NANYANG
TECHNOLOGICAL
UNIVERSITY
SINGAPORE

SC3030 Advanced Computer Networks

Term Paper

Network Security Protocols

Submitted By: Lim Dong Wan

Matriculation Number: U2122455D

School of Computer Science and Engineering

Contents Page

1. Network Security Introduction

The Internet has indubitably become indispensable to many people's livelihoods today. The COVID-19 pandemic has catalyzed the digital transformation process worldwide (Pure Cloud Solutions, 2020), given the social restrictions put in place to curb transmission. This has made the Internet much more accessible and convenient for people as they go about their everyday lives.

In an annual study conducted by Info-comm Media Development Authority (IMDA) in Singapore on info-communication usage by Singaporeans, each Singapore household owned more connected devices from 2020 to 2021 amidst the COVID-19 pandemic (Figure 1) (Cyber Security Agency (CSA), 2023, p.25).

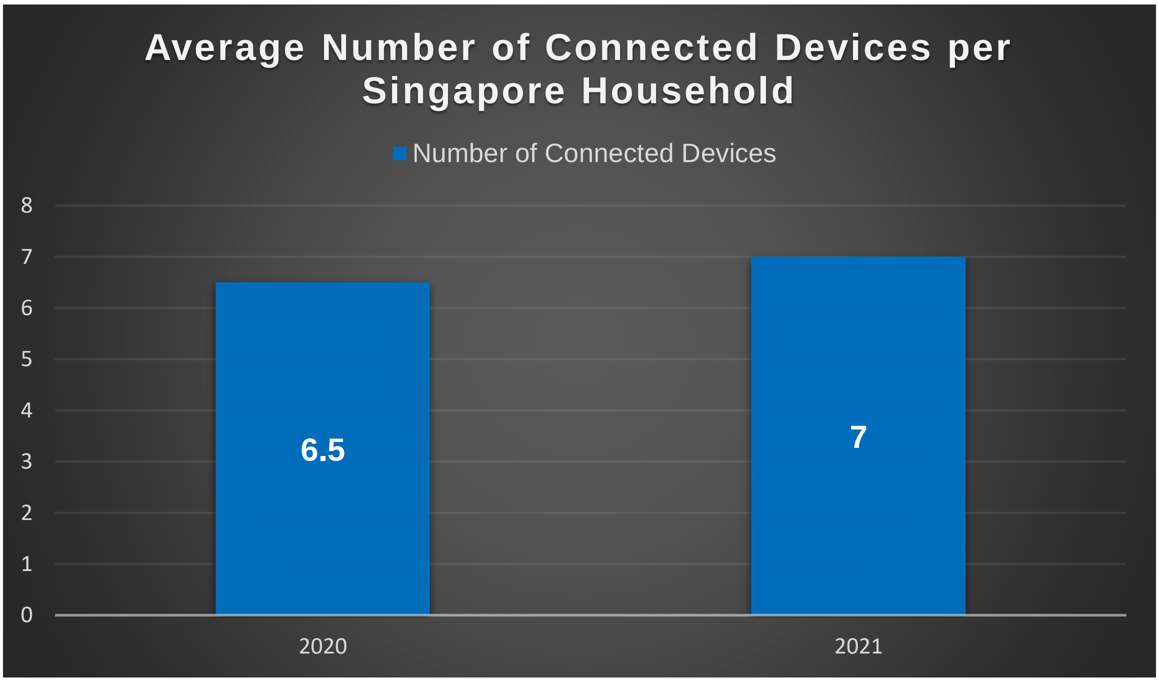


Figure 1: Number of Devices Per Household in Singapore (2020-2021)

Australia also experienced a similar trend during the same period (Figure 2) (Statista, 2023).

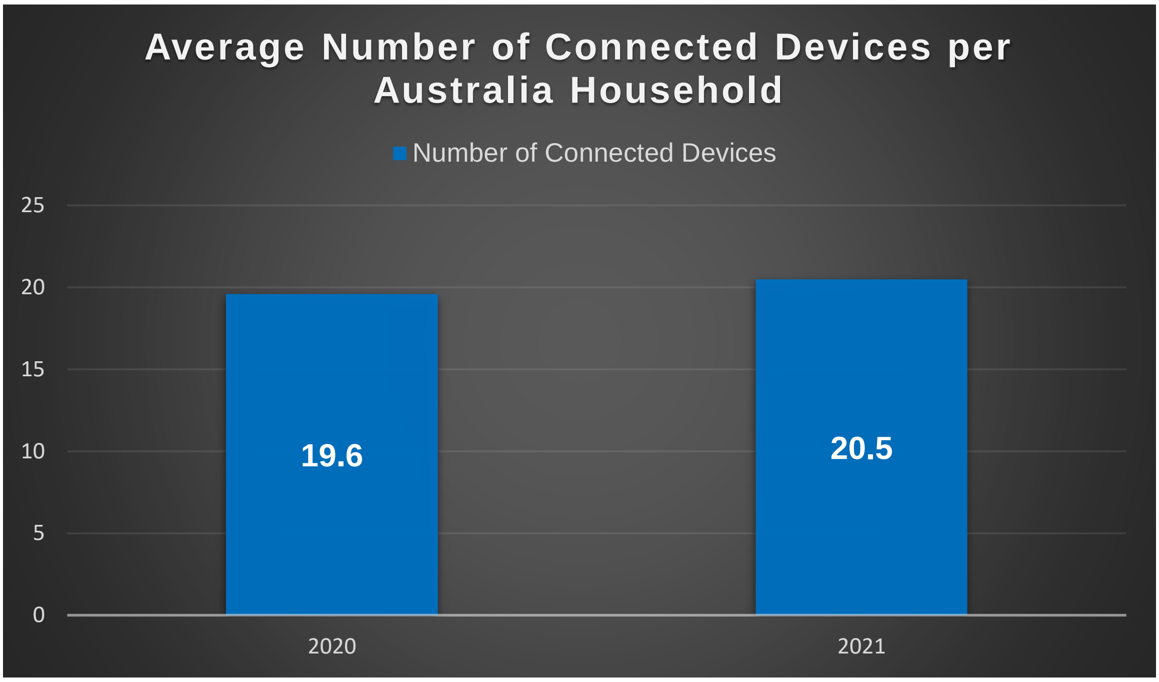


Figure 2: Number of Devices Per Household in Australia (2020-2021)

The proliferation of the Internet and technological advancements, coupled with the exponential growth of networked devices, have resulted in the rising complexity of the network environment (Zhang & Li, 2023, p.168) and the continuous expansion of the boundaries of our digital world over the years. However, the dynamicity of the global cyber threat landscape, due to new emerging security threats worldwide, has made computer networks more vulnerable in this aspect. Moreover, with greater convenience comes greater cybersecurity risks. Increasingly, it is difficult to strike a fine balance between these two aspects of the Internet (Figure 3), making the Internet a double-edged sword in today's digitally connected world. Hence, the need for robust security measures to protect critical data in a system has become greater than before.

