# An Analysis of the Privacy and Security Risks of IOS VPN Permission – Enabled Apps

[1]C.Kesavan, [2]Mr.S.Vijayakumar

**Abstract**—Millions of Users at worldwide resort to mobile VPN clients to either circumvent censorship or to access geo-blocked content and more generally for privacy and security purposes. In this paper we provide a first comprehensive analysis of 6 apps that use IOS VPN permission, which we extracted from a corpus of more than 2.2 million applications available for the iPhone. We perform in light of the Representative decision to allow broadband internet providers to sell your browsing data without your consent, web searches for Virtual Private Network (VPNs) spiked virtually overnight. We perform a number of passive and active measurements designed to investigate a wide range of security and privacy features and to study the behavior of each VPN-based app. We can access a virtual private network (VPN) on your iPhone this enables you to securely access your company`s network behind firewall using an encrypted internet that acts as secure "tunnel" for data. There are many reasons to consider a VPN service for your iPhone or iPad for easy to target for cybercriminal, so you need to protect yourself.

## 1 Introduction

IOS (formerly iPhone OS) is a mobile operating system created and developed by Apple Inc. exclusively for its hardware. It is the operating system that presently powers many of the company's mobile devices, including the iPhone, iPad, and iPod Touch. Originally unveiled in 2007 for the iPhone, iOS has been extended to support other Apple devices such as the iPod Touch (September 2007) and the iPad (January 2010). As of January 2017, Apple's App Store contains more than 2.2 million iOS applications, 1 million of which are native for iPads. These mobile apps have collectively been downloaded more than 130 billion times. Major versions of iOS are released annually. The current version, iOS 11, was released on September 19, 2017. It is available for all iOS devices with 64-bit processors; the iPhone 5S and later iPhone models, the iPad (2017), the iPad Air and later iPad Air models, all iPad Pro models, the iPad Mini 2 and later iPad Mini models, and the sixth-generation iPod Touch. A VPN is a private network that uses a public infrastructure (usually the Internet) to connect remote sites or users.VPN as the name suggest uses "virtual "connections routed through the Internet from the business's private network to the remote site or remote employee. It is a new technology which can be applied to LAN as well as to WLAN. A VPN maintains privacy of data through security procedures and tunneling protocols. In effect, data is encrypted at sender's side and forwarded via "tunnel" which is then decrypted at receiver's side. An additional layer of security can be added by encrypting not only the data, but also the originating and receiving network addresses. Two VPN technologies that are being used are:

### 1.1 Site-to-site VPN

A site-to-site VPN allows multiple offices in fixed locations to establish secure connections with each other over a public network such as the Internet. It also provides extensibility to resources by making them available to employees at other locations.

### 1.2 Remote Access VPN

A remote-access VPN allows individual users to establish secure connections with a remote computer network. These users can access the secure resources on that network as if they were directly plugged in to the network's servers

### 1.3 Third-party user tracking and access to sensitive IOS permissions

Even though 67% of the identified VPN IOS apps offer services to enhance online privacy and security, 75% of them use third-party tracking libraries and 82% request permissions access sensitive resources including user accounts and text messages.

### 1.4 SSL Pinning

Note that some apps implement SSL certificate pinning which means they specifically validate the root certificate. Because the app is itself verifying the root certificate it will not accept Charles`s certificate and will fail the connection. If you have successfully installed the Charles root SSL certificate and can browse SSL websites SSL proxy in Safari, but an apps fails, then SSL pinning is probably the issue.

