VPNalyzer: Systematic Investigation of the VPN Ecosystem

Reethika Ramesh
University of Michigan
reethika@umich.edu

Leonid Evdokimov
Independent
leon@darkk.net.ru

Diwen Xue
University of Michigan
diwenx@umich.edu

Roya Ensafi
University of Michigan
ensafi@umich.edu

***Abstract*—Use of Virtual Private Networks (VPNs) has been growing rapidly due to increased public awareness of online risks to privacy and security. This growth has fueled the VPN ecosystem to expand into a multi-billion dollar industry that sees a frequent influx of new VPN providers. Nevertheless, the VPN ecosystem remains severely understudied, and the limited research concerning VPNs has relied on laborious manual processes. There is a need for a solution which empowers researchers and average users to investigate their VPN providers.**

In this work, we present *VPNalyzer*, a system that enables systematic, semi-automated investigation into the VPN ecosystem. We develop a cross-platform tool with a comprehensive measurement test suite containing 15 measurements that test for aspects of service, security and privacy essentials, misconfigurations, and leakages. Using the *VPNalyzer* tool, we conduct the largest investigation into 80 desktop VPNs.

Our investigation reveals several previously unreported findings highlighting key issues and implementation shortcomings in the VPN ecosystem. We find evidence of traffic leaks during tunnel failure in 26 VPN providers, which seriously risk exposing sensitive user data. We are the first to measure and detect DNS leaks during tunnel failure, which we observe in eight providers. Overall, we find a majority of providers lack IPv6 support, and five even leak IPv6 traffic to the user's ISP. We observe that adoption of practices we consider security and privacy essentials is not uniform across VPN providers. Multiple providers share underlying infrastructure, and 29 providers use third-party, public DNS services. Alarmingly, 10 VPN providers leak traffic even in their most secure configuration, with six leaking data even with a "kill switch" feature enabled. Our results highlight the effectiveness of *VPNalyzer* in finding issues even in the most popular VPN providers. Consumer Reports used *VPNalyzer* in their efforts to create data-driven recommendations for their users.

I. Introduction

Internet service providers, advertisers, and online threat actors are increasingly disrupting, tampering with, and monitoring Internet traffic [17], [48], [78], [81]. High-profile security incidents, widespread reports of ISPs selling data about their users, and the increasing prevalence of geographic discrimination have fueled an increased public awareness of online risks and access restrictions [7], [54], [76]. As a result, the use of virtual private networks (VPNs) has been growing rapidly, not only among activists and journalists but also among average users [4], [6], [30], [51]. This trend has been further accelerated by more people working from home due to the COVID-19 pandemic [31]. Notably, statistics from Egypt, France, the UK, and the US point to a surge in VPN adoption over the past year [53].

Despite being a growing multi-billion dollar [61] industry, the VPN ecosystem remains severely understudied. Previous security evaluations of VPN products [26], [38], [43] have been limited in the scale and types of VPN products analyzed and have used inconsistent heuristics that prevent monitoring of issues in the VPN ecosystem over time. Specifically, the latest reliable investigation into the VPN ecosystem was performed in 2018, as a one-time study of mostly free and trial versions of commercial products [43]. These previous studies, though valuable, all involved a large amount of manual effort.

The VPN ecosystem is extremely dynamic, with constant changes in the features offered with new providers frequently entering the market. This means that a large-scale and continuous empirical assessment of the VPN ecosystem requires methodology that can scale easily across many providers and can be repeated across time, thus making manual investigation as in previous work impractical. Any solution should ultimately empower researchers and average users with an extensible and convenient tool that facilitates investigation into VPN providers.

In this work, we present ***VPNalyzer***—a system that enables systematic, semi-automated investigation into the VPN ecosystem—and perform large-scale empirical assessments of 80 popular VPN providers using *VPNalyzer*. As part of the *VPNalyzer* system, we build a cross-platform tool that has a comprehensive measurement test suite combined with a simple installation and user interface. *VPNalyzer* is also designed to be modular and configurable to facilitate additions and upgrades to adapt to frequent changes of the VPN ecosystem. Our tool is equipped with 15 measurements that test for aspects of service, security and privacy essentials, misconfigurations, and leakages including whether the VPN has implemented an effective mechanism to protect users during tunnel failure. All in all, we cover essential tests from previous work, with six measurements that take direct inspirations, and nine new measurements for which we implement our own methods.

