Illuminating Router Vendor Diversity Within Providers and Along Network Paths

Taha Albakour, Oliver Gasser, Robert Beverly, and Georgios Smaragdakis.

April 18, 2023

CiscoPSIRT
Product Security Incident Response Te

Security

Threat Actors Exploiting SNMP Vulnerabilities in Cisco Routers

Omar Santos

ALERT

Juniper Releases Security Advisory for Multiple Vulnerabilities in Junos OS

Release Date: August 18, 2023

CISA pulls the fire alarm on Juniper Networks bugs

Hate to ruin your Friday

Jessica Lyons Hardcastle

NISC | Cybersecurity Advisory

TLP:CLEAR

People's Republic of China-Linked Cyber Actors Hide in Router Firmware

MALWARE & THREATS

US, UK: Russia Exploiting Old Vulnerability to Hack Cisco Routers

US and UK government agencies have issued a joint warning for Russian group APT28 targeting Cisco routers by exploiting an old vulnerability.

State-sponsored campaigns target global network infrastructure

By Matt Olney

TUESDAY, APRIL 18, 2023 11:04

US bans Chinese telecom devices, citing 'national security'

US Federal Communications Commission decision includes devices from Huawei, ZTE and other manufacturers.

Cisco blocked in China as trade war heats up

"We're being uninvited to bid" says CEO

August 15, 2019 By: Sebastian Moss Have your say

State of the Art

- Generic tools
  - Nmap
  - Xprobe
- Services and banner
  - Rapid7 Recog
  - Third Time’s Not a Charm: Exploiting SNMPv3 for Router Fingerprinting

Recog https://github.com/rapid7/recog
Nmap https://nmap.org/

Contribution

- **LFP**, a **L**ightweight **F**inger**P**rinting technique aimed toward routers
- Evaluation and compared to other tools
- Study router vendor on the Internet
  - Within a network
  - Along a network path
- Explore the possibility of informed routing decision based on vendor on path

LFP: A Lightweight Fingerprinting Technique

Assumptions

- Routers typically do not expose services to the public internet
- Routers typically respond to ICMP probes

Requirements

- Simple Ping probe, no malformed packets
- Minimal network overhead

→ (Mostly) IP layer information

Methodology

Single SNMPv3 → Ground Truth

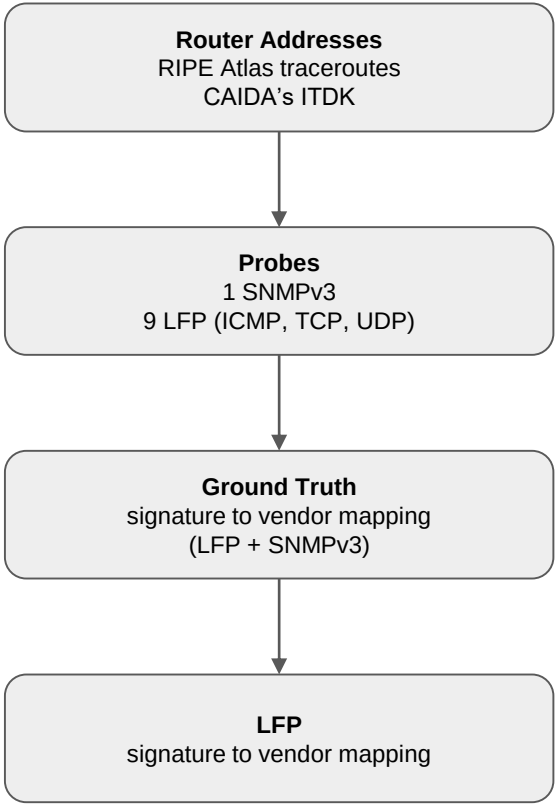
9 Consecutive probes, 3 per transport protocol

- 3x TCP ACK → TCP RST
- 3x UDP → ICMP Port Unreachable
- 3x ICMP Echo Request → ICMP Echo Reply

TCP and UDP, target high numbered port

Build a signature from the responses:

