Viewpoints: OpenVPN

October 15th, 2019

CSUF; CPSC 311

Professor Peralta

Group Research Project

Chukwudi Ikem 889294070

David Huang 889433256

Namanh Tran 889433595

Derrick Lee 889227930

Outline

1 Abstract

A VPN is a virtual private network that allows a user to browse the internet securely. There are many different variations of the tool, but most notable is an open-source version called OpenVPN, first developed by James Yonan. OpenVPN is fairly simple to install and use and has a multitude of uses, most notably for network encryption.

2 Introduction

With the increasing capabilities of modern technology, user privacy is becoming more important than ever. Small things, such as connecting to a coffee shop network, could jeopardize your personal information in the form of passwords or banking information. Tracking from your ISP (internet service provider) could record your internet activity to sell your data to big companies. Additionally, search engines, social networks, and even online marketplaces track your activity to personalize the advertisements given to you. This can all be avoided, however, with the use of a VPN, or virtual private network. A VPN is not necessarily a cure-all but can alleviate some of the malicious activity that happens online.

3 The Purpose of VPN

A VPN extends a private network by sending information from a user across the internet to a private server. This server then acts as a proxy to then allow the user to browse the internet anonymously and securely. The connection between the user and the proxy server is typically encrypted to allow for better security, allowing a user to protect

their information and activity better online. This protection acts against companies such as Facebook, Google, Amazon, or even one's ISP from tracking your information to then sell to big advertising companies. Additionally, a VPN may allow for location spoofing. Depending on the location of the proxy server, a VPN user may access websites or content that would not typically be available.

4 The Battle of Security and User Experience

Proprietary software is usually tailored to a specific company; because of that, it typically has its source code hidden from the public. This leaves room for grey areas and trust concerns with the legitimacy of the companies' promise to maintain our privacy. Since companies are tasked to garner revenue, it is hard to imagine one that is solely focused on the maintenance of its customer privacy. OpenVPN ushered in a new generation of VPN that did not tailor simply to one operating system, such as Windows or Mac OS. The consequence of an open-source, cross-platform, non-proprietary VPN (one that is non-specific and transparent) is that it can and will be improved upon as needed by the user. The transparency allows us to gain a deeper understanding of how the virtual private network operates. Often times in the technological realm, we use the idea of abstraction to aid in our understanding of foreign concepts. Although learning about the process can be helpful, knowing the mechanisms of each encryption algorithm will not help it run faster. Instead, to understand OpenVPN, we will dive into what a virtual private network is in general and all the basic machinations which govern it. Reiterating on our definition of a virtual private network, a standard VPN is one that would call upon a "tunnel protocol". This protocol acts as a conduit for information interchange. The data

being transferred encrypted and decrypted by the VPN provider to provide the user with a more secure browsing experience.

4.1 Tunnel Protocols

Normally people use ISPs (internet service providers) to access data throughout the internet. Unfortunately, ISPs are not secure; the data traveling from your device to the service provider and eventually to the internet is not protected. Unprotected data expose potentially sensitive information to anyone interested in finding it. While the average user may not care much about this - it is imperative that our company takes this into consideration. As stated earlier, VPN protocols such as OpenVPN seek to create a tunnel so that incoming and outgoing data takes a much more secure journey to and from the internet. There are many other VPN protocols such as PPTP, SSTP, L2TP, IKEv2, each with its own set of advantages and disadvantages. The choice of VPN protocol and the associated VPN client will directly affect network performance alongside the security and stability of data transfer in different amounts (Lawas et al.).

4.2 Speed Security & Stability

PPTP is known as the point-to-point tunneling protocol. This is traditionally the easiest to setup. While PPTP may appeal to the average user, it is important to note that it is not as secure as other VPN protocols. Being that it loses in security, it does excel in speed because its free encryption does not require as many resources to maintain. Layer 2 Tunnel Protocol (L2TP) is set up similarly to PPTP, except it does not come with an algorithm to encrypt your data. This means if you do not pair it with some encryption

algorithm such as IPSec - it would no longer make sense to maintain the client. L2TP is considered to be more secure than PPTP. Secure Socket Tunnelling Protocol (SSTP) allows data to pass through firewalls (routers that block unauthorized traffic) that block traffic from different protocols. SSTP is owned by Microsoft, and it is, by all means, a very secure protocol. SSTP is thought to be as secure are the Hypertext Transfer Protocol Secure (HTTPS), a common protocol used to secure your data by an "https:/" extension of your web address (Lawas et al.). SSTP utilizes a Secure Socket Layer, which has higher-layer security protocol encryption. In layman's terms, it is "more secure" than PPTP and L2TP. Internet Key Exchange (IKEv2) is similar to L2TP as it does not come with encryption; it needs an algorithm such as IPSec to secure its data. When set up is complete, IKEv2 boasts an even more secure and fast experience than that of SSTP (Lawas et al.). OpenVPN runs in such a way that their tunnels are "camouflaged" between connections which are not using the VPN. The ambiguity of tunnel channels, along with the strong AES Encryption, is why OpenVPN boasts the most privacy and speed of all VPN protocols.

