



Bypassing Tunnels: Leaking VPN Client Traffic by Abusing Routing Tables

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

KU LEUVEN



NYUAD



NEW YORK UNIVERSITY

Contributions

We make VPN clients leak traffic

- › By **manipulating the client's routing table**
- › Attacks are independent of the crypto protocol

Tested 67+ VPN clients

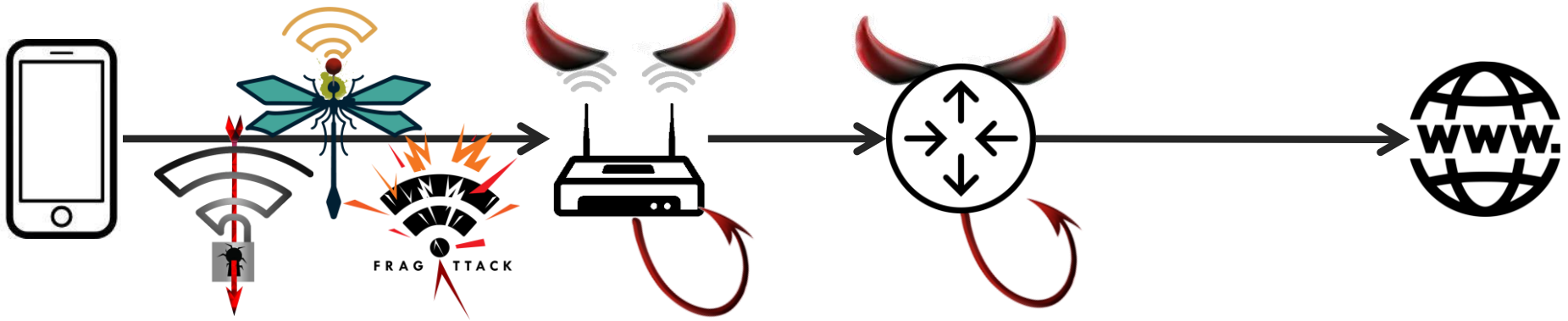
- › >248 experiments → **66% attack success**
- › Every VPN is vulnerable on at least one OS

→ **Widespread design issues!**

Usage of VPNs: watch videos from other country

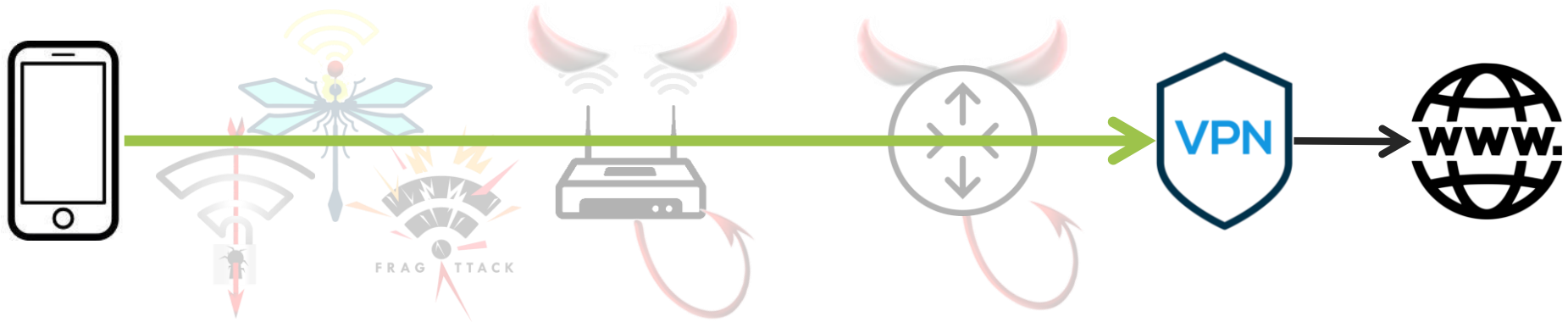


Usage of VPNs: protect your traffic



- › 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 → **~66% vulnerable!**
 - › Attacks are independent of the crypto protocol

Background: VPN client routing table



```
$ ip route # Detailed output
1 default via 10.0.0.1 dev tun0
2 192.168.1.0/24 dev eth0 proto kernel scope
   link src 192.168.1.2 metric 100
3 2.2.2.2 via 192.168.1.2 dev eth0
```

Background: VPN client routing table



1

```
$ ip route          # Simplified output  
default via tun0
```

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

Background: VPN client routing table



```
$ ip route          # Simplified output
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          # Simplified output
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

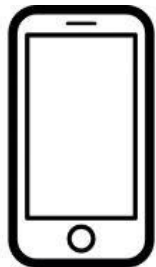


