Comparative Analysis of Network Security Controls in the Modern Era

Sabeeruddin Shaik

Independent Researcher
Albany, New York
sksabeer8500@gmail.com

Abstract

In the current Digital world, to protect Data and provide secure communication internally and externally, Network security Protocols like Transport Layer Security (TLS), Internet Security Protocol (IPsec), and Hypertext Transfer Protocol Secure (HTTPS) play a crucial role in maintaining Security. This Research paper analyses the comparison of these protocols and explains their Functions, Use cases, and Limitations. This case study provides insights and explains the importance of these protocols in maintaining Security and protecting confidentiality, Integrity, and Availability. By Evaluating each protocol's Characteristics and Operational Frameworks, the research further explains their impacts on Internet security standards.

Keywords: Network Security, TLS, IPsec, HTTPS, Protocol Analysis, Cybersecurity, Data Transmission, Digital Communication

1. Introduction

In an Evolving world, providing Security for data in Transit has become more difficult. As cyber-attacks and data breaches increase, it is crucial to provide security and data integrity for data in motion across networks, both public and private. Also, due to the increase in demand for the adaptation of Robust security protocols to secure emerging domains like IOT Things, Cloud computing and, 5G Networks, Remote and Hybrid Work Environments, it is critical to protect confidentiality and data Integrity. To overcome these challenges and provide data security, these protocols HTTPS, TLS, and IPsec, are being implemented on the network. [1][6][7]

Each protocol has its purposes, and all these protocols greatly impact providing data security. TLS provides Security by encrypting the data in transit so that only authenticated users can access the data. It secures web traffic and application layer communications[1][6]. IPsec provides Security for all the IP based traffic[7]. HTTPS is a combination of HTTP and TLS, which helps secure online Transactions[10]. This Research paper will compare all these protocols and explain the Positives, Negatives, and suitability of different protocols in different scenarios. This paper provides the impacts of these protocols in securing data and different use cases.

2. Main Body

A. Problem Statement

Due to the increase in cyber threats in a rapidly growing world, such as Data Breaches, man-in-the-middle attacks, Phishing, Data Integrity, cross-site scripting, and many others, traditional security measures are not able to secure data.[8]
Even after we started using Network protocols like TLS, HTTPS, and IPsec, these protocols also have some unique challenges or drawbacks, like vulnerabilities in older versions, Certificate management, higher latency, difficulty in configuring, and compatibility issues.[6][7]There are also some unique challenges for these Network protocols. Considering Quantum computing, the encryption algorithm for TLA and IPsec is undermined[3].Also, HTTPS has sometimes been issued with authenticating the CA's. Also, it should be monitored and renew the Certificates. This could cause vulnerability[10]. These issues necessitate not only updates to protocol standards but also the integration of additional security mechanisms, such as intrusion detection systems (IDS) and zero-trust architectures[9].This research paper compares the protocols and analyses these challenges. It also provides solutions to improve cybersecurity measures.

B. Solutions

1) Transport Layer Security (TLS)

Advantages:

- Protects Confidentiality by encrypting the data between the client and server at the Transport layer. It also provides Data Integrity by using cryptographic hashes
- Enables Mutual Authentication Via Digital Certificates.[1]
- Provides stronger encryption and Security than the older protocols like SSL.[1]

Disadvantages:

- Increases Latency due to the encryption/Decryption and Handshake process.
- Complex certificate management
- Vulnerable to Potential Downgrade attacks if not configured properly[1][6]

2) Internet Protocol Security (IPsec)

Advantages:

- Provides Security for the IP based traffic at Network layer by maintaining confidentiality, Integrity and Availability.
- Supports both Transport mode & Tunnel mode and secures individual packets or entire network
- Can be used for secure remote access for VPNs[7].

Disadvantages:

- Due to the layered architecture and encryption/Decryption process. It is difficult in case of trouble shooting IPsec connections
- Complex in configurations and compatibility issues with NAT if it is not added with an extra element (NAT-T) [12]

3) Hypertext Transfer Protocol Secure (HTTPS)

Advantages:

- Protects data by encrypting the data during the transmission of data from client to server and server to client
- Verifies the identity of the server through SSL/TLS certificates
- Protects data integrity
- HTTPS Provides critical Security for web-based services like Online banking, e-commerce, and many other services.

Disadvantages

- Maintenance of certificate is extra load of work. Purchasing, Revoking and renewing the Certificates should be managed.
- Misconfiguration can compromise Security
- Complexity in configuration

4) Transport Layer security

TLS plays a crucial role in Encrypting the traffic and securing web traffic. It also protects the protocols like SMTP, FTP, and IMAP. TLS supports the Perfect forward secrecy by creating session keys for each session, establishing secure connections, preventing loss of data, and maintaining the integrity of the data. Additionally, the latest version of TLS 1.3 has brought up the handshake process for the establishment of connection, improving the security of the data Transfer, and this latest version has addressed the vulnerabilities from previous versions, enhanced security, and reduced latency. [7]

