Brief Report

Virtual Private Networks: Fundamentals, Security Issues and Solutions

Zulekha Mahmood

University of Bradford, Bradford, United Kingdom; zmahmo35@bradford.ac.uk

Abstract: The recent COVID-19 pandemic has showcased the implications of using virtual private networks (VPNs) as home-working is now common. Establishing the current state of knowledge on VPNs and their processes is vital. This corroborates an up to date understanding on the fundamentals of VPNs and their usage in today's society; it informs on how to better use VPNs too. Insight into the security issues VPNs face and possible solutions to these allows for the identification of gaps for potential future research. Addressing these gaps would then indicate how to further improve VPNs, making sure VPNs are indeed beneficial to users.

Keywords: VPNs; protection; privacy; security; data

1. Introduction

Protection and privacy are key elements we as individuals desire and as the rapid advancement of the internet proves to challenge this, there is a constant battle between the two. Browsing websites continuously poses the risk of personal data and information being stolen or compromised. As we can often find ourselves passing through untrusted networks that can be susceptible to network attacks and allow unauthorized access with the aim of performing malicious activity such as this.

Identity theft is one of the direct effects of a privacy and data breach that can often occur when exposed to the internet too. However, implementing a defence mechanism that fully ensures the privacy of identity on the internet is near to impossible [18]. Therefore, an approach that makes it more difficult for you to be identified and your activity to be tracked is the next best solution. Hence, virtual private networks (VPNs) are go-to services as they provide an encrypted connection that hides location and data to ensure the security of information. Cryptography is an important factor in VPNs with the use of algorithms to certify security [1]. Although, they do not provide true anonymity, VPNs are still commonly utilised.

Interesting uses of VPNs include the privatising of internet activity from internet providers, preventing their profit from your data. Also, the connection to VPNs servers in other countries which displays an IP address within those locations to overcome restrictions placed by countries on viewing certain Netflix shows. Whilst laws are enforced to target providing justice to victims who have been subjected to their data being stolen and their privacy breached, this does not undo the extent of the damage. Cybercriminals will use the data acquired to commit fraud and identity theft; there is no certitude on who or how many individuals will possess the stolen data [19]. If VPNs are not used to increase protection and privacy on the internet, there will be a significant rise in those affected. This is not just limited to individuals but, also employees who can be affected by data loss which can lead to consequential reputational damage for the companies they work at.

The initial popularity of VPNs links to the discovery of their potential to provide the same quality of service as other networks but without any dependencies to use it. Companies' escalating need for the secure transmission of their data across their office locations globally is also a predominant factor. As, VPNs have quickly become an affordable method; they are used by many companies today. This has resulted in the widespread accessibility of VPNs; available to not only organisations but also individuals. Whereas, previously they were constrained to large organisations who could afford the cost of infrastructure [2]. Despite VPNs protection and privatisation of data, they are also affected by security issues outside of their scope such as spoofing, sniffing and the

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 June 2023 doi:10.20944/preprints202306.1105.v1

alteration or deletion of packet data in the network. Attackers can pose as a legitimate user to insert packets or sniff and alter packet data reinstating them into the network along the way [20]. There are solutions to mitigating certain security issues in relation to VPNs and this highlights that VPNs alone can not provide full protection. But, rather a combination of useful services will guarantee privacy and the protection of data.

This paper reviews the fundamentals of VPNs such as controlling the direction of VPN traffic is often referred to as routing and is a part of VPNs operation [3]. It covers definition, services, history, types, benefits/challenges and examples of their use. Delving into the security issues VPNs face and possible solutions to apply, it advises on how to achieve better protection with VPNs. Through discussing best approaches and a variety of perspectives, VPNs effectiveness can be elevated exponentially.

2. Fundamentals of Virtual Private Networks

2.1. Virtual Private Networks Definition and Services

Virtual private networks allow a secure virtual connection to be initiated between private networks over a shared or public network. This connection is encrypted which enables personal devices to send and receive data in a safe way through the internet [4], Figure 1. Internet traffic is hidden, protecting data as it passes through the VPNs server onto the internet; a public network. VPNs provide various security services through a variety of protocols; confidentiality, integrity, authentication, availability and anti-replay [21–23]. Confidentiality is the data encryption process performed to prevent the disclosure of information intentionally and unintentionally.