IPID Behavior	iTTL	Response Size	TCP RST Seq #



Signatures

16 different vendors, 112 signatures

- Unique 89
- Non-unique 23

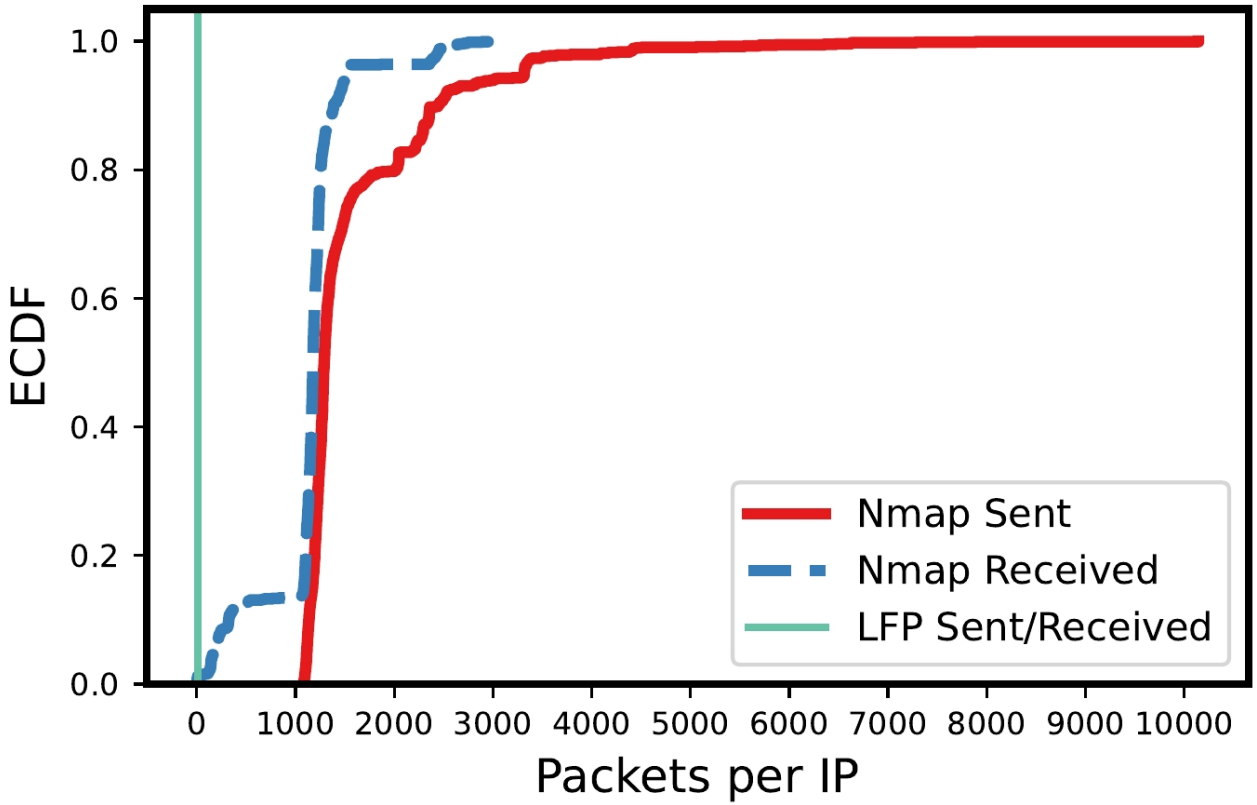
Vendor	Ground Truth	Unique	Non-unique
Cisco	83,918	25 (82,020)	1 (1,898)
Mikrotik	28,989	26 (9,489)	4 (19,500)
Huawei	19,869	8 (17,034)	4 (2,835)
Juniper	17,665	15 (17,665)	0 (0)

Accuracy: LFP vs. Nmap

	Coverage		Accuracy	
Vendor	LFP	Nmap	LFP	Nmap
Cisco	40%	10%	95%	84%
Juniper	81%	31%	99%	98%
Huawei	49%	20%	55%	50%
Ericsson	93%	6%	80%	0%
Mikrotik	83%	15%	10%	5%
Alcatel	38%	11%	48%	16%