5. Internet Protocol Security (IPsec)

IPsec protocol provides solutions for the modern Network challenges, and it can support the IPV6 requirements. IPsec would be a trusted protocol for building and connecting to Untrusted networks like site-site VPN, Mobile workforce solutions, and cloud Environments. IPsec is flexible to work for both Tunnel and Transport modes. IPsec allows secure connections for the IOT Networks. IPsec also supports advanced algorithms for encrypting the traffic and ensures compliance with regulatory requirements satisfyingthe encryption standards.[12]

6) Hypertext Transfer Protocol Secure (HTTPS)

HTTPS has become crucial for the E-Commerce Industries. Organizations are allowing only HTTPS Connections to their portals for a secure connection. Despite online banking, HTTPS is also Being used by privacy-centric applications, Social Media platforms, Streaming services, the Healthcare sector, the Government, and Financial. The adoption of automated certificate management tools, such as Let's Encrypt, has democratized HTTPS deployment, reducing costs and complexity for smaller organizations.

C. Uses

All these Network Protocols TLS, IPsec, HTTPS are extensively being Used in the Hybrid security Models

TLS - TLS provides web security by protecting data in Transit, Encrypting email communications for SMTP, IMAP, POP3. Protecting VOIP Applications and For Ensuring secure File Transfers. TLS is frequently employed in microservices architectures to secure inter-service communication.[10]
IPsec - Used in providing secure remote access through VPN. IPsec's network-level security is leveraged in securing Software-Defined Networks (SDNs).

HTTPS - Highly utilized for secure web services and password protection, Personal PII Details. HTTPS is critical in e-commerce, banking services and for API's to provide secure communication. HTTPS forms the backbone of web-based APIs, ensuring secure interactions between distributed components in cloud-native applications.[12]

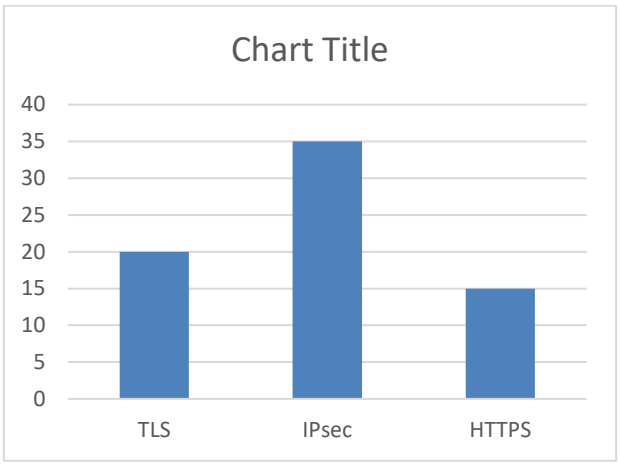
D. Impacts

The application of these protocols has improved the security standards across industries.
TLS and HTTPS Provide Security for web-based applications by encrypting data and maintaining data integrity. They also secure communication, which prevents cyber attacks like man-in-the-middle attacks and phishing.
IPsec- Provides secure remote access through VPN for employees. These protocols have kept the cyber world in better ways in terms of securing the data. For example, With the extensive usage of HTTPS, Browser developers has deprecated the use of HTTP for safer web practices.
The integration of IPsec with the cloud environment has made secure virtual networks for the Companies, reducing the attack surface.Organizations can use combine these protocols with Technologies like MFA and Endpoint detection tools and improve the layered security models.Despite these protocols, proper monitoring is required to maintain Security. Regular patches, Updating the certificates, and proper configuration management are crucial because misconfigurations and outdated versions might lead to vulnerability.

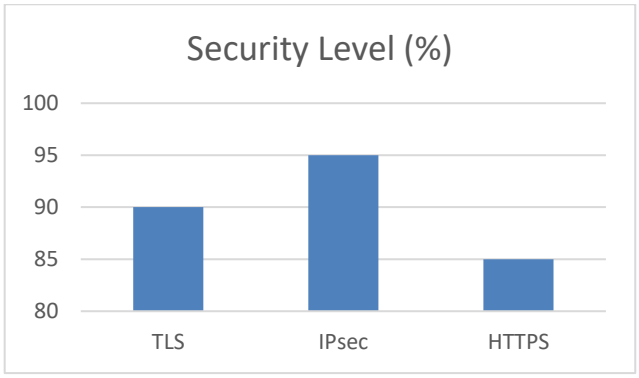
3. Scope

This Research Paper focuses on analysing the Principles, Positives, Limitations, and Impacts of these protocols. Determining their suitability and objectives for different domains that can be applied to improving the Security of the companies. Detailing the current challenges and explaining the need to implement these protocols to encrypt the data and maintain the CIA. [1][7][10]