```
$ cat /etc/resolv.conf  
nameserver 2.2.2.3
```

Can't trust the network's DNS server

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

LocalNet attack



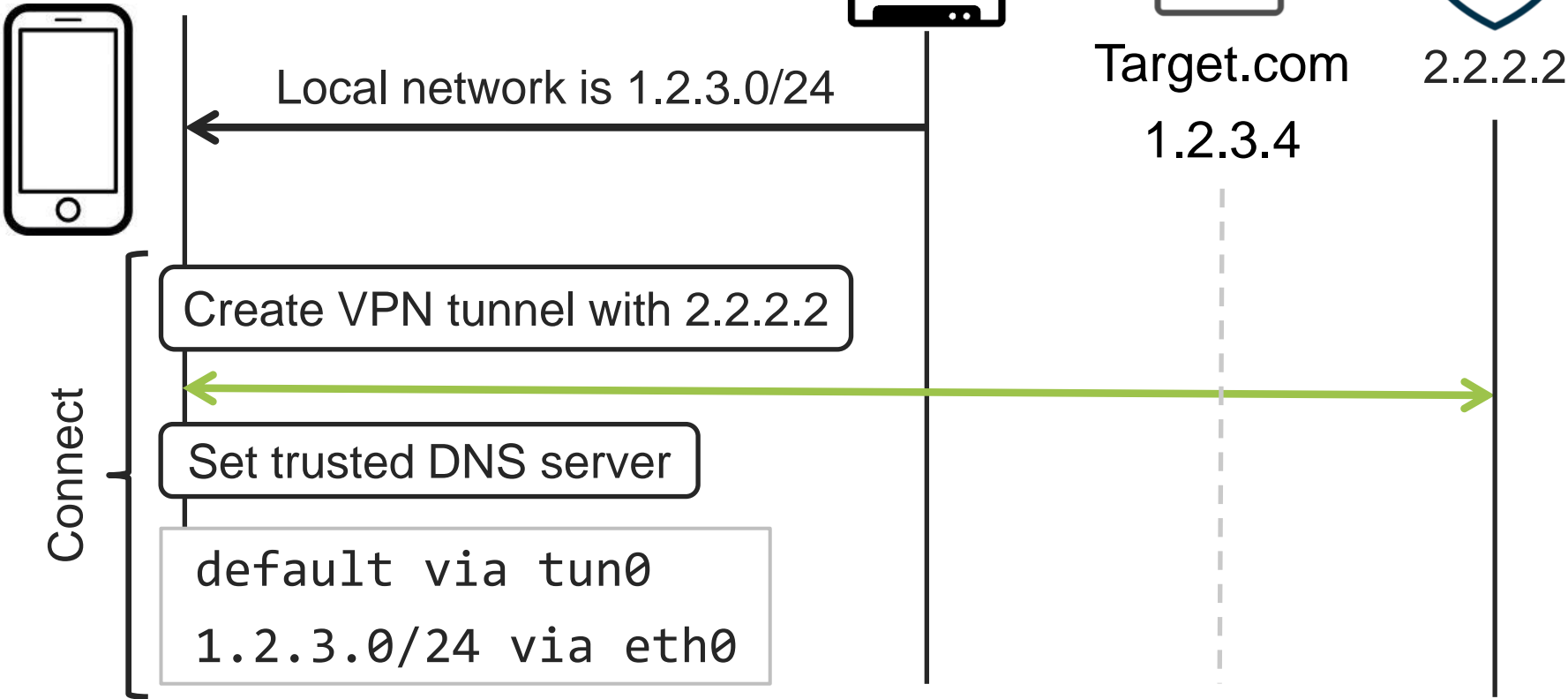
Target.com

1.2.3.4

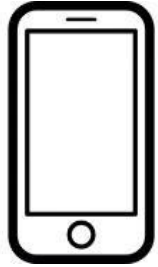


2.2.2.2

LocalNet attack



LocalNet attack



default via tun0
1.2.3.0/24 via eth0



Target.com

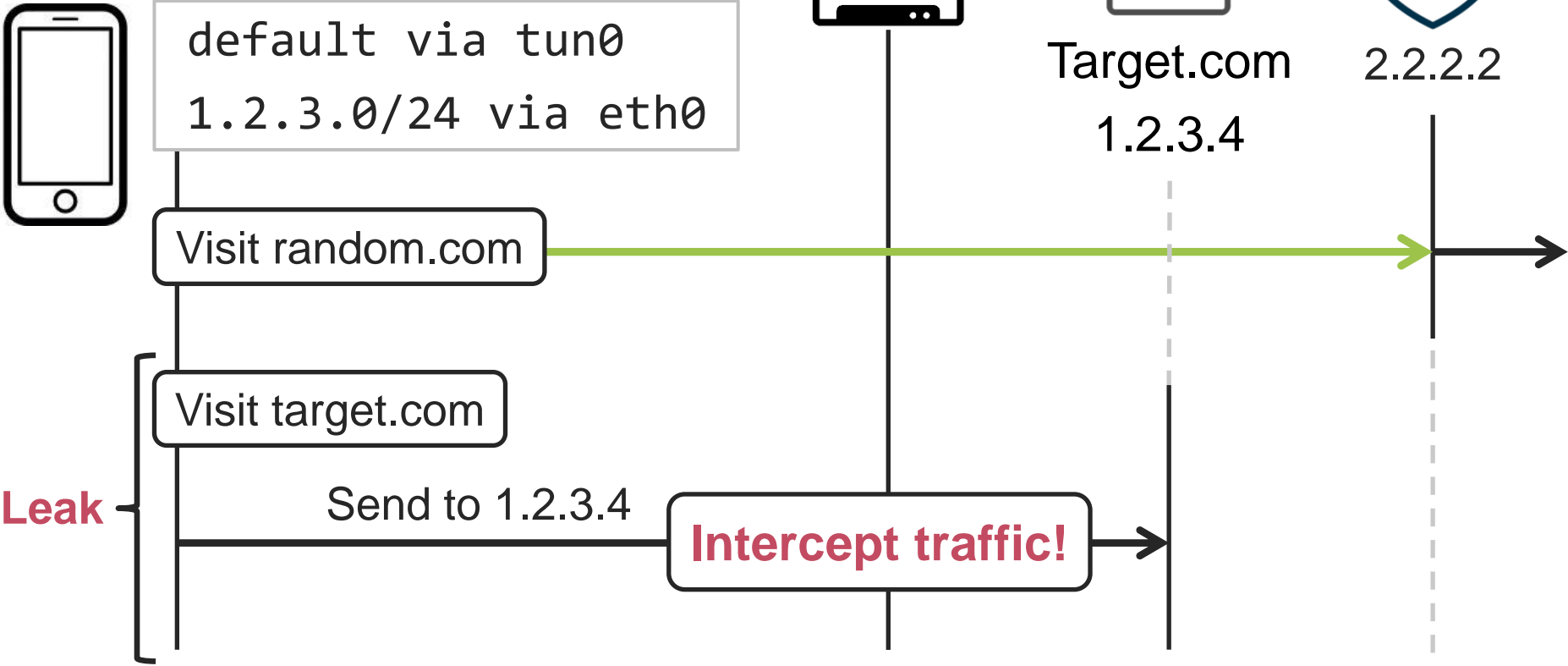
1.2.3.4



2.2.2.2



LocalNet attack

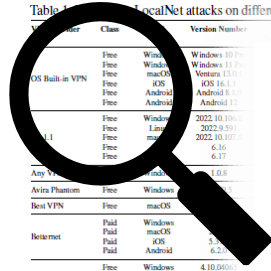


LocalNet attack: 195 experiments



Table 1: LocalNet attacks on different VPN clients.

VPN Provider	Class	OS	Version Number	LAN Setting	Result
OS Built-in VPN	Free	Windows	Windows 10 Pro	No N/A	✗
	Free	Windows	Windows 11 Pro	No N/A	✗
	Free	macOS	Ventura 13.0.1	No N/A	✗
	Free	iOS	iOS 16.1.1	No N/A	✗
1.1.1.1	Free	Android	Android 8.1.0	No N/A	✓
	Free	Windows	2022.10.106.0	No N/A	✓
	Free	Linux	2022.9.591	No N/A	✓
	Free	macOS	2022.10.107.0	No N/A	△
Hik-me VPN	Free	iOS	6.16	No N/A	✗
	Free	Android	6.17	No N/A	✓
	Free	Windows	2.0.2.274	No N/A	✗
	Free	macOS	2.5.6.158	No N/A	✗



VPN Provider

Class

OS

Version Number

LAN Setting | Result
Default LAN Access

OS Built-in VPN

1.1.1.1

