International Journal of Scientific Research and Management (IJSRM)
||Volume||12||Issue||12||Pages||8047-8052||2024||
Website: https://ijsrm.net ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v12i12.em03

Secure Sockets Layer/Transport Layer Security for E-Commerce

CPA Dr. Leonard W. Wakoli

Jaramogi Oginga Odinga University of Science and Technology, School of Informatics and Innovative Systems, P. O. Box 210 – 40601, Bondo – Kenya

Abstract
Digital commerce has revolutionized the global economy, offering many opportunities for businesses and consumers. The increase in volume and number of online transactions comes the critical need for robust security measures to protect sensitive data from malicious actors. The research paper aims to provide stakeholders with the knowledge and insights necessary to build trust and confidence in online transactions. T (i) to establish the fundamental principles underpinning Secure Sockets Layer/Transport Layer Security (SSL/TLS) encryption, (ii) to provide SSL/TLS mechanisms for securing online transactions and protecting sensitive customer information, (iii) to determine how SSL/TLS protocols establish secure communication channels between clients and servers, ensuring the confidentiality, integrity, and authenticity of data exchanged in digital marketplaces and (iv) to establish the effectiveness of SSL/TLS in safeguarding sensitive customer information and mitigating the cyber threats. The methodology used to achieve the objectives was a desktop survey. The outcome of the desktop survey includes the fundamental principles underpinning Secure Sockets Layer/Transport Layer Security (SSL/TLS) encryption, the SSL/TLS mechanisms for securing online transactions and protecting sensitive customer information, how SSL/TLS protocols establish secure communication channels between clients and servers, ensuring the confidentiality, integrity, and authenticity of data exchanged in digital marketplaces and the effectiveness of SSL/TLS in safeguarding sensitive customer information and mitigating the cyber threats

Keywords: Certificate Authorities, Compliance, Cyber-threats, E-commerce, Encryption, Protocol, Regulatory Security, SSL/TLS

Introduction

1.0 Background Information

E-Commerce Concept E-commerce (electronic commerce) refers to the buying and selling of goods or services over the internet. It's like having a virtual store where customers can browse through products, make purchases, and complete transactions without needing to visit a physical store. E-Commerce operates as a sophisticated technical framework, facilitating business transactions with rapidity and efficiency, thereby enhancing economic interactions from both a commercial and entrepreneurial standpoint. E-commerce has revolutionized the way businesses operate and how people shop. It offers a convenient way for consumers to access a wide range of products and services from the comfort of their homes, anytime and anywhere. For businesses, e-commerce provides a platform to reach a global audience and expand their customer base beyond geographical limitations.

Small businesses and entrepreneurs can also benefit from e-commerce by setting up online stores with minimal overhead costs compared to traditional brick-and-mortar stores. With the rise of e-commerce platforms and online marketplaces, such as Amazon, eBay, and Shopify, buying and selling goods and services online has become increasingly accessible to individuals and businesses of all sizes.

Characteristics of E-commerce

The main characteristics of e-commerce are:

1. Global Reach: E-commerce transcends geographical boundaries, enabling businesses to reach customers worldwide without the limitations of physical location.
2. Convenience: E-commerce offers unparalleled convenience, allowing customers to shop anytime, anywhere, using various devices such as computers, smartphones, or tablets.
3. Variety of Products and Services: E commerce platforms provide a vast array of products and services from diverse vendors, offering customers access to a wide selection of goods that may not be available in traditional stores.
4. Secure Transactions: E-commerce prioritizes security, with robust measures in place to ensure the confidentiality, integrity, and authenticity of transactions. Technologies such as encryption and secure payment gateways protect sensitive information and mitigate cyber threats.
5. Lower Overhead Costs: E-commerce typically involves lower overhead costs compared to traditional brick-and-mortar stores, making it more accessible for small businesses and entrepreneurs to enter the market and compete effectively. Challenges of Ecommerce The main challenges in e-commerce are:
6. Security: Ensuring the security of online transactions and protecting sensitive customer information from cyber threats such as hacking, data breaches, and identity theft is a significant challenge for e commerce businesses.
7. Technical Challenges: E-commerce websites and platforms require robust technical infrastructure and maintenance to ensure smooth operation. Challenges such as website downtime, slow loading times, and compatibility issues across devices and browsers can negatively impact user experience and sales.
8. Technological Advancements: Keeping pace with rapidly evolving technologies and trends in e-commerce, such as mobile commerce, voice commerce, and artificial intelligence, can be challenging for businesses. Failure to adapt to emerging technologies may result in loss of competitiveness and market share.
9. Customer Trust and Satisfaction: Building and maintaining customer trust is critical in e-commerce. Challenges such as poor product quality, inaccurate product descriptions, and subpar customer service can erode trust and lead to customer dissatisfaction.
10. Legal and Regulatory Compliance: E commerce businesses must comply with various legal and regulatory requirements, including consumer protection laws, privacy regulations, and taxation laws. Ensuring compliance across different jurisdictions can be complex and time-consuming.

