Bypassing Tunnels: Leaking VPN Client Traffic by Abusing Routing Tables

Nian Xue, Yashaswi Malla, Zihang Xia, Christina Pöpper, and **Mathy Vanhoef**

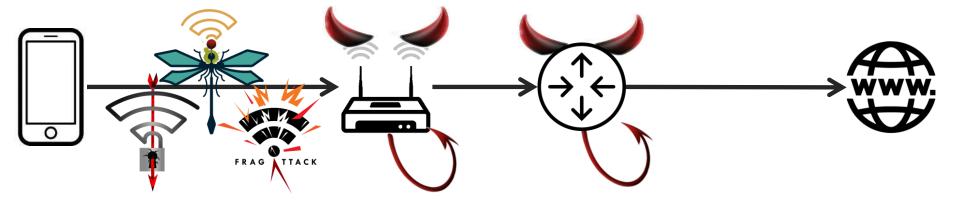
USENIX Security, 9-11 August 2023, USA



Usage of VPNs: watch videos from other country



Usage of VPNs: protect your traffic



- > Identify website visits: IP address, plaintext DNS, SNI,...
- > Attack TLS: no cert check, sslstrip, academic attacks,...

Usage of VPNs: protect your traffic



- > Defend against untrusted Wi-Fi & compromised core routers
- > Research goal: can we trick the client into leaking packets?
 - » Yes, by manipulating the client's routing table \rightarrow ~66% vulnerable!
 - » Attacks are independent of the crypto protocol

Background: VPN client routing table



\$ ip route 1 default via tun0

1. By default, send packets over tun0 = over the VPN tunnel

Background: VPN client routing table



\$ ip route
1 default via tun0
2 192.168.1.0/24 via eth0

1. By default, send packets over tun0 = over the VPN tunnel

2. LocalNet exception: local network is directly accessible

Background: VPN client routing table



\$ ip route
1 default via tun0
2 192.168.1.0/24 via eth0
3 2.2.2.2 via eth0

1. By default, send packets over tun0 = over the VPN tunnel

- 2. LocalNet exception: local network is directly accessible
- 3. ServerIP exception: avoid re-encryption of VPN packets

