**Virtual Private Networks and its Applications**

Samuel Barnes, Ian Schwartz, Jack Stoetzel

Henson School of Science and Technology

Salisbury University

Salisbury, MD, USA

**1 Abstract**

Virtual private networks gives users the ability to privately send information in a secure manner without the harms of accessing information over a public network. Many businesses and large firms use virtual private networks to protect sensitive information as well as give their employees access to information off the grid. The five protocols discussed include; OpenVPN, Secure Socket Tunneling Protocol (SSTP), Layer Two Tunneling Protocol (L2TP), Peer-To-Peer Tunneling Protocol (PPTP), and Internet Key Exchange Version 2 (IKEv2). SSL is known as the Secure Socket Layer and TLS is known as the Transport Security Layer which are both important when discussing common virtual private network protocols.

**2 Introduction**

Frequent internet users may be aware of the safety issues that can arise while using the internet. Viruses that attack personal information have been a long-standing threat prompting users to find safer alternatives for protection. A virtual private network (VPN) offers a method to employ encryption providing secure access to remote computers over the internet. VPN’s are used by employers, students, and everyday users who want to feel safe using the internet. Access to remote computers through a virtual private network makes working from home possible and allows access to information that users can only access on site from virtually anywhere. VPN’s can be broken down into five subtopics including OpenVPN, L2TP, SSTP, IKEv2 and PPTP. Virtual Private Networks are important because it expands the user’s capabilities that would be limited on any other type of network.

**3 Outline**

The outline of this paper will discuss five of the most common virtual private network protocols including the OpenVPN, Layer Two Tunneling Protocol (L2TP), Secure Socket Tunneling Protocol (SSTP), Internet Key Exchange Version Two (IKEv2), and Peer-To-Peer Tunneling Protocol (PPTP). The paper will also include an implementation of how a VPN can be simulated.

**4 OpenVPN**

OpenVPN uses the public internet to create a secure private network that is both economical and isolated. OpenVPN provides all the securities and benefits that virtual private networks offer at the open source level also allowing options for consumers and businesses. The software uses a custom security protocol which utilizes SSL/TLS. SSL is also known as the secure sockets layer and TLS is better known as the transport layer security. Both are cryptographic protocols designed to provide communications security over computer networks. Secure sockets layer preceded the transport layer security and is commonly used for browsing the web, using email, instant messaging, and voice over IP (VoIP). OpenVPN was created by James Yonan and published under the GNU General Public License (GPL). Pre shared secret keys and certificates allows peers to authenticate each other. Pre shared secret keys are the easiest and most used for authentication. OpenVPN uses the OpenSSL library to encrypt data and control channels which allows the use of all different cyphers in the OpenSSL library. [5] OpenVPN can be run over both TCP and UDP for the most optimal use for peers. Security of OpenVPN uses up to 256-bit encryption through the OpenSSL library allowing the fastest available VPN to its users. Running in user space rather than kernel space, OpenVPN has the option to drop root privileges which is a technique that divides up a program limiting each to specific privileges required in order to perform tasks which is often used for security purposes. The extensibility OpenVPN allows for third party applications that can both be called and defined within entry points to extend the advanced logging and enhanced authentication. The platform capabilities of OpenVPN allow for Linux, Mac, Windows, and several other machines. One of the main benefits of the OpenVPN is the cost, the cost for most firmware packages is free to use in open source.

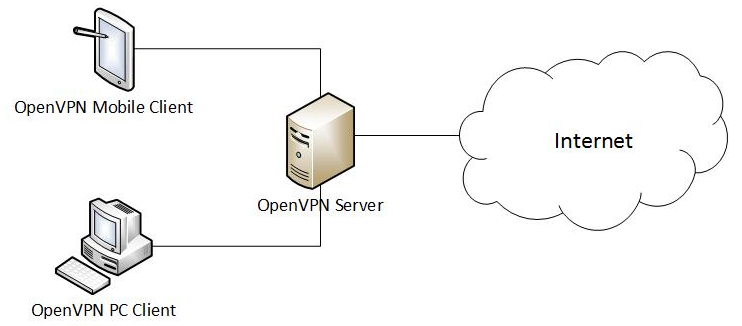


Figure 1: **OpenVPN diagram**

**5 L2TP**

Layer Two Tunneling Protocol (L2TP) is an extension to Point-to-Point Tunneling Protocol (PPTP) that is used by an internet service provider (ISP) to enable the operation of virtual private networks. The L2TP consists of two main components, the L2TP Access Concentrator (LAC) and the L2TP Network Server (LNS). The LAC is the device that physically terminates a call while the LNS is the device that terminates and authenticates the PPP stream. PPP stream is what allows the transmission of multiprotocol packets over layer two links. [2] Under the L2TP configuration, the L2 and PPP endpoints are on the same network access server (NAS). The L2TP uses packet-switched network connections to allow for endpoints to be located between different machines. The user begins with an L2 connection to the access concentrator which then tunnels individual PPP frames to the network access server so packets can be processed separately from location of circuit termination. This eliminates long distance charges because packets can be processes separately.

