

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

KU LEUVEN

DistriNet



NEW YORK UNIVERSITY

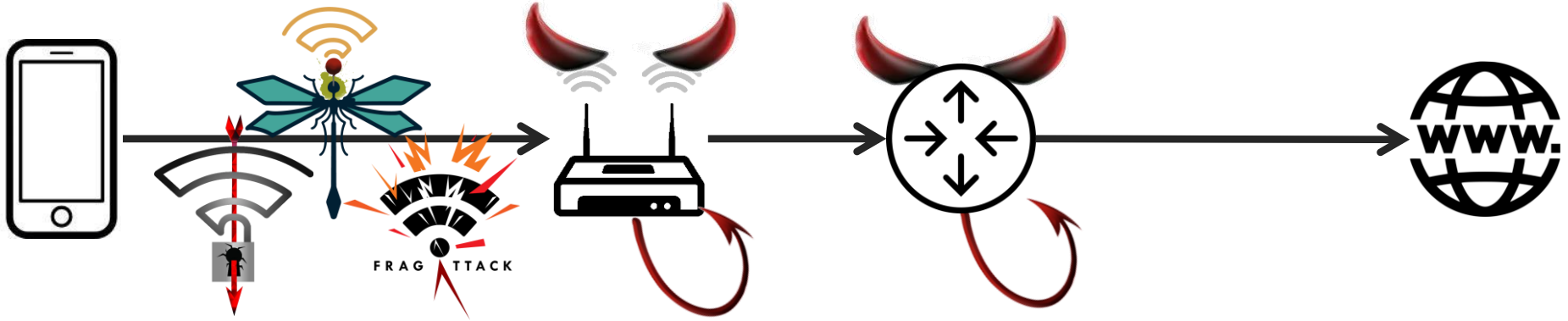


NYU ABU DHABI

Usage of VPNs: watch videos from other country

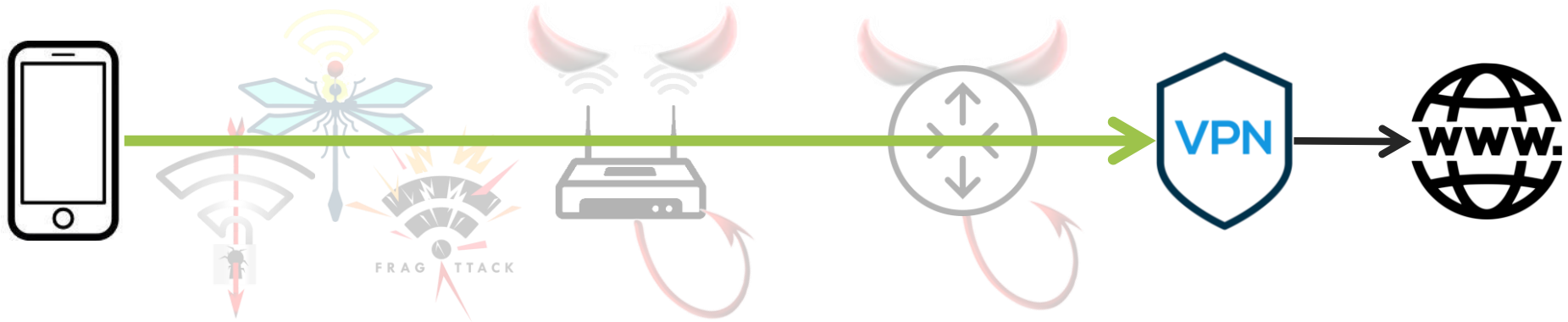


