Bypassing Tunnels:

Leaking VPN Client Traffic by Abusing Routing Tables

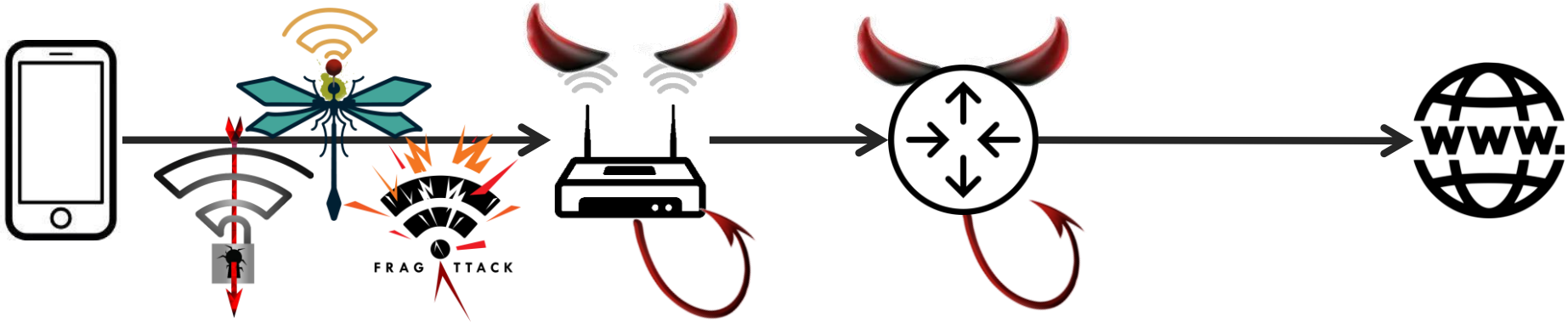
Nian Xue, Yashaswi Malla, Zihang Xia,
Christina Pöpper, and **Mathy Vanhoef**

USENIX Security, 9-11 August 2023, USA

KU LEUVEN
DistriNet
NEW YORK UNIVERSITY
NYU ABU DHABI

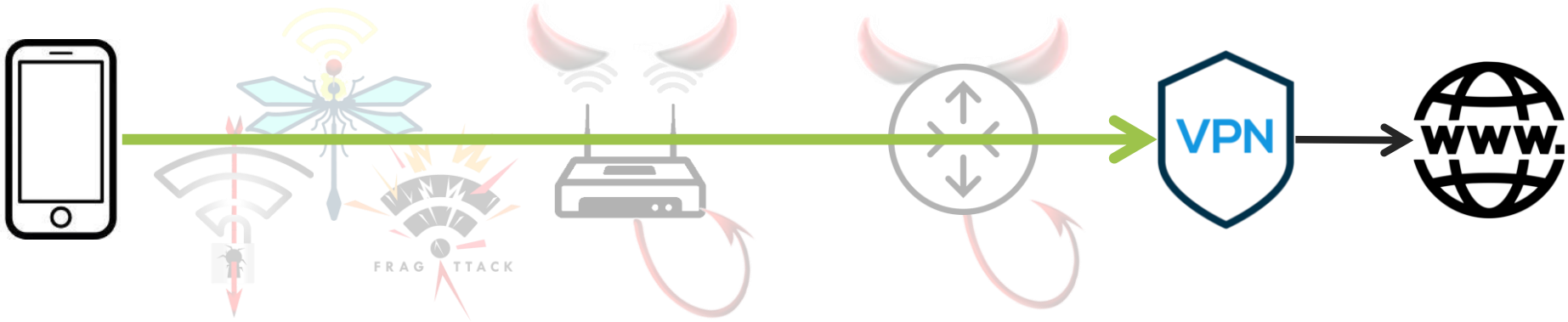