We assume secure DNS behavior



\$ cat /etc/resolv.conf
nameserver 6.6.6.6

Can't trust the network's DNS server

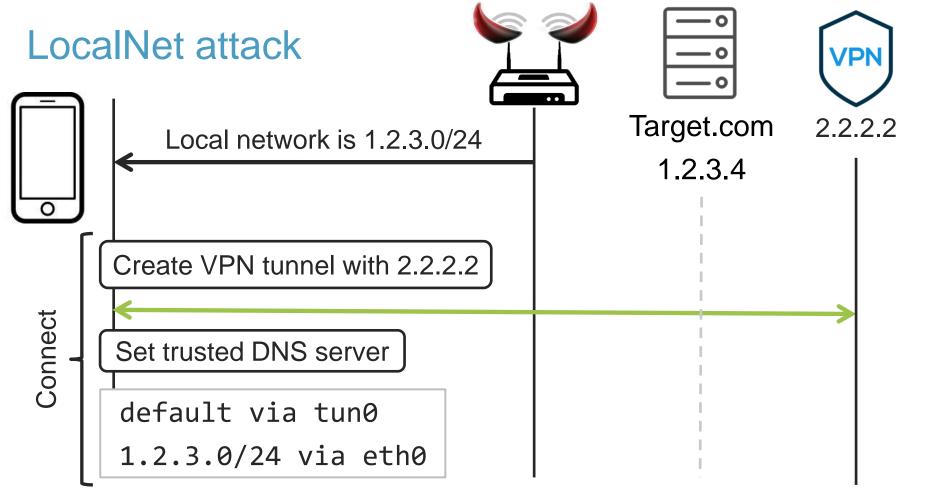
We assume secure DNS behavior

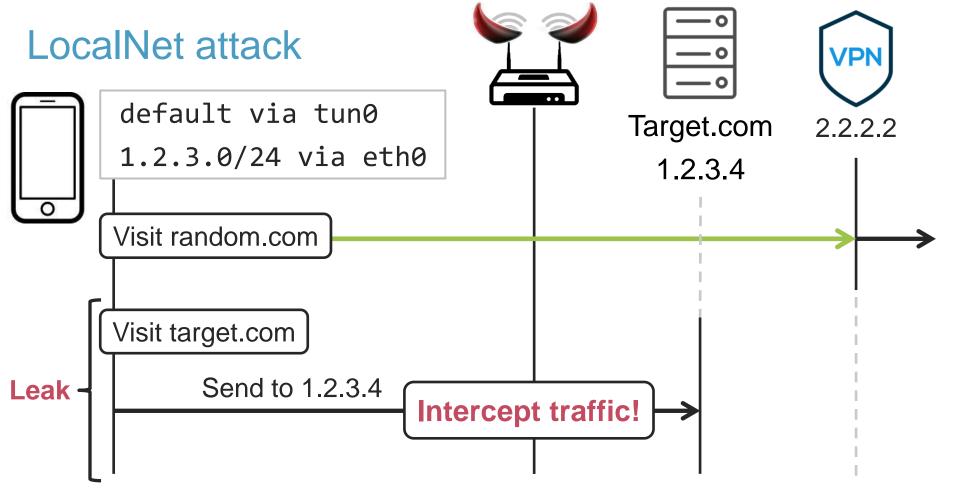


\$ cat /etc/resolv.conf
nameserver 2.2.3

Can't trust the network's DNS server. Once connected:

- 1. The VPN client sets a trusted DNS server
- 2. DNS is sent through the VPN tunnel
 - + we assume other routing-based attacks are prevented





		K: 195		ments	VALUATED USENIX ASSOCIATION ASSOCIATION FUNCTIONAL	EVALUATED USENIX ASSOCIATION REPRODUCED		
V Orient Class Wrinds Windswith Free Winds Windswith Free Winds Windswith Free Windswith Windsw	VPN Provider	Class	OS	Version Number	LAN Setting Default LAN Acco	8		
Any Vi mindo 1.03 Avira Phantom Pree Windows Best VPN Pree macOS Paid Windows		Free	Windows	Windows 10 Pro	No N/A	×		
Betternet Piád macOS - Piád iOS 5.3. Piád Android 6.2.0 Pirce Windows 4.10.0400 Pirce Linux 4.10.0509		Free	Windows	No N/A	×			
Cisco AnyConnect Free macOS 4.10.0406 Free iOS 5.0.0034 Free Android 5.0.0034 Paid Windows 5.9.1.166	OS Built-in VPN	Free	macOS	Ventura 13.0.1	No N/A	×		
Clario VPN Paid macOS 5.0.1160 Paid iOS 1.9.28 Paid Android 1.9.264209 Paid Windows 8.3.7979	US Duilt-III VPIN	Free	iOS	iOS 16.1.1	No N/A	×		
Paid Linux 1.3.4 CyberGhost Paid macOS 8.3.9.167 Paid iOS 8.4.0 Paid Android 8.6.17.116		Free	Android	Android 8.1.0	No N/A	 ✓ 		
Paid Windows 12.37.0 Paid Linux 3.36 ExpressVPN Paid macOS 11.12.0 Paid iOS 11.10.0 11.12.0 Paid iOS 11.00.0 10.63.2		Free	Android	Android 12	No N/A	 		