It uses an encryption algorithm, key and mechanism to replace plaintext with encrypted text; this is then transmitted over the network. This means that it will be incredibly tough for an individual to decipher the text if they happen to obtain it. Integrity refers to the novelty of data; hashing is used to determine a hash value via an algorithm which is transmitted with the data. At the receiver end, the hash value is calculated again using the same algorithm and is compared to the value received. If both values are the same this proves that the data remained consistent during transmission, otherwise the data was compromised and should be discarded. Authentication involves the comparison of credentials provided by the user with those held in a database file if there is a match, access is granted to the user. Availability refers to the users ability to access data or services at any given time during the VPNs connection and anti-replay uses sequence numbers to verify unique packets [4].

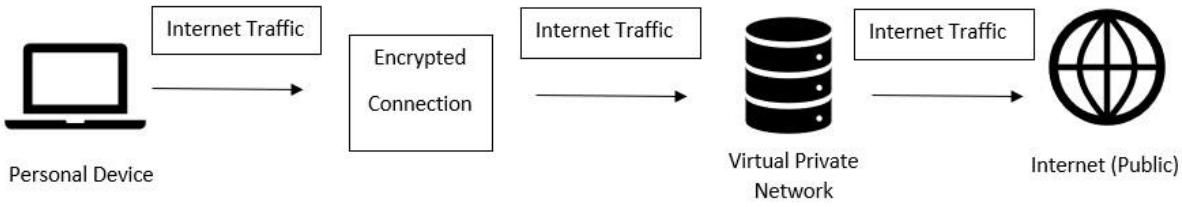

Figure 1. Virtual private network process.

2.2. Virtual Private Networks Origination and Types

Garbis and Chapman [5] indicate VPNs date back to the mid-90's; this is the time period in which they became widely issued and followed on from enterprise networks being favoured. Furthermore, they describe the types of VPNs to be categorized into consumer, enterprise and site-to-site VPNs. Consumer VPNs provide security and privacy of users internet traffic and are typically used to overcome restrictions for example those imposed by internet providers [24–26]. On the other hand,

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 June 2023 doi:10.20944/preprints202306.1105.v1

enterprise VPNs comprise of connections to enterprise networks for remote users. Site-to-site VPNs are a method adopted by enterprises to create wide area networks.

2.3. Benefits and Challenges of Virtual Private Networks

The benefits and challenges of employing VPNs as put forward by Sadiku and Akujuobi [6] is shown in [6], Table 1 below. It is further emphasized that attackers are aware of VPNs popularity with organisations and consequentially are more likely to target them to acquire data; Wi-Fi spoofing is one of the approaches that may be used to succeed in this aim of theirs.

TABLE I
VIRTUAL PRIVATE NETWORKS BENEFITS AND CHALLENGES
(SOURCE: AUTHOR)

Benefits	*Challenges*
Applicability to many businesses	Hidden costs
Reduced cost compared to leased lines	Complexity
Protection/privacy on any network/Wi-Fi hot spot	Administration

Zaman and Mousa [7] derive the notion of VPNs negatively impacting the network performance in terms of an increased time delay in the transferring of packets due to more hops occurring. Their rigorous research focuses on comparing the following three traffic generators, constant bit rate (CBR), file transfer protocol (FTP) and hypertext transfer protocol (HTTP) by varying their application in VPNs and non-VPNs. Throughput and time delay calculations allow for the deeper examination of performance [27]. Their results suggest a constant throughput in the case of CBR and a decrease in the case of FTP and HTTP for both situations and observed time delay increase as a consequence of changing the traffic generators.

2.4. Uses of Virtual Private Networks

VPNs are increasingly used in mobile environments to prevent the internet traffic of users being monitored; hiding their identity and location through encryption. Applications installed from app stores on smartphones allows users to benefit from this capability [8]. Company employees use site-to-site VPNs as they allow connectivity between their varying office locations [9].

The way in which company employees would access a VPNs server whilst being dispersed geographically in terms of office locations is expressed by Zhiwei and Jie [10] and depicts the use of encryption for a secure and private communication tunnel [10], Figure 2.