1.2 Overview of Secure Sockets Layer/Transport Layer Security (SSL/TLS)

SSL/TLS is a cryptographic protocol suite designed to secure communication channels over computer networks (the internet). It was initially developed by Netscape in the 1990s, and later SSL was succeeded by TLS which is the modern and widely adopted version. SSL/TLS provide a framework for ensuring the confidentiality, integrity, and authenticity of data exchanged between clients and servers in e-commerce ecosystem. SSL/TLS at its core encrypts data transmitted between a client, such as a web browser and a server, such as a website server. This encryption process prevents any unauthorized access to sensitive and crucial information by malicious actors attempting to intercept data during transit. SSL/TLS achieves this by employing a combination of symmetric and asymmetric encryption algorithms during an initial handshake process between the client and server. The SSL/TLS handshake involves several steps, including the negotiation of cryptographic algorithms and the exchange of digital certificates. Digital certificates are issued by trusted Certificate Authorities (CAs) and are used to authenticate the identities of the server and sometimes the client. When the handshake is complete and a secure connection is established then the data exchanged between the client and server is encrypted and decrypted using the agreed-upon cryptographic keys. This encryption protects the confidentiality and integrity of the data, making it unreadable to unauthorized parties even if intercepted during transmission. SSL/TLS has evolved over the years to address vulnerabilities and improve security. Various versions of the protocol exist, with TLS 1.2 and TLS 1.3 being the most widely used and recommended versions in the modern world. TLS 1.3 introduces several security enhancements and performance improvements over previous versions. SSL/TLS is paramount in ensuring secure e-commerce transactions, online banking, email communication, and other sensitive activities conducted over the internet ecosystem.

1.3 History of SSL/TLS

The evolution of SSL/TLS spans several key stages in internet security. It began with the publication of SSL 2.0 by Netscape in November 1994, introducing the concept of secure communication over the internet. However, SSL 2.0 suffered from several weaknesses, prompting the development of SSL 3.0 in November 1996, which addressed some vulnerabilities but still fell short of providing robust security.

In the process, more demands for improvements let to the emergence of TLS 1.0 in January 1999 as an Internet standard based on SSL 3.0, though it was not interoperable with its predecessor, necessitating upgrades for implementation. Subsequent versions aimed to strengthen security: TLS 1.1, published in 2006, introduced stronger cipher suites to strengthen defences against vulnerabilities, while TLS 1.2, released in 2008, further enhanced security with stronger cryptographic algorithms and support for extensions. Finally, in March 2018, TLS 1.3 was released offering improved speed and more robust security.

TLS 1.3 streamlined the handshake process, minimized latency, and eliminated the outdated cryptographic algorithms hence adapting the emerging threats and uphold the security standards in internet communication. Table 1 shows a summary of the history of SSL/TLS