5 OpenVPN's Encryption

OpenVPN uses OpenSSL library provide encryption. In cryptography, an encryption is like a locked door, and you can only get in if you have the "key". The OpenSSL library provides encryption to two parts, data channel and control channel. The purpose of a data channel in a virtual private network is to transfer data from the user's personal computer to the server and transfer data from the server to the user's computer. The control channel allows for a connection between the user and the virtual private

network. These two channels would require encryption to provide privacy. To acquire maximum security in a virtual private network, the provider would need to use two different encryption on these channels. Control channel encryption would rely on Transport Layer Security encryption (TLS). TLS is a handshake encryption would ensure a secure connection between two endpoints, similar to how hypertext transfer protocol (HTTP) would work. While the control channel would require a cipher, handshake encryption (TLS), and hash authentication. The data channel would only require a cipher and hash authentication because it would rely on the handshake encryption provided by the control channel. The OpenVPN can use a different amount of secret key ciphers to encrypt these channels.

To understand this next section, we need to understand two different types of ciphers, secret key cipher, and asymmetric ciphers. A cipher is an algorithm that is used to encrypt and decrypt data. A secret key cipher when the same key (or something similar) that is used to turn text into ciphertext is used to decode the ciphertext. An asymmetric cipher is when a private key is given to both users, and a public key is required to have access to the public to the private key from both users. By default, OpenVPN will use a symmetric cipher, Blowfish, as the default cipher. The main consensus from experts is that Blowfish should not be used as the primary defense due to some security weaknesses. AES is considered an industry-grade cipher. While AES-128 is active, the main consensus is that AES-256 is stronger. These are the two main cipher used for data channel or control channel. For control channels, there are options to use a secret key (alternatively called handshake encryption). RSA and Diffie-Hellman have

been the most used secret key cipher in the past 20 years. Due to security reasons that will be addressed in the next section, these two ciphers should not be used in practice. Elliptic curve Diffie-Hellman are immune to the security problems that RSA and Diffie-Hellman encounter.

6 Security Vulnerabilities

Transport Layer Security (TLS) has a history of security vulnerabilities due to its compression stage. Since OpenVPN relies on TLS, there have been security problems relating to the control channel. In the past, there was an attack called BREACH, which allowed users to read webpage responses from the users if they were receiving from a HyperText Transfer Protocol (HTTP) server. Luckily, HTTP has been slowly phased out replaced by its extension, HyperText Transfer Protocol Secure (HTTPS). Another attack called CRIME attacked TLS to allow hackers to leak information from encrypted packets from the connections. To prevent these attacks, you can turn off compression and only connect to websites that use HTTPS.

Some of the ciphers mentioned in the previous sections are prone to attacks by powerful adversaries. In 2013 Edward Snowden leaked that NSA had tools that can crack many ciphers that VPN use for their data channels and connection channels (Mitchell). For example, RSA and Diffie-Hellman have definitely been unencrypted by the NSA. An adversity like the NSA that has so much computing power and funding from the government it would be hard to prevent. To stop an entity like the NSA from looking at your VPN's activities, hiring experts to build your VPN can provide measures against these types of adversities.

7 How To Install OpenVPN

There are many different ways to install VPNs. Open VPN is a free software tool that is an excellent introduction to VPNs since you do not have to pay for it. It also has plenty of documentation and support from the community. The installation steps vary based on the operating system. For Windows installation, you will need one of the following supported operating systems Windows 10, Windows 8 or 8.1, Windows 7 Service Pack 1, or Windows Vista Service Pack 2. You will also need a username or password for the Access Server you are going to connect to. First, you will need to navigate to the OpenVPN Access Server client web interface and log in. After you log in, then select the windows option and let the download complete. Open and run to start the installation. After the installation is complete, you can access the OpenVPN Connect Client in the system tray. After you will need to download the config file from your VPN provider. Note that Open VPN works like a key to access the VPN. This means you will still need a VPN.

