Rough Edges for IPv6 in VPNs

Yejin Cho, John Heidemann
USC/ISI
yejincho@usc.edu, johnh@isi.edu

Introduction

Virtual Private Networks (VPNs) and IPv6 help users, but with "rough edges":

1. VPNs provide users privacy and avoid censorship
   ⇒ but we show that VPNs often leak IPv6 traffic
2. IPv6 supports more addresses and end-to-end connectivity
   ⇒ but we show that VPNs often de-preference IPv6

Data Source:WhatIsMyIPAddress

WhatIsMyIPAddress.com shared 7+ days (5 million observations) of anonymous users IPv4 and IPv6 addresses with us.

We thank Chris Parker for working with us to safely share this data.

1. VPNs Leak IPv6 Traffic (IPv6 traffic is sent with an IPv6 address from the user's local interface, not the VPN)

What do users want?

VPNs should provide privacy and censorship avoidance.

However, some VPNs send out IPv6 traffic using the user's local interface's IPv6 address (*an IPv6 leak*), rather than using an VPN IPv6 address

Detecting IPv6 Address Leaks

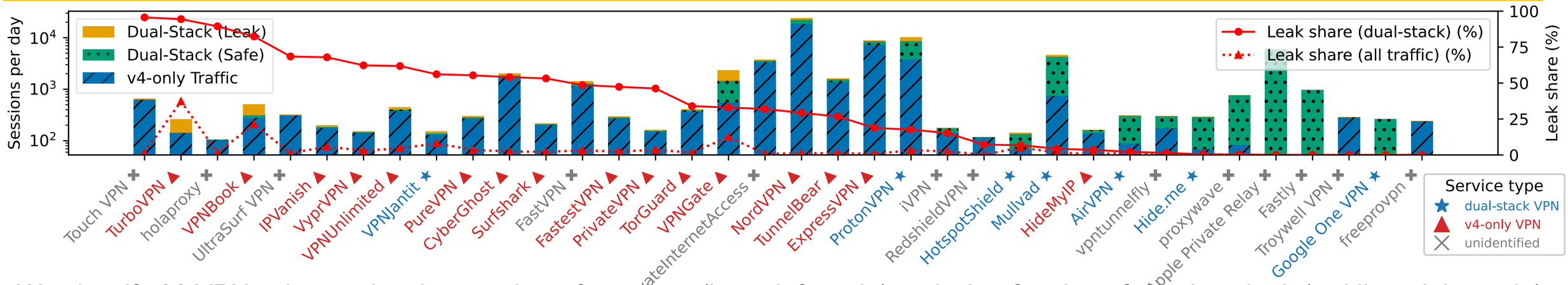
We detect VPN IPv6 leaks when:

	IPv4	**IPv6**	**Data Source**
IP's Org	From Different Organizations		CAIDA AS2Org
IP address	VPN	Not VPN	IPinfo
IP's AS	Not ISP	ISP	ASdb
Not from Cache Server	NOT from known Chrome Prefetch prefix		Google

Challenges

- IPinfo's VPN identification covers relatively few addresses.
- Last update of ASdb was 2024 Jan.

Observations and Implication



We classify 26 VPNs above, showing number of sessions (bars, left scale) and what fraction of sessions leak (red line, right scale).
For users that use both IPv4 and v6, **most VPNs leak many sessions:** maxing at 95%.
⇒ ▲IPv4-only VPNs leak traffic more frequently (around 6%) than ★dual-stack VPNs (around 3%).
⇒ **VPNs should implement proper IPv6 tunneling, instead of blocking.**

2. VPNs de-preference IPv6 (Using IPv4 even when IPv6 is available and comparably fast)

What do users want?

Users expect VPNs with IPv6 support to utilize IPv6 -- but in practice, IPv4 is used for visiting all dual-stack websites.

Observation

We observe that 98% of VPN visitors used IPv4, from WhatIsMyIP Address data.

Detecting in VPN Software

We installed and tested 6 Android VPNs

- ProtonVPN correctly does IPv6 preferencing
- Mullvad, AirVPN, hidemeVPN, Perfect Privacy, Anonine depreference IPv6

Why? Interaction of Address Selection and Preference Rules

We found that IPv6 de-preferencing occurs because of an interaction between how VPNs assign IPv6 addresses and OSes select which address to use.

VPN Address Configuration: We check how VPN interface is configured

```
$ adb shell ip addr show tun10
tun10:
    inet 10.132.3.96/32
    inet6 fc00:bbbb:bbbb:bb01:d:0:4:360/64
```

Source Address Type
IPv4 Private
IPv6 Private (ULA)

Destination: Dual-Stack destination has A record(with Public IPv4 address) and AAAA record (with Public (GUA) IPv6 address.

OS Address Preference Rules: RFC-6724 gives rules to select between different outgoing IP addresses, including between v4 and v6, and public and private.
That RFC ranks (source, address) pair of (IPv4 public, IPv4 private) higher than (IPv6 ULA, IPv6 GUA).

- **Problem:** IPv4 private addresses are commonly used, but use of IPv6 ULA addresses are discouraged.
- **Recommendation: Either** VPN operators should assign GUA addresses to clients inside the VPN, **or** IETF should revise the prioritization rules, perhaps creating VPN-specific ULA addresses

➢ **ULA + Priority Rules ⇒ Problems**

Conclusion

- VPNs implements should NOT leak IPv6
- VPNs should not dereference IPv6
  - Either VPNs should use GUA
  - Or IETF should change the prioritization
- For more information, contact yejincho@usc.edu (paper is in progress)

Rough Edges for IPv6 in VPNs ACM IMC 2025 Poster Session / October 2025. This work is partially supported by U.S. NSF CNS-2212480 and OAC-2530698, and USC IRB identified it as NHSR (#UP-25-00838).