# *Leaks in Commercial VPNs*

CS528 Network Security

Computer Science, Purdue University

Matt Hiatt, Nathan Leakeas

# Outline

I. Introduction

II. Background & Motivation

III. Types of VPN Leaks

IV. Project Setup

V. Next Steps

VI. Further Reading

# I. Introduction

- Virtual Private Networks (VPNs) are in wide use for
  - Protecting user privacy
  - Evading censorship/geo-locks (as discussed in class)
  - Securing public internet access
- Historically, both commercial and popular free-to-use VPN distributions have suffered from vulnerabilities
- Our idea was to develop a tool to automatically detect privacy leaks on VPN clients

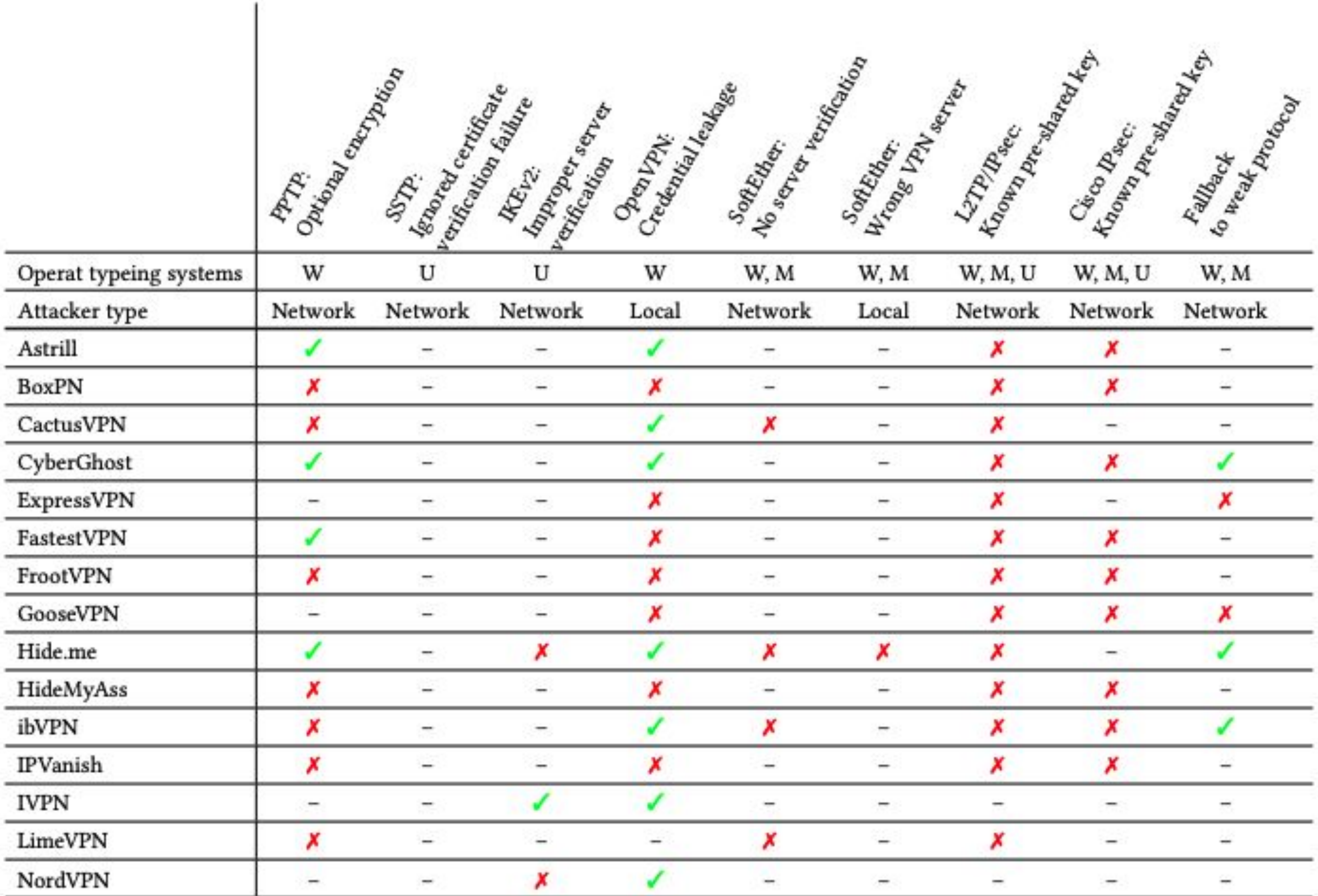
# II. Background & Motivation

- Both the news media and academic literature show many examples of publicly distributed VPNs being vulnerable
- Like most software products, vulnerabilities clustered around new features/updates
- Can be due to company malfeasance
  - Big Mama VPN selling user data - WIRED, Dec 2024
- We focus on accidental vulnerabilities, specifically those that arise from usage by inexperienced customers

