ISSN 2616-5775 Vol. 6, Issue 11: 52-59, DOI: 10.25236/AJCIS.2023.061108

Application and Security Analysis of Virtual Private Network (VPN) in Network Communication

Zuhe Liu

Hokuriku University, Kanazawa City, Ishikawa Prefecture, 920-0942, Japan

Abstract: *Virtual Private Network (VPN) is a network technology that has been widely used in Internet communications. This paper conducts an in-depth study of the definition of VPN, the importance of Internet communication, and its practice in application fields such as privacy protection, remote office, geographical location restrictions, and public Wi-Fi security. We also provide an in-depth analysis of VPN security, including a comparison of different encryption protocols, data logging and privacy, potential vulnerabilities and attacks, and the importance of vendor selection. Through real case studies, we explore the security practices of reputable VPN providers and past VPN data breaches to provide users with insights on how to choose a trustworthy VPN provider and manage potential risks. Finally, we summarize the main findings and observations of this paper and propose future research directions, including future trends in VPN technology and further research recommendations. This dissertation all about giving users a clearer picture of how VPN tech works, and ways to boost your internet privacy and security.*

Keywords: *Virtual Private Network (VPN) applications; security; privacy; encryption; communication*

1. Introduction

In today's hyper-connected world, the use of the Internet has become a critical component in the daily operations of individuals and organizations. The Internet's ability to facilitate the exchange of information across vast distances has transformed it into a powerful tool for communication. Nevertheless, this capability also introduces significant privacy and security concerns. As more sensitive data is transmitted online, the risk of unauthorized access and data breaches has escalated, making the security of Internet communication a paramount issue.

1.1 Background: Importance of Internet Communication

The revolution of Internet communication has enabled a global platform where information exchange is instantaneous and borderless. This has profound implications for personal connectivity, business operations, and even state-level governance. The Internet's role in fostering innovation, cultural exchange, and economic development is undeniable. However, this interconnectivity also exposes users to privacy risks and cyber threats. Malicious entities can exploit unprotected communications for nefarious purposes, such as identity theft, espionage, and fraud. Hence, securing Internet communication is not just beneficial but essential for maintaining privacy and safeguarding sensitive information.

1.2 Purpose of the Research

The purpose of this research is to provide an in-depth understanding of the mechanisms through which individuals and organizations can protect their online communications. Specifically, the study focuses on Virtual Private Networks (VPNs) as a pivotal tool for enhancing Internet communication security. By exploring the various applications of VPNs—including privacy protection, remote working, bypassing geo-restrictions, and securing public Wi-Fi connections—this research aims to elucidate the complex landscape of online security. Furthermore, a thorough analysis of VPN encryption protocols, data logging policies, and potential vulnerabilities will be conducted. The ultimate goal is to equip users with the knowledge to select the most secure and reliable VPN services, thereby improving their overall Internet communication security[1].

ISSN 2616-5775 Vol. 6, Issue 11: 52-59, DOI: 10.25236/AJCIS.2023.061108

1.3 Structure of the Thesis

This paper is meticulously structured into six distinct parts:

- **Section 1** introduces the background and sets the stage for the ensuing discussion. It outlines the importance of secure Internet communication and defines the scope and objectives of the research.
- **Section 2** delves into the nuts and bolts of VPN technology. It covers the genesis and evolution of VPNs, the underlying principles that govern their operation, and the various types of VPNs available today.
- **Section 3** examines the multifaceted applications of VPNs. From protecting user privacy against surveillance to enabling remote access to organizational resources, this section discusses how VPNs are instrumental in various scenarios. It also addresses how VPNs help in circumventing geographical content restrictions and safeguarding data on insecure public Wi-Fi networks.
- **Section 4** presents a critical analysis of VPN security. This part evaluates the strengths and weaknesses of different encryption protocols and examines the implications of various data logging practices. It also highlights the potential vulnerabilities that could be exploited by cyberattacks and the significance of choosing a reputable VPN provider.
- **Section 5** provides a comparative analysis of prominent VPN providers. By assessing the security features, privacy policies, and historical reliability of these services, the section offers practical guidance for users looking to select a VPN provider.
- **Section 6** concludes the paper by summarizing the main findings and insights gleaned from the research. It also proposes directions for future studies in the field of Internet communication security.