## 2 Content of Protect VPN for iPhone

In light of the House of Representatives' decision to allow broadband internet providers to sell your browsing data without your consent, web searches for Virtual Private Networks (VPNs) spiked virtually overnight. There are many reasons to consider a VPN service for your iPhone or iPad — if you use public Wi-Fi, for example, you're an easy target for cybercriminals, so you need to protect yourself. VPNs can also help you gain access to region-specific streaming catalogs — like those belonging to Netflix, for instance — even if you're technically located

- [1]*C.Kesavan, Second Year Master of Computer Applications in Priyadarshini Engineering College, Vaniyambadi, E-mail: kesavan.chandran01@mail.com*
- [2]*Mr.S.VijayaKumar, Associate Professor& Head Master of Computer Applications in Priyadarshini Engineering College, Vaniyambadi, E-mail: vijayviswak@mail.com*

outside the coverage area; and they can also help stop your internet service provider (ISP) from throttling your connection without your consent. AVPN most importantly enables you to protect your data from snoopers and mask your true location. It hides your online forays in a secure tunnel that outsiders can't penetrate, but you must choose wisely since you trust your VPN provider with all your online activities. If the service is free, you have to wonder how it's staying afloat. Do some research to make sure the company behind the VPN isn't selling your data or bandwidth to third parties? If you can't, check out the best VPN for the iPhone. If you're looking for additional ways to keep your data private, check out our encryption explainer to find out what it is and why it works. Keep in mind that you may need to install the Open VPN Connect client and follow a guide in order to take advantage of the Open VPN protocol on iOS. All the apps will work with IPSec or another protocol by default. You'll find guides on most of the service provider's websites to do this.

### 2.1 VPN by Nord VPN

Nord VPN is one of the most popular VPNs for Windows and MacOS, and, conveniently, it's also available for iOS. Nord VPN uses the IKEv2 security protocol, which is 30-percent faster than the last generation. The app allows you to browse servers using a map, or a created list of countries. There are currently more than 1,400 available servers spread across 61 countries. You can connect up to six devices with a single account, and bypass blocked websites and regional restrictions with zero lag. Nord VPN does not store any user information either, so your privacy is protected at all times. The app also supports a host of security protocols — including Open VPN, IKEV2, and L2TP — and your real IP address will show as the Nord VPN server IP address, thus securing your browsing experience on the go. Subscriptions vary from $12 a month to $69 annually. Nord VPN even offers a unique, double encryption system that applies military-grade AES-256-CBC encryption to inbound and outbound data twice. A hit with reviewers and users alike, Nord VPN should make anyone's shortlist when looking for a robust VPN solution.

### 2.2 Cyber Ghost VPN

Cyber Ghost is a solid VPN service that offers several options to secure your internet access. First, it protects your Wi-Fi, automatically securing your Wi-Fi connections. The app encrypts all your emails, as well as Messenger, Skype, Viber, and any other messaging app you care to use. Your passwords, payments, and banking are all secured. Not only will it work on Wi-Fi but it will also secure your connections while you're on 4G or LTE. You can select from more than 1,000 servers in more than 30 countries. If you're abroad, you'll be glad to know that it also gives you secure access to streaming services. The service supports PPTP, L2TP/IPSec, and Open VPN protocols and offers up to 256-bit encryption. Cyber Ghost has a decent privacy policy and doesn't log your activity or store personal data. Cyber Ghost VPN has a premium subscription plan that costs $10 per month or $30 per year. It is also compatible with Windows, MacOS, and Android.

### 2.3 Private Internet Access VPN

The Private Internet Access (PIA) Anonymous VPN service remains a popular option on iOS. It offers a decent selection of locations across the world — 27 in all — including some regional options for popular destinations. Speeds are generally fast, and the service supports 256-bit encryption and OpenVPN, though, it recommends 128-bit encryption for speed. It's also based in the United States and promises not to log traffic and VPN usage. While the desktop clients offer all sorts of configuration options, the iOS app is very straightforward. You log in, pick a destination from a list, and away you go. Speed information is an obvious omission, and it does sometimes disconnect you, too. There's no free trial for PIA, but the service does offer a seven-day, money-back guarantee. You can pay $7 a month, $36 for six months, or $40 for the year. That includes support for five simultaneous connections, which makes it good value for the money.