Usage of VPNs: watch videos from other country

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


```
$ ip route
default via tun0
```

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

Background: VPN client routing table


```
$ ip route
default via tun0
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
default via tun0
192.168.1.0/24 via eth0
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

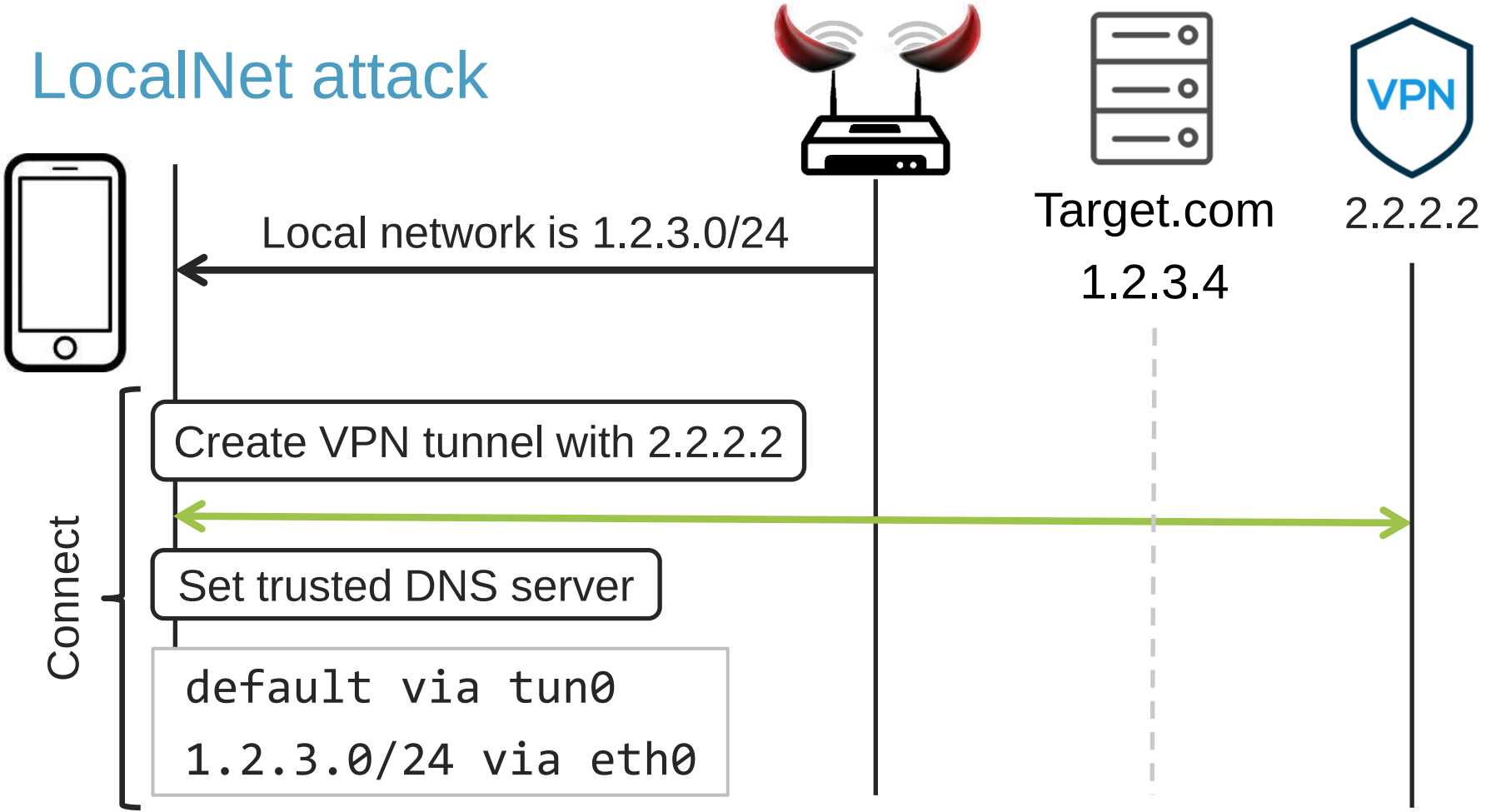

```
$ cat /etc/resolv.conf
nameserver 2.2.2.3
```

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

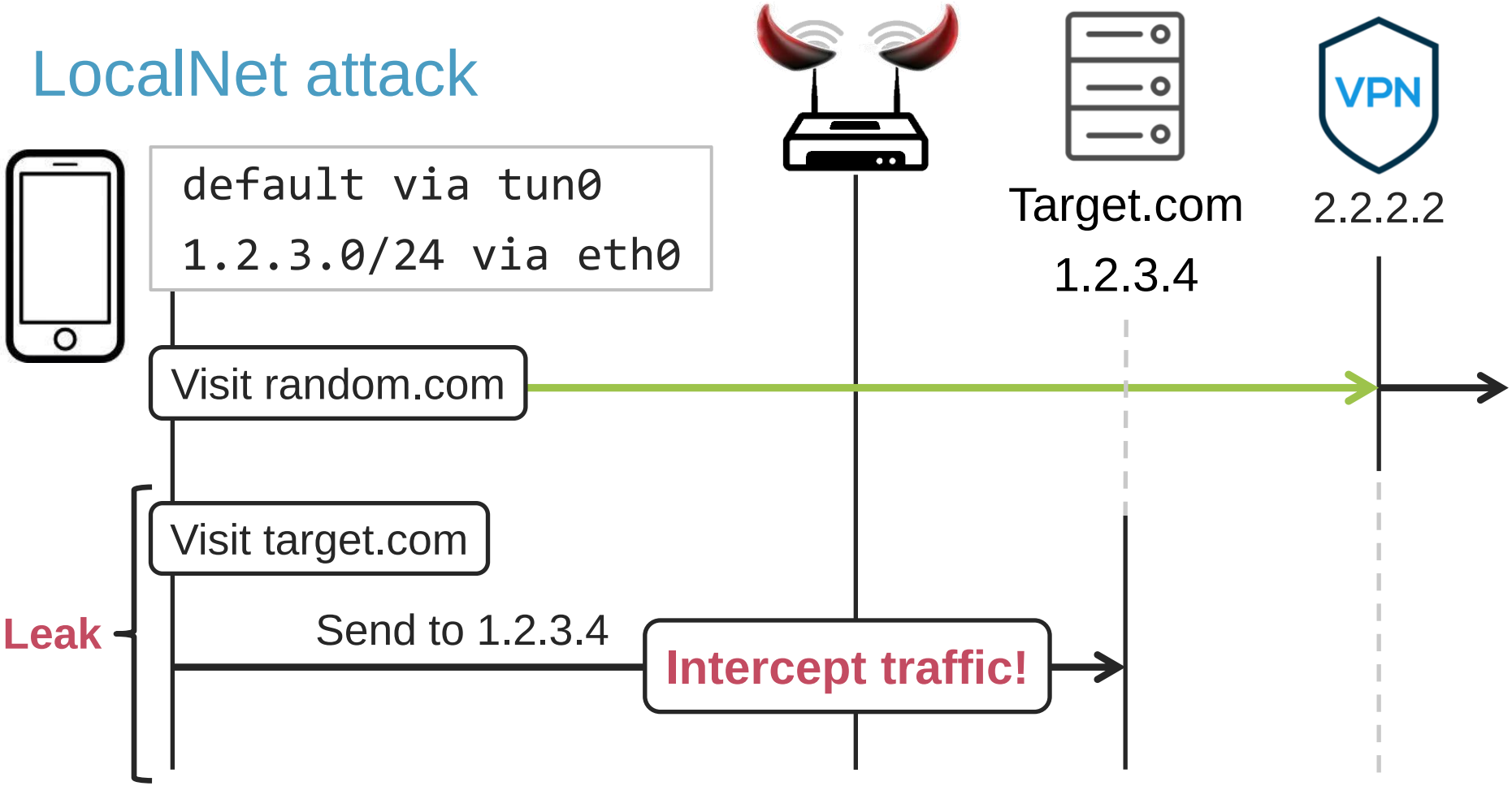
1. The VPN client sets a **trusted DNS server**
2. DNS is sent **through the VPN tunnel**