The subsequent sections will expand upon these foundational components, building a comprehensive narrative that articulates the critical role VPNs play in the current digital age.

2. Basic Concepts of VPN

2.1 Definition of Virtual Private Network (VPN)

Virtual Private Network, or VPN for short, is a network technology that allows a private network connection to be established over the public Internet through encryption and tunneling techniques, which are used to protect the privacy and security of data transmission. It allows users to establish secure communication links between different locations as if they were on the same private network [1].

2.2 Fundamentals of VPN

Virtual Private Networks (VPNs) form the cornerstone of modern digital privacy and security. At its core, a VPN's primary function is to forge a secure and encrypted connection over a potentially unsafe public network, such as the internet. This is accomplished through sophisticated encryption and tunneling protocols that together create a private network from a public internet connection.

Encryption is the process by which plaintext information is converted into a coded format, known as ciphertext, which conceals the data's true content from unauthorized observers. VPNs utilize a range of encryption algorithms, each designed to balance security with performance. The strength of a VPN's encryption can be measured by the complexity of the algorithm used and the length of the encryption key.

Tunneling, on the other hand, is a process that encapsulates data packets within another data packets. This encapsulation process serves as the 'tunnel' through which data travels across the internet. The VPN tunnel hides the underlying data, preventing onlookers from discerning the nature of the transmitted information.

A VPN client first establishes a connection with a VPN server, initiating what is known as a 'VPN handshake'. This handshake involves the authentication of the server and the client using digital certificates and establishes the secure encryption parameters for the session. Upon successful authentication, the VPN tunnel is established, and data can flow through this secure channel[2].

ISSN 2616-5775 Vol. 6, Issue 11: 52-59, DOI: 10.25236/AJCIS.2023.061108

The implications of this technology are profound. In an age where internet service providers (ISPs), government entities, and malicious actors seek to monitor or intercept data, a VPN provides a means of maintaining privacy and security. It ensures that sensitive information such as login credentials, financial data, and personal communications are kept private and secure when transmitted over the internet.

2.3 History of VPNs

The genesis of VPN technology can be traced back to the early 1990s, a time when the internet was burgeoning, and the need for secure remote access to networks became apparent. The initial VPNs were essentially point-to-point connections secured by dedicated lines or through dial-up connections, which were prohibitively expensive and complex to manage.

As the internet gained prominence, VPNs evolved to leverage IP networks, offering a cost-effective and scalable solution for secure communications. The introduction of secure protocols like PPTP (Point-to-Point Tunneling Protocol) in the mid-1990s marked a significant advancement in VPN technology, allowing users to access corporate networks securely over the internet.

The use cases for VPNs expanded rapidly. Not limited to corporate environments, VPNs began to appeal to individual users concerned with privacy and censorship. With the advancement of encryption technologies such as SSL (Secure Sockets Layer) and its successor TLS (Transport Layer Security), VPNs became more robust and easier to use.

Modern VPNs support various protocols, each with unique features and security levels. Protocols such as OpenVPN, L2TP/IPsec, and IKEv2/IPsec offer users options ranging from balanced security and speed to maximum security. Additionally, advancements in cryptographic methods have led to the development of protocols like WireGuard, which aims to streamline the process while enhancing performance and security[3].

Today, the relevance of VPNs extends beyond their initial use case of remote access. They are instrumental in bypassing geo-restrictions imposed by countries and content providers, thus advocating for a free and open internet. In the realm of public Wi-Fi, which is notoriously insecure, VPNs provide a shield against potential threats like man-in-the-middle attacks, ensuring users can browse with confidence.