Fast VPN-solo unlimited proxy Pree iOS 2.2.4 Paid Windows 3.4.0.0 Fast VPN Paid macOS 3.9.0 by Namecheap Paid Android 3.7.0 Paid Android 3.4.2 3.4.0		Free	Windows	2022.10.106.0	No N/A	 		
Free VPN Free macOS 3.884 by Free VPN.org Free iOS 3.879 Free Android 3.9		Free	Linux	2022.9.591	No N/A	V		
Goose VPN Paid Windows 5.0.0.9 Paid macOS 5.1.3 Paid iOS 5.1.4 Paid Android 5.1.4(19)	1.1.1.1	Free	macOS	2022.10.107.0	No N/A	\bigtriangleup		
Free / Paid Windows 3.14.0 Free / Paid Linux 0.9.2 Hide.me VPN Free / Paid macOS 4.7.1 Free / Paid iOS 4.11.0 Free / Paid Android 3.10.0		Free	iOS	6.16	No N/A	×		
Paid Windows \$.21.674 Paid Linux 0.5 HideMyAss Paid macOS 5.4.7 Paid riOS 5.10.0 5.10.0 Paid nodroid \$.58.651 5.10.0		Free	Android	6.17	No N/A	V		
Fine Mindows 2.10.8 Hotspot Shield Pree macOS 5.3.06.102 Pree iOS 7.9.0 Pree Android 9.9.0					,			
Paid Windows 4.1.2.122 IPVanish Paid macOS 3.3.0(6747 Paid iOS 4.4.0 Paid Android 4.0.3.0	2 Yes Yes Jé Paid Windows 9) Ns N/A X TerGuard Paid macOS Ns N/A X TerGuard Paid macOS Yes No ✓ Paid Android	4.8.13 No NA X 4.8.13 No NA X 4.8.13 No NA X 2.2.8 No NA X 1.60.9 No NA X	Pice Android L0.20220316 Pice Windows 73.0.2674 XVPN Pice macOS 73.1.0.2791 Pice iOS 31.3					
Paid Windows 2022.5.0 Paid macOS 2022.5 Mullvad Paid Linux 2022.5 Paid ioS 2022.5 Paid Solution Paid ioS 2022.2 Paid Android 2022.3		2.0.2.274 No VA X 2.5.6.158 No VA X 4.4.1 No VA X 2.0.8 No VA X	Prec KAS Free Android 180.2778 ¥ always vulnenkle, ¥ vulnenkle by default LAN-Access-Setti ♥ vulnenkle by using special use IP addresses ✔ always secure, ✔ secure by default LAN-Access-Setting, △ local traffic blocket	No N/A V		12		