Usage of VPNs: protect your traffic



- › 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



1

```
$ ip route  
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

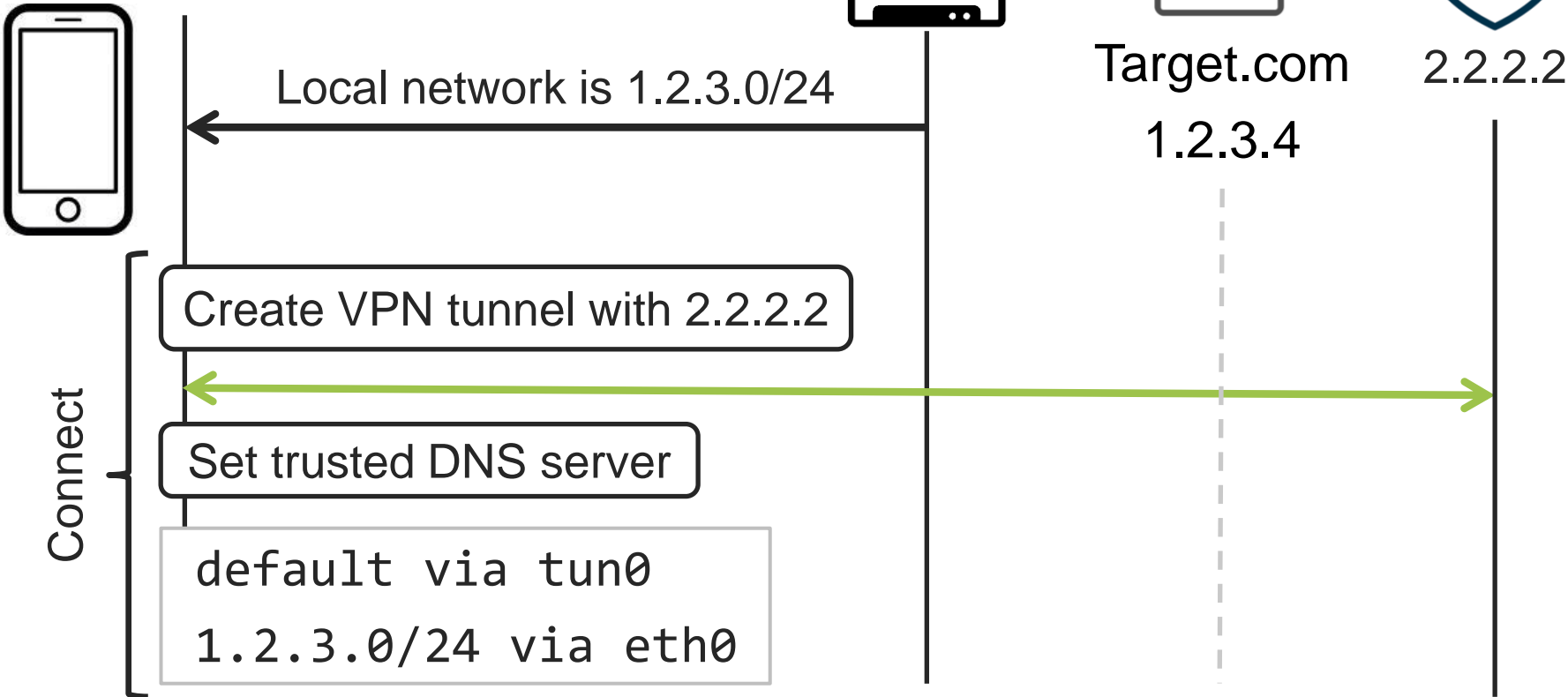