As internet usage grows, so does the sophistication of threats against privacy and data security. This has led to continuous innovation in VPN technologies, making them a critical tool in the arsenal of individuals and organizations aiming to protect their digital footprint. With the onset of an era where data is considered the new oil, the historical evolution of VPNs reflects an ongoing struggle to maintain control over one's own information in an increasingly interconnected world.

3. Application Areas for VPNs

3.1 Privacy Protection

Application of VPN in privacy protection

Virtual Private Networks (VPNs) play an important role in privacy protection. By connecting to a VPN server, users can hide their real IP address and make their online activities more private. In an age of internet surveillance and data collection, this is important to maintaining personal privacy. And by encrypting communications, VPN protects users' data from being intercepted by third-party observers during transmission [4].

Data Encryption and Privacy Protection

VPNs use strong encryption technologies like AES (Advanced Encryption Standard) to encrypt users’ data traffic. This data encryption ensures user privacy and security. Even if the data is intercepted in transit, only the VPN client and server can decrypt the data. This provides users with additional protection to protect their privacy as much as possible [5].

3.2 Telecommuting and Enterprise Applications

VPN Practices for Enterprise Telecommuting

ISSN 2616-5775 Vol. 6, Issue 11: 52-59, DOI: 10.25236/AJCIS.2023.061108

VPN technology is widely used in enterprises, especially for remote working. Employees can securely access company networks and resources by connecting to the company's VPN, no matter where they are. This teleworking practice makes organizations more flexible, allowing employees to work from anywhere in the world while also protecting network and data security [6].

Applications for Multi-Location Connectivity

Enterprises often have multiple offices or branches, and VPN technology can be used to connect networks in these different locations to form a secure internal network. This enables protected and seamless transfer of data and communications within a company between locations. No matter where employees are located, they can connect to the corporate network via VPN and access the resources they need.

3.3 Geolocation restrictions and streaming

How VPNs can bypass geolocation restrictions

VPNs can also be used to bypass geo-location restrictions, allowing users to access restricted content. By connecting to a VPN server located in another geographical location, users can hide their true location. And users can unlock geo-restricted content, such as streaming services, websites, or apps in specific countries or regions [7]. For example, a user is located in country A, but wants to watch streaming content from country B. By connecting to a VPN server in country B, users can bypass the geographical restrictions of country A and watch streaming media in country B. This increases the variety and convenience of user content access.

3.4 Public Wi-Fi Security

Importance of VPNs in public Wi-Fi networks

Public Wi-Fi networks often present security risks because they do not have adequate encryption protection. Hackers can exploit these networks to steal users' sensitive information. And using a VPN to connect to public Wi-Fi provides extra security because it encrypts data traffic, making it undetectable to hackers. This helps prevent data breaches and theft of sensitive information.

Enhanced Security and Risk Reduction

Users can increase security when using public Wi-Fi by connecting to a VPN. Even if hackers try to steal data, they can only see the encrypted information but not understand its content. This reduces the risk of users being targeted by cyberattacks and ensures their online experience is more secure.

4. VPN Security Analysis

4.1 Encryption Protocols

Different VPN services use different encryption protocols to protect user data. When choosing a VPN service, it is crucial to understand the differences between these protocols.

Comparison of different VPN encryption protocols

1) OpenVPN: OpenVPN is often considered the most secure and flexible encryption protocol. It uses the SSL/TLS protocol to provide strong encryption and authentication. Due to its open source nature, its code is publicly available for review, making it easier to find and fix potential vulnerabilities[8].

2) L2TP/IPsec: The combination of Layer 2 Tunneling Protocol (L2TP) and IPsec protocol provides good security. However, it may not be as flexible as OpenVPN and may have some impact on connection performance.

3) PPTP: Point-to-Point Tunneling Protocol (PPTP) is relatively weak on security and is no longer recommended because its encryption can be broken relatively easily[9].

4) SSTP: Secure Socket Tunneling Protocol (SSTP) is a Microsoft-developed protocol typically used in Windows systems. It offers a high level of security, but may not be as flexible as OpenVPN[10].