# II. Lit Review: Bui, et al. 2019

- *Client-Side Vulnerabilities in Commercial VPNs*
- Authors examined many commercial VPN clients on Windows, Mac, and Ubuntu
- Found many configuration flaws which led to
  - Stripping of traffic’s encryption
  - Bypassing of VPN gateway authentication
  - Stealing VPN user’s credentials
- Emphasized the importance of strong configuration instructions and default values rather than relying only on strong cryptographic fundamentals

# II. Lit Review: Bui, et al. 2019



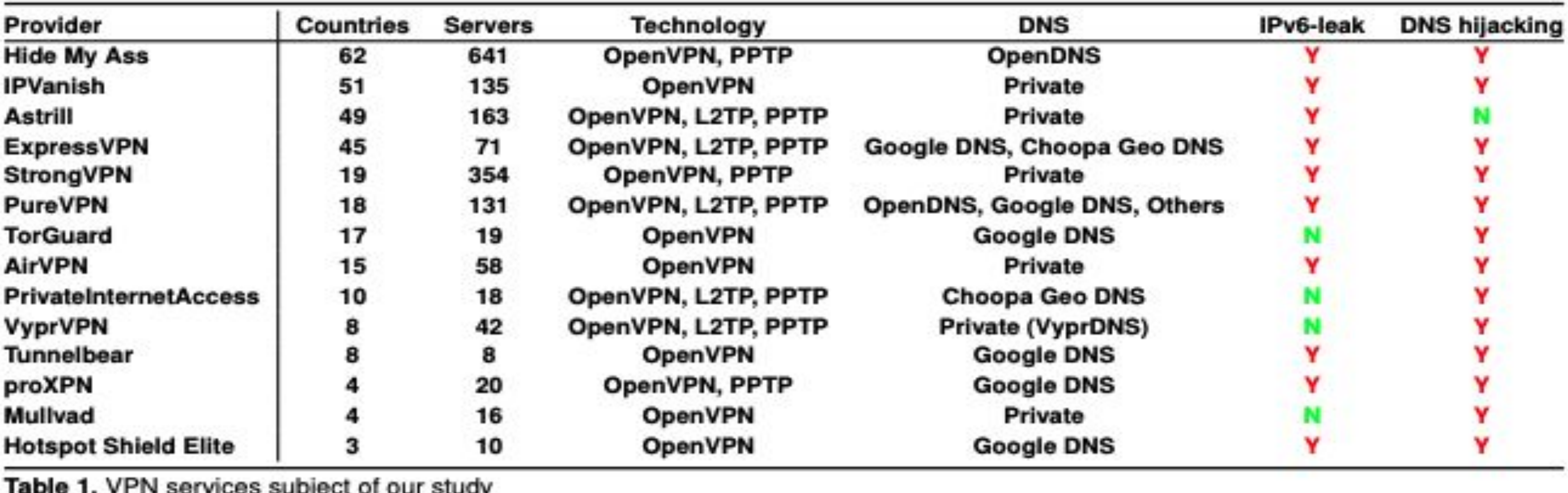
| | PPTP: Optional encryption | SSTP: Ignored certificate verification failure | IKEv2: Improper server verification | OpenVPN: Credential leakage | SoftEther: No server verification | SoftEther: Wrong VPN server | L2TP/IPsec: Known pre-shared key | Cisco IPsec: Known pre-shared key | Fallback to weak protocol |
|---|---|---|---|---|---|---|---|---|---|
| Operat typeing systems | W | U | U | W | W, M | W, M | W, M, U | W, M, U | W, M |
| Attacker type | Network | Network | Network | Local | Network | Local | Network | Network | Network |
| Astrill | ✓ | – | – | ✓ | – | – | ✗ | ✗ | – |
| BoxPN | ✗ | – | – | ✗ | – | – | ✗ | ✗ | – |
| CactusVPN | ✗ | – | – | ✓ | ✗ | – | ✗ | – | – |
| CyberGhost | ✓ | – | – | ✓ | – | – | ✗ | ✗ | ✓ |
| ExpressVPN | – | – | – | ✗ | – | – | ✗ | – | ✗ |
| FastestVPN | ✓ | – | – | ✗ | – | – | ✗ | ✗ | – |
| FrootVPN | ✗ | – | – | ✗ | – | – | ✗ | ✗ | – |
| GooseVPN | – | – | – | ✗ | – | – | ✗ | ✗ | ✗ |
| Hide.me | ✓ | – | ✗ | ✓ | ✗ | ✗ | ✗ | – | ✓ |
| HideMyAss | ✗ | – | – | ✗ | – | – | ✗ | ✗ | – |
| ibVPN | ✗ | – | – | ✓ | ✗ | – | ✗ | ✗ | ✓ |
| IPVanish | ✗ | – | – | ✗ | – | – | ✗ | ✗ | – |
| IVPN | – | – | ✓ | ✓ | – | – | – | – | – |
| LimeVPN | ✗ | – | – | – | ✗ | – | ✗ | – | – |
| NordVPN | – | – | ✗ | ✓ | – | – | – | – | – |