VPN Provider	Class	OS	Version Number	LAN Setting	Result
TorGuard	Free	Windows	4.8.13	No N/A	✗
	Free	Linux	4.8.13	No N/A	✗
	Free	macOS	4.8.13	No N/A	✗
	Free	Android	1.60.9	No N/A	✗
XVPN	Free	Windows	73.0.2674	No N/A	✓
	Free	macOS	73.1.0.2791	No N/A	✗
	Free	iOS	31.3	No N/A	✗
	Free	Android	180.2778	No N/A	✓
TouchVPN	Free	Windows	2.0.2.274	No N/A	✗
	Free	macOS	2.5.6.158	No N/A	✗
	Free	iOS	4.4.1	No N/A	✗
	Free	Android	2.0.8	No N/A	✓

✗ always vulnerable, ✗ vulnerable by default LAN-Access-Setting
 ✓ vulnerable by using special use IP addresses if always secure,
 ✓ secure by default LAN-Access-Setting, △ local traffic blocked

LocalNet attack: 195 experiments

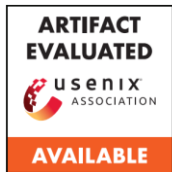


Table 1: LocalNet attacks on different VPN clients.

VPN Client	OS	Version Number	LAN Setting	Result
OS Built-in VPN	Free	Windows 10 Pro	No N/A	✗
	Free	Windows 11 Pro	No N/A	✗
	Free	macOS Monterey 13.0.1	No N/A	✗
	Free	iOS 16.1.1	No N/A	✗
	Free	Android 8.1.0	No N/A	✗
Cisco AnyConnect	Free	2022.10.106.0	No N/A	✗
	Free	2022.9.59.1	No N/A	✗
	Free	2022.10.107.0	No N/A	✗
Avira Phantom	Free	10.8	No N/A	✗
	Free	10.5	No N/A	✗
Betternet	Paid	Windows	No N/A	✗
	Paid	macOS	No N/A	✗