ISSN 2616-5775 Vol. 6, Issue 11: 52-59, DOI: 10.25236/AJCIS.2023.061108

Security and Performance Tradeoffs

Choosing an encryption protocol involves a trade-off between security and performance. Stronger encryption generally requires more computing resources and may have some impact on connection speeds. Users should choose the right protocol based on their needs and threat model. For users who are highly concerned about security, OpenVPN or L2TP/IPsec may be better choices. For performance-focused users, PPTP or SSTP may be more suitable.

4.2 Logging and Privacy

Understanding your VPN provider's data logging policies is critical to user privacy. Different providers have different policies, so users should choose carefully.

VPN provider's data logging policy

Using a VPN can help protect user privacy, but you still need to be cautious. Users should check the provider's privacy policy to see if it logs user activity and connection data. Some providers may log connection times, IP addresses, and other information, while others may promise not to log any data. Users should choose a provider that promises not to log user data and ensures that data is encrypted during transmission. Additionally, changing passwords and credentials regularly is key to keeping your account secure.

4.3 Potential Vulnerabilities and Attacks

Although VPNs provide a certain level of security, there are still potential vulnerabilities and attack methods, and users need to be aware of these potential risks.

VPN vulnerabilities and possible attacks

1) DNS leakage: In some cases, a VPN connection may cause DNS requests to leak a user's real IP address, thereby exposing their online activities [11].

2) WebRTC leakage: WebRTC technology may bypass VPN connections, causing IP address leakage [12].

3) Malware: Malware on a user's device can compromise the security of a VPN connection, so it is crucial to keep the device clean and secure[13].

4) Social engineering: Hackers may try to trick users into obtaining VPN credentials, so users should be wary of social engineering attacks.

Security Policy and Protection

In order to prevent these potential risks, users can adopt the following security strategies to ensure security:

1) Use a VPN client with DNS leak protection.

2) Disable WebRTC or use a browser plug-in to prevent leaks.

3) Regularly scan your device for malware and remove it.

4) Keep your VPN client and operating system updated for the latest security fixes.

5) Be wary of information and requests from unknown sources to avoid becoming the target of social engineering attacks [14, 15].

4.4 Importance of Vendor Selection

Choosing a trustworthy VPN provider is a crucial step in staying safe online. Users should research the reputation and reviews of different VPN providers to understand their service quality and privacy protection policies. Trustworthy providers typically offer strong encryption, have a no-data-logging policy, and professional customer support. Users can also refer to security assessments and reviews to understand the performance and security of different providers [16].

ISSN 2616-5775 Vol. 6, Issue 11: 52-59, DOI: 10.25236/AJCIS.2023.061108

5. Practical Case Studies

5.1 Analysis of VPN Providers

Security Practices of Several Prominent VPN Providers

When choosing a VPN provider, it is crucial for users to understand the security practices of different providers. The following is an overview of the security practices of some prominent VPN providers:

1) ExpressVPN: ExpressVPN uses strong encryption, offers a no-data-logging policy, and has an extensive server network. They also conduct independent security audits to verify their security practices[17].

2) NordVPN: NordVPN uses advanced encryption, offers a no-data-logging policy, as well as an auto-disconnect switch and dual VPN functionality. They have also undergone an independent security audit[18].

3) CyberGhost: CyberGhost emphasizes user privacy and takes extensive technical measures to protect user data. They also have a dedicated no-log server[19].

Vendor's Security Record

Users should also consider the vendor's track record. A supplier's safety record can provide a record of the supplier's past performance. Users can query whether data breaches have occurred in the past to learn how the provider responded. However, past record is no guarantee of that provider's future security, but it can serve as a factor when choosing a VPN provider.

5.2 Data Leakage Incidents

Analyzing Past VPN Data Breach Incidents

In the last year, there have been multiple VPN data breaches, some of which exposed users' privacy. These incidents highlight the vulnerability of VPN services and the importance of providers.