# II. Lit Review: Khan, et al. 2018

- *An Empirical Analysis of the Commercial VPN Ecosystem*
- Examined 62 commercial VPN providers
  - Many VPNs leak user traffic
  - At least 10% of services lie about where there servers are
  - A few of 153 VPN providers who the authors inquired to expressed interest in selling user data
- Also reported on the marketing strategies of VPN providers
  - *“Military grade encryption”*
  - 88 of 153 VPN providers used affiliate programs

# II. Lit Review: Perta, et al. 2015

- *A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN Clients*
- Found that majority of VPNs suffered from IPv6 & DNS traffic leakage



| Provider | Countries | Servers | Technology | DNS | IPv6-leak | DNS hijacking |
|---|---|---|---|---|---|---|
| Hide My Ass | 62 | 641 | OpenVPN, PPTP | OpenDNS | Y | Y |
| IPVanish | 51 | 135 | OpenVPN | Private | Y | Y |
| Astrill | 49 | 163 | OpenVPN, L2TP, PPTP | Private | Y | N |
| ExpressVPN | 45 | 71 | OpenVPN, L2TP, PPTP | Google DNS, Choopa Geo DNS | Y | Y |
| StrongVPN | 19 | 354 | OpenVPN, PPTP | Private | Y | Y |
| PureVPN | 18 | 131 | OpenVPN, L2TP, PPTP | OpenDNS, Google DNS, Others | Y | Y |
| TorGuard | 17 | 19 | OpenVPN | Google DNS | N | Y |
| AirVPN | 15 | 58 | OpenVPN | Private | Y | Y |
| PrivateInternetAccess | 10 | 18 | OpenVPN, L2TP, PPTP | Choopa Geo DNS | N | Y |
| VyprVPN | 8 | 42 | OpenVPN, L2TP, PPTP | Private (VyprDNS) | N | Y |
| Tunnelbear | 8 | 8 | OpenVPN | Google DNS | Y | Y |
| proXPN | 4 | 20 | OpenVPN, PPTP | Google DNS | Y | Y |
| Mullvad | 4 | 16 | OpenVPN | Private | N | Y |
| Hotspot Shield Elite | 3 | 10 | OpenVPN | Google DNS | Y | Y |

**Table 1.** VPN services subject of our study

# II. Motivation

- In summary, VPN leaks have many causes:
  - Intentional sale of user data by the VPN provider, as well as misleading representation of the product’s capabilities
  - Accidental bugs introduced in standard development cycles
  - Misconfiguration by end users who lack technical knowledge, or overrate the security guarantees of the service
- Thus, end users may want a tool to test their VPN for leaks
  - To verify the VPN is actually secure
  - To ensure their active configuration is actually secure

# III. VPN Leaks: DNS Leak

- DNS queries bypass the VPN tunnel and go the user’s ISP
- Exposes websites you visit, even if your IP is spoofed
- Causes
  - VPN misconfiguration
  - Operating system overrides
  - Bugs: ExpressVPN’s introduction split tunneling feature in 2022 led to a DNS leak on Windows that wasn’t discovered until 2024
- Completely undermines the privacy guarantees VPNs make
- Mitigation: audit your VPN to ensure leaks are not present

