Mapping the Commercial VPN Ecosystem: An Empirical Analysis

Privacy, Security and Methodological Enhancements

S. Feng

NIMS Lab
USRA Summer 2023

July 5, 2023

DALHOUSIE
UNIVERSITY

Table of contents

1. Introduction
   - Purpose of the Presentation
   - Background Information
2. Methodology
   - Candidate Selection and Data Collection
   - Testing Infrastructure
3. Summarize
   - Result and Related Works
4. Future Work
   - Rework on VPN Service Selection
   - Simulate Certain Environments

DALHOUSIE UNIVERSITY

Purpose of the presentation

Paper: An Empirical Analysis of the Commercial VPN Ecosystem

- Reproduce the process of exploration
- Summrize the result and related works

Project: Analyze IMA traffic over VPNs

- Gather required knowledge
- Propose possible improvements
- Seek potential path for integration

Background information

- The increasing demand for privacy, security and freedom
- The VPN ecosystem is highly opaque

Background information

- The increasing demand for privacy, security and freedom
- The VPN ecosystem is highly opaque
- Service providers might be evil, unintentional leakage exists
- The absence of independent and peer-reviewed evaluation

DALHOUSIE UNIVERSITY

Background information

- The increasing demand for privacy, security and freedom
- The VPN ecosystem is highly opaque
- Service providers might be evil, unintentional leakage exists
- The absence of independent and peer-reviewed evaluation

Remarks

The authors designed a relaible approach to test a wide range of VPN service providers in multiple dimentions

DALHOUSIE UNIVERSITY

Candidate selection and data collection

62 test subjects in 200 candidates

- Popularity: search engine, community, and rating websites
- Diversity: referral, international, technical uniqueness, price

Candidate selection and data collection

62 test subjects in 200 candidates

- Popularity : search engine, community, and rating websites
- Diversity : referral, international, technical uniqueness, price
- Limitation : maximize coverage, free or has free trial
- Diversity : random selection

Candidate selection and data collection

62 test subjects in 200 candidates

- Popularity: search engine, community, and rating websites
- Diversity: referral, international, technical uniqueness, price
- Limitation: maximize coverage, free or has free trial
- Diversity: random selection

Public Information: business relationship, business location

Geolocation: IP2Location Lite, MaxMind's GeoLite2, and Google

Testing infrastructure

Traffic Interception and Manipulation Tests

- DNS manipulation
- DOM and request collection
- TLS interception and downgrade detection

Testing infrastructure

Traffic Interception and Manipulation Tests

- DNS manipulation
- DOM and request collection
- TLS interception and downgrade detection

Infrastructure Inference Tests

- Recursive DNS origins
- Ping and traceroute data
- Geolocation via Google API

Testing infrastructure

Leakage Based Tests

- DNS leakage
- IPv6 leakage
- Recovery from tunnel failure

Testing infrastructure

Leakage Based Tests

- DNS leakage
- IPv6 leakage
- Recovery from tunnel failure

VPN Metadata and packet captures

- Routing and ARP tables
- Interface lists
- Configured DNS resolvers
- Pings to any /32 IPv4 routes

Result

Traffic manipulation

- URL redirection, TLS downgrade
- Traffic injection/modification

Result

Traffic manipulation

- URL redirection, TLS downgrade
- Traffic injection/modification

Traffic monitoring

- Header-based proxy detection
- Soliciting providers

Result

Traffic manipulation

- URL redirection, TLS downgrade
- Traffic injection/modification

Traffic monitoring

- Header-based proxy detection
- Soliciting providers

VPN server infrastructure

- Shared server

Result

Geographic distribution

- Comparing with Geo-IP databases
- Identifying ‘virtual’ vantage points.

Traffic leakage

- DNS leakage
- IPv6 leakage

Result

Geographic distribution

- Comparing with Geo-IP databases
- Identifying ‘virtual’ vantage points.

Traffic leakage

- DNS leakage
- IPv6 leakage

Peer-to-peer traffic

Related Works

- Vulnerabilities in VPN services
- VPN-based measurements
- Open HTTP proxies

Rework on VPN Service Selection

Problems:

- The information in the paper is outdated
- Cancellation of free trial period
- The original work cannot be accessed[1]

[1] The website by authors: vpnselection.guide

[2] *Most* commercial VPN services use OpenVPN or WireGuard

Rework on VPN Service Selection

Problems:

- The information in the paper is outdated
- Cancellation of free trial period
- The original work cannot be accessed[1]

Solution:

- Reproduce the entire selection process
- **Self-host** OpenVPN service[2]

[1] The website by authors: vpnselection.guide

[2] *Most* commercial VPN services use OpenVPN or WireGuard

Simulate Certain Environments

Problems:

- Envolving anti-proxy methods[3]
- Potential legal issue
- Difficult to gain full-control

[3] Netflix finds new strategy to cope with password sharing and VPN

Simulate Certain Environments

Problems:

- Envolving anti-proxy methods[3]
- Potential legal issue
- Difficult to gain full-control

Solution:

- Use cloudflare to mimic Geo-Block etc.
- Use VPS in certain location like Russia
- Use script to automate repetitive tasks

[3] Netflix finds new strategy to cope with password sharing and VPN