Using the *VPNalyzer* tool, we conduct the largest state-of-the-art investigation into desktop VPNs on both MacOS and Windows, which includes free and paid VPN providers, as well as self-hosted VPN solutions, and our institutional VPN. In total,

Network and Distributed Systems Security (NDSS) Symposium 2022
24-28 April 2022, San Diego, CA, USA
ISBN 1-891562-74-6
https://dx.doi.org/10.14722/ndss.2022.24285
www.ndss-symposium.org

we have 230 experiments from 80 unique VPN providers. This study, in addition to contributing valuable insights about the providers, highlights the value and effectiveness of VPNalyzer.

Our investigation reveals several previously unreported findings highlighting key issues and implementation shortcomings in the VPN ecosystem. Surprisingly, we find that a majority of VPN providers do not support IPv6, and worse, five providers even leak IPv6 traffic to the user's ISP, including our own university VPN. We find evidence of traffic leaks during tunnel failure in 26 VPN providers which seriously risk exposing sensitive user data, especially to adversaries such as governments and ISPs that are capable of inducing such failures. More specifically, we are the first to measure and detect DNS leaks during tunnel failure, which we observe in 8 providers. Further, we observe that multiple VPN providers use the same underlying infrastructure, making colocated servers easier to block, and 29 providers (including paid ones) configure clients to use public DNS services. Two providers do not tunnel all user traffic in their default configuration, which deviates from users' expectation. Finally, we conduct a case study testing custom "secure" configurations of 39 top providers. Alarmingly, even in their secure configuration, 10 VPN providers leak traffic, six of which even had a "kill switch" feature enabled. These results are shocking considering that these VPNs are popular, with millions of users that trust them with sensitive data.

VPNalyzer is designed to empower researchers and users, and to be easily adoptable as a user-friendly tool empowering the community to be vigilant about issues in the VPN ecosystem. Consumer Reports, a leading consumer research and advocacy organization, used VPNalyzer as part of their efforts to produce a data-driven and reliable recommendation for their millions of users [27]–[29]. Following our future public release, we hope that VPNalyzer benefits users and helps the general public choose better VPN providers.

II. Background and Related Work

The VPN ecosystem is especially dynamic due to the constant influx of new providers and frequent changes in their popularity. This has been attributed to a variety of factors, such as increasing user demand, varying censorship trends, prevalence of geographic restrictions on content, countries banning VPN use, providers' loss of reputation, and companies being acquired or rebranded [1], [4], [30], [42], [51], [53], [54].

Users of VPN products get conflicting advice from online recommendations and often lack the time and knowledge to conduct evaluations of their own. Moreover, VPN providers often employ marketing tactics that use jargon and exaggerated claims, making it hard for users to discern what is true. Different VPN providers also offer a variety of subscription models: free services, freemium models (sometimes with limited features), and paid VPN services that range anywhere from about $5–$20 a month, often with discounts for long-term plans. Although there has been a plethora of reports ranking these commercial VPNs, they are either limited, or lack objectivity and use inconsistent heuristics to evaluate VPN providers [22], [52]. There is a dearth of trusted, objective reviews and the few that exist are limited in scale, only capture a snapshot of the VPN ecosystem at the time, and are not repeated across time.

A small number of prior academic studies and closely related research efforts have analyzed VPN products. These studies, though limited, have been adept at identifying problems plaguing the ecosystem. In 2016, Ikram et al. performed static and dynamic analysis of 283 VPN permission–enabled Android apps and revealed serious privacy and security issues, including instances of malware in VPN apps' source codes [38]. In 2018, Khan et al. conducted an empirical analysis of 62 commercial VPN providers and found that many VPNs leak user traffic through a variety of means [43]. But they also found that commercial VPN providers are less likely to intercept or tamper with user traffic than previously studied forms of traffic proxying. However, they predominantly tested providers with free and trial versions of desktop applications or used OpenVPN configuration files. Another study explored vulnerabilities in 30 commercial VPN products focusing on the configuration of VPN clients and software [5] and found that vulnerabilities can stem from unsafe instructions to users, insecure third-party binaries, and use of fixed pre-shared keys. These studies, while valuable in measuring and identifying issues with VPN providers, involved a large amount of manual work and hence are not scalable, and cannot be repeated easily.