Some of the notable VPN data breaches include:

1) User data stolen from Neopets: a virtual pet platform where nearly 70 million user accounts may have been compromised, including information such as usernames, emails, passwords, birthdays, countries, zip codes and genders, which were sold for four bitcoins.

2) Kiwi Farms' forums were hacked: a community forum known for malice and hate, with 16,000 active users, linked to multiple suicides. The forum was hacked and users' passwords, emails and IP addresses were compromised. Security Lessons and Risk Management.

3) Data ransomed from the Los Angeles Unified School District: One of the largest public school systems in the United States was attacked by the Russian hacker group Vice Society, with 500GB of data encrypted and ransom demanded. The data included passports, social security numbers, tax forms, contracts, legal documents, financial reports, bank accounts, health information, new crown test data, and more.

4) cryptocurrency theft from Crypto.com: a cryptocurrency trading platform that was hacked in January, resulting in the loss of $30 million in cryptocurrencies, including Ether, Bitcoin, and more, for 439 users.

5) Uber's internal network was breached: this is one of the world's largest ride-hailing services that was attacked in September by an 18-year-old hacker who joined the company's internal Slack and sent a data breach message to all employees. The hacker may have been able to access and modify Uber's cloud services, email, cloud storage, and codebase, among other things.Uber also admitted to a data breach in 2016 that affected 57 million users.

6) user data of SuperVPN, GeckoVPN, and ChatVPN was compromised: these are some VPN apps which are used to hide user's online identity and location. They were leaked in 2021 alone with data of 21 million users including full names, usernames, countries, billing details, email addresses, and more. This data was released for free in May 2022 in some Telegram groups[20].

Security lessons and risk management

ISSN 2616-5775 Vol. 6, Issue 11: 52-59, DOI: 10.25236/AJCIS.2023.061108

There are a number of security lessons users can learn from these data breaches. This includes:

1) Not relying on a VPN as the only security measure while taking other security measures to protect privacy.

2) Update your VPN client regularly for the latest security fixes.

3) Choose a VPN provider with a good security record and transparency.

4) Handle personal information carefully to avoid the risk of leakage.

5) Risk management is a key component of online security and users should strive to mitigate potential threats and protect their personal information.

6. Conclusion

6.1 Summary of the thesis

In this article, we first provide an in-depth analysis of the use and security of virtual private networks (VPNs) in Internet communications. We then explored the definition of VPN, the importance of Internet communication, and the purpose of the study. We then examine in detail the basic concepts, application areas, and security analysis of VPNs, including encryption protocols, logging and privacy, potential vulnerabilities and attacks, and the importance of vendor selection. Through real case studies, we analyze reputable VPN providers and past VPN data breaches to provide insights into how to choose a trustworthy VPN provider and how to avoid potential information security risks.

6.2 Future Research Directions

Future trends in VPN technology

As network communications continue to evolve, so does VPN technology. Future research may focus on emerging VPN technologies, such as WireGuard, and VPN applications in Internet of Things (IoT) and 5G networks. In addition, with the development of quantum computing, VPN encryption technology may also face new challenges.

Suggestions for further research

Although this paper has conducted extensive research on VPN applications and security, there are still many future research directions, including the following areas:

1) The impact of user behaviour and habits on VPN usage.

2) The impact of VPNs on network performance, especially in high-speed network environments.

3) The use and challenges of VPNs in government regulatory and censorship environments.

4) Market competition and trends among VPN providers.

In summary, although there are still many issues to be studied in the field of VPN technology and applications, future research will continue to promote the development and improvement of this field.

References

[1] Wood, D., Stoss, V., Chan-Lizardo, L., Papacostas, G. S., & Stinson, M. E. (1988, June). Virtual private networks. In 1988 International Conference on Private Switching Systems and Networks (pp. 132-136). IET.

[2] De Laet, G., & Schauwers, G. (2005). Network security fundamentals. Cisco press.

[3] Daya, B. (2013). Network security: History, importance, and future. University of Florida Department of Electrical and Computer Engineering, 4.

[4] Song, Y., & Hengartner, U. (2015, October). Privacyguard: A vpn-based platform to detect information leakage on android devices. In Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (pp. 15-26).