- Test sample: 500 IPs per vendor
- LFP has similar accuracy but better coverage

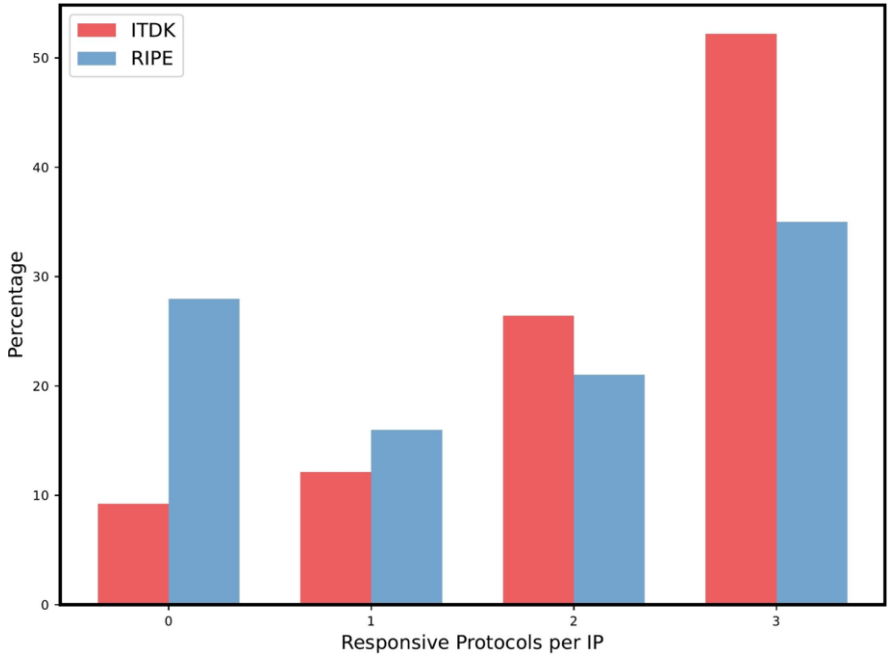
Traffic (in #packets): LFP vs. Nmap



Datasets and coverage

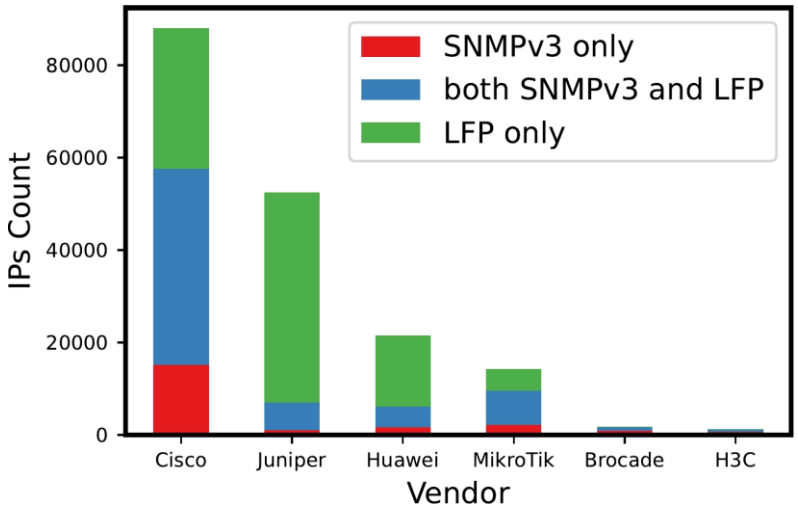
	Date	# IPv4 Add.	# AS
RIPE	2022-11	476k	18.8k
ITDK	2022-02	343k	9.9k