# III. VPN Leaks: WebRTC Leak

- Web Real-Time Communication (WebRTC): browser feature that enables peer-to-peer communication (ex. Video calling or file sharing)
  - Default on most browsers
- Necessitates the exchange of real IPs, allowing exploitation
- Attacker tries to expose your real IP address, even when connected to a VPN
- Mitigation: Some VPNs promise to find and block WebRTC leaks, disable WebRTC on your browser entirely, WebRTC leak test tools

# III. VPN Leaks: IP Leaks

- Real IPs can also leak through a variety of more general attacks/errors
- Misconfiguration
    - Disabled kill switch
    - Network settings/lack of VPN support for IPv6 fails to route IPv6 traffic through VPN
- Bugs introduced in the development cycle
- Mitigation: ensure VPN has IPv6 support, use leak testing tools offered by someone other than your VPN provider, test after every change to configuration

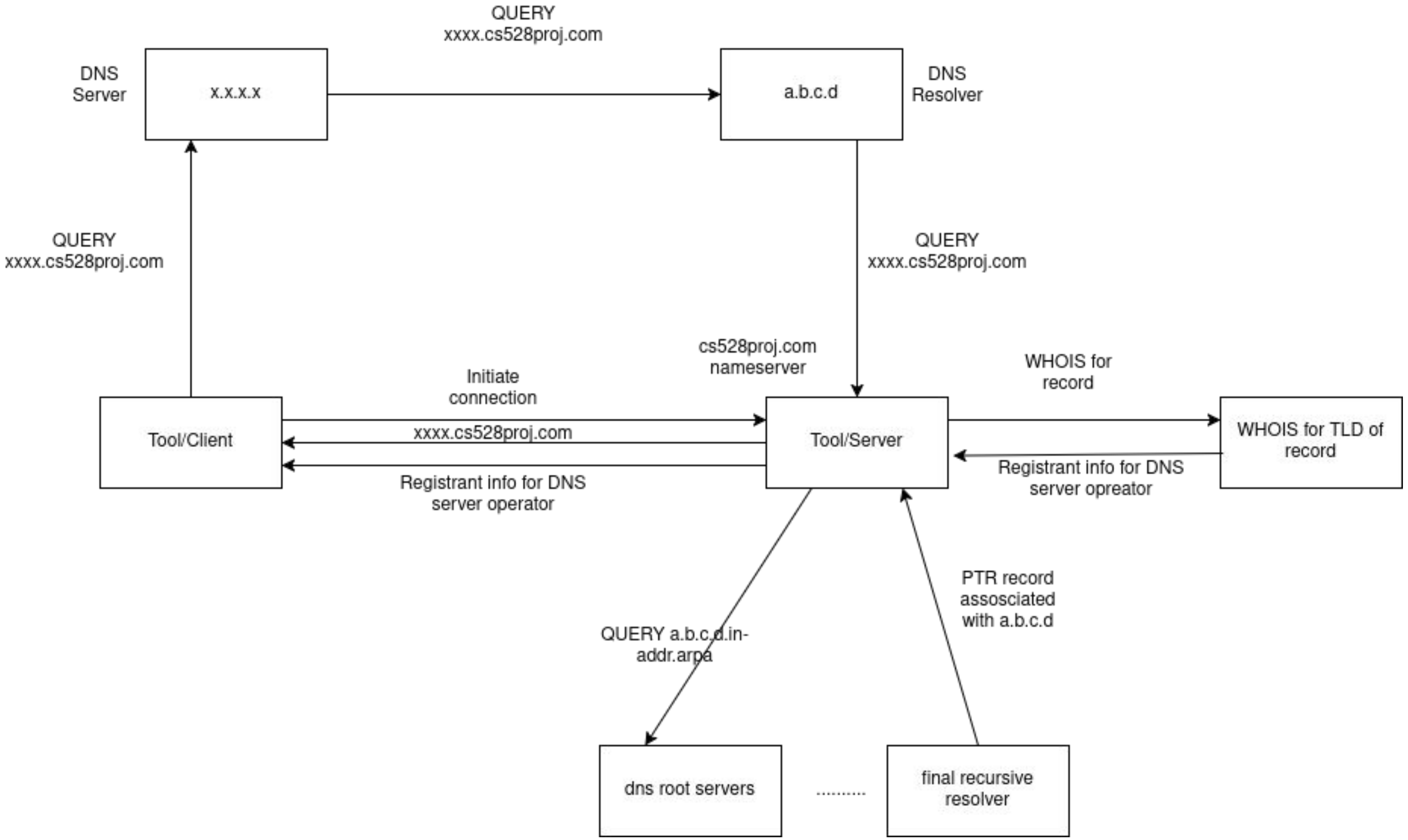
# IV. Project Setup

- We focus on DNS leaks in our auditor
- To detect a DNS leak, we need to find out where the DNS request ultimately comes from
  - This can be tricky, because DNS requests from the same organization can come from different source IPs
  - At face value, the request comes from different machines, but they might still be controlled by the same organization
- To reliably detect where DNS requests arrive from, we acquired cs528proj.com and set up a nameserver for the domain