	Paid	iOS	No N/A	✗
	Paid	Android	No N/A	✗
Clarion VPN	Paid	Windows	No N/A	✗
	Paid	macOS	No N/A	✗
	Paid	iOS	No N/A	✗
	Paid	Android	No N/A	✗
CyberGhost	Paid	Windows	No N/A	✗
	Paid	macOS	No N/A	✗
	Paid	iOS	No N/A	✗
	Paid	Android	No N/A	✗
ExpressVPN	Paid	Windows	No N/A	✗
	Paid	Linux	No N/A	✗
	Paid	macOS	No N/A	✗
	Paid	iOS	No N/A	✗
Fast VPN	Free	Windows	No N/A	✗
	Free	Linux	No N/A	✗
	Free	macOS	No N/A	✗
	Free	iOS	No N/A	✗
Hik-me VPN	Free / Paid	Windows	No N/A	✗
	Free / Paid	Linux	No N/A	✗
	Free / Paid	macOS	No N/A	✗
	Free / Paid	iOS	No N/A	✗
HikMyAss	Paid	Windows	No N/A	✗
	Paid	Linux	No N/A	✗
	Paid	macOS	No N/A	✗
	Paid	iOS	No N/A	✗
Hotspot Shield	Free	Windows	No N/A	✗
	Free	macOS	No N/A	✗
	Free	iOS	No N/A	✗
	Free	Android	No N/A	✗
IPVanish	Paid	Windows	No N/A	✗
	Paid	macOS	No N/A	✗
	Paid	iOS	No N/A	✗
	Paid	Android	No N/A	✗
Multivo	Paid	Windows	No N/A	✗
	Paid	macOS	No N/A	✗
	Paid	Linux	No N/A	✗
	Paid	iOS	No N/A	✗

Network Manager	Free	Linux	1.19.3	No	N/A	✗
OpenVPN	Free	Linux	1.8.2	No	N/A	✗
	Free	Linux	1.8.12	No	N/A	✗
	Free	Linux	1.8.18	No	N/A	✗
NordVPN	Paid	Windows	7.2.2.0	No	N/A	✗
	Paid	Linux	4.0.0	No	N/A	✗
NordVPN	Paid	macOS	7.1.3.7	No	N/A	✗
	Paid	iOS	7.1.3.7	No	N/A	✗

