Why VPNs Are Not Completely Secure Solutions for Protecting Your Data

Ryan Luu
Tufts University
December 13th, 2019

Abstract

Internet Service Providers (ISPs) today do not need your permission to monitor your traffic or sell your browsing history and internet data. When you browse the internet, most queries are routed through an ISP's DNS server, which means everything you search can be traced and logged. In efforts to keep private information away from ISPs, users most commonly rely on Virtual Private Networks (VPN) which create encrypted private tunnels to hide your IP address while you browse. Users trust powerhouse VPN companies such as ExpressVPN, NordVPN, IPVanish, and others to completely protect and encrypt their data, but are they completely protected? This paper will discuss the vulnerabilities associated with VPNs, such as the use of remote-access VPNs by employees, the improper storage of session and authentication cookies in memory/log files by VPN companies, and more. We will better understand how VPNs work and explore why they aren't the perfect solution for protecting private information.

I. Introduction

To access the Internet, the vast majority of users must have an Internet service provider that provides them services to access and use the Internet. ISPs such as Verizon or Comcast Xfinity who act as a gateway to the Internet are then able to log and trace all the activity from their customers. In addition, the House of Representatives voted against a set of regulations in 2018, effectively allowing ISPs to sell your personal history with minimal restrictions (Morran). As the need for data privacy is continuing to become more and more relevant, virtual private networks (VPNs) are becoming increasingly recognized as the go-to solution. Everyday users trust VPN providers to protect their data, search history, and Internet activity, but VPNs aren't as safe as they may seem. VPNs, like most technology, have vulnerabilities that can be and will eventually be exposed to the public.

II. To the Community

According to recent statistics, approximately one in four people globally are using VPNs, which means that millions and millions of users are trusting various VPN companies with their

data for different reasons. With this amount of usage, it is surely important that we address and understand how VPNs work and why they are not completely secure.

III. Virtual Private Networks

a. How do VPNs Work?

VPNs route internet connections on devices through whichever VPN server the user has access to. Internet queries are normally routed through an ISP's DNS server, allowing for monitoring and logging of information. However, by using a VPN, the source of the data that is being sent to the Internet comes from the VPN server. VPNs ultimately extend this private network across some public network, creating a "tunnel". In this VPN "tunnel," the data transmitted to the Internet is now encrypted (Hoffman). Instead of seeing the user's own IP address, ISPs will see the IP address of the VPN provider/server.

b. Why do people use VPNs?

In short, data is extremely valuable. There are multiple reasons for wanting to use a private network. Below, I will explore a few of the most common uses:

Hiding Data From ISPs and Third Parties: Millions of users simply want to browse the Internet without having to worry that their interactions and searches are being logged and monitored (Hoffman). In addition, with the Federal Communications Commission's regulations reversed in 2018 by the House of Representatives, ISPs are allowed to sell much more of users' data to third parties—most without even having to inform the user in the first place (Morran). Who would want this information? For starters: advertisers. Advertising thrives with an abundance of consumer data, and to not be a victim of targeted advertising, users may resort to using VPNs. Simply put, many users are (and should be) skeptical of third parties coming in and using their data with whatever intentions they have. In addition to this, there's a huge emphasis on the safety that VPNs provides users. For instance, VPNs may protect against attackers who are snooping over unsecured/public WiFi networks.

Remote Access to Business and/or Personal Networks: Users are able to securely connect to remote servers by using a VPN. With remote-access, employees may securely log into their company server and work remotely. There are actually VPNs designed and built specifically for the use of businesses and corporations. Other users may have their own network setup, in which VPNs are also able to remotely and securely establish a connection.

Bypassing Internet Censorships Imposed by Governments: Many countries have limitations on what they can browse on the Internet, usually restrictions set by their government (Hoffman).

For instance, multiple social media platforms are banned in China as well as in multiple countries throughout Asia. To access websites and networks that are restricted, VPNs are a popular solution.

Bypassing Geographic Restrictions: VPNs allow users to access networks or websites that have a certain geographic restriction. For example, certain Youtube content and Netflix shows are only accessible in specific countries. To bypass this restriction, VPNs can be utilized.

IV. Current Vulnerabilities

a. Improper Storage of Session and Authentication Cookies

The Vulnerability: Multiple instances have been reported of an improper storage of session and authentication cookies. One specific example is the exploitation of various Enterprise VPN applications (namely, Cisco, Palo Alto Networks, Pulse Secure, and F5 Networks). These SSL VPN applications were found to have stored the authentication tokens and/or session cookies insecurely in the memory/log files. Because of this, it gives attackers the ability to steal private credentials to the VPN (Cimpanu).

The Impact: If attackers are successful in retrieving files that contain private credentials, they would be able to access a secure VPN. This could account for attacks such as tampering with configurations and having the ability to connect to a deeper and possibly more secure level of a network.

The Solution: A patch has since been released to address this vulnerability by Palo Alto Networks for its enterprise VPN applications. Other vendors are currently addressing the issue.

b. Sniffing and Hijacking VPN Networks

The Vulnerability: Multiple operating systems have been found to be vulnerable to a new security flaw in which attackers have the ability to sniff, hijack, and ultimately analyze private VPN connections. This flaw was found through Linux, Unix-Based operating systems, MacOS, and Android, where researchers were sending unsolicited network packets to devices of these operating systems on the same network and from there, could learn information about the status of a VPN connection, the IP address of that connection, and which websites were visited.

The Impact: With this information, attackers would be able to inject data into the TCP stream. Knowledgeable attackers would then have enough pieces to be able to hijack the current VPN connection.

