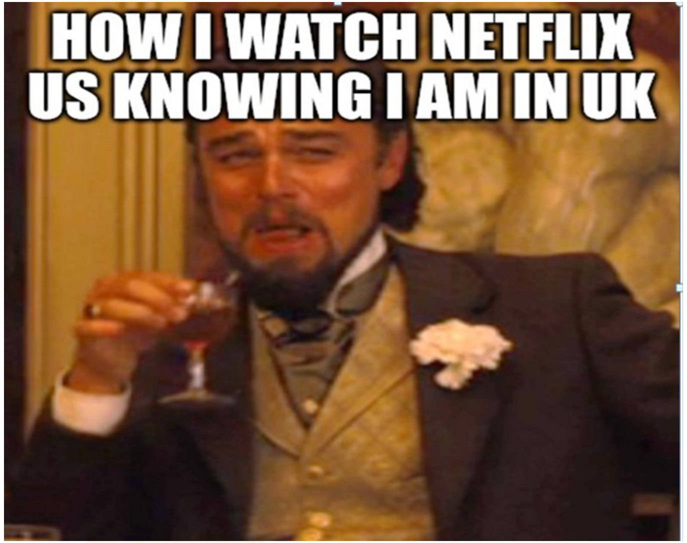
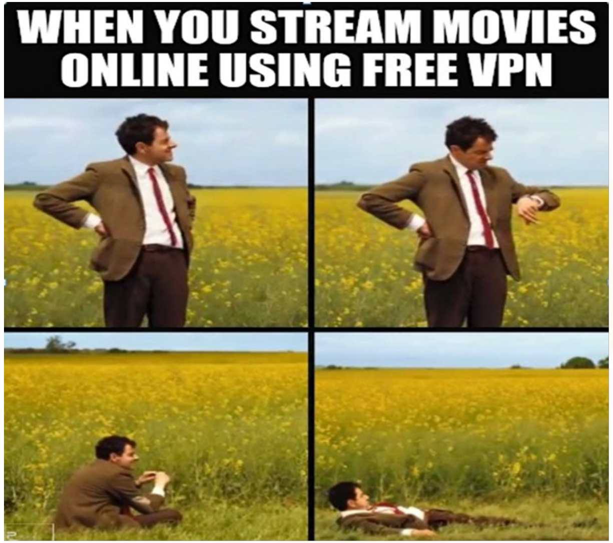
Leaking VPN Client Traffic by Abusing Routing Tables: A Deep Dive into LocalNet Attacks

About me

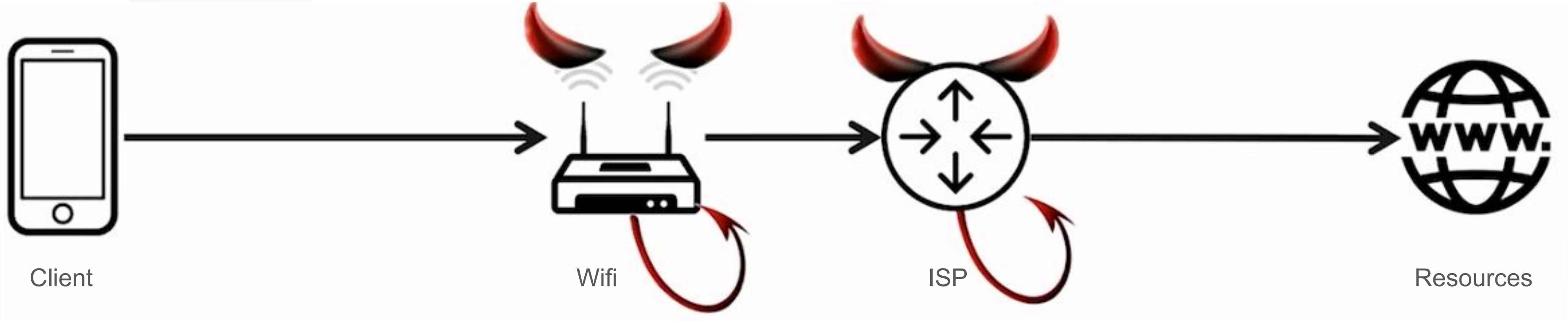
Dhruv Bhavsar
4+ Year of Cloud & Workspace Security Expert
miniOrange