TunnelBear	Paid	Windows <th>4.6.1</th> <th>No</th> <th>N/A</th> <th>△</th>	4.6.1	No	N/A	△
TunnelBear	Paid	macOS	4.1.8 <td>No</td> <td>N/A</td> <td>△</td>	No	N/A	△
	Paid	iOS	4.3.2 <td>No</td> <td>N/A</td> <td>△</td>	No	N/A	△
	Paid	Android	3.6.8 <td>No</td> <td>N/A</td> <td>△</td>	No	N/A	△
Tunnelblick	Free	macOS	3.8.7a <td>No</td> <td>N/A</td> <td>✗</td>	No	N/A	✗
	Free	Windows	2.10.10 <td>No</td> <td>N/A</td> <td>✗</td>	No	N/A	✗

ExpressVPN

Paid	Windows	12.37.0	Yes Yes	△
Paid	Linux	3.36	No N/A	△
Paid	macOS	11.12.0	Yes Yes	△
Paid	iOS	11.70.0	Yes Yes	✗
Paid	Android	10.63.2	Yes Yes	✓

VPN Proxy Master for iPhone

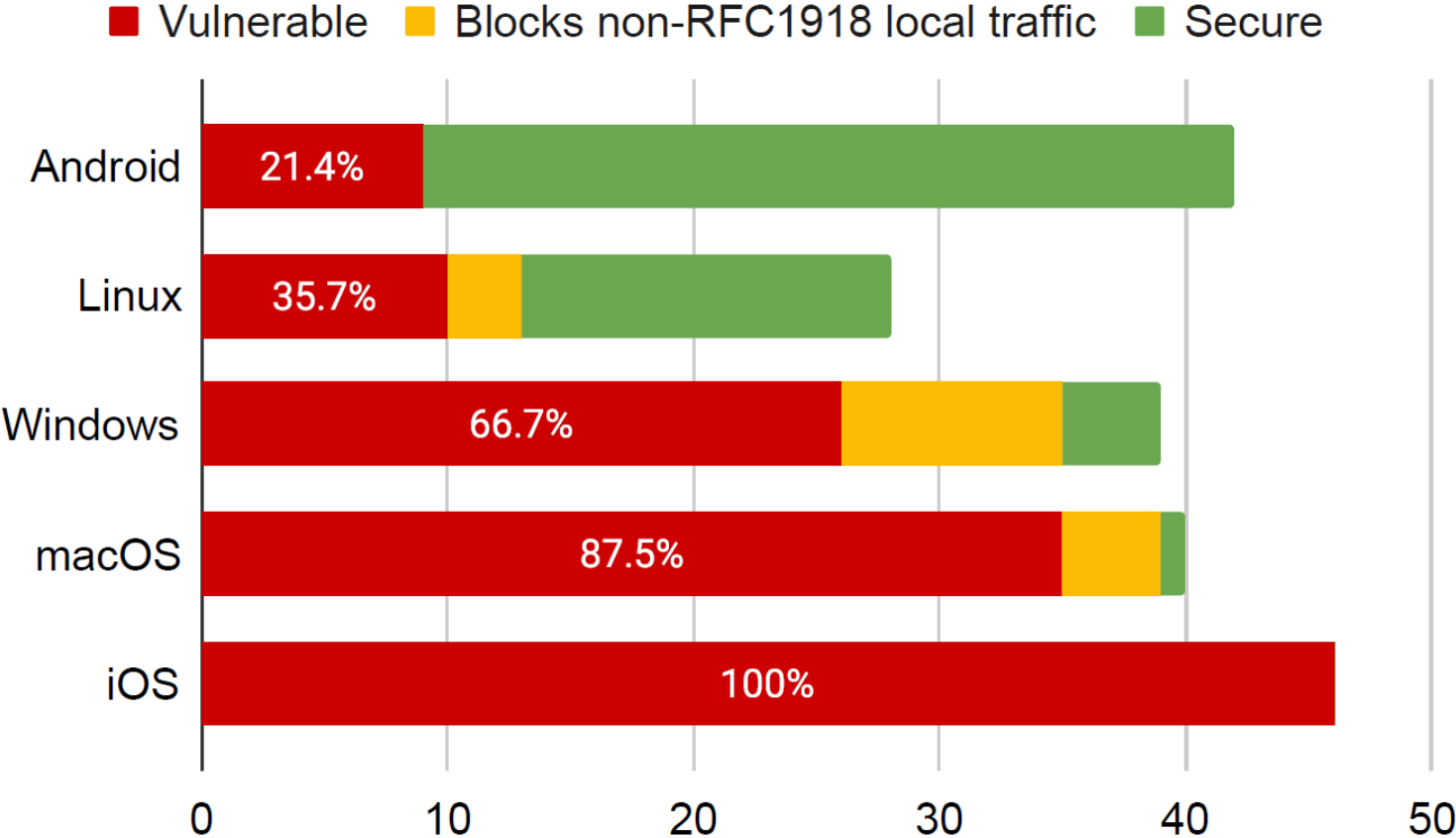
Free	iOS	2.1.5	No N/A	†
------	-----	-------	----------	---

Star VPN	Free	Windows <th>1.5.4</th> <th>No</th> <th>N/A <th>✗</th> </th>	1.5.4	No	N/A <th>✗</th>	✗
Star VPN	Free	macOS	2.11.0	No	N/A	✗
	Free	iOS	3.6.0	No	N/A	✗
	Free	Android	1.8	No	N/A	✗
Strong VPN	Paid	Windows	2.6.2.0	No	N/A	✗
	Paid	macOS	2.2.2	No	N/A	✗
	Paid	iOS	2.6.0	No	N/A	✗
Super VPN	Free	iOS	3.2.6	No	N/A	✗
	Free	Android	1.6.2	No	N/A	✗
T1S Tunnel	Free	Android	5.0.5	No	N/A	✓
	Paid	Windows	4.8.13	No	N/A	✗
TortGuard	Paid	Linux	4.8.13	No	N/A	✗