### 2.4 Express VPN

With Express VPN you can connect to servers in 78 countries worldwide. You'll also find support for 256-bit encryption and Open VPN. There's no logging policy, so you can rest assured the service won't log your online activities. It's generally fast and reliable; with good customer support should you need it. The iOS app shows locations in a list or on a map, too, and you can tap to connect. There are nearly 100 regions to choose from, with the option to set your favorite for later. You can try Express VPN for free for one day. After that, subscriptions run $13 a month, $60 for six months, or $100 for the year. There is also a 45-day, money-back guarantee. However, you can only connect to one mobile device and one computer or laptop simultaneously.

### 2.5 IP Vanish VPN

With more than 180 servers in more than 60 countries, you shouldn't have any trouble getting connected with IP Vanish. It promises zero logging, while still managing to offer support for Open VPN and 256-bit encryption. It also allows P2P traffic, which some services block. You'll find the iOS app pretty easy to use. You can browse using location and popular countries. Moreover, regions such as the United States list servers by individual cities. There's little else to it.

It has a wide range of subscription plans starting at $10 a month, $27 for three months, or $75 annually. It provides unlimited bandwidth, but you can only have two simultaneous connections — one Open VPN connection and one other protocol (L2TP or PPTP) connection.

### 2.6 Tunnel Bear VPN

Simple to use and packed with cute bear graphics and puns, Tunnel Bear is quickly becoming a popular iOS VPN app. It offers 256-bit encryption and supports minimal logging, though, it doesn't allow P2P. It offers servers in 15 major countries, and the speeds are generally pretty good. The iOS app runs on the IPSec protocol, but the company's other clients use Open VPN. The app is designed to be simple, requiring you to do little more than tap on a location on the map and wait, as your bear tunnels its way to the new region. The service allows for 500MB a month of free data if you want to try it out before you buy, but premium subscriptions will run you $4 a month or $60 annually for one iOS device. Opting for the more expensive packages will allow up to five simultaneous connections spanning multiple computers and mobile devices.

## 3 Access a VPN on Your IPhone

You can access a virtual private network (VPN) on your iPhone. This enables you to securely access your company's network behind a firewall — using an encrypted Internet connection that acts as a secure "tunnel" for data. The 2.0 version of the iPhone software supports something called Cisco IPSec VPN, which apparently provides the kind of security network administrators want. IPhone also supports VPN protocols known as L2TP (Layer 2 Tunneling Protocol) and PPTP (Point-to-Point Tunneling Protocol).You can configure a VPN on the iPhone by tapping VPN under Network, tapping Add VPN Configuration, and then tapping one of the aforementioned protocols. Then, using configuration settings provided by your company, fill in the appropriate server information, account, password, encryption level (if appropriate), and so on. Better yet, lend your iPhone to the techies at the place you work and let them fill in the blanks on your behalf.

After you've configured your iPhone for VPN usage, you can turn that capability on or off by tapping (yep) the VPN On or off switch inside Settings.

## 4 Static Analysis

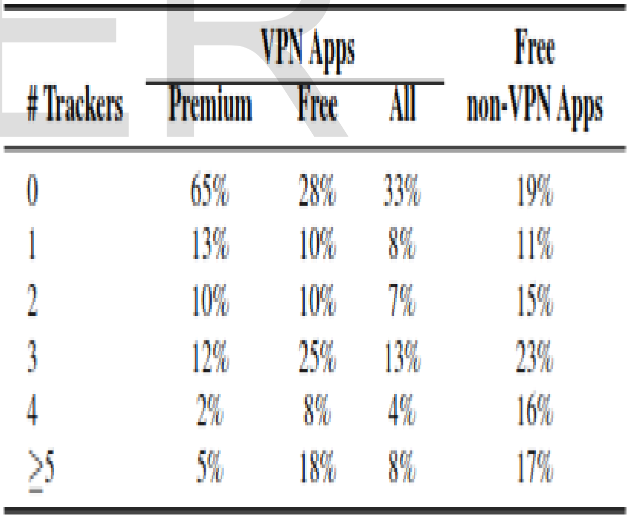
In this section, we analyze the source code for each VPN IOS app using static analysis. In particular, we reporting applications requesting sensitive permission analysis, the presence of tracking libraries in app have decompiled source code and the presence of malware activity according to the online antivirus aggregator, Virus Total.