Table 1: History of SSL/TLS

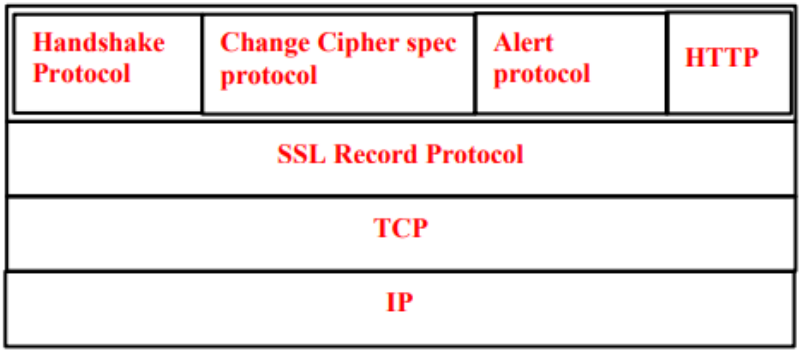
S/No.	Version	Description
1	SSL 2.0	Released by Netscape in November 1994, the first version of SSL with weaknesses.
2	SSL 3.0	Developed by Netscape and Paul Kocher in November 1996, addressed some SSL 2.0 weaknesses.
3	TLS 1.0	Introduced in January 1999 as an Internet standard based on SSL 3.0, not interoperable with SSL 3.0.
4	TLS 1.1	Published in 2006, updated TLS 1.0 with stronger cipher suites for enhanced security.
5	TLS 1.2	Released in 2008, provided further improvements over TLS 1.1 with stronger algorithms and extension support
6	TLS 1.3	Finalized in March 2018, offered faster speeds and improved security with streamlined handshake process and elimination of outdated cryptographic algorithms.

SSL (Secure Socket Layer) was initially released in 1994 as a cryptographic protocol designed to provide secure communication over the internet. In 1999, the Internet Engineering Task Force (IETF) standardized SSL into TLS (Transport Layer Security), which became the de facto standard for internet security. TLS is based on the SSL protocol but it introduced improvements and updates, with version 1.0 being the initial release.

The primary goal of the TLS protocol is to ensure privacy and data integrity between two communicating applications. It achieves this by encrypting data transmitted between clients, such as web browsers, and servers. TLS is widely deployed and integrated into nearly every web browser, making it essential for securing online communication. TLS is commonly used to protect information exchanged between browsers and web servers during online transactions, such as shopping or banking. Despite the transition to TLS, the term "SSL" is still often used colloquially when referring to TLS due to its historical association and widespread recognition.

Table 2 shows the location of SSL record protocol.

Table 2: Secure Socket Layer



Purpose of SSL/TLS

The purpose of SSL/TLS (Secure Socket Layer/Transport Layer Security) can be summarized into three main objectives:

- Confidentiality: SSL/TLS ensures that the data exchanged between the peers of a TLS connection remains confidential. This means that no third party intercepting the communication can understand or decipher the content being transmitted.
- Integrity: SSL/TLS guarantees the integrity of the data transmitted over a TLS connection. This ensures that the information exchanged between the client and server is not altered or tampered with during transit.
- Authentication: SSL/TLS provides a mechanism for authenticating the identity of the peers involved in the TLS connection. Each party can verify the identity of the other, ensuring that they are communicating with the intended recipient.

1.4 SSL/TLS Functionality

The functionality of SSL/TLS protocol is essential for securing data sent over the internet, typically integrated into applications to protect information exchanged between clients and servers. In an SSL/TLS-enabled application, the protocol begins with a client sending a hello message to the server, initiating a secure connection. Upon confirming negotiated parameters, the server responds with its hello message along with a digital certificate containing information about its public key, certificate validity, and ownership details. Once the client authenticates the server using its certificate, the client and server establish session keys for encrypting and decrypting data exchanged during the session.

This ensures data confidentiality using symmetric key encryption algorithms like AES and also the message integrity is maintained through message authentication codes. The SSL/TLS protocol consists of four subprotocols: Handshake, ChangeCipherSpec, Record, and Alert.

- The Handshake subprotocol facilitates server authentication, key exchange, and data confidentiality. It involves the client and server negotiating cipher suites, selecting suitable algorithms, and verifying certificates. Once the server is authenticated, a master secret key is established for generating key material.
- The Record subprotocol: Secures application data using keys computed during the Handshake.
- Alert subprotocol: Handles errors or warnings during the process.

SSL/TLS provides robust security and vulnerabilities such as MITM (Man-in-the Middle) attacks and SSL stripping pose serious threats in digital ecosystem. Man-in-the-Middle attacks involve intercepting communication between client and server, while SSL stripping undermines SSL/TLS protection, allowing attackers to view user traffic in plain text. These challenges highlight the importance of continually improving SSL/TLS protocols to mitigate emerging threats and ensure robust security in e-commerce and other digital applications.