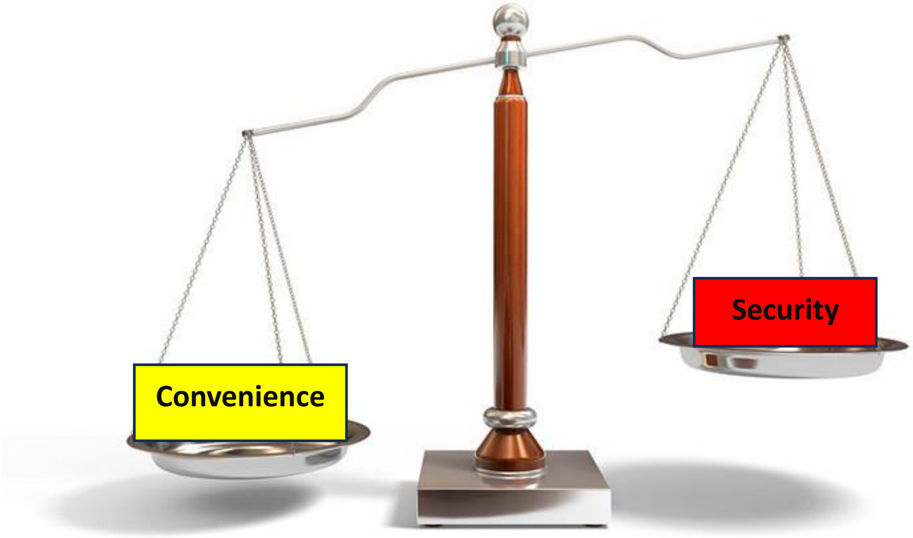


Figure 3: The Tricky Balance Between Convenience and Security in Digital Technology

Network security is an essential component and subset of computer security (Howard & Whittaker, 2005, p.1). It encompasses the establishment of a robust communication network and the implementation of mitigatory measures (Oluwasanmi, 2023, p.26) using various technologies to confer data Confidentiality, Integrity and Availability – the three elements of the CIA triad – while preventing unauthorized access from or malicious actions conducted by external parties at the same time. This is to safeguard the connection from the network's core to the network's edge within the network architecture (Gupta et al., 2023, p.75), as well as the network resources and assets.

As cybercriminals, who are malicious threat actors, become more skilled and sophisticated in crafting their attacks, coupled with human negligence, it is becoming more difficult for individuals and organizations to safeguard themselves against such attacks (Zhang & Li, 2023, p.168), which is worrying. Hence, network security must continuously evolve to effectively tackle these cybersecurity challenges.

This paper shall highlight the importance and present challenges of network security and in today's world, discuss and compare two widely used protocols in the field of network security, namely Internet Protocol Security (IPSec) and Transport Layer Security (TLS), as well as explore the future potential of network security.

2. Significance of Network Security

As the digital landscape continues to evolve, network security is a crucial aspect in ensuring the integrity and resilience of interconnected systems and network devices today. Thus, its significance cannot be overstated.

Figure 4 summarizes three key areas of significance of network security that this paper shall focus on.

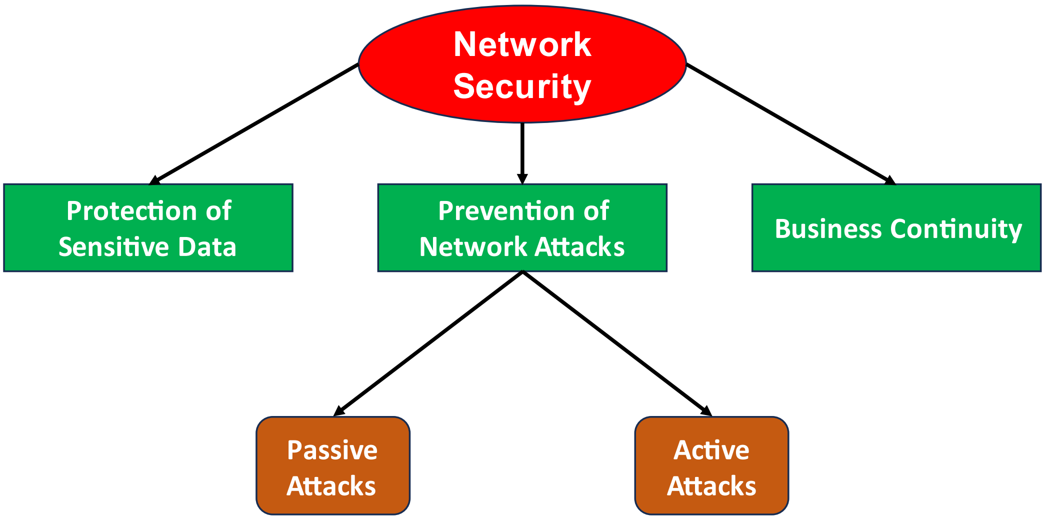


Figure 4: Overview of the Significance of Network Security

2.1. Protection of Sensitive Data

There are vast amounts of sensitive information, including personal, financial, and business data being regularly transmitted over networks, especially in organizations, nowadays. Hence, any loss of such data due to unauthorized access can potentially be catastrophic to any individual or organization in many facets, including individual privacy and organizational reputation (Visual Edge IT, n.d.).

Network security protocols thus become essential in safeguarding this information from unauthorized breaches, as a result of cyber-attacks, which compromise the CIA triad of data.

2.2. Prevention of Network Attacks

Nowadays, cybercriminals are becoming more adept at and sophisticated in launching attacks targeted at individuals and organizations. Today, cyber-attacks targeted at computer networks can be broadly categorized into passive and active attacks (Table 1) (Oluwasanmi, 2023, p.26; Forcepoint, 2021).

	Passive Attacks	**Active Attacks**
Purpose & Actions	Cybercriminals gain unauthorized access to a network to monitor and steal data, without altering any part of the network.	Cybercriminals alter and destroy data in a network, upon gaining unauthorized access to it.
Examples	• Packet sniffing (Ju et al., 2020, p.578) • Unauthorized access (Ju et al., 2020, p.578)	• Internet Protocol (IP) address spoofing (Al-Salqan, 1997, p.216) • Denial-of-Service (DoS) (Ju et al., 2020, p.578)

Table 1: Types of Computer Network Attacks

Hence, network security protocols come into play in alleviating the risks of such attacks (Visual Edge IT, n.d.).

2.3. Business Continuity

The impact of cyber-attacks to organizations is significantly greater and more severe than that to individuals, given that it affects a larger amount and coverage of data and assets across the entire company. Even if only one machine is down, it can potentially still disrupt business operations to a great extent, especially if the machine is used by the system administrator within the organization. Such disruptions lead to business downtime, which can incur substantial financial losses to the company and tarnish the organization’s reputation.

Therefore, network security should be an integral component of the organization’s Business Continuity Plan and must be prioritized, to maintain operational stability and robustness. This also enables organizations to swiftly recover from security breaches (Visual Edge IT, n.d.).

3. Network Security Vulnerability Issues

Network security continues to be a challenging problem today, given the presence of many vulnerabilities in three main aspects (Figure 5) (Ju et al., 2020, p.577; Fotra Digital Defense, n.d.). Ultimately, the responsibility of network security lies on the shoulders of everybody (Imperva, n.d.), not just the technical professionals alone.