	Paid	macOS	4.8.13	No	N/A	✗
	Paid	iOS	4.4.1	No	N/A	✗
TouchVPN	Free	Windows	2.0.2.274	No	N/A	✗
	Free	macOS	2.5.6.158	No	N/A	✗
	Free	iOS	5.4.1	No	N/A	✗

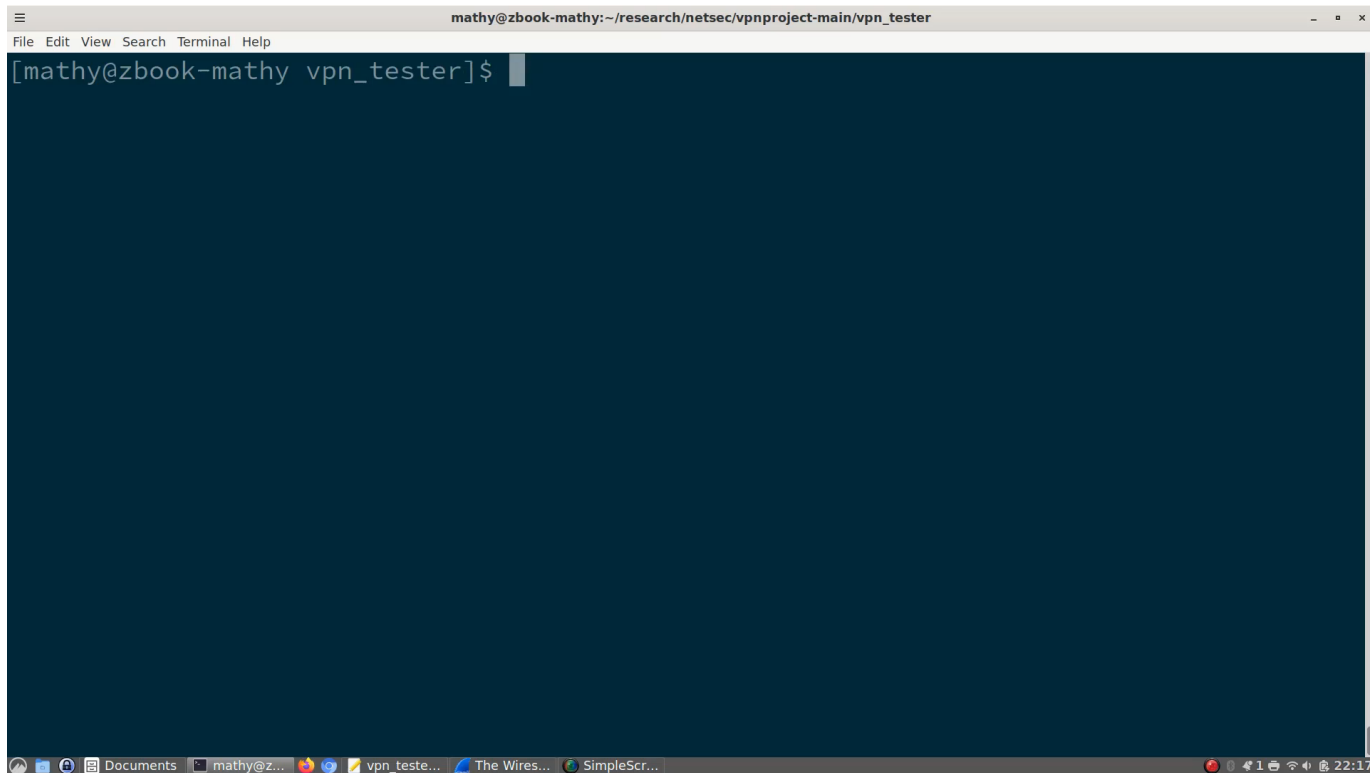
Windscribe built-in	Free	Windows <th>2.5.17</th> <th>Yes</th> <th>No</th> <th>△</th>	2.5.17	Yes	No	△
Windscribe built-in	Free	Linux	2.5.17 <td>Yes</td> <td>No</td> <td>✓</td>	Yes	No	✓
	Free	macOS	2.4.11 <td>Yes</td> <td>No</td> <td>△</td>	Yes	No	△
	Free	iOS	3.4.1(273) <td>Yes</td> <td>Yes</td> <td>✗</td>	Yes	Yes	✗
	Free	Android	3.3.1003 <td>Yes</td> <td>No</td> <td>✓</td>	Yes	No	✓
Windscribe 3rd-party	Free	Linux	2.5.17 <td>Yes</td> <td>No</td> <td>✓</td>	Yes	No	✓
	Free	Windows	0.5.3	No	N/A	△
WireGuard	Free	Linux	1.0.20210914	No	N/A	✓
	Free	macOS	1.0.15	No	N/A	✗
	Free	iOS	1.0.15	No	N/A	✗
	Free	Android	1.0.20220316	No	N/A	✓
XVPN	Free	Windows	731.0.267.4	No	N/A	✓
	Free	macOS	731.0.279.1	No	N/A	✓
	Free	iOS	31.3	No	N/A	✗

✗ always vulnerable, △ vulnerable by default LAN-Access-Setting
 † vulnerable by using special use IP addresses if always secure,
 ✓ secure by default LAN-Access-Setting, △ local traffic blocked

LocalNet attack: summary



DEMO



Selected special cases