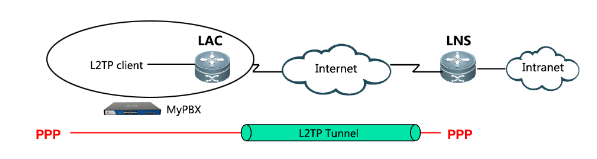


Figure 2: **L2TP how it works**

**6 SSTP**

Secure Socket Tunneling Protocol (SSTP) is a virtual private network tunnel used for transporting PPP traffic through an SSL/TLS channel. SSL/ TSL allows the SSTP to pass through all the firewalls and proxy servers except for authenticating web proxies. SSTP needs to be authenticated for proper use in the SSL/TLS phase. Clients have the option of authenticating during this phase as well but they must also be authenticated in the PPP phase.

[7] The structure of secure socket tunneling protocol uses an SSTP header followed by the bit offset, bits 0-7 used for the version, bits 8-14 used for reserved space, bit 15 for C, and bits 16-31 for the length and all bits following are used for data. The version is used to communicate and negotiate which version of SSTP is being used. The reserved space is allocated for future use and C is the control bit used for determining whether the packet is a control packet or data packet. The length field holds two values, reserved and length. The reserved field is used for future use and the length field is used for the length of the entire packet using up 12 bits length. The data variable is used for when the C bit is set, to hold the SSTP control message. When the C bit is not set, the field is used for a higher level protocol which can only be PPP.

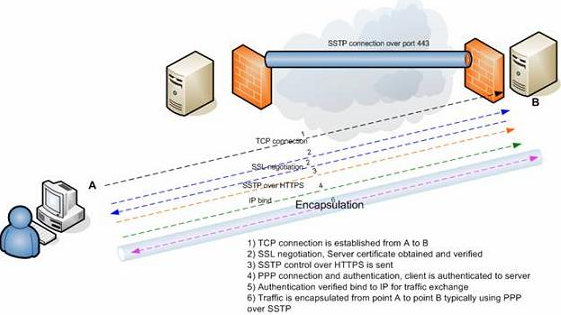


Figure 3: **SSTP implication example**

The control message of SSTP can hold the bit offset, message type, and attribute count followed by the physical attributes. The message type specifies which type of SSTP control message is being communicated holding the type and number of attributes that can be carried by the packet. The attributes count field is only used to specify the number of attributes being used while the attributes field contains the list of attributes associated with the SSTP control message.

**7 IKEv2**

[3] Internet Key Exchange (IKE) is a protocol for security association in the IPsec protocol suite. This protocol builds upon the Oakley protocol that uses X.509 certificates for authentication. Security policies between each and every peer must be done manually which is one of the minor setbacks to this protocol. IKEv2 created fewer RCF’s, standard mobility support, NAT traversal, SCTP support, fewer cryptographic mechanisms, reliability and state management and denial of service. These are the improvement that were made from the unstable release of IKEv1 which was quickly modified with the release of IKEv2. IKEv2 uses several protocol extensions for improvement which makes this protocol one of the better ones to be used in virtual private networks.

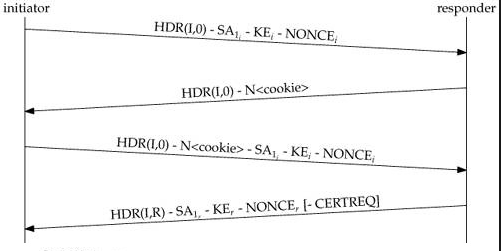


Figure 4: **IKEv2 Packet level exchange**

**8 PPTP**

Point-to-Point Tunneling Protocol (PPTP) is an older method used to implement virtual private networks. The fact that PPTP has several security issues is why this protocol fast became obsolete. PPTP tunnel is used to communicate with the peer on TCP port 1723. After the communication has been instantiated, the TCP connection is used to manage the Generic Routing Encapsulation (GRE) tunnel to the same peer. The GRE packet has a new acknowledgement field rather than the usual routing field in the header of the GRE. Normally, the GRE field are encapsulated within the IP packets and seen to the user as IP protocol 47. The GRE tunnel is then used to carry encapsulated PPP packets allowing tunneling for several different protocols that can be used within PPP.