   \+ we assume other routing-based attacks are prevented

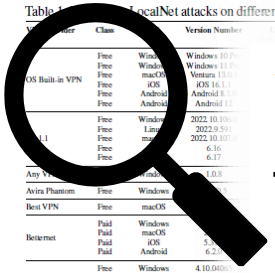
LocalNet attack



LocalNet attack

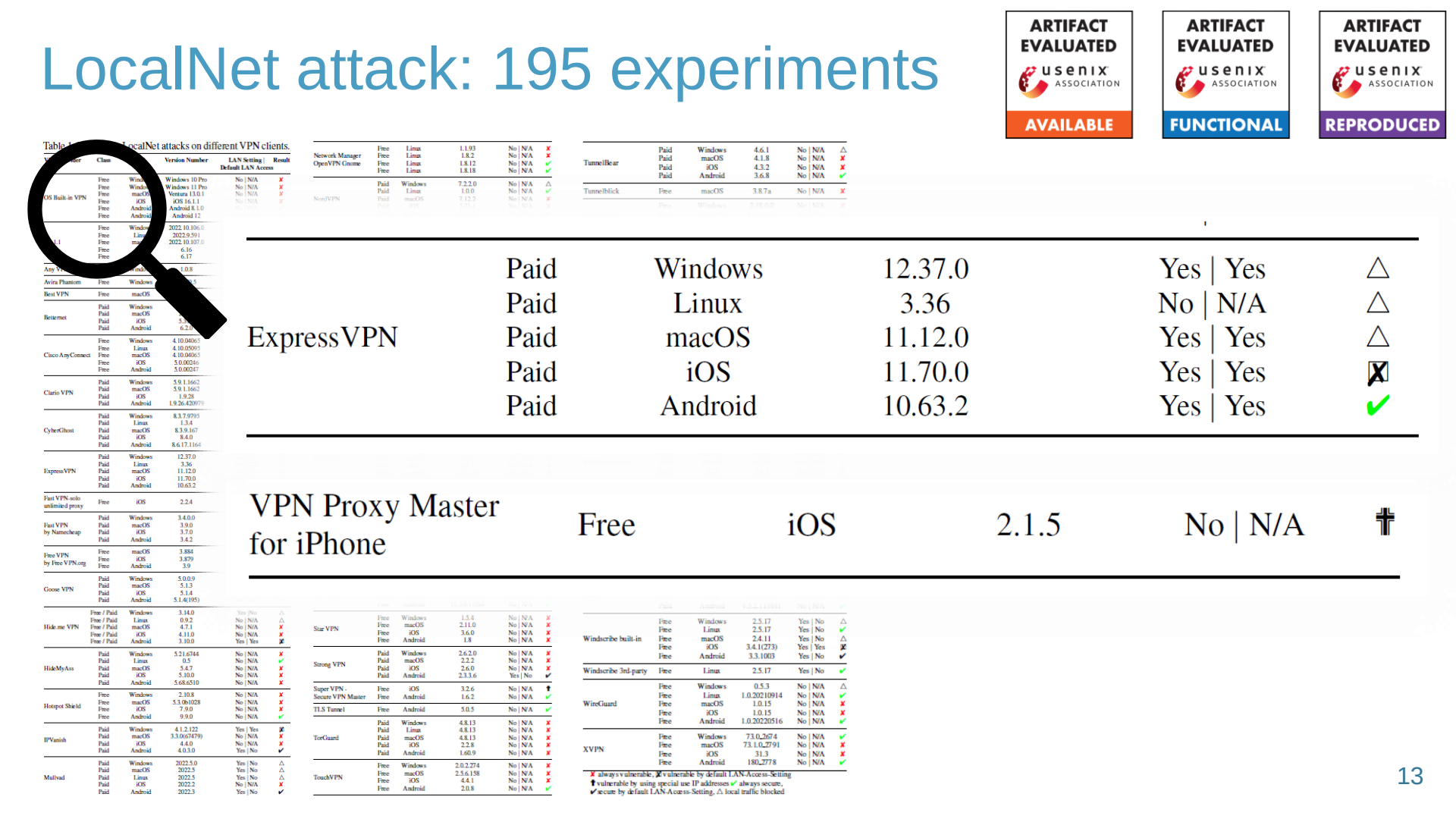


LocalNet attack: 195 experiments



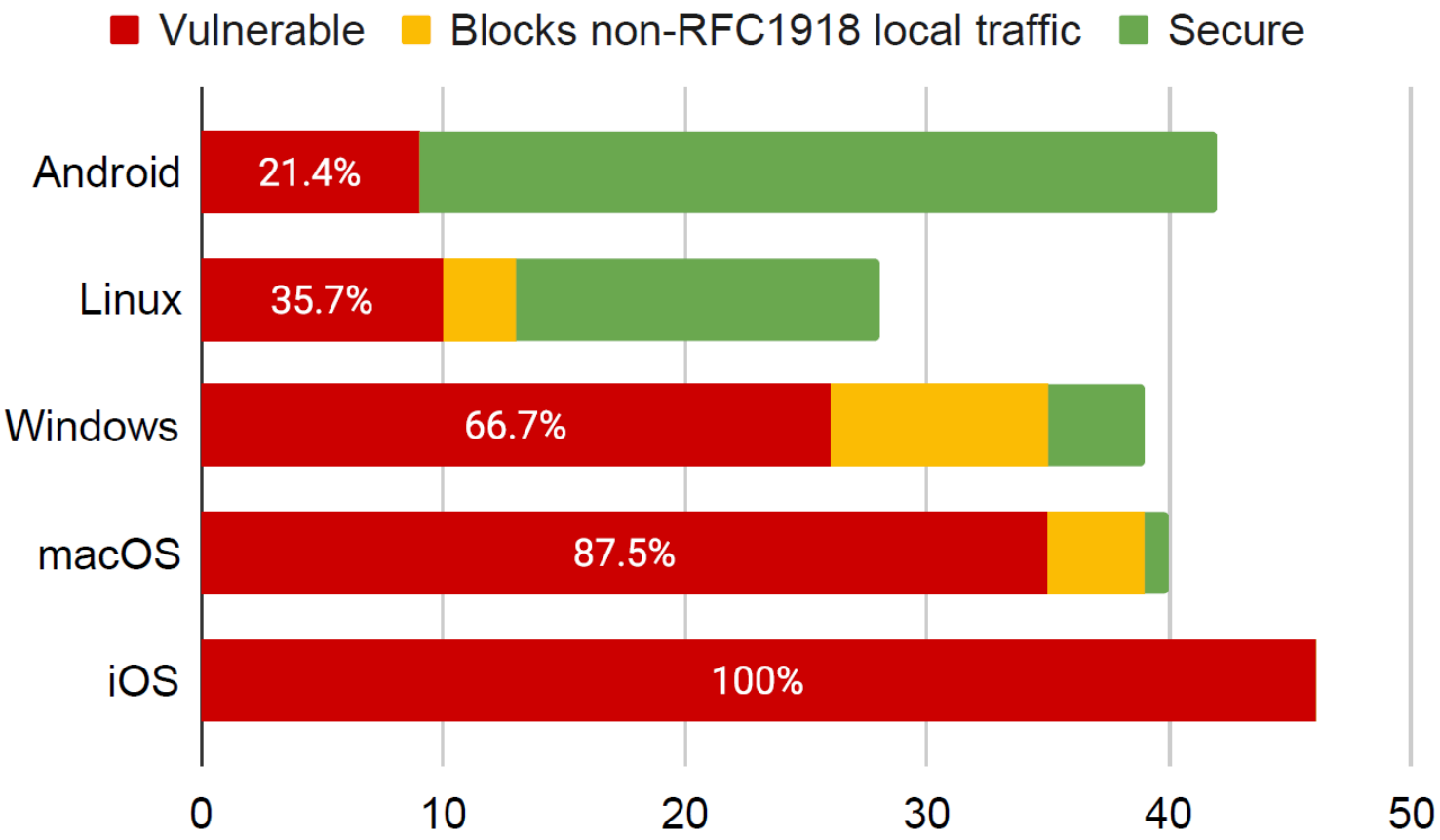
VPN Provider	Class	OS	Version Number	LAN Setting | Default LAN Access	Result