The Solution: Researchers have released possible solutions to mitigate this attack, while noting that this attack is quite advanced. For example, a possible solution listed is to turn on the reverse path filtering, with the acknowledgment that this still might not completely protect against this vulnerability (Tolley).

c. NordVPN

The Vulnerability: One of the largest VPN providers, NordVPN, accidentally allowed private internal keys to be exposed and stolen by attackers. This was caused by the installation of an insecure remote management system account on a single server which allowed the attacker to gain access and retrieve internal keys (Whittaker).

The Impact: If internal private keys are compromised by an attacker, it would then be possible to create a server with these same keys to impersonate NordVPN. If the attacker had extraordinary access to a victim's network, an attacker could access user credentials.

The Solution: Encryption of the hard disk of newly built servers.

V. Legal Cases with VPNs and Logs

Many zero log VPN providers make the hefty claim that they won't log anything, ensuring the highest level of security and anonymity by following a "zero log" policy (Summers). However, this did not prove to be the case for VPN provider, PureVPN, in 2017. At that time, a cyberstalker by the name of Ryan Lin took advantage of what he believed to be a "zero log" VPN while he went on to severely harass, cyberbully, and even hack into multiple personal accounts of his victim, stealing and exploiting private content to her contacts. PureVPN claimed to not monitor nor log any activity, stating it would not be possible to trace which user did what activity, yet when the FBI had a lead on the case, PureVPN was able to provide enough information that matched Lin's IP address to multiple gmail accounts where some of his attacks were made. After Lin was identified as the attacker, the US Department of Justice decided on a punishment of 17 years in jail. This incident brings two questions into attention: Are other VPN providers lying about what they promise users? If they are, is it possible to prove this?

VPNs mask users over an encrypted network and are legal to use through multiple countries, but this does not make illegal activity acceptable over these private networks. Incidents such as Lin's case of cyberbullying, and others including hacking, buying/selling on the dark web, and torrenting over a VPN, break the law and come with legal consequences if/when caught.

VI. Defenses

How can data privacy protection get more secure than VPNs? One solution is utilizing the zero trust network model. Companies are beginning to recognize the risks still associated with VPNs and perimeter security, and are being proactive with this mindset. They are turning to the zero trust network model in which much stricter identity verifications are required for every person and device on the network (Libfeld).

Another solution is to explore and utilize the different authentication methods used by VPNs. To add additional layers of security for authenticating users, companies are beginning to use/add methods such as two-factor authentication, risk-based authentication, smart cards, and biometrics (International). Incorporating authentication methods that go beyond just the standard username and password definitely comes with some trade offs, but ultimately will help better secure remote access through VPNs. For instance, because smart cards have the ability to store credentials on a physical piece of hardware, they are consequently more difficult to steal. However, this method adds the risk of possibly losing or misplacing the smart card.

VII. Conclusion

Virtual private networks offer an essential layer of security by encrypting data, hiding IP addresses, and establishing secure network connections. With the ever-increasing need for data privacy, VPNs are gaining popularity every day. In addition to just protecting user data, VPNs are being used by millions of users in various major countries to connect to networks all throughout the world. At some point, it becomes a matter of how researchers, engineers, companies, vendors, and users will be able to quickly and effectively respond to new vulnerabilities that become exploited over time. It is essential to understand how attackers are shaping their attacks, as most of these are based on the various purposes of VPNs. We will need to adapt to new and better methodologies in order to better prevent major data breaches as our world heads into a data-driven society.

VIII. Resources

Cimpanu, Catalin. “New Vulnerability Lets Attackers Sniff or Hijack VPN Connections.” *ZDNet*, ZDNet, 11 Dec. 2019, https://www.zdnet.com/article/new-vulnerability-lets-attackers-sniff-or-hijack-vpn-connections/.

Greenberg, Ran. “VPN Use and Data Privacy Stats for 2019.” *VpnMentor*, VpnMentor, 31 May 2019, https://www.vpnmentor.com/blog/vpn-use-data-privacy-stats/

Hoffman, Chris. “What Is a VPN, and Why Would I Need One?” *How*, How-To Geek, 23 Nov.

2019, https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/.

International, Stronger, and Stronger International. “Authentication Methods for VPNs.” *Stronger Tech Cyber Security IT Training*, https://stronger.tech/authentication-methods-for-vpns/.

Libfeld, Roey. “What Is Zero Trust?: Security Wiki.” *Secret Double Octopus*, https://doubleoctopus.com/security-wiki/network-architecture/zero-trust/.

Morran, Chris. “House Votes To Allow Internet Service Providers To Sell, Share Your Personal Information.” *Consumer Reports*, https://www.consumerreports.org/consumerist/house-votes-to-allow-internet-service-providers-to-sell-share-your-personal-information/.

Summers, Josh. “Zero Log VPN? Your VPN Is Absolutely Lying to You (& What You Can Do).” *All Things Secured*, 11 Nov. 2019, https://www.allthingssecured.com/vpn/truth-about-vpn-logging-policies/.

Tolley, William J. “Oss-Sec: [CVE-2019-14899] Inferring and Hijacking VPN-Tunneled TCP Connections.” *Sec*, https://seclists.org/oss-sec/2019/q4/122.

Tyson, Jeff, et al. “How VPNs Work.” *HowStuffWorks*, HowStuffWorks, 14 Apr. 2011, https://computer.howstuffworks.com/vpn3.htm#.

Whittaker, Zack. “Homeland Security Warns of Security Flaws in Enterprise VPN Apps.” *TechCrunch*, TechCrunch, 12 Apr. 2019, https://techcrunch.com/2019/04/12/enterprise-security-flaws/.

Whittaker, Zack. “NordVPN Confirms It Was Hacked.” *TechCrunch*, TechCrunch, 21 Oct. 2019, https://techcrunch.com/2019/10/21/nordvpn-confirms-it-was-hacked/.