[6] The security vulnerabilities of PPTP are a result of the underlying PPP authentication protocols used, the overall design of the MPPE protocol, and the integration between MPPE and PPP authentication used in session key establishment. MS-CHAP-v1 is one of these vulnerabilities that can extract the hash passwords from an exchange. Session keys can be analyzed through the streams going in either direction. In version two of MS-CHAP, attacks on captured packets can take place very rapidly before the protocol has time to respond. The brute force attack on the MS-CHAP was shown to be equivalent to the brute force attack on a single Data Encryption Standard (DES) key. Overall, the security issues of using PPTP protocols created the need for new, more secure protocols for the end user.

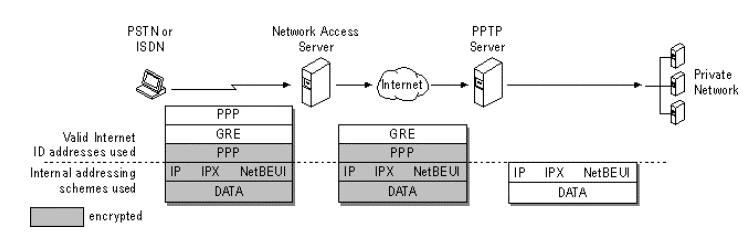


Figure 5: **Multilevel protocol support using PPTP**

**9 Implementation**

Simulating a virtual private network on a schools network can be rather difficult when it comes to accessibility and freely navigating on the server. Therefore, implementing a virtual private network that can encipher a message and pass that message between nodes is the route we chose to take. Our python program sends an enciphered message from one node to another node with no direct link to protect against packet sniffing. Packet sniffing is often used by hackers to collect information both sent and received to attain personal information unrightfully. The receiving node will use the cipher algorithm to decipher the message and securely communicate back and forth between different nodes. The act of enciphering and deciphering a message while being sent is how a VPN functions. Therefore by encrypting a message before it is sent and deciphering the encrypted message once the packet has arrived will simulate the functionality of a virtual private network.

One of the issues during the implementation process of a virtual private network is implementing on a school network. Implementing a VPN on a school network was difficult because we had to work around the schools permissions as the school blocked port forwarding on the routers. Therefore, instead of port forwarding, we decided to buy a router from Walmart to try and get around the issue. The problem with buying our own router was the pinging back from a computer. We were able to ping to a computer but pinging back to our own computer proved to be an issue. It was due to this that we could not make a virtual private network to simulate the pinging.

Our implementation of the virtual private network first started with a few functions including one to create a random IP address by randomly using one of eight predefined numbers at the beginning which are not restricted for use an IP address. That number is then followed by three numbers which are chosen randomly during execution of the algorithm. These numbers will never be greater than 255. This will create a realistic IP address for the user, and this IP address will not be theirs. This is used to simulate sending the information from another IP address which is a key feature of VPNs.

The next function uses a simple caesar cipher with a key of 15 to encrypt the message. This cipher algorithm was used for this implementation as this is a simple encryption algorithm which could easily be changed to implement another better encryption algorithm to make the information being sent more safe. However, for our implementation; a caesar cipher was simple enough to show how the encryption of information on VPNs work.

The following function is used to decipher the message that was previously enciphered by the above caesar cipher function. This function will be called once the user has received the message and can safely decrypt the message without the possibility of a hacker attempting to retrieve the information. It is important when this function is called to ensure the one deciphering the message is the correct user trying to receive the message and not someone who is trying to steal the information. Our implementation assumes that only the two nodes using the VPN have the algorithms to encipher and decipher.

After the decipher function, the send to function is used to correctly display where a message should be sent to. If the current node is less than the destination node, then the message should go to a higher node where the current node will be incremented by one. If the current node is greater than the destination node, the current node needs to be decremented by one to send to the previous node. Finally, if the current node is the same as the destination node, then return the current node because the message is not supposed to be sent anywhere and stays at the current node.

After the send to function is the sent from function. This function is to help determine were the sent message came from and if the current node is less than the destination node, then the message came from the current node minus one. If the current node is greater than the destination node, then the message came from a higher node which will be the current node plus one. However, if the current node equals the destination node then the message will go nowhere and the current node is returned.