Usage of VPNs: Watch videos from other country



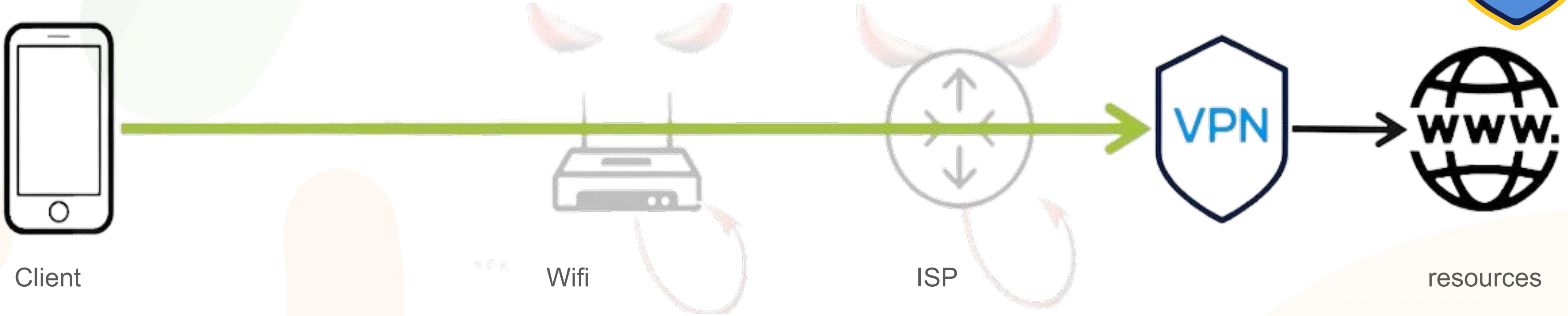


What if there is no VPN?



- Identify website visits: IP address, plaintext DNS,...
- Attack TLS: sslstrip

Usage of VPNs: Protect your traffic



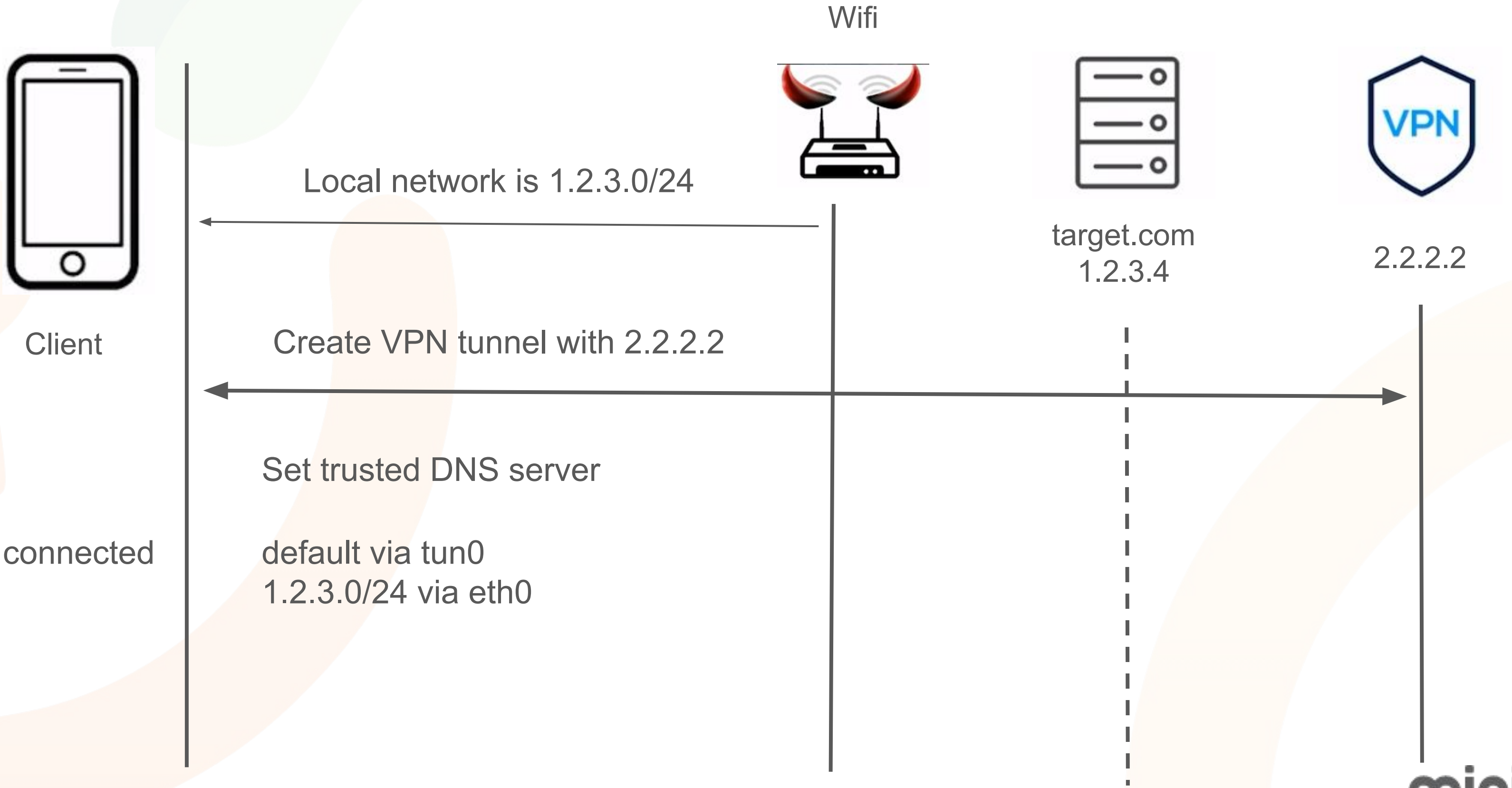
- Defend against untrusted Wi-Fi & compromised core routers
- Research goal: trick the client into leaking packets?
  - Yes, by manipulating the client's routing table -> **66% vulnerable!**
  - Attacks are independent of the cryptographic protocol