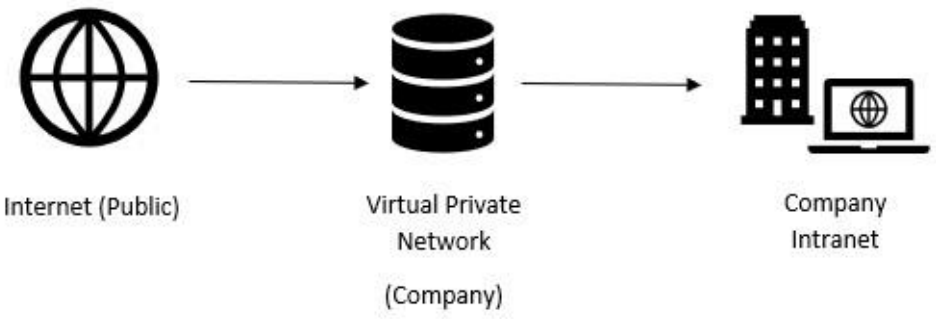

Figure 2. Virtual private network access for company employees.

 doi:10.20944/preprints202306.1105.v1

3. Security Issues and Solutions

Security is a necessary factor to consider when choosing to utilise VPNs; avoiding VPNs that do not serve their purpose is significant [28]. VPNs intention should be to alleviate malicious attacks both internally and externally but, insecure VPNs do more harm than good. Internet security association and key management protocol (ISAKMP), simple key-management for internet protocol (SKIP) are both a part of VPNs technology to ensure there is security of internet communication and user data/information. The former works to avoid password leakage retaining the disclosure of the key whereas, the latter participates in making the key known to users [11].

Jadhav and Sheth [12] disseminate how using VPNs can actually put your security at risk instead of providing protection; as the internet provider is exchanged for the VPNs supplier. The supplier will have access and retain logs of your internet activity whilst you are using the virtual private network. There could also be data leaks due to poorly designed connections and VPNs not using stronger encryption methods would allow attackers to use brute force, intercept and decipher internet traffic to access data. As a user, awareness of VPNs privacy policies is also vital due to essential information on whether logging of activity takes place; this is often not explicitly stated.

There are also external security issues that could affect VPNs, these include drive-by download attacks hidden and downloaded with VPNs when they are installed from app stores on smartphones. Malware such as ransom ware is one such affect of these used to extract money. Man in the middle attacks are another example where attackers take advantage of network connections, intervening between client and user communications [13]. Moreover, website fingerprinting attacks can also affect VPNs and is an area in which VPNs need to have adequate resistance, to avoid internet traffic being recognised [14].

VPNs in university environments propose a connection between campuses and allow sharing of information. An issue faced here is student login credentials as students are able to set their own passwords; too much freedom in this can increase pressure in VPNs management and in turn result in a network/system collapse. Encompassing password restrictions such as a password length can help mitigate this issue [15]. VPNs security can be enhanced by integrating the firewall with complex intrusion detection or prevention systems. Intrusion detection systems contain hardware/software that analyse traffic to and from a network [29–31]. They present alerts and log files if there is any suspected malicious activity in the network; storing these in databases for future reference. Oppositely, intrusion prevention systems focus on directly preventing attacks from occurring in networks. Some of their actions include resetting sessions, dropping packets/sessions and noting the host of the attack [16].

Iqbal and Riadi [17] discuss testing of systems as a solution to understand VPNs security risks and appropriate methods to mitigate these. Analysing VPNs in particular, throughput, delay, packet loss and bandwidth give a detailed outlook on VPNs weaknesses and areas of improvement. Additionally, performing security tests on VPNs linking across servers for data sharing is beneficial along with executing attacks to attain a visual expectation of how VPNs would perform if targeted.

4. Discussion

The evolution of the benefits and challenges of VPNs from various research is clear with them being applicable to nearly all businesses in today's era. Nonetheless, they may still require large amounts of computer power which is expensive and their complexity can be a frustrating factor. The need for experienced network administrators to maintain and manage the networks can also make it difficult for organisations to use them.

