**COMP90007 Internet Technologies**

**Project 2**

**Student Name: Handan Yu**

**User Name: HANDANY**

**Student ID: 1235484**

# Introduction

A virtual private network (VPN) is a kind of technology that extends a private network passing through a public network. VPN technology is widely used in business situations to enable users to securely communicate and share data over public infrastructure as if their computing devices, like computer, smartphone, or tablet are directly connected to the private network. Indeed, using VPN brings a quality number of benefits. However, VPN is used to provide data confidentiality, data integrity and user authentication, during that security threats will inevitably occur mainly related to the lack of support for the commonly by tunnel transmission caused by the traditional way of network protocol identification to filter illegal VPN traffic. This report will focus on the technologies to guarantee Internet security from the use of VPN.

In terms of security, VPN is commonly guaranteed by tunnel technology, identity authentication technology and data encryption technology. For tunnel technology, tunnel is created using several protocols. Three familiar used protocols are IPSec, Secure Sockets Layer (SSL) and point-to-point tunneling protocol (PPTP). Regarding to identity authentication technology, biometric authentication is currently the most prevalent authentication technology and the method is either used the Pre-shared Key (PSK) or RSA signature. Also, as for data encryption technology, several encryption algorithms were created, such as Triple Data Encryption Standard (3DES), Advance Encryption Standard (AES), and also Hash algorithms (like Message Digest-5 (MD5) and Secure Hash Algorithm (SHA)). Hence, this report will present the related works on the different methods among these technologies and also compare them.

# Related Work

Nowadays VPN technology has been commonly researched, typically in approaches to guarantee the security from the use of VPN. Based on the methods that were mentioned in the introduction of the report, the increasing number of researchers are also doing researches to improve them.

In terms of tunnel technology, some reports illustrate that although existing protocols indeed achieve the goal to transmit data over a public network for two private networks, the security requirements also cannot be guaranteed. Thus some papers present that adding other protection mechanism with the existing protocols can promote the performance of tunnel technology on the security issues. For instance, Jones et al., 2019 concluded that implementing DOS protection from all directions and including most commercial routers into PPTP VPNs while the client is under attack can improve the security and privacy of the VPN. In order to improve the security and scalability for IoT networks, Shif et al., 2018 introduced a Software-Defined Virtual Private Network (SD-VPN) solution under VxLAN based tunnels. The characteristic of this solutions is the combination of SDN and VPN. Y. Zhou et al., 2020 verified that the insecurity of IPSec VPN using IKEv1 protocol and then presented a denial of service attack method for IKE aggressive mode based on OSPF adjacent route deception, which improve the security from using VPN under IPSec. Based on DPDK technology and man-in-the-middle mechanism, G. Wang et al., 2018 proposed a content audit method for IPsec VPN. So that the protection of information in the audit work can be dealt with.

With regard to identity authentication technology, R. Garg et al., 2015 put forward a mobile phone-based authentication with session key agreement approach that provides strong authentication services to SOCKS V5 protocol and is secure against known attacks. V. Uskov, 2012 implemented experiment on the performance benchmarking of authentication for IPsec-based MVPNs. The report concluded that authentication schemes of both AH and ESP can be used in IPsec. Actually, currently PKI (Public Key Infrastructure) based certificate authentication and user ID/Password authentication are well used. Whereas, those authentication approaches cannot effectively avoid the malicious accesses, in case of password leakage and lost of mobile devices. Fortunately, Y. Jin et al., 2016 propsed an advanced method of VPN authentication using GPS information with geo-privacy protection. Specifically, to protect the user geo-privacy, the hash values of GPS coordinate ranges will be registered on the VPN authentication server. Therefore, using the enhancement method, the risk of intrusion attacks can be decreased significantly.

As for data encryption technology, V. Uskov, 2012 had the experiments on different encryption algorithms and concluded that HMAC(MD5) demonstrated the best performance among MD5, SHA-l, SHA-2–256, and SHA-2–512. Also, H. Qin et al., 2019 designed a point-to-point encryption method for power system communication data based on blockchain technology and proved that the larger the amount of encrypted data is, the more secure the communication data can be, and the stability performance is better than the traditional encryption method. In response to the requirement for confidentiality of data within the power grid, combined with the advantages and disadvantages of existing encryption technologies mentioned in the introduction of this report, R. Liu et al., 2021 proposed a hybrid encryption algorithm that combines PKI technology to enhance the secure transmission of mobile data, which can ensure the security of intranet applications. Furthermore, to optimize the data encryption technology, W. s. Chen et al., 2011 proposed and applied ECC algorithm. The report concluded that using this algorithm can greatly accelerated the data processing speed of the server.

# Comparison of Key Approaches

In this section, the advantages and disadvantages of the security technologies will be discussed and several real-life applications will be demonstrated as well. To improve the technologies, kinds of solutions have been proposed. For different Application scenarios and various Operating Systems, the researchers have attained the amount of experimental results and put forwards a certain number of improvement approaches.