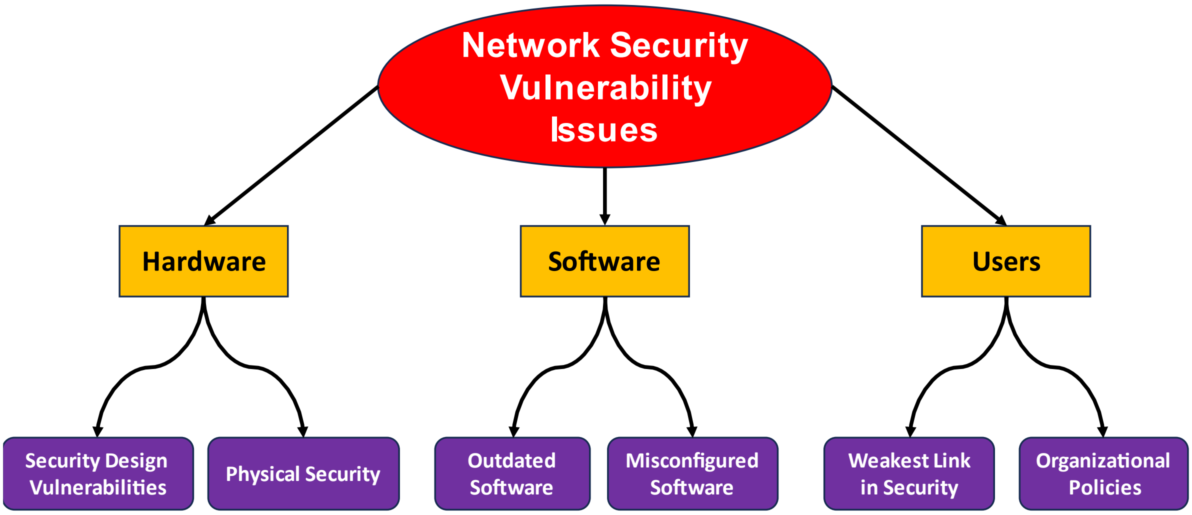


Figure 5: Overview of Network Security Vulnerability Issues in Today's Digital World

3.1. Hardware Issues

There are several security design vulnerabilities in different kinds of hardware devices (Ju et al., 2020, p.577), such as routers, switches and firewalls, in a network system. If these hardware devices are not properly configured, have default settings enabled or are not upgraded with the latest security patches, these vulnerabilities can be easily exploited by cybercriminals, rendering these hardware devices vulnerable to network security attacks.

Furthermore, physical security of hardware devices can be easily compromised. Cybercriminals can either physically install malware into these devices using a storage device like a USB drive or disk, or remotely do so by sending the malicious storage device to unsuspecting employees of an organization, who will then unknowingly inject malware into the system (Fotra Digital Defense, n.d.).

3.2. Software Issues

Like hardware devices, there are exploitable vulnerabilities in software too, especially in outdated or misconfigured software. For instance, an outdated software does not have the latest software security patches, while a misconfigured one typically contains default security settings for passwords (Fotra Digital Defense, n.d.) and firewall policies, which will make it easier not only for users and system administrators who set up the applications (Fotra Digital Defense, n.d.), but also for cybercriminals to illegally infiltrate and compromise the network.

3.3. User Issues

Humans are the “weakest link in cyber defence” (Hoe, 2021, p.23; Accenture Security, 2019). Most network users are not professionals in cybersecurity, which encompasses network security, so they lack the awareness of as well as the expertise and capabilities in this field (Ju et al., 2020, p.578). This often translates into poor cyber hygiene and behaviour, such as adopting weak, easily guessable passwords for critical systems and accounts, not activating 2FA and unknowingly divulge sensitive information to cybercriminals through various attacks like phishing and social engineering (Fotra Digital Defense, n.d.).

In addition, the Bring Your Own Device (BYOD) policy that many organizations currently adopt enlarges the attack surface for cybercriminals. With employees using their personal devices for work, this has created a larger and more sophisticated network within each organization (Imperva, n.d.). Remote working, which has become prevalent due to the COVID-19 pandemic, has also provided employees remote access to sensitive organizational data and resources over the Internet, which is less secure given that it is a public network (Imperva, n.d.).

4. Network Security Protocols

This paper shall primarily discuss two commonly used network security protocols (Figure 6) that operate on different layers of the Transmission Control Protocol (TCP) / IP (TCP / IP) model – a condensed version of the older Open Systems Interconnection (OSI) model (Figure 7).

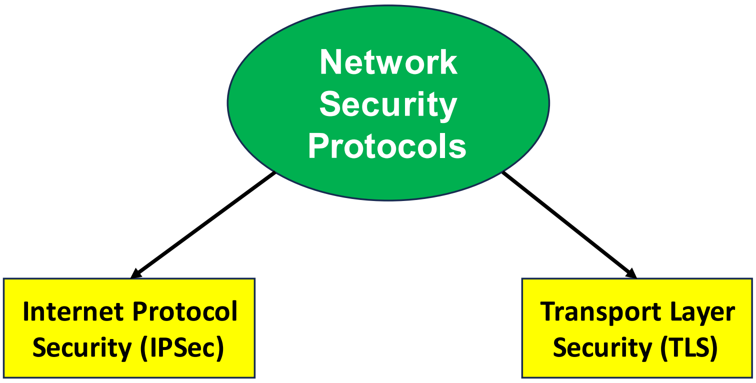

Network Security Protocols
Internet Protocol Security (IPSec)
Transport Layer Security (TLS)

Figure 6: Overview of Commonly Used Network Security Protocols

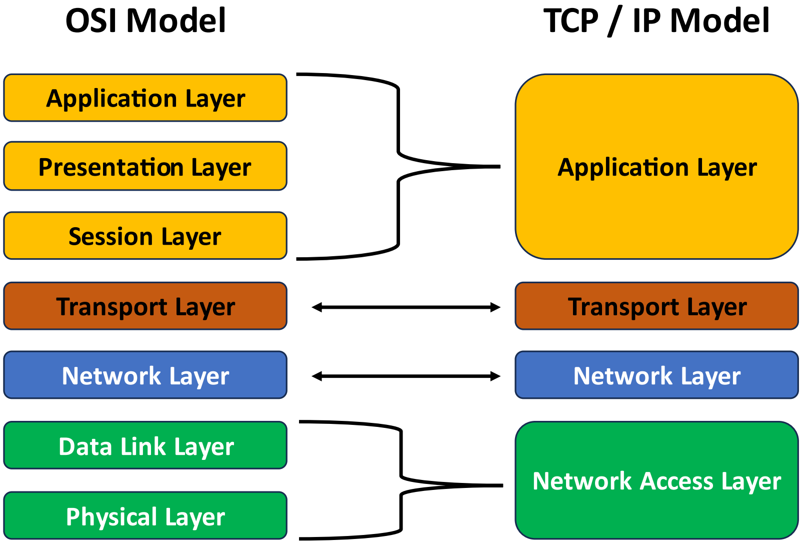


Figure 7: OSI Model in Comparison to TCP / IP Model

4.1. Internet Protocol Security

4.1.1. Overview

As the standard solution for strengthening data privacy (S & Sankaran, 2023, p.1) and preventing against security attacks since 1995 (Dufournet, 2021), IPSec has become more widely used nowadays, particularly in wireless networks (Rong & Djeddai, 2016, p.265).