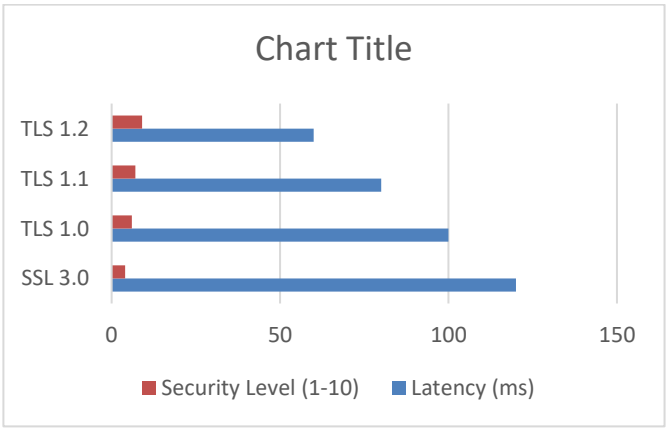
4. Graphs and Flow Charts



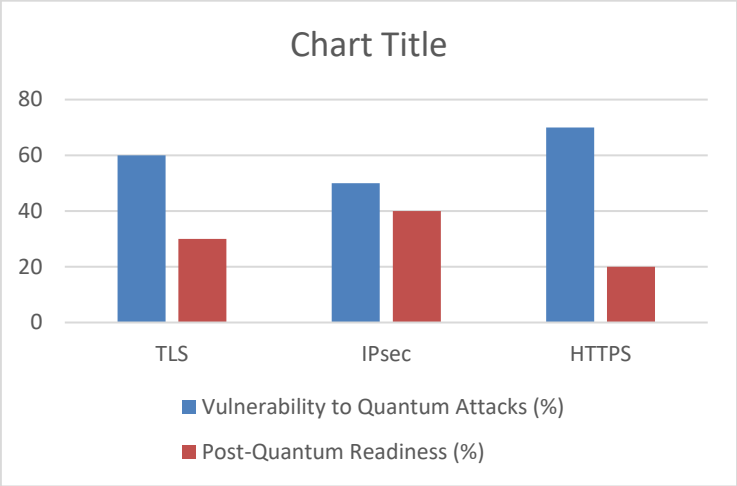
(i) Bar chart explaining the Comparison of performance overhead of TLS,IPsec, HTTPS



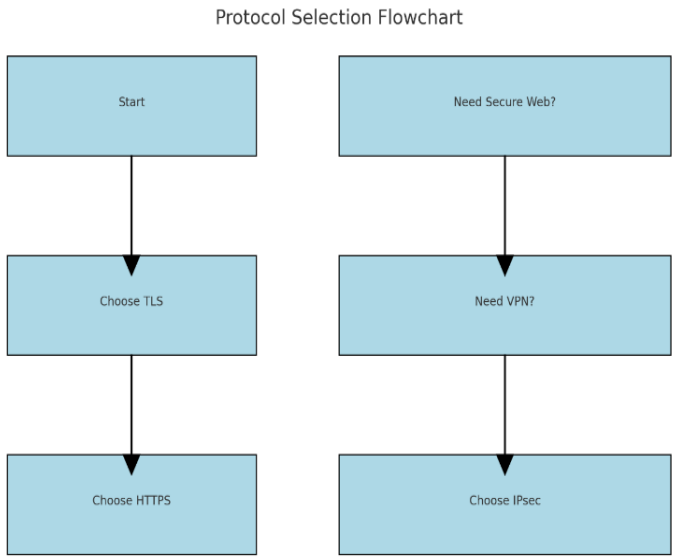
(ii) Bar chart explaining the Security level of these protocols



(iii)TLS Handshake Latency Over Protocol Versions



(iv)Impact of Quantum Computing



(v) Flowchart to guide the selection of appropriate protocol based on the use case

5. Conclusion:

TLS, IPsec and HTTPS These Network protocols provide critical Security for the data. Each protocol is unique and critical for their respective functions. But understanding these protocols is very important. The stake holders should have understanding about the advantages of these protocols and also Limitations. It is important to know how to use these protocols for different domains and situations to maintain data security. Based on the fasting moving world digital challenges, It is important to regularly monitor, regularly update to latest versions and perform perfect configurations to mitigate vulnerabilities.

Proper maintenance makes it possible to protect sensitive information and build a safer, more resilient digital future.

6. References

[1] IETF, The Transport Layer Security protocol version 1.3, RFC 8446, 2018.

[2] H. K. e. al, HMAC:Keyed-Hashing for Message Authentication, RFC 2104, 1997.

[3] D. Bernstein, The dangers of key recovery, key escrow, and trusted third party encyption, IEEE computer society press, 1997.

[4] A. shamir, How to share a secret, communications of the ACM, 1979.

[5] R. &. W. Sandhu, Role Based Access control, IEEE Computer society press, 1996.

[6] T. &. R. E. Dierks, The Transport layer security Version 1.2, RFC 5246, 2008.

[7] S. &. S. K. Kent, Security Architecture for the Internet Protocol, RFC 4301, 2005.

[8] B. Schneier, Applied cryptography: Protocols, Algorithms and source code in C (2nd ed). wiley, 1996.

[9] C. P. R. &. S. kaufman, Network security : Private communication in public world (2nd ed) prentice hall.

[10] J. e. a. Doe, Understanding the diference between IPsec and TLS, Browerscan, 2018.

[11] P. OWL., IEEE General Format, Purdue university online writing lab, 2018.

[12] S. e. al, Cryptographic key Management for Ipsec, IEEE Security &Privacy, 2005.