### 4.1 Permission Analysis

We investigate how VPN-enabled apps request other IOS permissions to access sensitive system resources. We exclude network-related permissions like Internet access which are inherent to any VPN client.

Figure 1 compares the permissions requested by VPN enabled apps with those requested by the top-1,000 free non-VPN IOS apps, which we included for reference. We use the method-to-permission mapping provided by Au et al to investigate the source code segments invoking the methods protected by each IOS permission or instance, in the case of apps requesting the READ_SMS permission, we investigate apps' calls to associated methods such as pre Send SMS Worker (a method used to send SMS which informs the user about the intended or wanted text)and handle SMS Received (a method that handles formatting-related aspects in received SMS) in order to determine the actual use of the permission by the app. There are IOS permissions that are more common on VPN apps than in other app categories. For instance, antivirus and MDM solutions request READ_LOGS permission to inspect other apps' activities. However, we observe that standard VPN clients like Nord VPN and Cyber Ghost VPN also request permission to read system Logs. IOS documentation flags this permission as highly sensitive as any app developer may carelessly misuse IOS's logging capabilities and (unintentionally) expose personal information (including passwords)to any other apps requesting it. Similarly, antivirus apps request READ_EXTERNAL_STORAGE permission to check the stored files for possible virus and malware activity. Much other permission listed in Figure 1 may appear unusual requirements for VPN apps. However, VPN apps may provide additional and richer features to their users beyond a typical VPN tunnel. For each case, we manually checked the Legitimacy of these requests by inspecting the API calls executed by the apps and checking the description for related functionalities without ending any evidence for deliberate abuse of granted permissions. For instance, we found that antivirus apps as well as spyware VPN apps (which we further investigate in Section 4.3) request the READ_SMS permission to read text messages and, in the case of antivirus apps, to scan them for possible malware presence. Similarly, apps requesting READ_CONTACTS incorporate functions incorporate functions in the like of blocking text and calls from specific phone numbers or sharing features through SMS or email.

### 4.2 Tracking Libraries in VPN Apps



| | VPN Apps | | | Free |
|---|---|---|---|---|
| # Trackers | Premium | Free | All | non-VPN Apps |
| 0 | 65% | 28% | 33% | 19% |
| 1 | 13% | 10% | 8% | 11% |
| 2 | 10% | 10% | 7% | 15% |
| 3 | 12% | 25% | 13% | 23% |
| 4 | 2% | 8% | 4% | 16% |
| ≥5 | 5% | 18% | 8% | 17% |

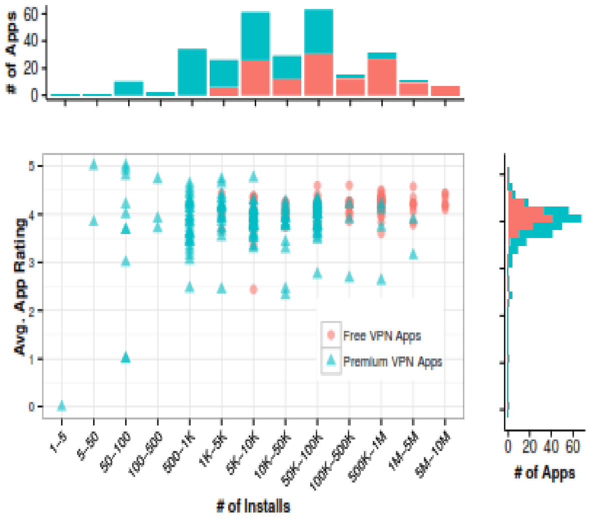
With the help of Apk Tool, we examine the presence of embedded third-party libraries (in the form of external jar files) for analytics, tracking or advertising purposes in the source code of each VPN-enabled app. Therefore, we consider our results as a lower bound of third-party tracking libraries presence in VPN apps. Table 1 compares the number of trackers used by VPN enabled apps with the presence of trackers in the reference set of 1,000 free non-VPN apps. 67% of the VPN apps embed at least one third-party tracking library in their source code. The use of tracking libraries in VPN apps is significantly lower than in the top 1,000 non-VPN apps with an almost 81% of the latter having at least one embedded tracking library.