IPSec operates on the **Network** Layer of the TCP / IP model (Rong & Djeddai, 2016, p.265), and uses the connectionless User Datagram Protocol (UDP) (CloudFlare, n.d.).

4.1.2. Functions

IPSec comprises a few core protocols and support components (Figure 8) to fulfil the following objectives:

- Create a shareable set of security protocols.
- Allow key exchange for authentication.
- Encrypt / Hash data for secure data transmission across a network.

These are essential when establishing a secure connection, which may pass through several intermediate systems that may be untrusted (Rong & Djeddai, 2016, p.265), to transmit data from network to network or host to host (S & Sankaran, 2023, p.2).

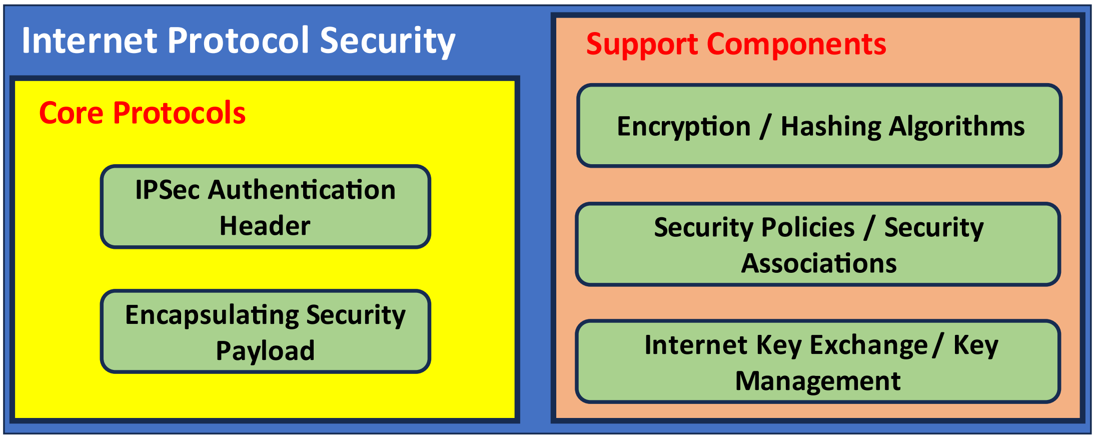

Internet Protocol Security
Core Protocols
IPSec Authentication Header
Encapsulating Security Payload
Support Components
Encryption / Hashing Algorithms
Security Policies / Security Associations
Internet Key Exchange / Key Management

Figure 8: IPSec Core Protocols and Support Components

Firstly, the Authentication Header (AH) contains a cryptographic checksum that confers integrity and authentication to the data contents of the IP packet. The Encapsulating Security Payload (ESP) authenticates and encrypts the data contents in the payload to confer confidentiality, and it usually resides in the AH (S & Sankaran, 2023, p.2; Tawde & Pedamkar, 2023).

Secondly, some encryption and hashing algorithms that are typically supported by IPSec include Advanced Encryption Standard 128 (AES-128), which adopts symmetric (private-key) encryption, and Hashed Message Authentication Code-Secure Hash Algorithm-1 (HMAC-SHA-1) (WatchGuard Help Center, n.d.), which contains a cryptographic key for authentication purposes.

Thirdly, when two devices want to establish an IPSec connection, they need to settle on a set of IPSec specifications, also known as Security Associations (SAs) or security policies, that entail the type of authentication and encryption algorithms, as well as IPSec protocols to be used in the connection. SAs can either be preset or made dynamic using Internet Key Exchange (IKE) protocol, the latter being more secure by having the highest levels of encryption and authentication (Juniper Networks, 2021).

Finally, IKE protocol and in particular, Internet Security Association and Key Management Protocol (ISAKMP), ensure that the connection between devices are secure, by providing mechanisms for authentication and key exchange. The former performs dynamic exchange of encryption keys, whilst the latter helps to create and set SAs to provide a security framework (S & Sankaran, 2023, p.3).

IPSec adopts two main modus operandi (Figures 9 & 10) (Rong & Djeddai, 2016, p.265; Sanoja, 2021), each serving a different purpose (Table 2) (S & Sankaran, 2023, p.3; Sanoja, 2021).

Figure 9 also illustrates a typical IP packet without IPSec.