[5] Paulus, S., Pohlmann, N., Reimer, H., Alkassar, A., Scheibel, M., Stübel, M., ... & Winandy, M. (2006). Security architecture for device encryption and VPN. In ISSE 2006—Securing Electronic Busines Processes: Highlights of the Information Security Solutions Europe 2006 Conference (pp.

ISSN 2616-5775 Vol. 6, Issue 11: 52-59, DOI: 10.25236/AJCIS.2023.061108

54-63). Vieweg.
[6] Thomas, R. K. (2016). Vpn Solutions: Balancing Productivity and Security For Business. Global journal of Business and Integral Security.
[7] Muir, J. A., & Oorschot, P. C. V. (2009). Internet geolocation: Evasion and counterevasion. Acm computing surveys (csur), 42(1), 1-23.
[8] Iqbal, M., & Riadi, I. (2019). Analysis of security virtual private network (VPN) using openVPN. International Journal of Cyber-Security and Digital Forensics, 8(1), 58-65.
[9] Arora, P., Vemuganti, P. R., & Allani, P. (2011). Comparison of VPN protocols–IPSec, PPTP, and L2TP. Department of Electrical and Computer Engineering George Mason University, Project Report ECE, 646.
[10] Lawas, J. B. R., Vivero, A. C., & Sharma, A. (2016, July). Network performance evaluation of VPN protocols (SSTP and IKEv2). In 2016 Thirteenth International Conference on Wireless and Optical Communications Networks (WOCN) (pp. 1-5). IEEE.
[11] Mohaisen, A., & Ren, K. (2017). Leakage of. onion at the DNS Root: Measurements, Causes, and Countermeasures. IEEE/ACM Transactions on Networking, 25(5), 3059-3072.
[12] Hazhirpasand, M., & Ghafari, M. (2018). One Leak Is Enough to Expose Them All: From a WebRTC IP Leak to Web-Based Network Scanning. In Engineering Secure Software and Systems: 10th International Symposium, ESSoS 2018, Paris, France, June 26-27, 2018, Proceedings 10 (pp. 61-76). Springer International Publishing.
[13] Tahir, R. (2018). A study on malware and malware detection techniques. International Journal of Education and Management Engineering, 8(2), 20.
[14] Singh, A. K., Samaddar, S. G., & Misra, A. K. (2012, March). Enhancing VPN security through security policy management. In 2012 1st International Conference on Recent Advances in Information Technology (RAIT) (pp. 137-142). IEEE.
[15] Shan, R., Li, S., Wang, M., & Li, J. (2003, April). Network security policy for large-scale VPN. In International Conference on Communication Technology Proceedings, 2003. ICCT 2003. (Vol. 1, pp. 217-220). IEEE.
[16] Pasley, K. (2014). VPN Deployment and Evaluation Strategy. Information Security Management Handbook, Volume III, 3, 149.
[17] Gao, P., Li, G., Shi, Y., & Wang, Y. (2020, December). VPN traffic classification based on payload length sequence. In 2020 International Conference on Networking and Network Applications (NaNA) (pp. 241-247). IEEE.
[18] Khan, M. T., DeBlasio, J., Voelker, G. M., Snoeren, A. C., Kanich, C., & Vallina-Rodriguez, N. (2018, October). An empirical analysis of the commercial vpn ecosystem. In Proceedings of the Internet Measurement Conference 2018 (pp. 443-456).
[19] Khan, E., Sperotto, A., van der Ham, J., & van Rijswijk-Deij, R. (2023, March). Stranger VPNs: Investigating the Geo-Unblocking Capabilities of Commercial VPN Providers. In International Conference on Passive and Active Network Measurement (pp. 46-68). Cham: Springer Nature Switzerland.
[20] Rutland, D. (2022, December). The 5 Biggest Data Breaches of 2022. MakeUseOf. https://phys.org/news/2023-07-korean-team-room-temperature-ambient-pressure-superconductor.html