# IV. Project Setup

- The tool consists of a client and server, which coordinate to learn about the DNS provider
- The server performs reverse DNS lookup for incoming DNS query
- It then performs a WHOIS request for the domain name from previous step
- This information is sent back to the client, who can use it to determine who is actually handling their DNS requests

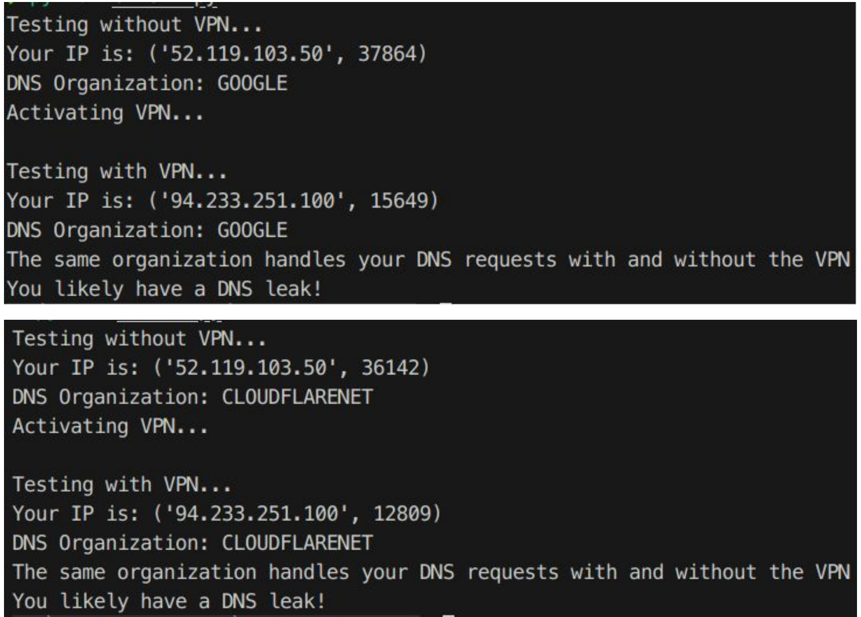
# IV. Project Setup



# V. Preliminary Results

- Our tool can detect whether bad or poorly configured VPNs leak with respect to DNS requests

Bad Config Examples



```
Testing without VPN...
Your IP is: ('52.119.103.50', 37864)
DNS Organization: GOOGLE
Activating VPN...

Testing with VPN...
Your IP is: ('94.233.251.100', 15649)
DNS Organization: GOOGLE
The same organization handles your DNS requests with and without the VPN
You likely have a DNS leak!
```

```
Testing without VPN...
Your IP is: ('52.119.103.50', 36142)
DNS Organization: CLOUDFLARENET
Activating VPN...

Testing with VPN...
Your IP is: ('94.233.251.100', 12809)
DNS Organization: CLOUDFLARENET
The same organization handles your DNS requests with and without the VPN
You likely have a DNS leak!
```

# V. Preliminary Results

- We find small alterations to default VPN configurations can cause complete breakdowns in security
- Recommendations
  - VPN users should deploy leak tests every time they change their configuration
  - VPNs themselves, or 3rd party services could issue warnings when configurations change in dangerous ways
  - Increased government regulation of VPN providers and their practices with user data may be warranted

# VI. Further Reading

- *Shedding Light on Hidden Dangers: A New Perspective on DNS Leaks* - Membrey, 2024
- *Bypassing Tunnels: Leaking VPN Client Traffic by Abusing Routing Tables* - Xue, et al., 2023
- *One Leak Will Sink a Ship: WebRTC IP Address Leaks* - Al-Fannah, 2017
- *The History of Data Breaches* - De Groot, 2018
- *This VPN Lets Anyone Use Your Internet Connection. What Could Go Wrong?* - Matt Burgess [WIRED], 2024

# *Questions?*

CS528 Network Security

Computer Science, Purdue University

Matt Hiatt, Nathan Leakeas