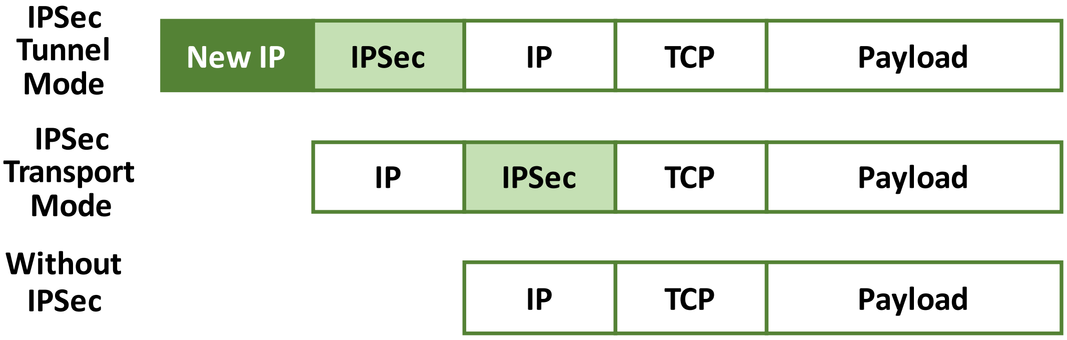


Figure 9: A High-Level Overview of IPSec Packets in Transport and Tunnel Modes

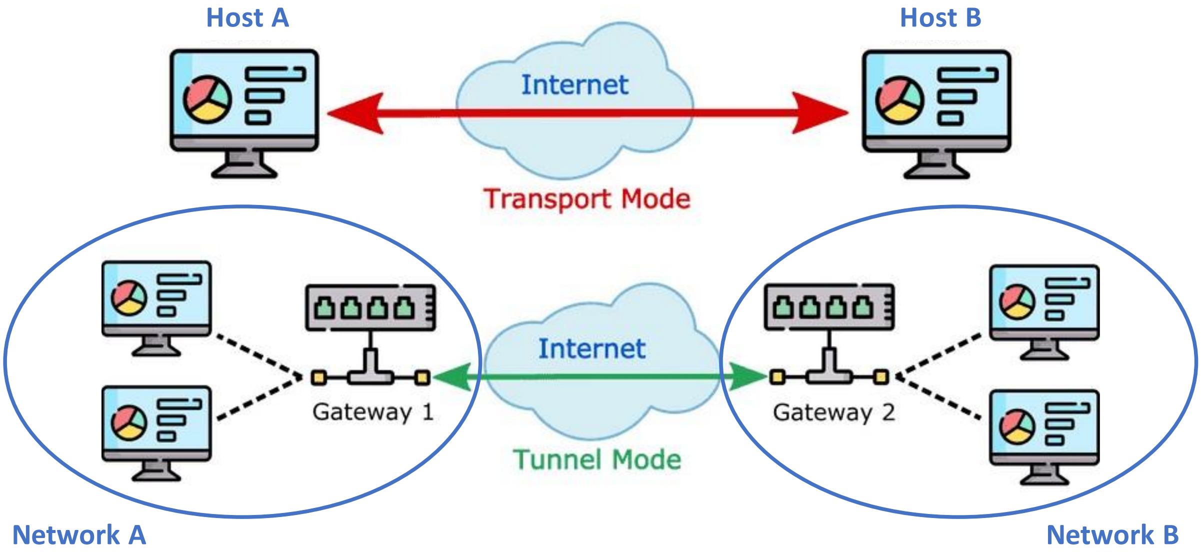


Figure 10: Transport and Tunnel Modes of IPSec

	Tunnel Mode	Transport Mode
Purpose	This secures network-to-network connections.	This secures server-to-server or host-to-host connections within a network.
Operation	IPSec creates and adds a new IP header to the original IP packet before encrypting the entire packet.	No new IP header is generated, nor the original IP header is altered. It encrypts the TCP header and payload but not the entire packet.
Advantages	• It is easy to travel over Network Address Translation (NAT) protocol. • The original IP address header is hidden for enhanced confidentiality.	• It incurs low overhead and latency. • It has a large MTU. • It is fast.
Disadvantages	• It incurs high overhead and latency. • It has a small Maximum Transmission Unit (MTU). • It is slow.	• It is hard to travel over NAT protocol. • Original IP address header is not kept secret.
Application	Gateway-to-gateway connection in a Virtual Private Network (VPN)	Client-server connections

Table 2: Transport and Tunnel Modes of IPSec

4.1.3. Real-World Application

IPSec is commonly used in VPNs, which provide encrypted connections over the unsecure Internet for remote user access, using the tunnel mode of operation (Figure 11), as it effectively fulfils the CIA triad for VPNs (S & Sankaran, 2023, p.1).

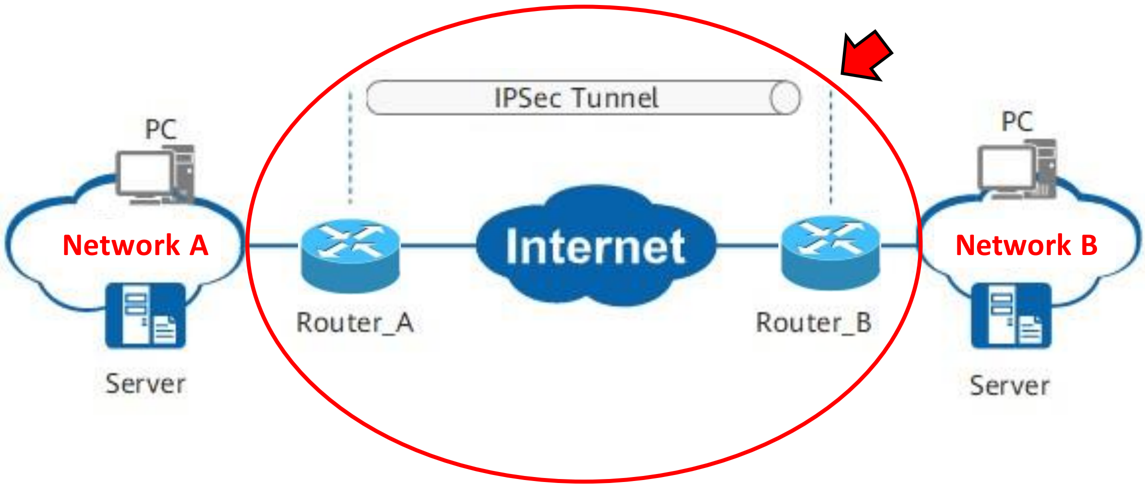


Figure 11: Use of IPSec in a VPN

4.2. Transport Layer Security

4.2.1. Overview

TLS supersedes Secure Socket Layer (SSL) to become the new security standard primarily in web security nowadays, aside other domains including Cloud and Internet of Things (IoT) (Chung & Vlajic, 2022, p.1). From the origination of SSL – SSLv1.0 – back in 1994, to the evolution of SSLv3.0 and its conversion to TLS 1.0 in 1999, and finally to its present form – TLS 1.3 – since 2018 (Alqaydi, Yeun & Damiani, 2017, p.275), SSL / TLS has seen a thorough transformation for the better over the decades.

Even though TLS is a **Transport** Layer protocol based on the TCP / IP model, it operates at Layers 4 through 7 of the OSI model (Joshua, 2023). It uses the connection-oriented TCP (Mankowski, Wiggers & Moonsamy, 2023, p.528), which is more reliable than UDP, via port 443 (Zheng et al., 2020, p.15).

For brevity reasons, this paper shall refer to the latest version of TLS – TLS 1.3.

4.2.2. Functions

TLS comprises two layers (Figure 12) (Alqaydi, Yeun & Damiani, 2017, p.275) to fulfil the following objectives (CloudFlare, n.d.):

- Authenticate and validate parties that are exchanging information with one another.
- Encrypt data transmission between client and server for confidentiality.
- Safeguard the integrity of transmitted data between client and server.

These are crucial in establishing a secure connection between a client (ie. web browser) and a server (ie. web server), for data transmission (Alqaydi, Yeun & Damiani, 2017, p.274).

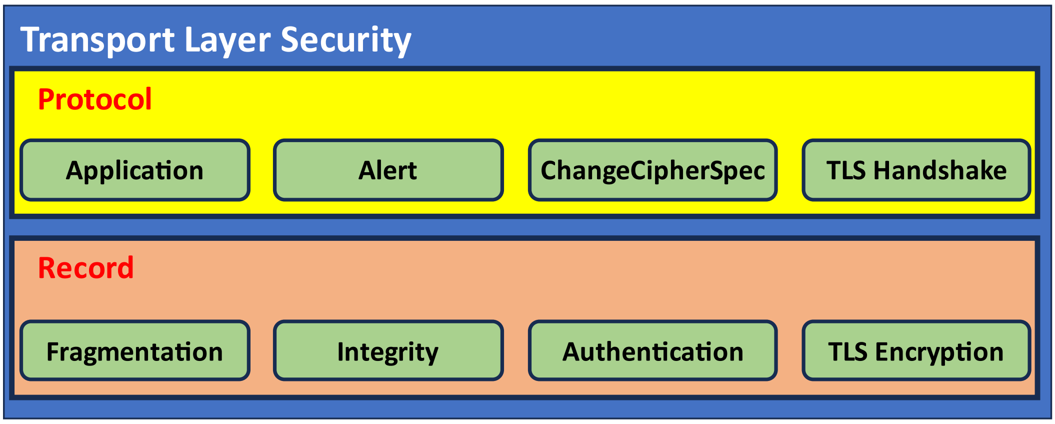


Figure 12: TLS Protocol Layer Above TLS Record Layer

In the Protocol layer of TLS (Alqaydi, Yeun & Damiani, 2017, p.275):

- Application protocol contains the actual data to be transmitted.
- Alert protocol detects and alerts errors in the client-server transmission.
- ChangeCipherSpec protocol negotiates with the client / server on the specified parameters to be used.
- TLS handshake protocol provides the primary medium for the client-server communication.

As for the TLS Record layer, it confers data confidentiality and integrity and offers an additional payload compression to the receiving entity on top of the shared transaction layer (Alqaydi, Yeun & Damiani, 2017, p.275).