In order to improve the performance of network based on different VPN technologies, L2TP/IPSec combines L2TP's tunnel with IPSec's secure channel has been introduced in A. A. Jaha et al., 2008, which increases the overhead packets and it indeed had a good performance values for both TCP-and UDP-based user applications. By contrast, T. Lackorzynski et al., 2019 argued that the classic solutions such as IPsec exhibited shortcomings in the future, on the other hand, MACsec and Wireguard should be preferred in the future, where and whenever possible. Since according to the experimental results, Wireguard showed the best throughput performance, while MACsec showed the lowest latency on Freescale LayerScape LS1020A, HP ProLiant MicroServer Gen7, Raspberry Pi.

For security issues, Two-Factor Authentication Service (TFAS) was presented by P. N. Thanh et al., 0212. This service is open and highly reliable for VPN because it includes not only the traditional credentials (username and password) but also the second factor. Also it has been implemented and being deployed in a bank (300 concurrent users) with some add-on features and monitoring services to insure the High Availability (HA). However, this service also could not deal with the case of password leakage and lost of mobile devices. Fortunately, Y. Jin et al., 2016 propsed an advanced method of VPN authentication using GPS information with geo-privacy protection.

The security issues exist in many different scenarios. For instance, IoT networks is prevalent currently, while the security issues are still existing at the same time. Therefore, L. Shif et al., 2018 presented a method combines SDN and VPN. This method can improve the security of IoT by separating the VPN traffic and utilizing service chaining. At the same year, A. Arfaoui et al., 2018 presented another solution to solve this problem. The report addressed the adaptive security for VPN tunnel negotiation and proposed a Stackelberg game between a remote user and an IoT gateway to negotiate the security parameters. The above two methods all not only improve the security but also reduce the complexity and cost of operation, since they are all automatic approaches.

To improve the commonly three tunneling technologies, As for operation environment, the results shown in Narayan et al., 2009 indicates that different types of tunneling technologies do not affect the performance of VPN in Linux environment, while the performance of VPN in Window environment are diverse due to using different tunneling technologies.

Additionally, Cloud computing architecture is customary nowadays. Also, VPN plays a key role to keep the private cloud securely. However, with the increasing number of connections, the traditional VPN technologies cannot handle the flexible adjustment feature of cloud computing. Therefore, K. Ishimura et al., 2010  propose dynamic IP-VPN architecture with secure IPsec tunnels. Similarly,

MACsec was consistently best or second best performing solution for latency and Wireguard showed the highest throughput achievable on 4 of 5 platforms.

The classic and well established solutions, like OpenVPN and IPsec, were found to exhibit significant drawbacks in the face of new and upcoming solutions.

Through reading the public resources, this report will compare the three commonly tunneling technologies from two main perspectives, namely performance and application. Then the advanced tunneling technologies proposed nowadays can be ca

In order to

IPSec

the introduction of the virtual interface mechanism makes it likely to process one same packet multiple times, which leads to a waste of time and resources, reduces the throughput of the system, increases the response delays and even may lead to loss of data packets.

# Conclusions and Future Direction

1. In conclusion, this report introduced the concept of VPN. Then the security problem from using VPN was presented and proposed three kinds of common approaches to eliminate this issue or at least decrease the risks of this issue. Through reading the papers related to these three approaches respectively, I found parts of papers experimented on different types of protocols or algorithms under various operation system and discuss their performance. Other parts of papers only discuss how to improve the security of a certain real life application. Also, there are some papers focus on the its application in cloud computing system. Through comparison, to be honest, the better approach to keep security is the most suitable method for a certain application scenario.
2. However, this report only roughly describe and compared several papers’ main ideas. The scope of this research is wide so that the detailed knowledge cannot be covered. In the future research, I aim to study on a certain small field like comparison of these encryption algorithms in remote access VPN environment since more workers nowadays are working remotely from their office.

Future work could include comparison of these algorithms in remote access VPN environment for cabled and wireless network as more workers nowadays are working remotely from their office.

As for different protocols, numerous papers did experiments to analyze the performance evaluation of VPN using three common protocols and used various metrics like throughput, jitter, and delay, RTT and packet loss. Many experimental results shown in their papers indicated that PPTP has the relatively better performance, due to the smallest overhead packets that have been add by PPTP. However, it is vulnerable to meet attack. For example, it is potential to get blocked by firewalls. To solve this problem, J. Jones et al., 2019 suggested that limiting the number of network packets that pass through without replies to prevent DDoS Attack. Additionally, IPsec results in a waste of time and resources and even may lead to loss of data packets because processing one same packet multiple times due to the introduction of the virtual interface mechanism, this disadvantage was proved by Z. Xu et al., 2020. Thanks to J. E. Cruz de la Cruz et al., 2020, proposed OpenVProxy to Provide Confidentiality, Integrity and Availability and this teleworking environment reduce the cost of common openVPN.

## References

J. Jones, H. Wimmer and R. J. Haddad, "PPTP VPN: An Analysis of the Effects of a DDoS Attack," 2019 SoutheastCon, 2019, pp. 1-6, doi: 10.1109/SoutheastCon42311.2019.9020514.

\