The print output function prints what happens when nothing needs to be sent. The print start function prints the beginning of the message. While the print send function prints where the message is sent and received from. The print start function prints the IP change followed by the message and where the message is being sent to. Finally, the print end function prints after the message has been received showing where the message came from, the message, and where the message was received at. These help show what the message looks like at each stage of its journey from the start node to the destination node.

The main function initializes the IP addresses as well as the nodes being used for the program. The program prints where the message has started enciphering then calls the appropriate functions to initiate the enciphering of the messages then prints when the message has been received and when the message starts to be deciphered. At then end of the program, there is a series of print statements that prints the encipher in lower case, upper case, and mixed followed by the deciphered message in lower, upper, and mixed cases. These were used to test for correctness of the encipher and decipher functions and will not automatically run as the program will exit before that code is reached.

**10 Conclusion**

The five main protocols of virtual private networks are Peer to Peer Tunneling Protocol, Secure Socket Tunneling Protocol, Internet Key Exchange version 2, OpenVPN, and Layer Two Tunneling Protocol. Each of these protocols are important because they help to protect user information from the dangers of using the internet today. OpenVPN is the most secure virtual private network today as it is the newest and its open source software also provides a level of security in showing the user how their software works before a user decides to use it or not. PPTP is one of the weakest protocols due to its age and its encryption methods as it does not use as strong of an encryption algorithm in hiding the message being sent. With the level of data mining that occurs today, using a virtual private network is important in protecting users important information from being hacked as well as protecting sensitive data. Our implementation of virtual private networks is important because simulates how VPNs work as well as the importance of VPNs and how they can be used to encrypt messages to hide them from packet sniffers. Since our implementation only uses a caesar cipher, it is important to note that our encryption algorithm is not recommended in protecting users’ information from packet sniffers, and it is recommended to use an encryption stronger than the blowfish algorithm when using a real world virtual private network application. The VPNs discussed do use better encryption algorithms, but some are better than others.

**11 Acknowledgements**

[1] “IKEv2 VPN - What Is IKEv2 & Benefits of IKEv2 Protocol.” *Img*, www.purevpn.com/what-is-vpn/protocols/ikev2.

[2] “Layer 2 Tunneling Protocol.” *Wikipedia*, Wikimedia Foundation, 10 Apr. 2019, en.wikipedia.org/wiki/Layer\_2\_Tunneling\_Protocol.

[3] Mocan, Tim. “What Is IKEv2? (Your Guide to the IKEV2 VPN Protocol).” *CactusVPN*, 20 Feb. 2019, www.cactusvpn.com/beginners-guide-to-vpn/what-is-ikev2/.

[4] Mocan, Tim. “What Is L2TP (Layer 2 Tunneling Protocol)?” *CactusVPN*, 25 Feb. 2016, [www.cactusvpn.com/beginners-guide-to-vpn/what-is-l2tp/](http://www.cactusvpn.com/beginners-guide-to-vpn/what-is-l2tp/).

[5] Mocan, Tim. “What Is OpenVPN & How Does OpenVPN Work?” *CactusVPN*, 1 Feb. 2019, www.cactusvpn.com/beginners-guide-to-vpn/what-is-openvpn/#safety.

[6] Mocan, Tim. “What Is PPTP? (Everything You Need to Know).” *CactusVPN*, 22 Jan. 2019, www.cactusvpn.com/beginners-guide-to-vpn/what-is-pptp/.

[7] Mocan, Tim. “What Is SSTP? (Your Guide to the SSTP VPN Protocol).” *CactusVPN*, 5 Feb. 2019, www.cactusvpn.com/beginners-guide-to-vpn/what-is-sstp/.

[8] “Secure Socket Tunneling Protocol.” *Wikipedia*, Wikimedia Foundation, 11 Apr. 2019, en.wikipedia.org/wiki/Secure\_Socket\_Tunneling\_Protocol.

[9] “Virtual Private Network.” *Wikipedia*, Wikimedia Foundation, 2 May 2019, en.wikipedia.org/wiki/Virtual\_private\_network.

[10] “VPN Software Solutions & Services For Business.” *OpenVPN*, openvpn.net/.

[11] “What Is L2TP VPN And How To Setup L2TP with VPN.” *What Is L2TP VPN And How To Setup L2TP with VPN*, www.purevpn.com/what-is-vpn/protocols/l2tp.

[12] “What Is PPTP And How To Setup a PPTP VPN.” *What Is PPTP And How To Setup a PPTP VPN*, www.purevpn.com/what-is-vpn/protocols/pptp.

[13] “What Is SSTP And How To Setup VPN With SSTP.” *PureVPN*, www.purevpn.com/what-is-vpn/protocols/sstp.