Virtual Private Network Security

Seminar

Antonio Aguilar

Seminar in Computer Science – CS4960

Dr. Martin

11/20/2017

Contents

Introduction

Now days a lot of information flows in the internet. This information contains highly personal information like credit card and social security numbers among additional personal information. Businesses and normal users want their information to remain confidential as it travels through the World Wide Web. A way to address this circumstance is by the creation of a Virtual Private Network (VPN).

VPN is a networking architecture which is implemented over public network to support privacy in a shared public network, it emerged as a cost efficient and reliable solution in networking and telecommunication organizations [1]. Businesses leased lines to connect different offices to a main location typically a corporate office, leasing a line can cost a lot of money for a company. Instead of using a leased line a VPN creates a tunnel for the computers to communicate in a network in a secure way. The P in VPN comes from the added protection to make the virtual network private [3].

As an illustration of VPN, if you need the client computer to communicate to a server across the country the client computer would create the tunnel to the server. Once the tunnel is created, the Virtual Private Network would be dodging firewalls and defenses in the network. It's virtually a direct connection from client to server. The VPN connection tunnel between the two computers is known as IP tunnel. Several types of VPNs will be defined to show if a VPN is secure or if we should avoid using a VPN.

Varieties of VPN

Virtual Private Networks come in many different flavors from basic to advance and each one allows you to do similar tasks. We have PPTP (Point-to-Point Tunneling Protocol), L2TP

(Layer 2 Tunneling Protocol), IPsec encapsulation, and Secure Sockets Layer (SSL) Virtual Private Networks among others.

Point-to-Point Tunneling Protocol is an old VPN protocol commonly used by Windows computers. PPTP was developed by Microsoft and Ascend in 1999 [3]. The way PPTP works is by using password authentication. The VPN has two channels, one channel is used to establish a connection with the other computer. The second channel is used to direct the information. The first channel is the control channel and it uses port 1723 over TCP. The second channel uses Generic Routing Encapsulation IP protocol 47. PPTP is consider an insecure VPN because if the password is not strong, it can make the connection insecure. Most PPTP setups use the MS-CHAPv2 protocol for encrypting passwords, and it is this protocol which is fundamentally broken [3].

Layer 2 Tunneling Protocol uses PPTP structures along with Layer 2 Forwarding. We can think of L2TP as a solution to the insecurity of PPTP. L2TP was developed by CISCO Systems [1]. When the tunnel is set up it uses multiple stages of encapsulation. L2TP work along with IPsec to be able to encrypt the information.

IPsec is the standard official of the Institute of Electrical and Electronics Engineers (IEEE) and the Internet Engineering Task Force (IETF). The job of IPsec is to encrypt several layers of information like the User Datagram Protocol (UDP Header), Layer 2 Tunneling Protocol (L2TP header), Point-to-Point Protocol (PPP Header), and the payload. The payload or frame body is the actual data being transmitted, 0-2304 bytes whose structure depends on the application handling the data [4]. IPsec has an additional function build-in for additional security, it contains IPv6. IPv6 holds an Authentication Header (AH) and Encapsulated Security Payload (ESP). ESP makes sure the destination address is protected by using a hash function.

The hash function contains a confidential key that ensures integrity, confidentiality, and authentication of the data packet.

Secure Sockets Layer uses the SSL/TLS protocol. It authenticates the connection by using a username and a password. Most of the time it uses port 443 which is the same port used by Hyper Text Transfer Protocol Secure (HTTPS) in a secure website. An example of a VPN that uses SSL is OpenVPN. In 1999, the Internet Engineering Task Force upgraded SSL 3.0 and named the upgrade TLS, for transport layer security [4].

Some users might confuse OpenVPN with SSL because OpenVPN uses the SSL/TLS protocol. It is worth mentioning that OpenVPN contains an additional feature. OpenVPN uses Hash-based Message Authentication Code (HMAC) in combination with a digest algorithm [3]. Digest algorithm is known as hashing. Hashing makes sure the packet has not been altered so that when the packet arrives to the destination it remains its integrity. If the user wants to use OpenVPN he or she must install the software for the VPN to work, most modern devices already come with the necessary hardware to use this feature. If the device does not come with the necessary hardware, a virtual private network adapter must be used. OpenVPN has the notion of a control channel and a data channel, both of which are encrypted and secured differently [3].

VPN Advantages and Disadvantages

With numerous options of VPNs we can expect advantages and disadvantages on each VPN. As a user, one has to determine what the best VPN is. To determine what type of VPN the user will need to look at the privacy and integrity the data requires. If a company wants to setup their own VPN, the process can be complex because of the different layers of security each VPN has.