At the core of the functionality of the TLS protocolary dichotomy, lies the TLS Handshake (Figure 13). This occurs when a client-server connection, typically over Hypertext Transfer Protocol Secure (HTTPS) (CloudFlare, n.d.), is established, and after TCP initiates the connection via a 3-way handshake.

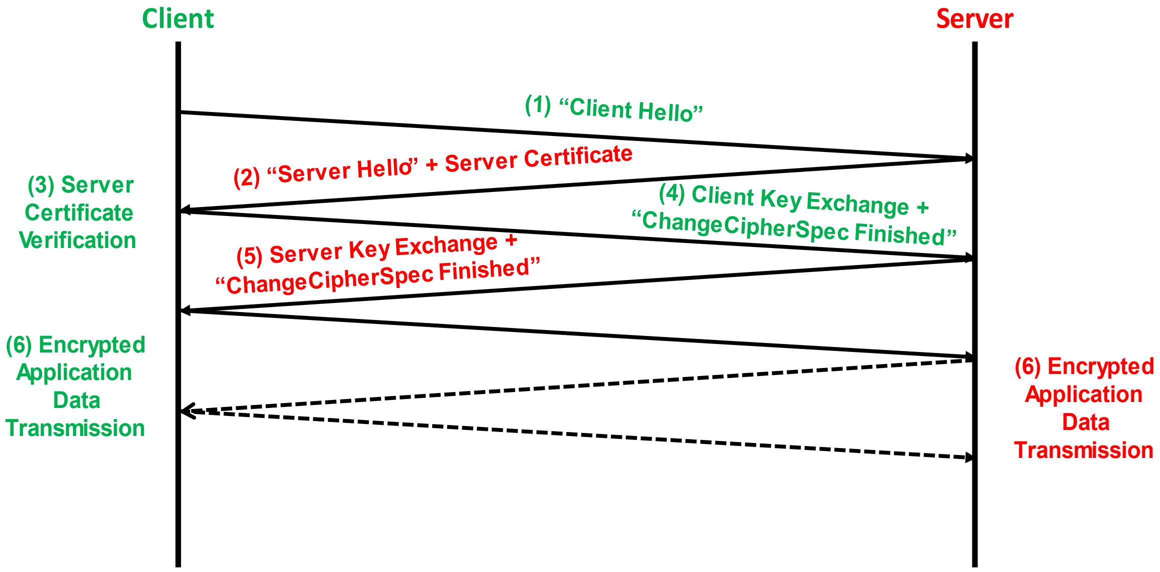

Client
Server
(1) "Client Hello"
(2) "Server Hello" + Server Certificate
(3) Server Certificate Verification
(4) Client Key Exchange + "ChangeCipherSpec Finished"
(5) Server Key Exchange + "ChangeCipherSpec Finished"
(6) Encrypted Application Data Transmission
(6) Encrypted Application Data Transmission

Figure 13: Client-Server TLS Handshake

In summary, the following occurs in each stage of the TLS handshake (Alqaydi, Yeun & Damiani, 2017, p.276; Holguin & Errapotu, 2023, p.4; Hussein et al., 2016, p.2; Nohe, 2019; CloudFlare, n.d.):

1. A TLS-enabled client initiates the connection, sending "**Client Hello**" messages, which carry various information, including cipher suites, the TLS version that are supported by the client, as well as a string of random bytes called *client random*, to a TLS-enabled server.
2. The server replies with "**Server Hello**" messages containing its chosen cipher suite, a string of random bytes called *server random*, as well as its digital certificate, which is typically a X.509 certificate that binds the server's identity to the server's public key using a digital signature.
3. The client uses the server's public key to validate the server's certificate with a trusted Certificate Authority (CA) issued, in order to ascertain that the identity of the server matches the certificate information.

4. Once the server is successfully authenticated, the client sends another random nonce – the *premaster secret* – that is encrypted using the server's public key to the server. This helps the client and server create a session key to be shared and used in encrypting subsequent transmissions of actual application data. Additionally, the client generates a session key based on the *client random* and encrypted *premaster secret* byte strings. The client then signals to the server that the handshake is complete on the client side, by sending "**ChangeCipherSpec Finished**" messages that are encrypted with the negotiated session key.
5. Similarly, the server uses its own private key to decrypt the *premaster secret*. It then generates a session key based on the *server random* and decrypted *premaster secret* byte strings. The server then signals to the client that the handshake is complete on the server side too, by sending "**ChangeCipherSpec Finished**" messages that are encrypted with the same negotiated session key.
6. From this juncture, the handshake is successful, and both the client and the server can easily transmit and receive subsequent messages of actual application data using the shared session key.

TLS handshake adopts symmetric (private-key) and asymmetric (public-key) cryptosystem. The former involves the usage of a shared session key to encrypt messages. As for the latter, SSL and older versions of TLS adopted the popular Rivest-Shamir-Adleman (RSA) algorithm (Luo & Lin, 2009, p.613; Holguin & Errapotu, 2023, p.3), whose security is based on the factorization of large prime numbers, such that the larger the prime number values are, the more secure the algorithm will be (GeeksForGeeks, 2022).

However, RSA does not support forward secrecy for key exchange. In fact, TLS now uses Diffie-Hellman key exchange (Urien, 2021, p.1) that supports this feature (Huang et al., 2014, p.44), thereby significantly enhancing TLS's security today. This ensures that session keys used for encryption and decryption of client-server messages are periodically renewed (Kim, 2023) to prevent past communication from getting decrypted in the future, in the event that the session key for that communication is compromised by cybercriminals.

4.2.3. Real-World Application

Today, TLS has become the most popular web security standard in cryptographically enhancing HTTPS to become HTTPS (Figure 14), which runs over TCP port 443, and is widely deployed on many web browsers, such as Google Chrome, Safari and Firefox.

HTTPS ensures that information transmitted between a web browser on a client's machine and a web server across a public network is always encrypted, to prevent anyone from easily snooping or sniffing on the network (CloudFlare, n.d.).