ITDK dataset is more responsive than RIPE Atlas

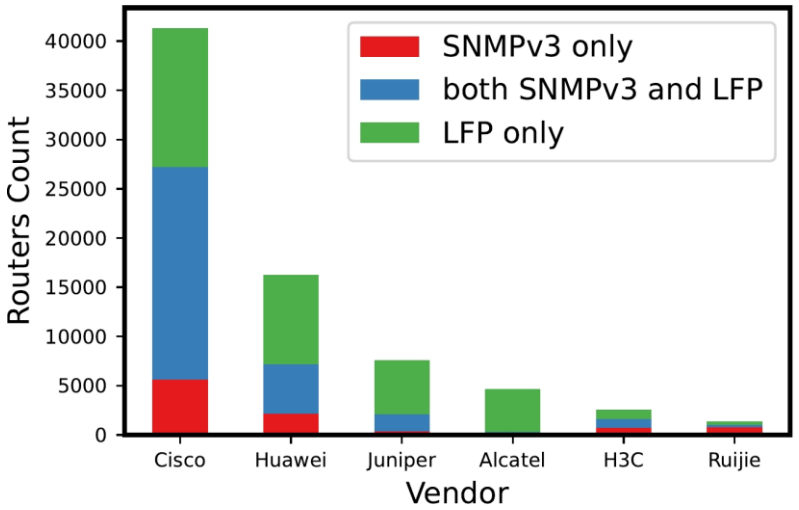


Fingerprinting Results

RIPE Atlas

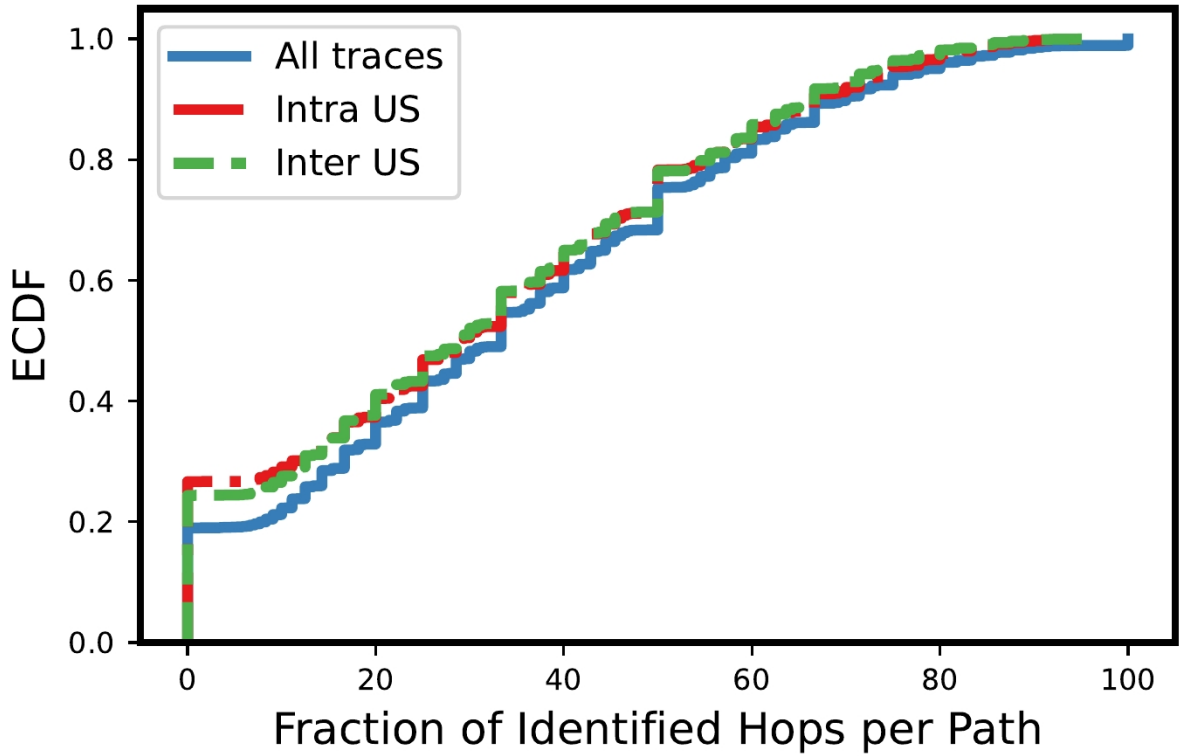


ITDK



Datasets can be bias toward certain vendors, e.g., Mikrotik present in RIPE but not in ITDK

Vendor Fingerprinting on a Path



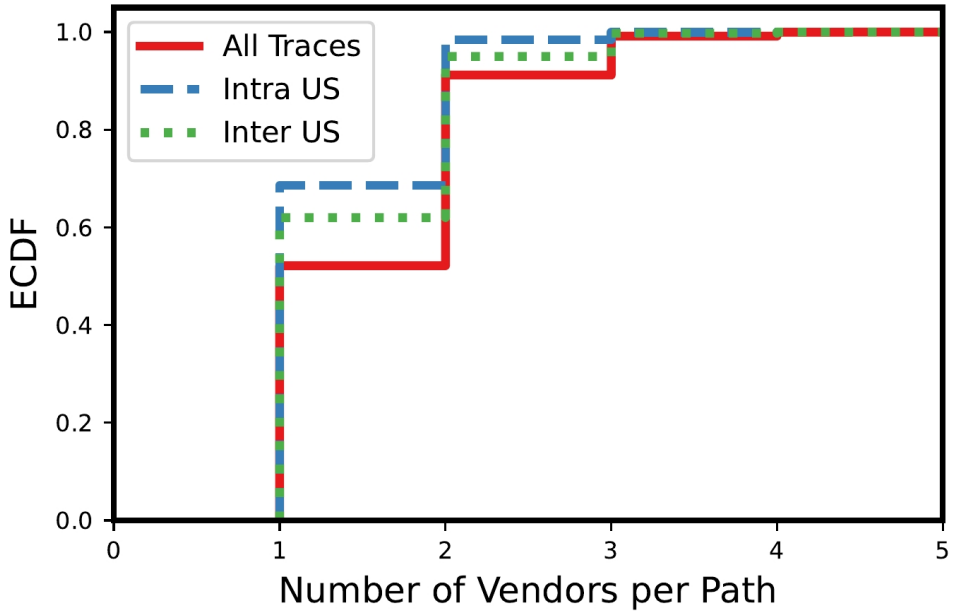
Vendor Fingerprinting on a Path

US-Traces:

- 70% single vendor
- 30% two vendors

All Traces:

- 50% single vendor
- 40% two vendors
- 10% three or more vendors



Conclusion

- Lightweight fingerprinting technique
- Study router vendor on the Internet
- Data available at: https://routerfingerprinting.github.io/

European Research Council
Established by the European Commission