The studies above suggest virtual private networks are also subject to security risks whether that be directly through using them or indirectly by attacks that target them. There can be cases in which VPNs in fact lead to your data being compromised, this is because of the exploitation of certain vulnerabilities that a specific virtual private network will have incurred. For instance this may be because of poor encryption standards which arguably appears to be one of the more serious security issues a virtual private network can pose. If VPNs are resulting in loss of your data not only are they negatively impacting you but, they are also committing the exact opposite of their purpose.

 doi:10.20944/preprints202306.1105.v1

Secure VPNs that are well designed to satisfy user needs are important as they retain the reputation and credibility of a virtual private network. A user's positive perspective of VPNs is key in driving up demand; security of VPNs needs to be maintained to evade the viewpoint that VPNs do not provide protection of data and privacy of your identity. Furthermore, suppliers of VPNs need to be clearer in their privacy policies about the handling of user data, as it is not fair to the user to only briefly mention this and decreases trust levels in VPNs services.

The effects of insecure VPNs are not limited to just data loss but also expands to powering down entire networks and systems. A company utilising an insecure virtual private network could potentially have their sensitive company data exposed or lost, severely damaging their reputation and leading to a loss in profit. Recovering from this event would not only be expensive but also require time which could affect the company operation and processes. If this is a software company that is affected for example, their customers may seek software elsewhere and so the effects may be long-term or even permanent.

On the contrary, cybercriminals and attackers will benefit from insecure VPNs. As, this makes it easier for them to perform successful attacks and gain access to sensitive information such as passwords, banking details and more. This information may then be used to impersonate you, make purchases or even sold to others to use.

Attackers will see VPNs as being vulnerable and will target them further, affecting more users, resulting in an increase in victims of fraud or identity theft. This will accumulate pressure on governments with additional people filing reports and in need of compensation for the loss or damage they have suffered. Moreover, the research proposed by Baohui [11] suggests that both ISAKMP and SKIP existing in VPNs guarantee user security in relation to data and information. They are linked to the encryption process and specifically depict key management. Although this may true, it can be argued that these protocols may not be effective when faced with security issues such as weaker encryption methods and brute force attacking [12].

It is evident from the above that strong solutions need to be deployed to evade these issues with VPNs being tested thoroughly before being supplied. Performing security tests allows for a better understanding of weaknesses within VPNs and suggests areas of improvement such as being able to handle large amounts of users. The outcome of this will be long-term trust in VPNs and VPNs being able to perform their purpose effectively. Intrusion detection and prevention systems appear to be a good and worthy solution as they aid in detecting malicious activity before it has taken effect, stopping them at their source. They also prevent attacks in networks; providing extra protection to the user. A hybrid approach combing both would be an ideal strategy to implement.

Taking all of the above into account, there are external security issues that are hard to avoid such as attacks not intended for VPNs specifically but affecting them regardless. The feasible approach with this in mind is to apply the most promising solutions in conjunction with each other to ensure wider security. For example, installing other anti-malware to reduce risk of attacks and increasing user awareness on VPNs security risks as both individuals and employees.

5. Conclusions

VPNs in general are typically successful in verifying privacy and protection of users and their data when traversing through websites online and in accessing company services remotely. However, there are times where they may be insecure due to a large number of internal and external factors. This could be due to poor design of connections/communications, feeble encryption methods or cyberattacks that are not targeted at VPNs but will indirectly affect them too.

This does not eliminate the need for VPNs or discredit their worth as they are still quite useful to individuals and companies. Nevertheless, it does indicate areas for improvement and suggests solutions need to be implemented to strengthen the usefulness and benefits of VPNs to users whilst aiding in decreasing security issues faced. Therefore, it is important to obtain strong VPNs from safe suppliers that have been thoroughly tested and also incorporate multiple approaches such as antimalware, increased user awareness and intrusion detection and prevention systems. As, this will lead to VPNs being truly effective.

It would be highly advantageous to build upon the current conclusions determined through further research in the future. Specifically looking at how often users are in fact affected by insecure VPNs and how serious this issue is. Confirming what the effects are, if they are long-term and the severity is of equal importance. Further denoting whether it is internal or external factors that are more of a cause of concern would be promising.