SSL in real word SSL/TLS protocols are ubiquitous in securing online transactions, encrypting data between web browsers and servers, ensuring privacy and data integrity. Deployed in nearly every web browser, they safeguard sensitive information during e-commerce, banking, and other online activities, fostering trust and

confidence in digital interactions. Figure 2 shows SSL in real world. Figure 2 and 3 shows where SSL lies and in the real world

Figure 1 shows the secure socket layer location.

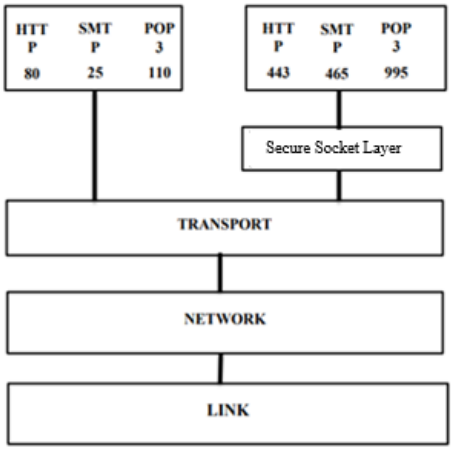


Figure 1: Location of the Secure Socket Layer (SSL)

Figure 2: Secure Socket Layer (SSL) in the Real World

Conclusion

In conclusion, the paper has discussed SSL/TLS encryption, beginning with the overview, functionality of SSL/TLS as used in strengthening the security infrastructure of digital commerce.

As online transactions become increasingly integral to the global economy, robust security measures are paramount to safeguard sensitive data from malicious actors. SSL/TLS ensures data confidentiality, integrity, and authenticity in digital marketplaces. The paper also explored history and architecture of SSL/TLS and highlights the evolution of SSL/TLS security protocols. Despite challenges, SSL/TLS emerges as a cornerstone of trust-building in e commerce, enabling stakeholders to transact with confidence and navigate the digital marketplace securely.

References

1. Al-Dawi, I. A. A. (2016). E-Commerce: An Applied Study on Libraries. King Fahd National Library for Printing and Publishing.
2. Al-Janabi, N. M., Al-Zaidi, M., & Nima, M. (2018). Economic Intelligence is the only entry point to Knowledge Intelligence. Al-Qadisiyah University.
3. Boss, W. R. (2007). E-Commerce for Libraries. McGraw Hill.
4. Dai, H. (n.d.). Secure Socket Layer (SSL) / TLS (Transport Layer Security).
5. Das, M. L., & Samdaria, N. (2014). On the security of SSL/TLS-enabled applications. Applied Computing and Informatics, 10(1–2), 68–81. https://doi.org/10.1016/j.aci.2014.02.001. Last accessed on 23/7/2024
6. Gean, E. (2015). Chapter 13 IPSec. California State University.
7. Li, X. Y. (2014). IPSec. Illinois Institute of Technology.
8. Sayal, M. A., Alameady, M. H., & Albermany, S. A. (2020). The Use of SSL and TLS Protocols in Providing a Secure Environment for e-commerce Sites. Webology, 17(2), 503–523. https://doi.org/10.14704/WEB/V17I2/W EB17048. Last accessed on 23/7/2024
9. Shmatikov, V. (2004). IP security. Internet Key Exchange (IKE) protocol.
10. Stallings, W. (2016). Cryptography and Network Security: Principles and Practice (8th ed.). Pearson.
11. Zaid, A., & Thanaa, D. (2017). The Reality of E-Commerce and the Challenges Facing it Arably and Globally. Tishreen University Journal for Studies and Scientific Research, Economic and Legal Sciences Series, 27(4)

Author Profile

Dr. CPA Leonard Wakoli, PhD.

CPA Dr. Leonard Wakoli is currently a Lecturer at Jaramogi Oginga Odinga University of Science & Technology (JOOUST), School of Informatics & Innovative Systems (SIIS). He is the Acting Dean, School of informatics and innovative systems. Leonard has a PhD in Information Technology (IT) Security and Audit from Jaramogi Oginga Odinga University of Science and Technology, a Master of Science in Software Engineering, a Bachelor of Science Degree in Mathematics and Computing, a a Post Graduate Diploma in the Management of Information Systems from University of Greenwich UK, a Diploma in Science Education (Mathematics & Physics). Leonard is also a Certified Public Accountant - CPA(K).