```
$ cat /etc/resolv.conf  
nameserver 2.2.2.3
```

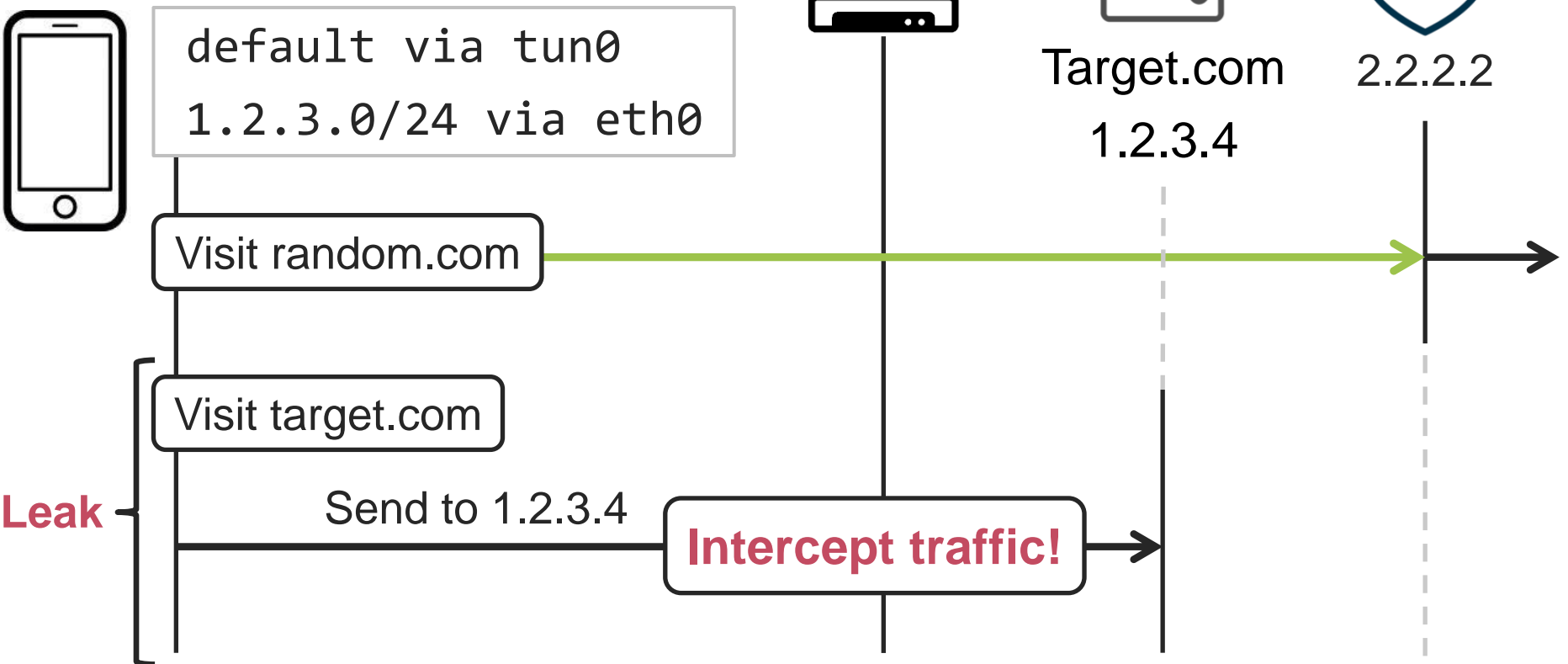
Can't trust the network's DNS server. Once connected:

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

LocalNet attack



LocalNet attack



LocalNet attack: 195 experiments

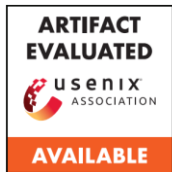
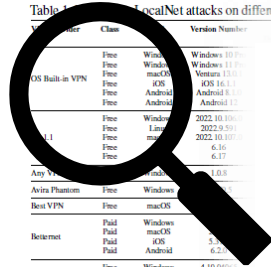


Table 1: LocalNet attacks on different VPN clients.

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	Android	Android 12	No N/A	✓
Fast 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	✗
CyberGhost	Free	Android	Android 8.1.0	No N/A	✓
	Free	Android	Android 12	No N/A	✓
	Free	Windows	2022.10.106.0	No N/A	✓
	Free	Linux	2022.9.591	No N/A	✓
HikMe 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	✗
HikMyAss	Free	Android	Android 8.1.0	No N/A	✓
	Free	Android	Android 12	No N/A	✓
	Free	Windows	2022.10.106.0	No N/A	✓