Background: VPN client routing table

```
$ ip route                          #Simplified output
default via tun0  #main routing rule
192.168.1.0/24 via eth0 - #IP range of within local N/W
```

- By default, send packets over tun0 = over the VPN tunnel
- **LocalNet exception:** local network is directly accessible
- Once connected, VPN client sets a **trusted DNS server**

LocalNet attack



Wifi

Client

target.com
1.2.3.4

2.2.2.2

Local network is 1.2.3.0/24

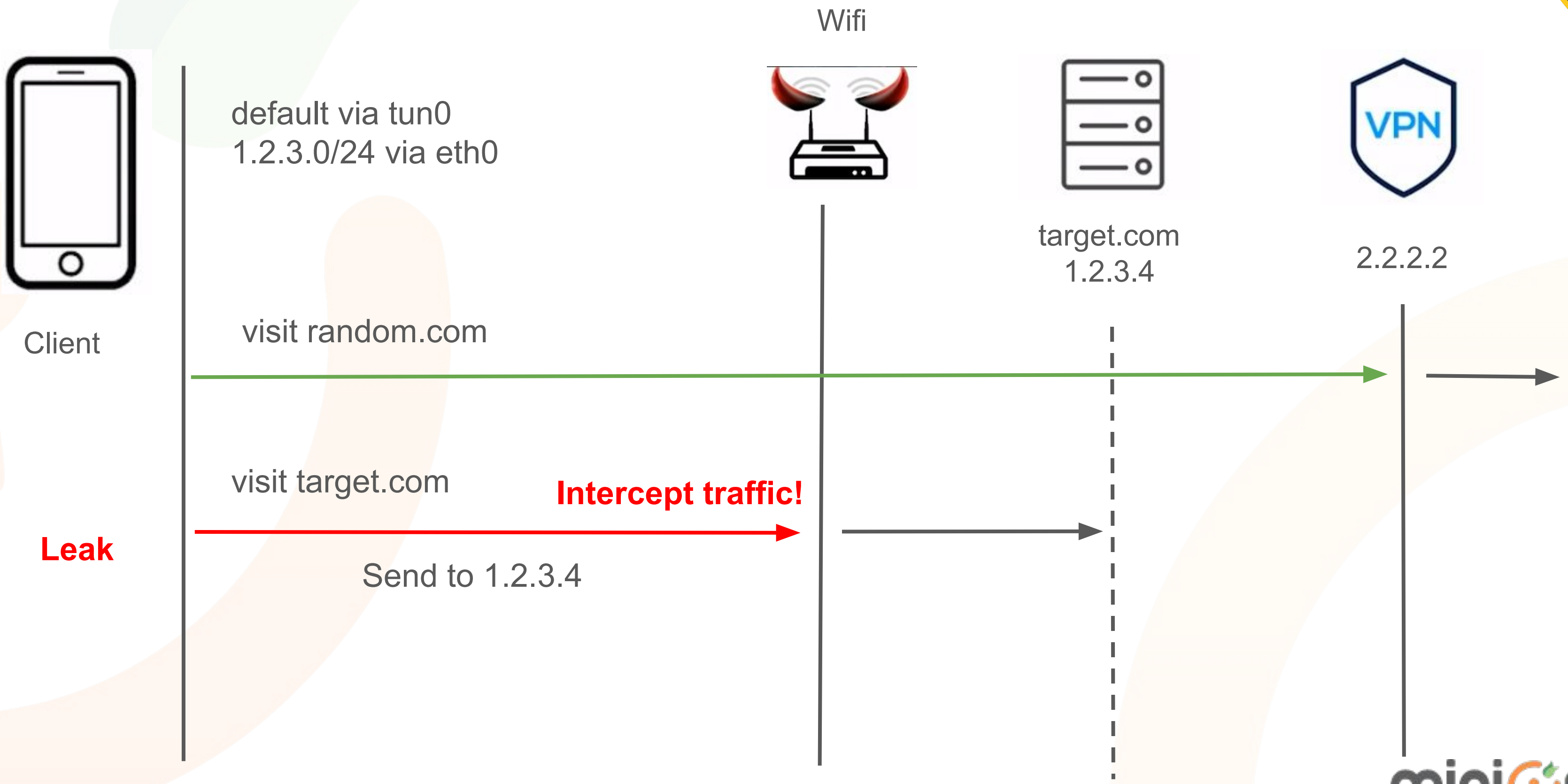
Create VPN tunnel with 2.2.2.2

Set trusted DNS server

connected

default via tun0
1.2.3.0/24 via eth0

LocalNet attack



Wifi

default via tun0
1.2.3.0/24 via eth0

target.com
1.2.3.4

2.2.2.2

Client

visit random.com

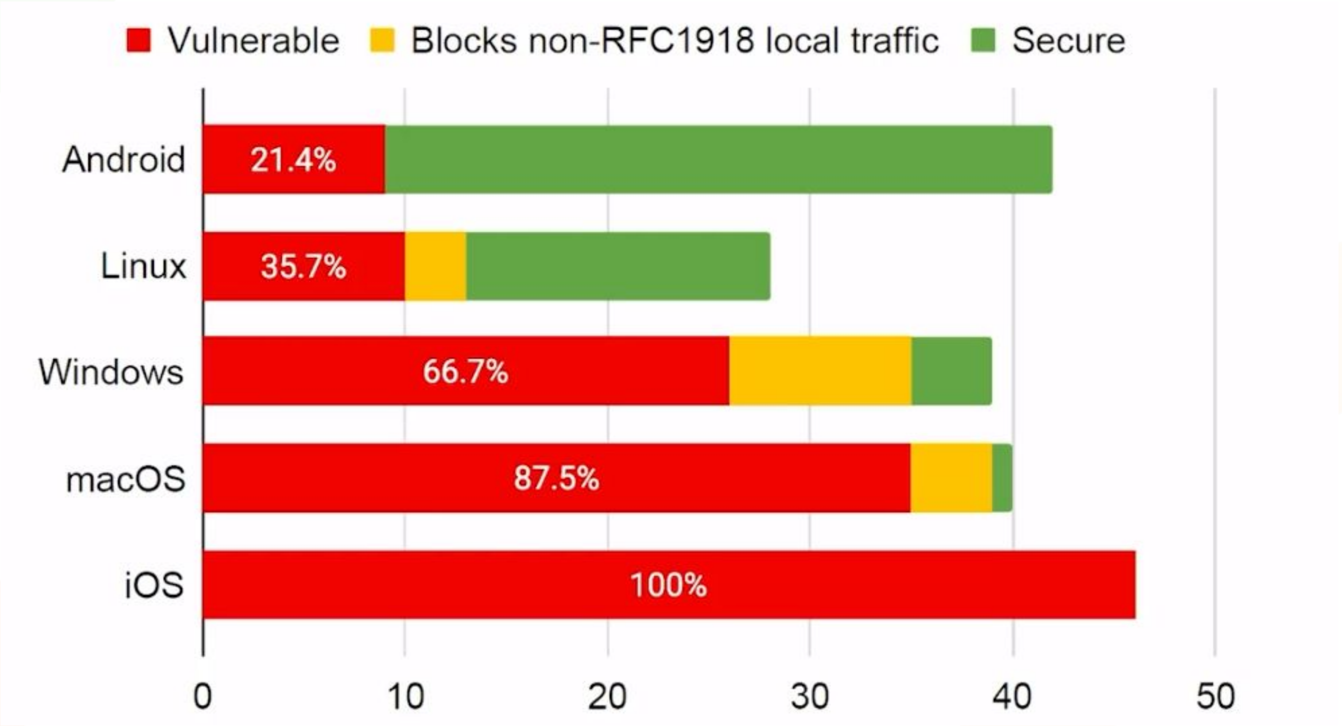
visit target.com

Intercept traffic!

Leak

Send to 1.2.3.4

LocalNet attack: Summary



Reference: [Usenix2023 tunnelcrack]()

LocalNet attack: Special cases

- Some clients block traffic to local network
- VPN Proxy Master (and others)
  - DNS server returns special-use IP addresses
  - VPN server forwards traffic to real IP address

LocalNet attack: The IOS case

Prevent attacks by setting **includeAllNetworks=True**

- And **excludeLocalNetworks=False** on IOS >= 14.2
- Vendors didn’t enabled it in their VPN client.

LocalNet attack: Take away

- Disable local network access when it’s using public IP addresses.
- OS should have API to create a VPN tunnels

References

- Mathy Vanhoef
- Professor, KU Leuven University
- https://papers.mathyvanhoef.com/usenix2023-tunnelcrack.pdf

End of Presentation
ANY QUESTIONS?
memecreator.org

Your feedback is important

Thank You