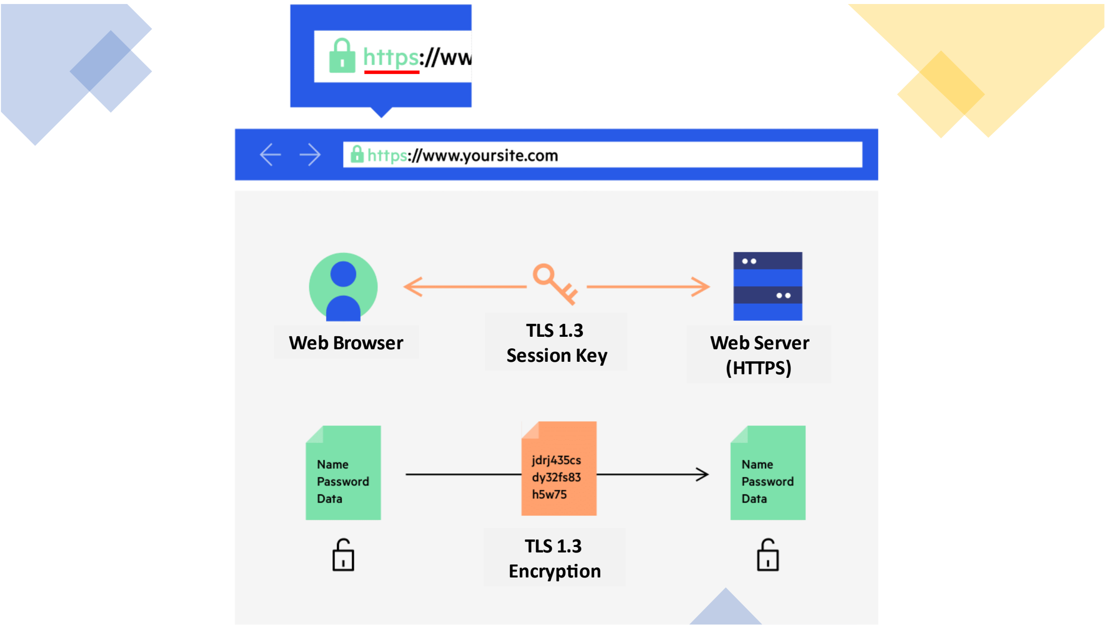
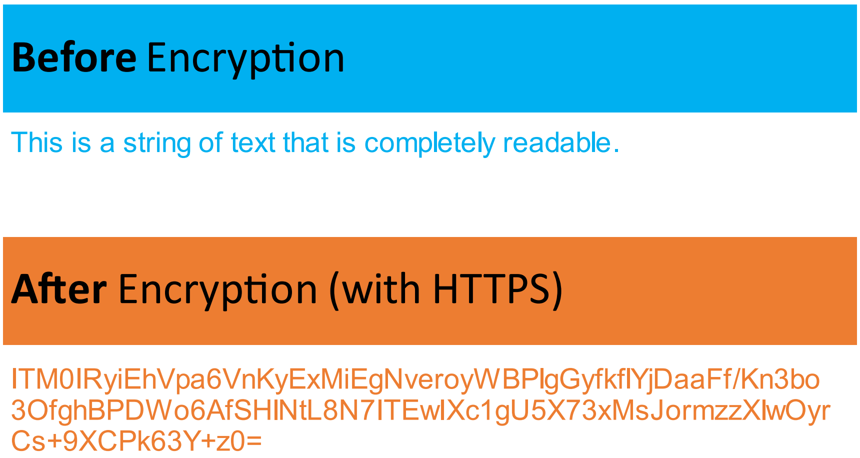


Figure 14: Use of TLS in a HTTPS Connection

Figure 15 provides an example of a sentence before and after HTTPS encryption:



Before Encryption

This is a string of text that is completely readable.

After Encryption (with HTTPS)

ITM0IRyiEhVpa6VnKyExMiEgNveroyWBPlgGyfkflYjDaaFf/Kn3bo
3OfghBPDWo6AfSHINtL8N7ITEwlXc1gU5X73xMsJormzzXlwOyr
Cs+9XCPk63Y+z0=

Figure 15: Plaintext and HTTPS-Encrypted Text

5. Comparison Between Network Security Protocols

Table 3 compares the two network security protocols, IPSec and TLS, in today's context.

	IPSec	TLS
Advantages	- It is transparent to end users. (Simplilearn, 2023) - As it is a Network Layer protocol, it is independent of the applications used and only operating system modifications are needed (Sijin, 2019).	- It is more secure compared to IPSec (N-able, 2019). - It offers lower latency and overhead coming from TLS Handshake Protocol and TLS Record layers (Hussein et al., 2016, p.3) compared to IPSec.
Disadvantages	- It incurs higher latency and overhead coming from IP header addition (for tunnel mode), AH and ESP (Hussein et al., 2016, p.3) compared to TLS. - It is less secure than TLS (N-able, 2019).	- Few platforms support TLS 1.3, since it is harder to integrate into existing systems (Vladimir, 2022) - As it is an Application Layer protocol, it requires modification to applications, on top of the operating system (Sijin, 2019).
Types of Attacks the Protocol is Vulnerable To	- Man-in-the-Middle (MitM) (S & Sankaran, 2023, p.1) - DoS (S & Sankaran, 2023, p.1) - VPN tunnel compromise (S & Sankaran, 2023, p.1) - Cross-protocol attack (S & Sankaran, 2023, p.1)	- Application Layer Protocol Confusion Attack (ALPCA) (S & Sankaran, 2023, p.2) - Reflection ("Selfie") attack (Urien, 2021, p.1) - Bleichenbacher's attack (Cyware Hacker News, 2019) - Forced downgrade attacks (Trend Micro, 2023)

Table 3: IPSec and TLS Advantages & Disadvantages

6. The Future of Network Security

Technological advancements and evolving cyber threats are and will continue to be the norm in the digital real. Thus, the security infrastructure must be made more robust and adaptable than ever before. Ultimately, individuals and organizations should practise good cyber hygiene and adopt proper network security measures to safeguard their digital infrastructure.

Today, with Artificial Intelligence (AI) and Machine Learning (ML) at the forefront of digital technology, this has sparked new areas of integration in network security solutions, to enhance the adaptability of threat prevention, detection and response within the networks. For instance, both AI and ML can be employed in real-time network traffic analysis and anomaly detection. Moreover, AI can be used in malware analysis and the automation of incident response, whilst ML models can be trained and implemented to predict cybersecurity trends and potential threats (TrollEye Security, 2023).

Such advancements can go a long way in further strengthening the role of network security in the digital realm for the longer term.

7. Conclusion

Network security, being a vital subset of cybersecurity, is constantly evolving in today’s digital world, with its primary role to safeguard our digital infrastructure and create a secure and resilient environment for all. Despite the present challenges and vulnerabilities, network security continues to be imperative in safeguarding against the multifaceted challenges posed by a dynamic and interconnected digital world of the future.

8. References

- Use of GAI to assist in generating key ideas for the Introduction, Significance of Network Security, Network Security Vulnerability Issues and Future of Network Security sections of this paper.
- Accenture Security. (2019). The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study. Retrieved November 24, 2023, from https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf
- Alqaydi, L., Yeun, C. Y., & Damiani, E. (2017). Security enhancements to TLS for improved national control. *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, 274–279. https://doi.org/10.23919/ICITST.2017.8356398
- Al-Salqan, Y. Y. (1997). Future trends in Internet security. *Proceedings of the Sixth IEEE Computer Society Workshop on Future Trends of Distributed Computing Systems*, 216–217. https://doi.org/10.1109/FTDCS.1997.644727
- Chung, J., & Vlajic, N. (2022). Survey of remote tls vulnerability scanning tools and snapshot of tls use in banking sector. *2022 IEEE Conference on Communications and Network Security (CNS)*, 1–2. https://doi.org/10.1109/CNS56114.2022.9947230
- Cloudflare. (n.d.). *What happens in a TLS handshake? | SSL handshake*. Retrieved November 26, 2023, from https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/#:~:text=What%20is%20a%20TLS%20handshake,communication%20session%20that%20uses%20TLS
- Cloudflare. (n.d.). What is IPsec? | How IPsec VPNs work. Retrieved November 24, 2023, from https://www.cloudflare.com/learning/network-layer/what-is-ipsec/#:~:text=Transmission%3A%20Encrypted%20IPsec%20packets%20travel,transport%20protocol%2C%20rather%20than%20TCP
- Cloudflare. (n.d.). *What is TLS (Transport Layer Security)?* Retrieved November 24, 2023, from https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/