Other studies that focus on identifying vulnerabilities that exploit leakages and privilege escalation attacks demonstrate how adversaries can use these attacks to infer the identity of the user or execute arbitrary code. Perta et al. in their manual analysis of 14 popular VPN providers, identify developer-induced bugs and misconfigurations which lead to IPv6 and DNS leaks, which could deanonmyize users [70]. Fazal et al. showed how an attacker could penetrate into the VPN tunnel by exploiting VPN clients with a dual-NIC to bypass connection to the VPN server and gain control over the VPN tunnel [18].

Further, there have been studies focusing on verifying the locations of network proxies. VPN providers advertise servers in many countries with little proof of their claims. A study by Weinberg et al. [82] found that of the 2,269 servers studied, over one-third of them are definitely not in the geolocation or the country advertised, and another one-third might not be.

Finally, studies such as Netalyzr [46], IoT Inspector [33], Wehe [56] and others [14], [20], [49] paved the way for leveraging end-users to conduct network measurements, and they also provide insights to future measurement tools on effectively involving users in conducting end-host measurement [45].

The inconsistencies of online recommendations and the limitations of previous work have emphasized the need for a system that can that can help users perform systematic investigation of the VPN ecosystem. We fill this research gap with VPNalyzer and show its benefits and value by performing empirical assessments of 80 popular VPN providers.

III. VPNalyzer Design

Our aim is to build a system that has sufficient functionality combined with a simple installation process and user interface to empower average users to investigate different security and privacy aspects of VPN providers.

We build a cross-platform desktop application for Windows, MacOS, and Linux using the open-source Electron framework [16], chosen for its cross-platform compatibility and native

Figure 1: VPNalyzer Architecture — (1) User downloads application. (2) User installs the application, reviews our privacy policy, consents to be part of study. (3) User runs an “experiment” consisting of three stages: ensuring VPN is disabled and either granting or denying administrative privileges, enabling VPN and running VPN case, and disabling VPN and running ISP case. (4) Once experiment is done, the application seeks explicit consent from user to upload experiment data to Google Cloud Storage. (5) Analysis pipeline works on the uploaded data. (6) Extracted results appear on website front-end. (7) User visits unique link pertaining to their “experiment” to view detailed results.

API availability. We develop the UI for the application with React and implement the measurements using Node.js . Initially, we explored creating a browser-based test suite, extension, or plugin. But none of these alternatives provide the level of functionality, fine-grained access for robust measurements, and convenience that a desktop application affords us. Furthermore, desktop VPNs have not been previously studied at scale, since methods to test them are notoriously hard to automate.

A. System Architecture and Components

Our system architecture (as described in Figure 1) starts with a user visiting our website to download the application for their specific platform in the form of a .zip file. Once the application is extracted and run, the user is first presented with our privacy policy and consent form (more details provided in §III-B). Upon agreeing, the user proceeds to the homepage where the user's current public IP address, Autonomous System (AS) Name, and geolocation are displayed, as shown in Figure 2.

Figure 2: VPNalyzer Application — The homepage (left) contains the user's current AS Name, public IP address, and geolocation detected using the public IP. The results page (right) contains a link to detailed results, and a summary displayed upon completion of an experiment.

Desktop Application: Currently, the VPNalyzer test suite contains 15 “measurements” that test for aspects of service misconfigurations, leakages, and support for a set of security and privacy essentials, (more details in §IV). Each run of the application is termed an “experiment” that takes ≈ 20 minutes. An experiment flow is divided into three stages: bootstrapping in the ISP stage, performing measurements with VPN on (VPN case), and performing measurements with VPN off (ISP case). We perform the 15 measurements sequentially with the VPN and again without the VPN. This flow is necessary to confirm and corroborate our observations in the case of VPN leaks and misconfigurations. There are also essential background services, such as packet capture, that run throughout an experiment.

Building a system such as VPNalyzer comes with various technical challenges. Cross-platform development requires specialized knowledge especially since our tool requests administrative privileges. Designing a test suite conducive for testing VPNs, as well as ensuring that results are comparable between the VPN and ISP cases is a significant task. Further, considering the dynamic nature of the VPN ecosystem, VPNalyzer must be modular and configurable to facilitate additions and upgrades to the test suite. To facilitate broad distribution, our Windows and MacOS applications must be code-signed and notarized.

Experiment Flow: In the bootstrapping in ISP stage, the user is asked to confirm that the VPN is disabled. Then, the