Conducting user research into the above would be one way of achieving answers to the questions however, it may be difficult to find willing participants. Overall, addressing these areas as future research will further improve the successfulness of VPNs. As, this will enlighten us to the size of impact insecure VPNs are having and whether it is a frequent enough occurrence to warrant a solution. Deciphering whether internal or external factors are the prominent cause will allow for the refocus of research and analysis. So that acceptable approaches can be examined to support in the elimination of users being affected.

Funding:

Institutional Review Board Statement:

Informed Consent Statement:

Data Availability Statement:

Conflicts of Interest:

References

1. W. Easttom, Modern Cryptography: Applied Mathematics for Encryption and Information Security, Cham, Switzerland: Springer, 2021.
2. G. Kuntal, K. Anshuman, G. Jyoti, B. Mohammad, G. Andrei and L. Madhusanka, "A Survey of Virtual Private LAN Services (VPLS): Past, Present and Future," Computer Networks, vol. 196, no. C, pp. 108245 [25 pages], Sept. 2021. doi: 10.1016/j.comnet.2021.108245.
3. I. Ghafir, V. Prenosil, A. Alhejailan and M. Hammoudeh, "Social Engineering Attack Strategies and Defence Approaches." International Conference on Future Internet of Things and Cloud. Vienna, Austria, pp. 145-149, 2016.
4. J. Svoboda, I. Ghafir, V. Prenosil, "Network Monitoring Approaches: An Overview," International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 5(2), pp. 88-93, 2015.
5. Y. F. Khan, "Cisco Secured Virtual Private Networks: A Review," Asian Journal of Computer Science and Technology, vol. 7, no. 2, pp. 30-33, Aug. 2018. doi: 10.51983/ajcst-2018.7.2.1886.
6. Z. Ashraf, Virtual Private Networks in Theory and Practice, Beau Bassin, Mauritius: Scholars' Press, 2018.
7. M. Lefoane, I. Ghafir, S. Kabir, and I. Awan, "Machine Learning for Botnet Detection: An Optimized Feature Selection Approach". International Conference on Future Networks & Distributed Systems. Association for Computing Machinery, New York, NY, USA, 2021.
8. I. Ghafir, M. Hammoudeh, V. Prenosil, L. Han and R. Hegarty, K. Rabie and F. J. Aparicio-Navarro, "Detection of Advanced Persistent Threat Using Machine-Learning Correlation Analysis," Future Generation Computer Systems, vol. 89, pp. 349-359, 2018.
9. J. Garbis and J. W. Chapman, Zero Trust Security: An Enterprise Guide, California, USA: Apress, 2021.
10. S. Eltanani and I. Ghafir. "Coverage Optimisation for Aerial Wireless Networks." 2020 14th International Conference on Innovations in Information Technology (IIT). IEEE, 2020.
11. I. Ghafir, V. Prenosil, M. Hammoudeh and U. Raza, "Malicious SSL Certificate Detection: A Step Towards Advanced Persistent Threat Defence," International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, 2017.
12. M. N. O. Sadiku and C. M. Akujuobi, Fundamentals of Computer Networks, Cham, Switzerland: Springer, 2022.
13. N. Zaman and W. K. Mousa, "Virtual private network impacts on the computer network performance with different traffic generators," IOP Conference Series: Materials Science and
14. Engineering, vol. 881, no. 1, pp. 012126 [7 pages], July. 2020. doi: 10.1088/1757-899X/881/1/012126.
15. S. A. Alashi and H. A. Aldahawi, "Cybersecurity Management for Virtual Private Network (VPN) Applications: A Proposed Framework for the Governance of their Use in the Kingdom of Saudi Arabia," Journal of Information Security and Cybercrimes Research, vol. 3, no. 2, pp. 31-57, Dec. 2020. doi: 10.26735/VSDJ4585.
16. M. Lefoane, I. Ghafir, S. Kabir, I. Awan, "Unsupervised Learning for Feature Selection: A Proposed Solution for Botnet Detection in 5G Networks", IEEE Transactions on Industrial Informatics, 2023.