- Cyware Hacker News. (2019, February 11). *New variant of Bleichenbacher's attack found impacting the latest TLS 1.3 protocol*. Retrieved November 27, 2023, from https://cyware.com/news/new-variant-of-bleichenbachers-attack-found-impacting-the-latest-tls-13-protocol-d95ab311
- Dufournet, A. (2021, December 7). *What is transport layer security and what does it do?* TheGreenBow. Retrieved November 24, 2023, from https://www.thegreenbow.com/en/ressource/blog-en/why-choose-ipsec-vpns-over-ssl-tls-vpns/#:~:text=Turning%20to%20Internet%20Protocol%20Security,suite%20(TCP%2FIP)
- Forcepoint. (2021, February 17). *What is a network attack?* Retrieved October 26, 2023, from https://www.forcepoint.com/cyber-edu/network-attack
- GeeksForGeeks. (2022, December 3). *How to generate Large Prime numbers for RSA Algorithm*. Retrieved November 25, 2023, from https://www.geeksforgeeks.org/how-to-generate-large-prime-numbers-for-rsa-algorithm/
- Gupta, S. et al. (2023). *Evolving networking technologies: Developments and future directions*. John Wiley & Sons.
- Hoe, K. W. (2021, June 14). *Culture and Cyber Security: How Cultural Tightness-Looseness Moderates the Effects of Threat and Coping Appraisals On Mobile Cyber Hygiene*. [PhD Dissertation, Singapore Management University]. Institutional Knowledge at Singapore Management University. Retrieved September 24, 2023, from https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=1354&context=etd_coll
- Holguin, I., & Errapotu, S. M. (2023). Mitigating common cyber vulnerabilities in dnp3 with transport layer security. *2023 North American Power Symposium (NAPS)*, 1–6. https://doi.org/10.1109/NAPS58826.2023.10318788
- Hussein, A., et al. (2016). Securing diameter: Comparing TLS, DTLS, and IPSec. *2016 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)*, 1–8. https://doi.org/10.1109/IMCET.2016.7777417
- Imperva. (n.d.). *Network Security*. Retrieved October 27, 2023, from https://www.imperva.com/learn/application-security/network-security/

- Joshua, C. (2023, November 21). *What is transport layer security and what does it do?* Avast. Retrieved November 24, 2023, from https://www.avast.com/c-what-is-transport-layer-security
- Ju, J., et al. (2020). Analysis and protection of computer network security issues. *2020 22nd International Conference on Advanced Communication Technology (ICACT)*, 577–580. https://doi.org/10.23919/ICACT48636.2020.9061266
- Juniper Networks. (2021, January 13). *IPsec Security Associations Overview*. Retrieved November 18, 2023, from https://www.juniper.net/documentation/us/en/software/junos/security-services/topics/topic-map/ipsec-security-associations-overview.html
- Kim, C. (2023, June 8). *What Is Perfect Forward Secrecy?* Venafi. Retrieved November 26, 2023, from https://venafi.com/blog/importance-forward-secrecy-tls-13/
- Marin, G. A. (2005). Network security basics. *IEEE Security and Privacy Magazine*, *3*(6), 68–72. https://doi.org/10.1109/MSP.2005.153
- N-able. (2019, April 15). *Difference Between IPsec and SSL*. Retrieved November 26, 2023, from https://www.n-able.com/blog/ipsec-vs-ssl
- Nohe, P. (2019, April 30). Taking a Closer Look at the SSL/TLS Handshake. Hashedout. Retrieved November 26, 2023, from https://www.thesslstore.com/blog/explaining-ssl-handshake/
- Oluwasanmi, R. A. (2023). Network security concepts, dangers, and defense best practical. *Computer Engineering and Intelligent Systems*. https://doi.org/10.7176/CEIS/14-2-03
- Pure Cloud Solutions. (2020, September 2018). *How covid-19 made cyber security a hot topic—Pure cloud solutions*. Retrieved October 23, 2023, from https://www.purecloudsolutions.co.uk/how-covid-19-made-cyber-security-a-hot-topic/
- Rong, K. L. & Djeddai, L. (2016). IPSecOPEP: IPSec over PEPs architecture, for secure and optimized communications over satellite links. *2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, 264–268. https://doi.org/10.1109/ICSESS.2016.7883063

- S, A., & Sankaran, S. (2023). Cross protocol attack on ipsec-based vpn. *2023 11th International Symposium on Digital Forensics and Security (ISDFS)*, 1–6. https://doi.org/10.1109/ISDFS58141.2023.10131787
- Sanoja, D. (2021, August 19). *IPsec Tunnel Mode vs. Transport Mode*. Twingate. Retrieved November 21, 2023, from https://www.twingate.com/blog/ipsec-tunnel-mode
- Sijin, G. (2019, February 13). *Advantages and Disadvantages of IPSec – A quick view*. Bobcares. Retrieved November 27, 2023, from https://bobcares.com/blog/advantages-and-disadvantages-of-ipsec/
- Statista. (2023). Australia: Average Number of Internet-Connected Devices Per Household 2025. Retrieved October 24, 2023, from https://www.statista.com/statistics/1202887/australia-average-number-of-internet-connected-devices-per-household/
- Tawde, S. & Pedamkar P. (2023, March 20). *IPSec*. Educba. Retrieved November 18, 2023, from https://www.educba.com/ipsec/
- Trend Micro. (2023, January 20). *TLS Connection Cryptographic Protocol Vulnerabilities*. Retrieved November 26, 2023, from https://www.trendmicro.com/en_vn/devops/23/a/tls-connection-cryptographic-protocol-vulnerabilities.html
- TrollEye Security. (2023, August 24). *The Role of AI in Cybersecurity*. LinkedIn. Retrieved November 27, 2023, from https://www.linkedin.com/pulse/role-ai-cybersecurity-trolleyesecurity/
- Urien, P. (2021). A new iot trust model based on tls-se and tls-im secure elements: A blockchain use case. *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, 1–2. https://doi.org/10.1109/CCNC49032.2021.9369485
- Visual Edge IT. (2023, May 22). *Security in networking and reasons why it is important for business*. Retrieved October 26, 2023, from https://visualedgeit.com/7-reasons-why-security-in-networking-is-important-for-your-business/#:~:text=Protect%20your%20sensitive%20data&text=If%20you%20lose%20this%20information,prevent%20unauthorized%20access%20and%20breaches

- WatchGuard Help Center. (n.d.). About IPSec Algorithms and Protocols. Retrieved November 28, 2023, from https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/mvpn/general/ipsec_algorithms_protocols_c.html
- Zhang, Y. & Li, Y. (2023). The security and protection of computer network information in the era of big data. *2023 International Conference on Mobile Internet, Cloud Computing and Information Security (MICCIS)*, 168–172. https://doi.org/10.1109/MICCIS58901.2023.00032
- Zheng, R., et al. (2020). Detecting malicious TLS network traffic based on communication channel features. *2020 IEEE 8th International Conference on Information, Communication and Networks (ICICN)*, 14–19. https://doi.org/10.1109/ICICN51133.2020.9205087