On the other hand if it's regular user, who only uses a VPN to keep its information private from other users in the same network the setup process may be fairly simple. A private user will need to purchase the VPN from a company who already did all the setup process in their end. The user may have to install VPN software into their computer or in some case just used the web browser.

Some of the advantages of a PPTP VPN is that it is less of a process to set up because it's included in Windows computers as well as Linux and Mac OS. The PPTP client has been included in Windows ever since 1995 and is still included in most operating systems [3]. Since it's included in most computers most servers also support this feature, it has a wide compatibility. Another advantage for PPTP is that it supports Network Address Translator (NAT). The NAT allows computers to communicate across gateways.

One disadvantage of PPTP is the low security standard. The user only identifies once and the security is based in how strong the password is. Second, it contains security and firewall problems [5]. PPTP cannot warranty the integrity of the information going from one computer to another because it does not have a way of checking to see if the information has been altered. Moreover, PPTP does not have a way to verify the connection is coming from the correct computer.

The benefits of Layer 2 Tunneling Protocol is that it can support multiple protocols by IP or Non-IP networks. It uses multiple levels of encapsulation that are L2TP, UDP (User Datagram Protocol), IPsec (IP security), IP (Internet protocol) and Data-Link [1]. The IPsec is in charge of encrypting the tunnels. The PPP payload is encapsulated with the L2TP header and the UDP header encapsulates both the payload and L2TP. Due to the multiple levels of

encapsulation the data is secure from being altered as it travels through the network to arrive at its final destination.

Despite of all the great benefits L2TP offers it also contains a few drawbacks. Since the information is encapsulated multiple times the performance is reduced because the computer has to go over the different layers to decrypt the information. Another drawback is that less connections of L2TP are supported in a VPN server [5]. The complexity of encapsulation makes the set-up process longer to configure.

Most of the time L2TP uses the encryption of IPsec and it contains many benefits. One of the greater benefits is that it has a build in IPv6. IPv6 is the future of the IP protocol, it was created to address the shortness of IPv4 and security issues. Some of these are the fundamental shortcomings such as being subject to spoofing, eavesdropping, and session hijacking, the IPsec protocol defines a standard means for handling encrypted data [4]. IPv6 takes the integrity and confidentiality to a greater level compare to IPv4. Another benefit of IPsec is able to support multiple encryption algorithms because it was designed to be independent. It allows the client and the server to reach agreement for a supported protocol. This gives the benefit to IPsec to be flexible. The Authentication Header (AH) secures the source and destination address of the IP header by using a hash function with a secret key [1]. An additional benefit of IPsec is that it comes in most operating systems.

IPsec comes with great added security; however, this comes at a price. IPsec is a lot more complex compare to PPTP connections. The performance of the network is reduced do to the complex encryption algorithm. Since IPsec was design based on the IP protocol, it is the only protocol that will be supported. Not all the data may be secure in an organization if the data traffic is in a subnet. The reason for this is because the data would be outside of IPsec. One of

the main disadvantages of IPsec is that many vendors have implemented extensions to the standard, which makes it hard (if not impossible) to connect two IPsec endpoints from different vendors [3].

SSL is used with OpenVPN and one of the advantages of this VPN is that it uses SSL/TLS protocol. This protocol allows Secure Socket Layer to encrypt the information the same way a web browser encrypts the information. SSL operates between applications (such as browsers) and the TCP/IP protocols to provide server authentication, optional client authentication, and an encrypted communication channel between client and server [4]. The client and the server agree in the encrypted algorithm they will use. Some of the protocols the client and the sever negotiate are what type of authentication, the encryption of the session, and the hashing. The process of negotiation is called the cypher suite. Another advantage of OpenVPN using SSL is the channel who carries the data is custom encrypted. This allows for extra security because it allows the organization or the user to come up with their encryption for the data, no one else will know what standard is being used to encrypt the information.

Even though custom encryption can be done in OpenVPN it can also be a disadvantage if the custom encryption is not strong enough. Another drawback is the encryption can only be done in web-based applications because it uses the SSL/TLS protocol. An additional downside in OpenVPN is the requisite of installing a virtual network adapter also known as a tun or tap device. If the user does not have the virtual network adapter because the operating system does not support the VPN it's an inconvenience. The virtual network adapter is the interface between user-level OpenVPN software and the operating system [3]. A drawback to note is the information is only encrypted from the server to the web application, after those two points the information becomes vulnerable to an attack.

Packet Encapsulation Tunnel

An encryption consist in many important layers of security for any virtual private network. It has been mentioned a general idea of different common PVNs used in the world along with the advantages and disadvantages on the distinct virtual private networks. A layer that is worth describing is the IP Tunnel. An IP Tunnel is an IP packet encapsulated in another IP packet [2]. The IP Tunnel is formed from one endpoint to another. When the two endpoints form, both agree the IP protocol they will use.

