new roman 10)

# How SSL/TLS secure data ?

When it comes to transferring data via the internet in today's digital era, security is a huge problem. TLS (Transport Layer Security) and SSL (Secure Sockets Layer) are protocols used to encrypt communication between two devices over the internet. They use encryption, authentication, and integrity checking techniques to offer a safe channel for data transfer. In this report, we will look at how TLS and SSL operate together to protect data.

Graphical user interface, application, chat or text message

Description automatically generated

**Encryption**: Encryption is a major function of TLS and SSL. The process of converting plain text into ciphertext, which is unreadable without the correct key, is known as encryption. TLS and SSL encrypt data using symmetric encryption, which means that the sender and receiver share a secret key that is used to encrypt and decode the data.

**Authentication:** TLS and SSL also enable authentication to verify that data is only delivered between the parties intended. To authenticate the persons participating in the connection, TLS and SSL require digital certificates. Digital certificates are issued by trusted certificate authority and contain information about the parties' identities.

**Integrity**: Another critical component of TLS and SSL is integrity. The integrity of the data assures that it has not been tampered with during transmission. TLS and SSL implement message digests to ensure the data's integrity. A hash function, which is a mathematical function that accepts an input and returns a fixed-length output, is used to generate message digests. Because the hash function's output is unique for each input, even little changes in the input data result in a completely new hash value. The message digest is delivered with the data, and the receiver may use the same hash algorithm to ensure that the data is not tampered with.

Diagram

Description automatically generated

**TLS Handshake**: The TLS handshake is the process by which two devices establish a secure connection. The TLS handshake involves the following steps:

1. The client initiates the TLS handshake by submitting a request to connect to the server.
2. The server responds with its digital certificate, which provides the public key of the server.
3. The client validates the digital certificate issued by the server to confirm that it is legitimate and issued by a trusted certificate authority.
4. The client generates a random symmetric key and encrypts it with the public key of the server.
5. The server uses its private key to decode the symmetric key.
6. All throughout the session, both the client and the server utilize the symmetric key to encrypt and decode data.

`Graphical user interface, Word

Description automatically generated

**Certificate Validation**: Certificate validation is the process of verifying the authenticity and validity of digital certificates used for secure communication. A digital certificate is issued by a trusted Certificate Authority (CA) and contains information about the entity using it. Certificate validation ensures that the certificate is not compromised and is valid. It prevents unauthorized access to communication and ensures the privacy and security of sensitive data.

**Key Exchange**: Key exchange is the process of securely exchanging keys between the sender and receiver to ensure that the data transmitted between them is encrypted and cannot be intercepted. The key exchange process involves generating a unique symmetric key that is used to encrypt and decrypt data during the session. The key exchange process ensures that only the sender and receiver have access to the symmetric key, and it prevents unauthorized access to the communication.

**Data Encryption**: Data encryption is the process of transforming plain text into encrypted text, which cannot be deciphered without the right key. Even if an attacker intercepts the data, they won't be able to read it because of the encryption procedure. Data encryption preserves the secrecy and privacy of sensitive information and is a key component of secure communication.

**Session Termination**: The process of terminating a secure communication connection is known as session termination. The data transferred during the communication session is inaccessible after the communication session ends because the symmetric key used for encryption and decryption is destroyed. To protect sensitive data's privacy and security, session termination is crucial for preventing unwanted access to communications.

Top of Form

Bottom of Form

Top of Form

# Vulnerabilities in SSL/TLS-Software based

PRANATHI & SARAT

(Times new roman 10)

# Concluding Thoughts

##### References

1. G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*
2. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
3. I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.
4. K. Elissa, “Title of paper if known,” unpublished.
5. R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.
6. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
7. M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 198

[8] https://blogs.sap.com/2021/09/08/demystifying-ssl-tls/

[9] <https://www.seobility.net/en/wiki/Transport_Layer_Security>

[10]