ARTIFACT

ARTIFACT

ARTIFACT

					anac								AVAILABLE	FUNCTIONAL	REPRODUCED
Table 1 V v vie OS Built-in V	Fitte Fitte Fitte Fitte Fitte	Wind Window macOS iOS Android Android Window Linn	Version Number Windows 10 Pro Windows 11 Pro Ventura 13.0.1 iOS 16.1.1 Android 8.1.0 Android 12 2022 10.106.0 2022 9.501	Erent VPN clients. LAN Setting Result Default LAN Access No: INA X No: INA X No: INA X No: INA X	Network Manager Fine Lin OpenVPN Gnome Fine Lin Pine Lin Lin Paid Lin Lin New/VPN Paid Lin Paid Lin Lin New/VPN Paid Lin	ux 1.8.2 ux 1.8.12 ux 1.8.18 lows 7.2.2.0 ux 1.0.0	No NA X	TunnelBear Pa Pa Pa Pa Tunnelblick Pin Tunnelblick Pin	id macOS id iOS id Android	4.1.8 Ni 4.3.2 Ni 3.6.8 Ni	N/A △ N/A ★ N/A ★ N/A ★ N/A ★				
Li Any Vi Avira Phanice Best VPN Besternet Clario VPN CyberGhost	Free Free Free Free Free Paid Paid Paid Paid Free Free	ma Windows MacOs Windows MacOs iOS Android Windows Linux Linux MacOs iOS Android Windows Linux MacOs iOS Android Windows Linux	2022 10.1070 6.16 6.17 1.0.8 1.0.8 1.0.26 4.10.20405 4.10.20405 4.10.20405 4.10.20405 4.10.20405 5.00.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.000247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247	Exp	ressVPN		Paid Paid Paid Paid Paid		Vindov Linux macOs iOS Androi	S S		12.37.0 3.36 11.12.0 11.70.0 10.63.2		Yes Yes No N/A Yes Yes Yes Yes Yes Yes	
Express VPN Fast VPN-sole anlimited prot Fast VPN by Namecheap Free VPN by Free VPNJ	Paid Paid Paid Paid Paid Paid Fitee	Android Windows Linux macOS iOS Android iOS Windows macOS iOS Android macOS iOS Android	8617.1164 12.37.0 3.36 11.12.0 11.70.0 10.63.2 2.2.4 3.40.0 3.9.0 3.7.0 3.4.2 3.884 3.879 3.9		N Proxy I iPhone	Master		Free		iO	DS		2.1.5	No N/A	t
Goose VPN Hide.me VPN HideMyAss	Paid Paid Paid Paid Paid Pree / Paid Pree / Paid Pree / Paid Paid Paid Paid Paid Paid	Linux macOS iOS	\$00.9 \$.13 \$.14 \$.14(195) 3.14.0 0.92 4.7.1 4.11.0 3.10.0 \$.21.6744 0.5 \$.4.7 \$.100 \$.5.8.6510	Yes No A No N/A A No N/A X	Star VPN Pree in a Pree mac Pree in a Pree And Strong VPN Paid in a Paid Wind mac Paid And Strong VPN Paid And	OS 211.0 S 36.0 roid 1.8 lows 26.2.0 OS 22.2 S 26.0 roid 233.6	No NA X No NA X	Windscribe built-in Figure Fig	e Linux e macOS e iOS e Android e Linux	2.5.17 Yi 2.4.11 Yi 3.4.1(273) Yi 3.3.1003 Yi 2.5.17 Yi	IS NO A IS				i.
Hotspot Shield IPVanish Mullvad	d Free Free Free Paid Paid Paid Paid Paid Paid Paid Paid	Windows macOS iOS Android Windows macOS iOS Android Windows macOS Linux iOS Android	2.10.8 5.3.061028 7.9.0 9.9.0 4.1.2.122 3.3.0(67479) 4.4.0 2022.5.0 2022.5 2022.5 2022.5 2022.2 2022.3	No N/A X Yes No ✓ Yes No ✓ Yes No ✓ Yes No ✓ Yes No △ Yes No △ Yes No △ Yes No ✓	Super VTN- Free And TLS Turnel Free And TLS Turnel Free And TacGuard Paid Mind TacGuard Paid And TackAPPN Free Mind TouchVPN Free Mind	roid 1.62 roid 5.0.5 rows 4.8.13 or 4.8.13 or 4.8.13 or 4.8.13 or 4.8.13 or 4.8.13 or 2.2.8 roid 1.60.9 roid 1.60.9 roid 1.60.9 roid 1.62 or 4.8.13 or	No N/A t No N/A v' No N/A v' No N/A v' No N/A x	in Free Free Free XVPN Free X abways vulnerable, X Vulnerable by using app ✓ secure by default LAN	te Linux te macOS te iOS te Android te Windows te macOS te iOS te iOS te Android ulnerable by default LA cial use IP addresses 4/	1.0.20210914 Ni 1.0.15 Ni 1.0.15 Ni 1.0.20220516 Ni 7.3.0.2674 Ni 7.3.0.2791 Ni 31.3 Ni 1.80.2778 Ni N-Access-Setting aways secure,	N/A Z N/A Z				13