Some clients block traffic to local network

- › Problem when local network uses public IPs
- › Traffic to these public IPs gets blocked!



VPN Proxy Master for iPhone (and others)

- › DNS server returns private-use IP addresses
- › VPN server forwards traffic to real IP address

The iOS case



Prevent attacks by setting `includeAllNetworks=True`

- › And `excludeLocalNetworks=False` on iOS \geq 14.2
- › Causes reliability issues, vendors hesitant to enable this

Result is that **iOS remains less secure**

- › Context: VPNs on iOS were already known to leak traffic in certain scenarios.
- › E.g., OS traffic may leak, leaks when switching networks,...

We were warned in the past...



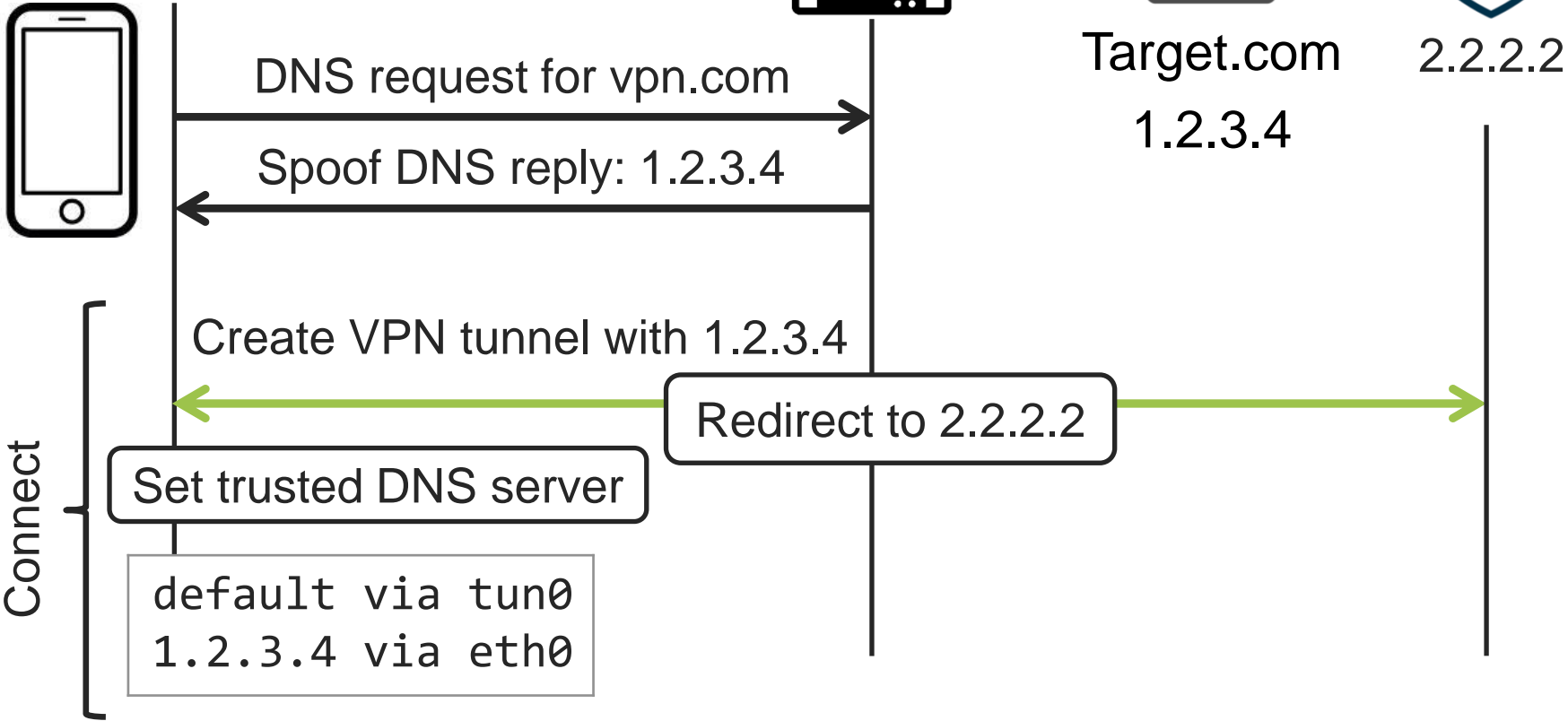
Andrew Ayer: [Hardening OpenVPN for DEF CON](#) (2015)

- › Guide for OpenVPN on Linux
- › Essentially suggested the risk of LocalNet attacks!

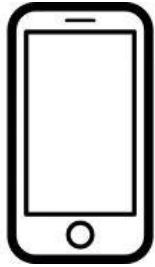
Unclear how widespread this issue (already) was at the time

- › VPN clients were not systematically tested → vendors were not warned, so clients never were not audited either
- › Using domain names would still enable ServerIP attacks...

ServerIP attack



ServerIP attack