### 4.3 Table 1: Distribution of third party trackers embedded in VPN apps

The fact that 65% of the premium VPN apps do not have any tracking library embedded (as opposed to only 28% of the free VPN apps) suggests that premium apps do not rely as much as free appson revenues from advertising and analytics services.

### 4.4 User Awareness Analysis

The previous subsection identified instances of VPN apps with malware presence. This section takes a user-centric perspective to understand if they publicly report on their iPhone store reviews any of the privacy and security issues which could be present on VPN apps. Our analysis reveals that VPN apps receive high user ratings:37% of the VPN apps have more than 500K installs and 25% of them have at least a 4-star rating as shown in Figure 2. We cannot distinguish whether Google Play's positive installs and reviews are organic or if they were acquired using paid services to promote app installs To better understand whether real VPN users publicly report any security or privacy concerns after installing and using a given VPN app, we analyze (with manual supervision) 4,593 app reviews with low ratings (i.e., one and two stars) for the 49 VPN apps with more than 1 million installs. Our reasoning to focus our analysis solely on negative app reviews is that users reporting concerning security-related issues will also provide a low app rating.



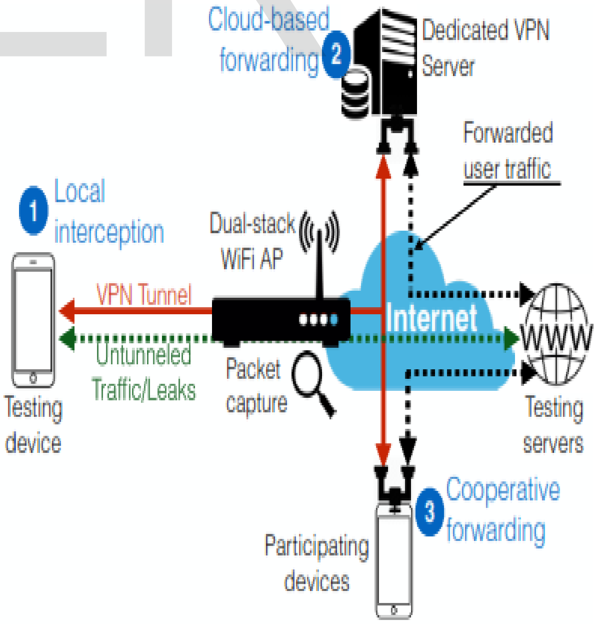
## 5 Network Measurements

In this section, we investigate the runtime and network behavior of 150 VPN apps. In particular we structure our analysis to illuminate the following aspects :( I) the traffic interception mechanisms implemented by each app (i.e., whether the app uses the VPN permission to implement local host proxies or to forward the traffic through a terminating end-point or another peer); (ii) the tunneling protocols implemented by each app as well as developer-induced misconfigurations which may cause traffic leaks; (iii) the presence of proxies and traffic manipulation techniques such as ad-blocking, JavaScript injection and traffic-redirection; and (iv) identify any possible occurrence of SSL interception.

### 5.1 Figure 2: Distribution of app rating vs. installs per VPN app

### 5.2 Figure 3: Our testbed and the 3 possible interceptionand forwarding modes for VPN apps: (1) local interception as a transparent proxy, (2) cloud-based forwarding through a VPN server, and (3) traffic forwarding through a participating node (peer forwarding) or other participating nodes.

We use a dedicated test bed, depicted in Figure 3, composed of a smart phone that connects to the Internet via a computer configured as a Wi-Fi access point (AP) with dual stack support. The Wi-Fi AP runs tcp dump to intercept all the traffic being transmitted between the mobile device and the Internet. This allows us to observe the traffic generated by each VPN app as seen by an in-path of server.



### 5.3 SSL Interception

The SSL VPN Client (SVC) provides a full tunnel for secure communications to the corporate internal network. You can configure access on a user by user basis, or you can create different Web VPN contexts into which you place one or more users.