OS Built-in VPN	Free	Windows	Windows 10 Pro	No | N/A	✘
	Free	Windows	Windows 11 Pro	No | N/A	✘
	Free	macOS	Ventura 13.0.1	No | N/A	✘
	Free	iOS	iOS 16.1.1	No | N/A	✘
	Free	Android	Android 8.1.0	No | N/A	✔
	Free	Android	Android 12	No | N/A	✔
1.1.1.1	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	△
	Free	iOS	6.16	No | N/A	✘
	Free	Android	6.17	No | N/A	✔

LocalNet attack: 195 experiments



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	✝

LocalNet attack: summary



The iOS case

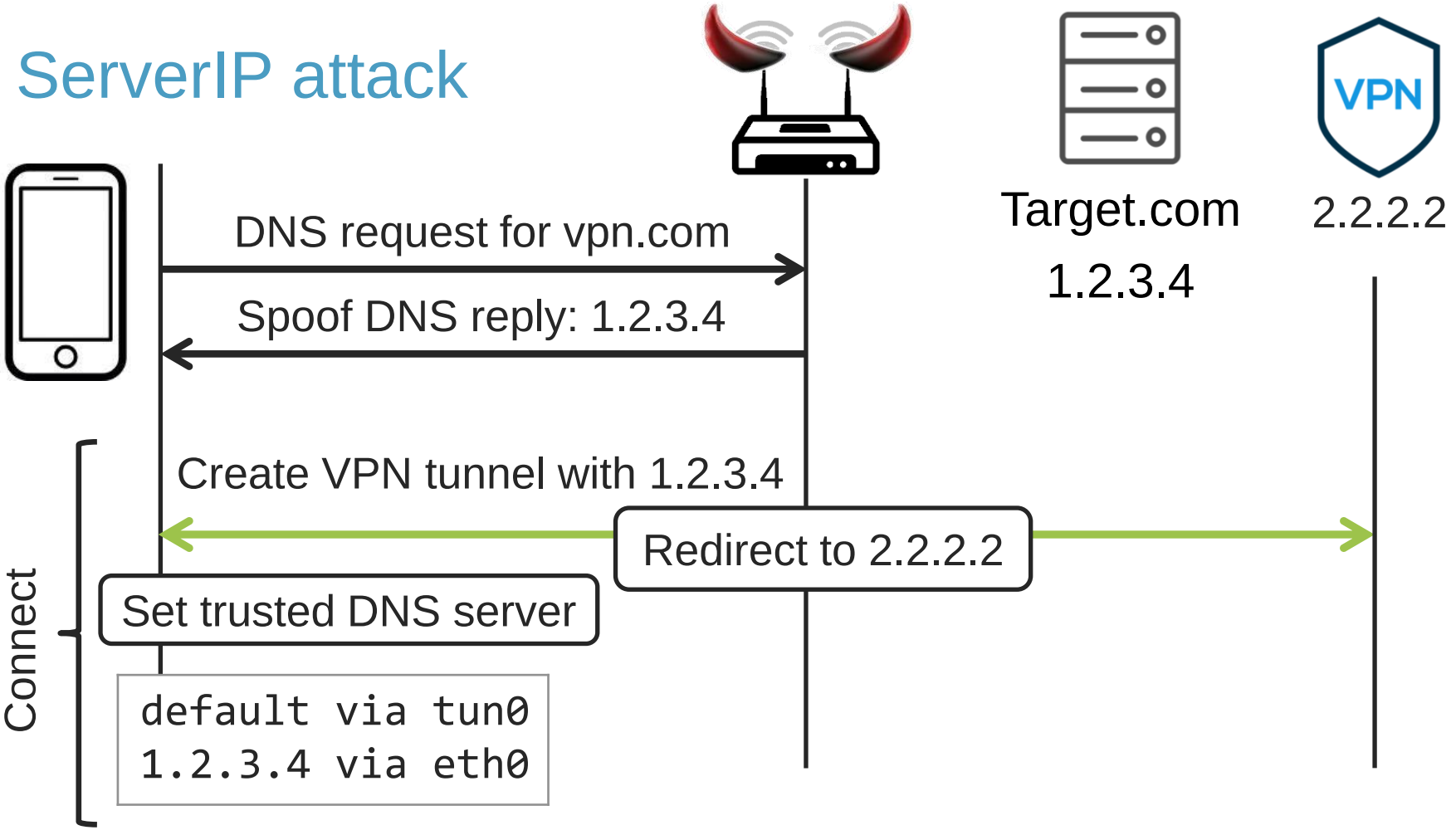
Attacks can be prevented by setting includeAllNetworks

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