```
default via tun0  
1.2.3.4 via eth0
```



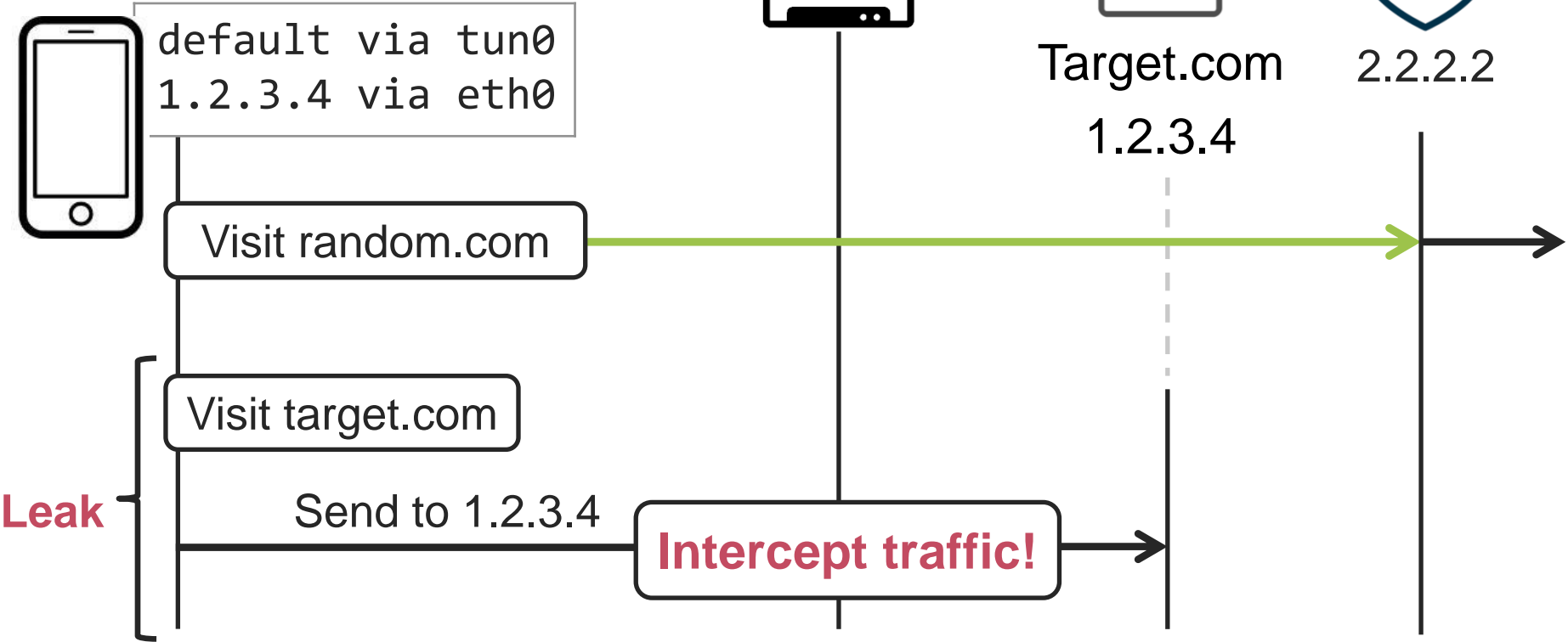
Target.com
1.2.3.4



2.2.2.2



ServerIP attack



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 for different IPs...

DEMO

```
mathy@mathy-VirtualBox:~/vpn_tester$  
mathy@mathy-VirtualBox:~/vpn_tester$  
mathy@mathy-VirtualBox:~/vpn_tester$  
mathy@mathy-VirtualBox:~/vpn_tester$ █
```

I

Defenses

LocalNet attack: disable local network access when it's using public IP addresses.

- › Or allow local network access when using 192.168.* or alike

ServerIP Attack: send all traffic over VPN, except packets generated by VPN process

- › On Linux, you can use fwmark (policy-based routing)
- › Or quick fix: use secure DNS to get VPN server's IP address

Disclosure

- › Reported to CERT/CC on May 10, 2023
- › Reported to selected vendors that had a security contact:
 - › Some had no e-mail contact, only a bug bounty program
 - › In report say we **deviate from T&Cs** and reserve **right to disclose**

Disclosure: special cases



Dubai-based ClarioVPN

- › Initially: *“MitM attacks are out of scope”*
- › Later: *“Clario isn’t interested in participating in this multi-party disclosure on VPN security”*



Ivanti Pulse Secure

- › Provided a test server! But at first didn’t work
- › Kept asking for time-consuming recordings
- › Seems like they didn’t try our PoC script...

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