ARTIFACT

EVALUATED

ASSOCIATION

ARTIFACT

EVALUATED

ASSOCIATION

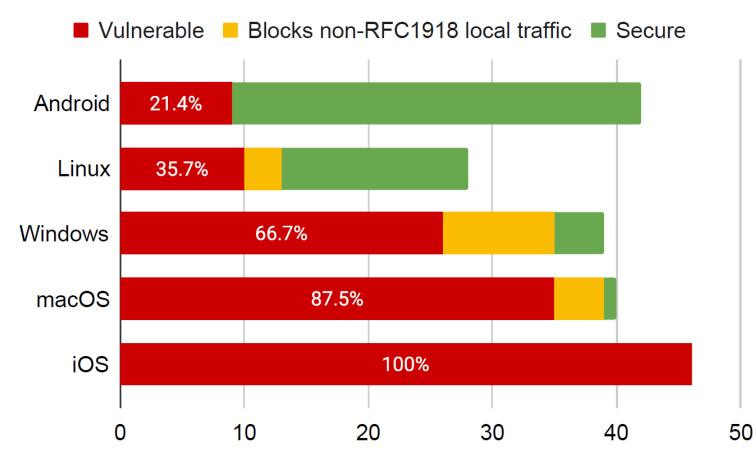
ARTIFACT

EVALUATED

ASSOCIATION

LocalNet attack: 195 experiments

LocalNet attack: summary



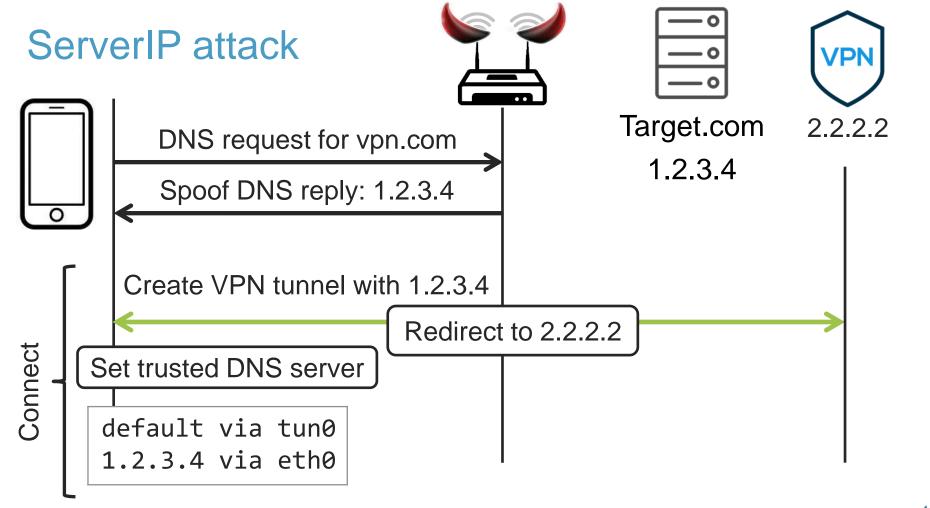
The iOS case

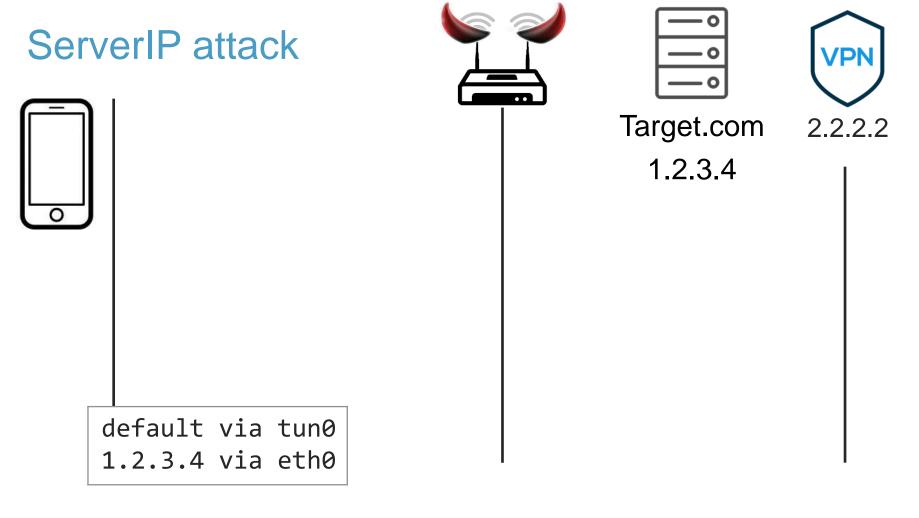
Attacks can be prevented by setting includeAllNetworks

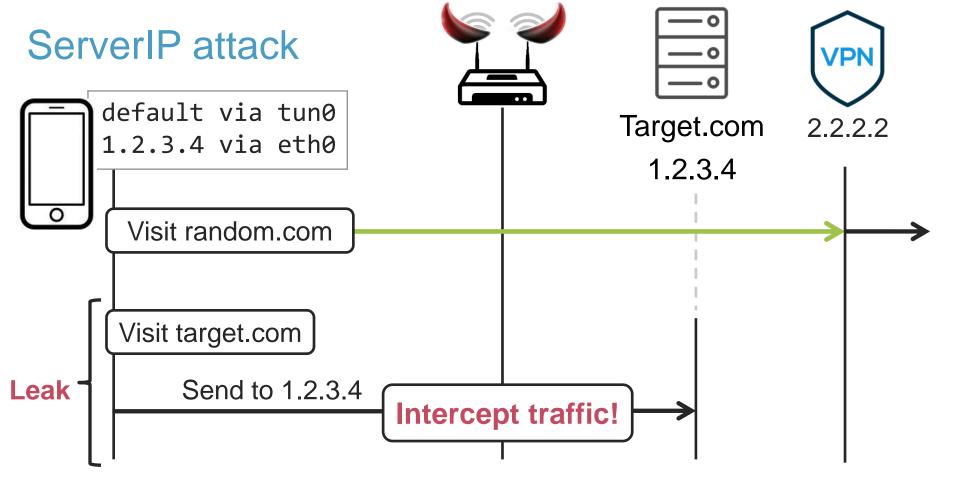
- > But causes reliability issues
- > Vendors very hesitant to enable it

Result is that iOS remains less secure

 Context: VPNs on iOS were already known to leak traffic in certain scenarios.







ServerIP attack: 53 experiments

- > Many built-in clients are affected (Windows, macOS, Linux)
- > Legacy built-in VPN on Android 11 and below was affected
- > Most iOS/Android apps not vulnerable

Impact: can leak traffic to single IP address

- > Can target the DNS server set by the VPN client ©
- > Or repeat the attack...

Defenses & Disclosure

- 1. LocalNet attack: disable local network access when it's using public IP addresses
- 2. ServerIP Attack: send all traffic over VPN, except packets generated by VPN process
- > Reported to CERT/CC on May 10, 2023
- > Contacted vendors that had a security contact
- > Practically all acknowledged the issue

Conclusion

- > Two wide-spread flaws in VPN clients
- > In hindsight easy attack, but ~66% vulnerable
- > Bad integration of protocols into real systems

Defense: more carefully configure routing tables
 OS should have API to create VPN tunnels





Questions?



- Two wide-spread flaws in VPN clients
- > In hindsight easy attack, but ~66% vulnerable
- Bad integration of protocols into real systems





- Defense: more carefully configure routing tables OS should have API to create VPN tunnels