You can configure SSL VPN technology in these modes:

### 5.3.1 Clientless SSL VPN (Web VPN)

Provides a remote client that requires an SSL-enabled Web browser to access HTTP or HTTPS Web servers on a corporate local-area network (LAN). In addition, clientless SSL VPN provides access for Windows file browsing through the Common Internet File System (CIFS) protocol. Outlook Web Access (OWA) is an example of HTTP access. Refer to Clientless SSL VPN (Web VPN) on Cisco IOS with SDM Configuration Example in order to learn more about the Clientless SSL VPN.

### 5.3.2 Thin-Client SSL VPN (Port Forwarding)

Provides a remote client that downloads a small Java-based applet and allows secure access for Transmission Control Protocol (TCP) applications that use static port numbers. Point of presence (POP3), Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP), secure shell (ssh), and Telnet are examples of secure access. Because files on the local machine change, users must have local administrative privileges to use this method. This method of SSL VPN does not work with applications that use dynamic port assignments, such as some file transfer protocol (FTP) applications. Refer to Thin-Client SSL VPN (Web VPN) IOS Configuration Example with SDM in order to learn more about the Thin-Client SSL VPN.

**Note:** User Datagram Protocol (UDP) is not supported.

### 5.3.3 SSL VPN Client (SVC Full Tunnel Mode)

Downloads a small client to the remote workstation and allows full secure access to resources on an internal corporate network. You can download the SVC to a remote workstation permanently, or you can remove the client once the secure session is closed.

## 6 Limitation and Future work

Our method to identify and characterize VPN apps on iPhone store presents several limitations, many of which are inherent to static and dynamic analysis. The first limitation is app`s coverage: our study is limited to IOS free iPhone store apps and excludes paid apps from alternative app stores.

This paper provides a first detailed analysis of VPN enabled apps but it also leaves many open questions beyond the scope of our analysis. Aspects such as possible traffic or device-location discrimination practices or the use of VPN apps as honey pots to harvest personal information have not been addressed in this study. In addition, reasons behind inadequacy of app actual behavior and terms of use or the identification of side-channels for the observed data-extraction have been left as pending questions.

## 7 Conclusions

IOS app developers benefits from native support to implements VPN clients via the VPN Permission to provide censorship circumvents, support enterprise customers and enhanced online security and privacy. In this paper, we presented a number a static and dynamic methods that allowed us to conduct in-depth analysis of VPN-enabled apps on Google Play. We investigate from the presence of tracking services and malware on VPN app binaries to artifacts implemented by these apps at the network level. Our comprehensive tests allowed us to identify instances of VPN apps embed third-party tracking services and implement abusive practices such as JavaScript injection, ad-redirections and even SSL interception.

## References

[1]Access a VPN on iPhone. http://www.dummies.com/consumer-electronics/mp3players/ipod/how-to-access-a-vpn-on-your-iphone/
[2]Best VPN on IOS.https://www.digitaltrends.com/mobile/best-vpn-for-the-iphone/
[3] SSL Interception. https://www.cisco.com/c/en /us/support/docs/security/ssl-vpn-client/70790-svcios.html
[4]About IOShttps://en.wikipedia.org/wiki/IOS
[5] About VPN https://en.wikipedia.org/wiki/Virtual_private_network
[6]VPN by Nord VPN https://www.digitaltrends.com/mobile/best-vpn-for-the-iphone/
[7]Cyber Ghost VPN https://www.digitaltrends.com/mobile/best-vpn-for-the-iphone/
[8]Private Internet Access VPN https://www.digitaltrends.com/mobile/best-vpn-for-the-iphone/
[9]Express VPN https://www.digitaltrends.com/mobile/best-vpn-for-the-iphone/
[10] IP Vanish VPN https://www.digitaltrends.com/mobile/best-vpn-for-the-iphone/
[11]Tunnel Bear VPN https://www.digitaltrends.com/mobile/best-vpn-for-the-iphone/