8 Conclusion

Internet security is becoming more critical in today's age with the risk of privacy breaches continuing to increase it a good idea to look into using a VPN. VPN or virtual private network is a software tool that helps the user maintain a secure encrypted network connection. By using a VPN, you can alleviate some malicious activities from happening to you and prevent social networks and search engines from monitoring your activity. A VPN works like a third party that bridges between you and the network you are trying to connect to. By doing this, you can browse the web anonymously and

securely. There are proprietary variates of VPNs; however, there is also a non-proprietary open-source VPN called OpenVPN. Since OpenVPN is a non-proprietary, this means that the community can update the software, and anyone can download the source code. OpenVPN's encryption uses two parts, a data channel and a control channel. The encryption acts like a locked door, and a key is needed to open it. The data channel requires a cipher and hash authentication, while the control channel requires the cipher and hash encryption plus a handshake(TLS) encryption as well. TLS encryption has many vulnerabilities due to its compression stage. TLS makes it difficult for people to view your activity but is not perfect at preventing all attacks. There are many ways to install VPNs. OpenVPN is supported on all Operating Systems. It has plenty of documentation and is updated by the community. Overall, OpenVPN is an excellent tool whether you are looking to get a better understanding of VPN's or looking to protect your privacy.

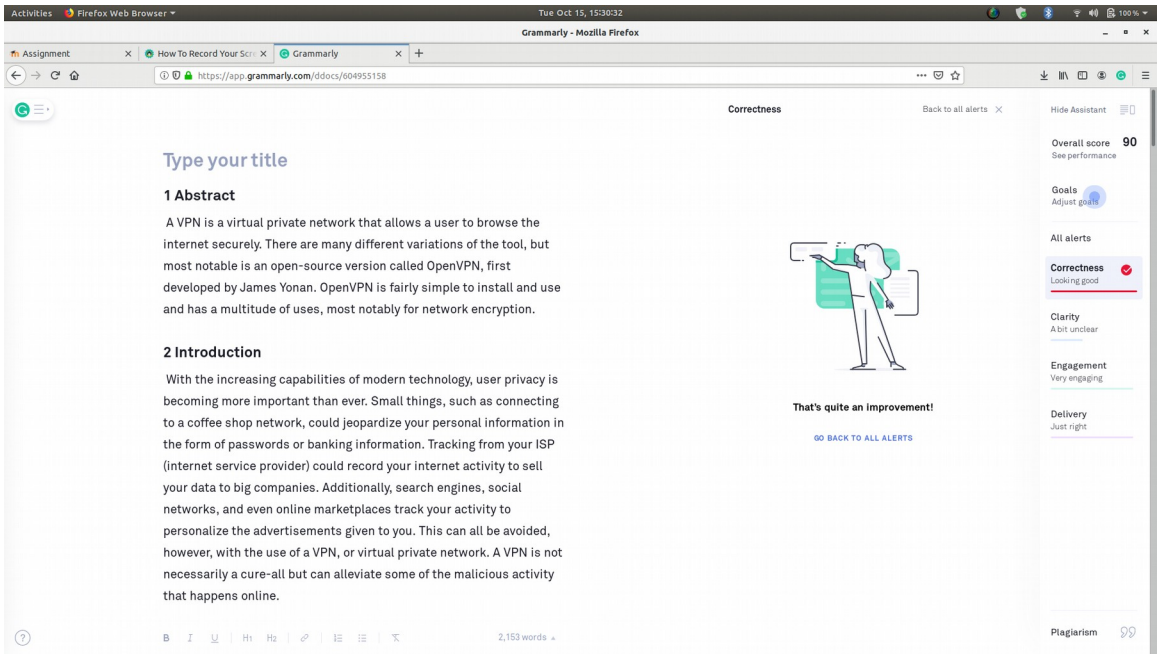
Works Cited

"Guide to Install OpenVPN for Windows." *Install OpenVPN GUI on Windows | OVPN.com*, www.ovpn.com/en/guides/windows-openvpn-gui.

Lawas, Jay R., et al. "Network Performance Evaluation of VPN Protocols (SSTP and IKEv2)." *IEEE Explore*, IEEE, 2016, ieeexplore-ieee-org/document/7759880/citations#citations.

Mitchell, Alex. "A Deeper Look into OpenVPN: Security Vulnerabilities." *SD Times*, 16 Apr. 2019, sdtimes.com/softwaredev/a-deeper-look-into-openvpn-security-vulnerabilities/.

Grammarly



Some discrepancies:

- Grammarly wants us to change secure into secured but SSTP is a defined acronym that stands for Secure Socket Layer.
- Secret key cipher is a specific name for a type of cipher.
- Grammarly wants us to change the word network into system but system is a different definition.