17. I. Ghafir, V. Prenosil, M. Hammoudeh, T. Baker, S. Jabbar, S. Khalid and S. Jaf, "BotDet: A System for Real Time Botnet Command and Control Traffic Detection," IEEE Access, vol. 6, pp. 1-12, 2018.
18. S. T. Aung and T. Thein, "Comparative Analysis of Site-to-Site Layer 2 Virtual Private Networks," Presented at the 2020 IEEE Conf. on Computer Applications (ICCA), Yangon, Myanmar, February 2728, 2020, pp. 1-5.
19. X. Zhiwei and N. Jie, "Research on network security of VPN technology," Presented at the 2020 Int. Conf. on Information Science and Education (ICISE-IE), Sanya, China, December 4-6, 2020, pp. 539542.
20. S. Baohui, "Computer Network Information Security Protection Based on Virtual Private Network," Journal of Physics: Conference Series, vol. 1646, no. 1, pp. 012121 [6 pages], Sept. 2020. doi: 10.1088/1742-6596/1646/1/012121.
21. R. R. Jadhav and P. S. Sheth, "VPN: Overview and Security Risks," International Journal of Advanced Research in Science, Communication and Technology, vol. 7, no. 1, pp. 305-309, July. 2021.
22. doi: 10.48175/IJARSCT-1649.
23. B. Rama and G. Anup, "Common Vulnerabilities Exposed in VPN – A Survey," Journal of Physics: Conference Series, vol. 1714, no. 1, pp. 012045 [9 pages], Jan. 2021. doi: 10.1088/17426596/1714/1/012045.
24. A. Abdulhamid, S. Kabir, I. Ghafir and C. Lei, "Dependability of the Internet of Things: Current Status and Challenges," International Conference on Electrical, Computer, Communications and Mechatronics Engineering, Maldives, Maldives, 2022.
25. I. Ghafir, J. Saleem, M. Hammoudeh, H. Faour, V. Prenosil, S. Jaf, S. Jabbar and T. Baker, "Security Threats to Critical Infrastructure: The Human Factor," The Journal of Supercomputing, vol. 74(10), pp. 1-17, 2018.
26. K. M. A. Kamal and S. Almuhammadi, "Vulnerability of Virtual Private Networks to Web Fingerprinting Attack," in Advances in Security, Networks, and Internet of Things: Proceedings from SAM'20, ICWN'20, ICOMP'20, and ESCS'20, K. Daimi, H. R. Arabnia, L. Deligiannidis, MS. Hwang and F. G. Tinetti, Eds. Cham, Switzerland: Springer International Publishing, 2021, ch. 2, pp. 147-165.
27. Y. Chengrui, "Application of Virtual Private Network Technology in University Network Information Security," Journal of Physics: Conference Series, vol. 1915, no. 4, pp. 042071 [7 pages], May. 2021. doi: 10.1088/1742-6596/1915/4/042071.
28. A. F. Gentile, P. Fazio and G. Miceli, "A Survey on the Implementation and Management of Secure Virtual Private Networks (VPNs) and Virtual LANs (VLANs) in Static and Mobile Scenarios," Telecom, vol. 2, no. 4, pp. 430-445, Nov. 2021. doi: 10.3390/telecom2040025.
29. M. Lefoane, I. Ghafir, S. Kabir and I. U. Awan, "Multi-stage Attack Detection: Emerging Challenges for Wireless Networks," International Conference on Smart Applications, Communications and Networking, Palapye, Botswana, 2022.
30. I. Ghafir, V. Prenosil, and M. Hammoudeh, "Botnet Command and Control Traffic Detection Challenges: A Correlation-based Solution." International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 7(2), pp. 27-31, 2017.
31. M. Iqbal and I. Riadi, "Analysis of Security Virtual Private Network (VPN) Using OpenVPN," International Journal of Cyber-Security and Digital Forensics, vol. 8, no. 1, pp. 58-65, May. 2019. doi: 10.17781/P002557.
32. I. Ghafir, V. Prenosil, J. Svoboda and M. Hammoudeh, "A Survey on Network Security Monitoring Systems," International Conference on Future Internet of Things and Cloud, Vienna, Austria, pp. 7782, 2016.
33. M. Yazdi, S. Kabir, M. Kumar, I. Ghafir, F. Islam, "Reliability Analysis of Process Systems Using Intuitionistic Fuzzy Set Theory". In: Garg, H. (eds) Advances in Reliability, Failure and Risk Analysis. Industrial and Applied Mathematics. Springer, Singapore, 2023.