	Free	Linux	2022.9.591	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
TortGuard	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	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	✓
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.

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	✗
Clario VPN	Paid	Windows	5.9.1.1662	✗
	Paid	macOS	5.9.1.1662	✗
	Paid	iOS	5.9.1.1662	✗
	Paid	Android	1.9.26.420979	✗
CyberGhost	Paid	Windows	8.3.7.9795	✗
	Paid	macOS	8.3.9.667	✗
	Paid	iOS	8.4.0	✗
	Paid	Android	5.6.17.1664	✗
ExpressVPN	Paid	Windows	12.37.0	✗
	Paid	Linux	3.36	✗
	Paid	macOS	11.12.0	✗
Fast VPN	Free	iOS	2.2.4	✗
	Paid	Windows	3.0.0	✗
	Paid	macOS	3.0.0	✗
Hik-me VPN	Free / Paid	Windows	3.10.0	✗
	Free / Paid	Linux	4.7.1	✗
	Free / Paid	iOS	4.11.0	✗
HikMyAss	Paid	Windows	5.21.0744	✗
	Paid	Linux	0.5	✗
	Paid	macOS	5.4.7	✗
Hotspot Shield	Free	Windows	2.10.8	✗
	Free	macOS	5.3.0b1028	✗
	Free	iOS	7.9.0	✗