The Generic Routing Encapsulation (GRE) is an IP packet encapsulation that was developed by Cisco. This type of protocol is commonly used for site to site VPN because it can support many types of protocols. In an IP packet you have the IP source address, the IP destination, and the data that you want to transmit. As an example, the IP source will have an IP address of 10.10.15.2 and the IP destination of 10.10.15.1. The IP source and destination get their IP from the home network 10.x.x.x. The encapsulation is used to transport the data across the networks [2].

The tunnel contains different IP addresses from the IP packet. A tunnel will carry the VPN tunnel source address, tunnel destination address, and the IP packet. Once the packet arrives to the destination address the layer of encapsulation is removed. Since the packet no longer has a layer, the data will show as if it was transported from the home network. As an example, the tunnel will have a VPN tunnel source with IP address 192.168.200.4 and a VPN destination address of 192.168.310.6. The two IP addresses are used to deliver the IP packet. The tunnel includes the actual physical interface IP addresses for the VPN tunnel [2]. There are more complex encapsulations, but this is a good example to show how a VPN tunnel is made along with the encapsulation of information.

VPN Protects

A VPN was developed to connect different sites in different locations that belong to the same organization. Eventually an organization wants this information to travel securely from site to site. The VPN will protect the user in case of wiretapping. Wiretapping is the name given to data interception, often covert and unauthorized [4]. A way to protect against wiretapping is by using a virtual private network that carries the information encrypted.

Encryption is the strongest and most commonly used countermeasure against interception [4]. Another type of attack a VPN protects against is a man-in-the-middle attack. In a man-in-the-middle attack, the attacker will try to altered and mislead two to make them believe they are communicating directly. Because the communication travels through a tunnel encrypted the man-in-the-middle attack will not succeed. There are a lot more attacks where a VPN protects but those are examples to show where a VPN guards the information.

VPN Vulnerability

A VPN is great for transferring information from site to site in an encrypted secure form. However, a site is only protected from attacks in between the two connecting points. Encryption protects the message in transit between two computers, but the message is in plaintext inside the hosts [4]. This makes the information vulnerable inside the host computer. A VPN will not protect the user data from a keystroke logger because the information resides before it enters the encrypted tunnel.

If a company fails to use the appropriate VPN to transfer secure information, then the VPN will not maintain integrity and confidentiality of the data. As an example, in VoIP, even if the voice traffic is solidly encrypted, the source and destination of the phone call will be somewhat exposed through packet headers [4].

Conclusion

In the final analysis, a VPN is a great way to maintain integrity and confidentiality between two end points. There many different types of VPNs and the organization or the user must be able to select the VPN that will fulfill the needs of the organization or user regarding privacy. It has been mention in a brief summary of what some of the advantages and disadvantages of the different VPNs. Basic VPNs like PPTP come included in most operating systems. Complex VPNs like OpenVPN that uses SSL must be set up by and individual and it might require additional hardware.

We know were a VPN can be effective in protecting privacy, but it must also be noted where a VPN fails to protect the information. Since the encryption tunnel is between two end points, attacks to the data before entering the encrypted tunnel makes the data vulnerable. VPNs are vulnerable to keystroke loggers and viruses as an example. Additional measures must be taken to address the vulnerabilities of a VPN.

References

[1] V. V. Singh, K. K., & Gupta, H. (2016). In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies (ICTCS '16). In *A New Approach for the Security of VPN*. Retrieved September 9, 2017. http://dx.doi.org/10.1145/2905055.2905219 [2] Beasley, J. S. (2015). *Practical guide to advanced networking*. Place of publication not identified: Pearson. Retrieved October 1, 2017, from http://proquest.safaribooksonline.com.libproxy.csustan.edu/book/networking/9780132882996

[2] Beasley, J. S., & Nilkaew, P. (2012). *A Practical Guide to Advanced Networking, Third Edition*. Pearson Certification. Retrieved October 1, 2017, from http://proquest.safaribooksonline.com.libproxy.csustan.edu/book/networking/9780132882996

[3] Crist, E. F., & Keijser, J. J. (2015). *Mastering OpenVPN: Master building and integrating secure private networks using OpenVPN*. Birmingham; Mumbai: Packt Publishing. Retrieved October 1, 2017, from http://proquest.safaribooksonline.com.libproxy.csustan.edu/book/networking/vpn/9781783553136

[4] Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). *Security in Computing* (Fifth ed.). Westford, MA: Pearson Education, Inc.

[5] Gupta, H., & Sharma, V. K. (2011). Role of Multiple Encryption in Secure Electronic Transaction. *International Journal of Network Security & Its Applications, 3*(6), 89-96. doi:10.5121/ijnsa.2011.3606