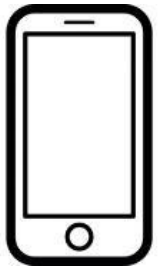
Result is that **iOS remains less secure**

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

ServerIP attack



ServerIP attack



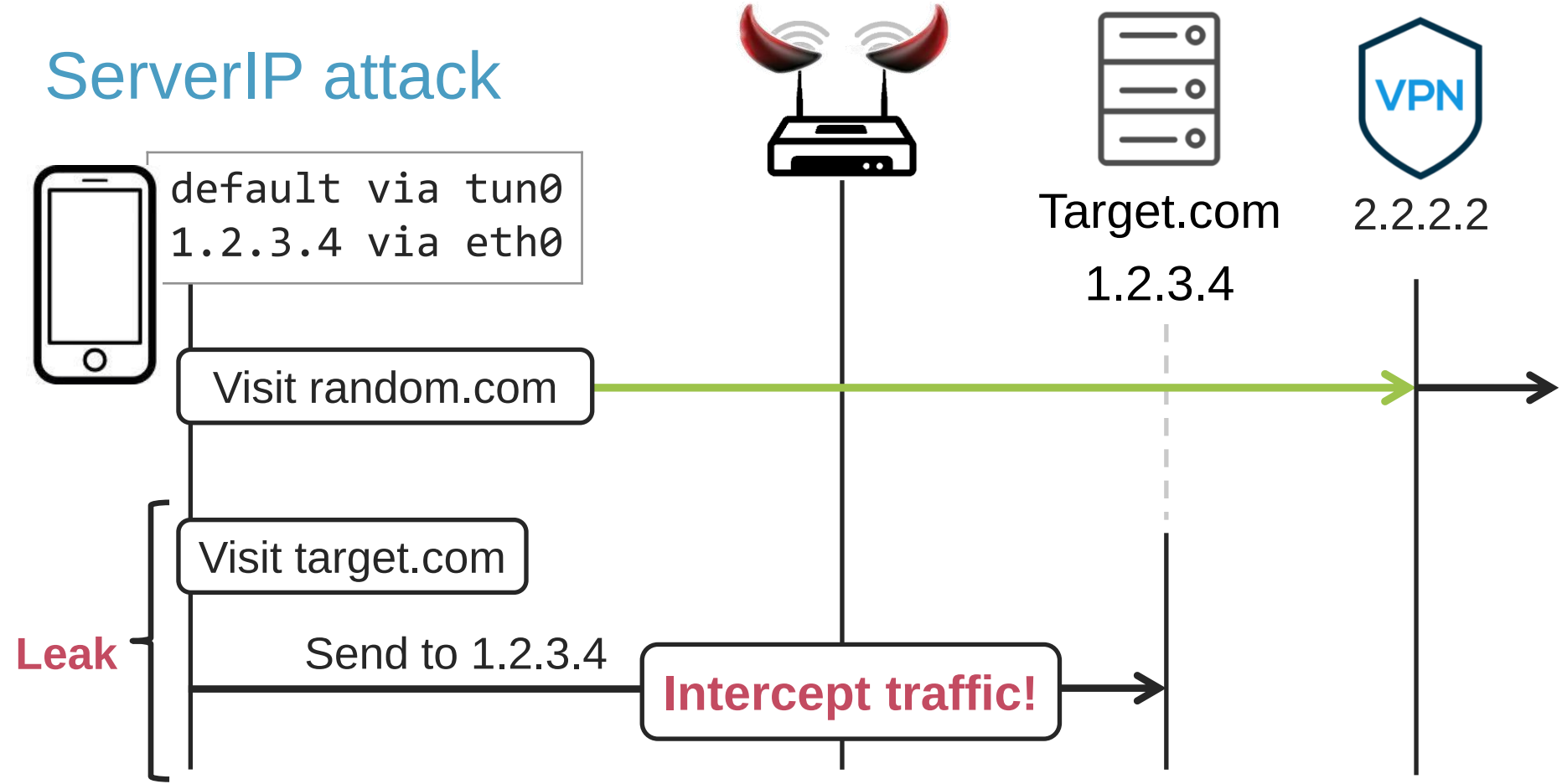
Target.com

1.2.3.4

2.2.2.2

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

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