IPVanish	Paid	Windows	4.1.2.122	✗
	Paid	macOS	3.3.0b07499	✗
	Paid	iOS	4.4.0	✗
Malvad	Paid	Windows	2022.0	✗
	Paid	macOS	2022.0	✗
	Paid	Linux	2022.0	✗

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

VPN Proxy Master for iPhone

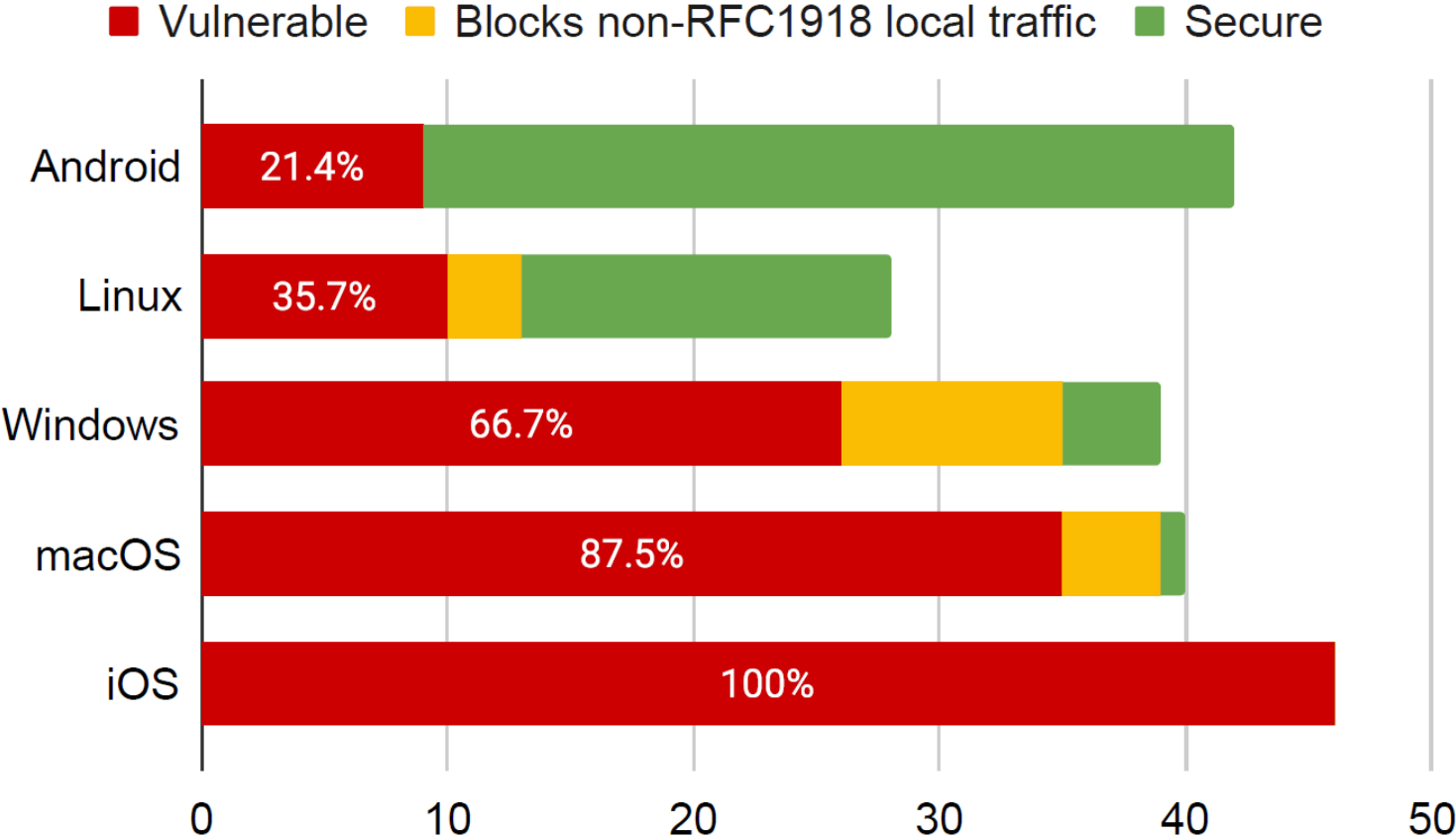
VPN Proxy Master for iPhone	Free	iOS	2.1.5	No N/A	†
-----------------------------	------	-----	-------	----------	---

Star VPN	Free	Windows <th>1.5.4</th> <th>No</th> <th>N/A</th> <th>✗</th>	1.5.4	No	N/A	✗
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	✗
Strong VPN	Paid	Android	2.3.3.6	Yes	No	✗
	Free	iOS	3.2.6	No	N/A	✗
Secure VPN Master	Free	Android	1.6.2	No	N/A	✗
	Free	Android	5.0.5	No	N/A	✓
TortGuard	Paid	Windows	4.8.13	No	N/A	✗
	Paid	Linux	4.8.13	No	N/A	✗
	Paid	macOS	4.8.13	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)	Yes	Yes	✗
	Free	Android	3.3.1003	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	731.0.2674	No	N/A	✓
	Free	macOS	731.0.2791	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



The iOS case

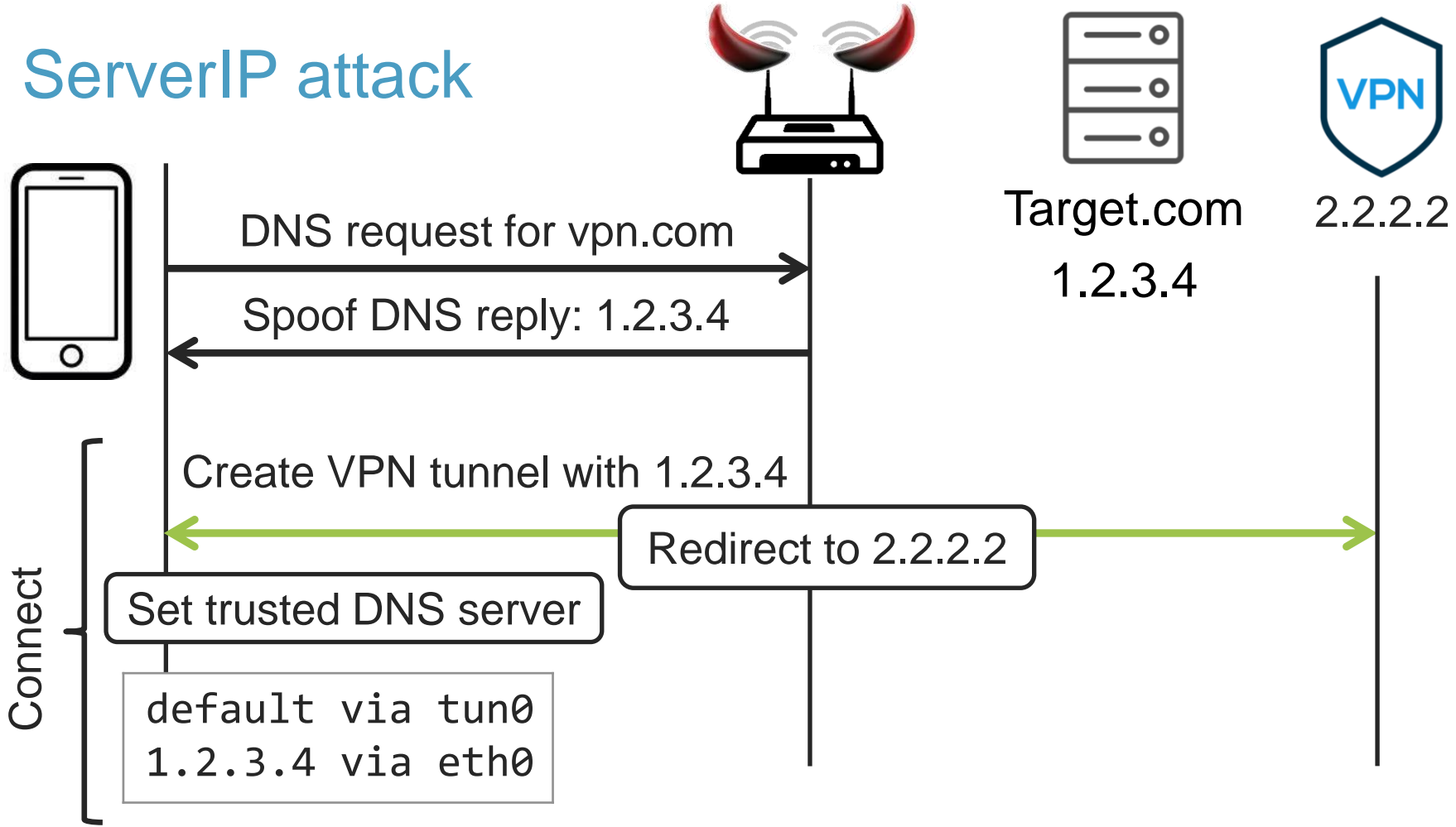
Attacks can be prevented by setting `includeAllNetworks`

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

Result is that **iOS remains less secure**

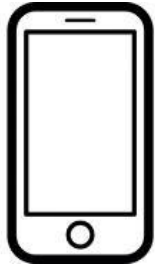
- › Context: VPNs on iOS were already known to leak traffic in certain scenarios.

ServerIP attack



Connect

ServerIP attack



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



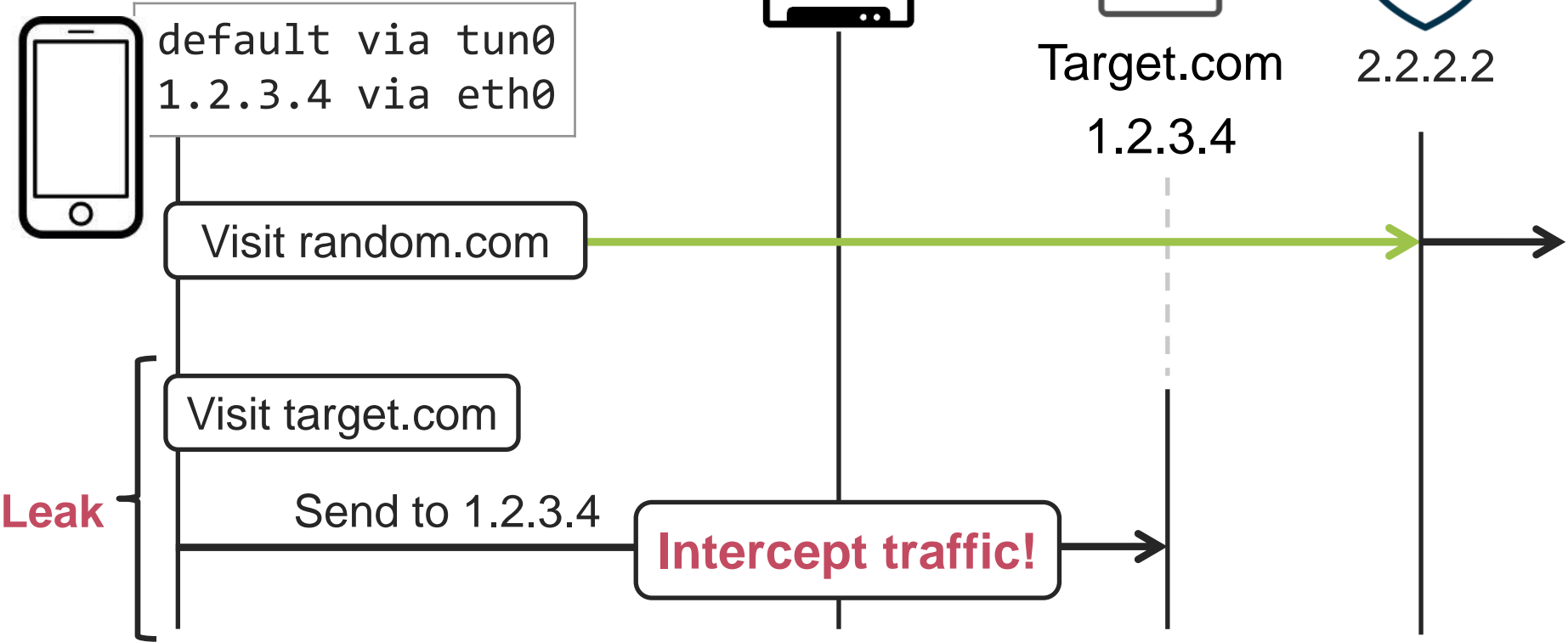
Target.com
1.2.3.4



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

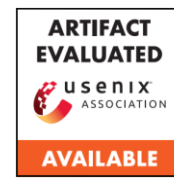
Impact: can leak traffic to single IP address

- › Can target the DNS server set by the VPN client 😊
- › Or repeat the attack...

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