NETWORK FINGERPRINTING:

Routers under attack

Emeline Marechal *Benoit Donnet*

September 7, 2020

ROADMAP

- Research Questions
- Fingerprinting
- Methodology
- Key findings
- Conclusion

TWO RESEARCH QUESTIONS

RQ-1: *What is the **hardware ecosystem** within Internet and operators?*

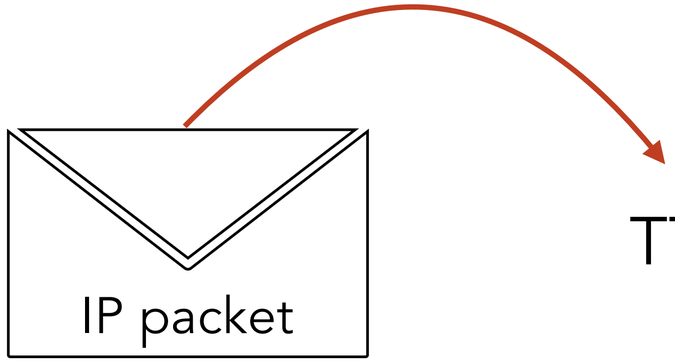
- *Where are located the different brands?*
- *What role do they play?*

RQ-2: *Knowing this, what could happen if an attacker can easily identify router brands and **target specific vendors** with (known) security breaches?*

- *Five vulnerabilities found in Cisco devices, leading to RCE and DoS vulnerabilities [7]*
- *One RSA vulnerability found in several other manufacturers [9]*

BACKGROUND: LIGHTWEIGHT FINGERPRINTING

➤ *Principle [3]*



TTL: {30, 32, 64, 128, 255}

➤ *Main router brand signatures*

Cisco

Juniper Junos

Juniper JunosE

Brocade, Alcatel, Linux

TTL	
time-exceeded	echo-reply
255	255
255	64
128	128
64	64

← *Signature*

DATA COLLECTION AND PROCESSING

COLLECTION

TNT [11, 12]

- *Traceroute extension with fingerprinting (and MPLS discovery)*
- *November 1st to13th, 2019*
- *28 vantage points (VPs)*
- *1.2 M addresses discovered*

ALIAS RESOLUTION

MIDAR [15]

- *Router topology from address topology*
- *65,778 routers with 221,464 addresses*

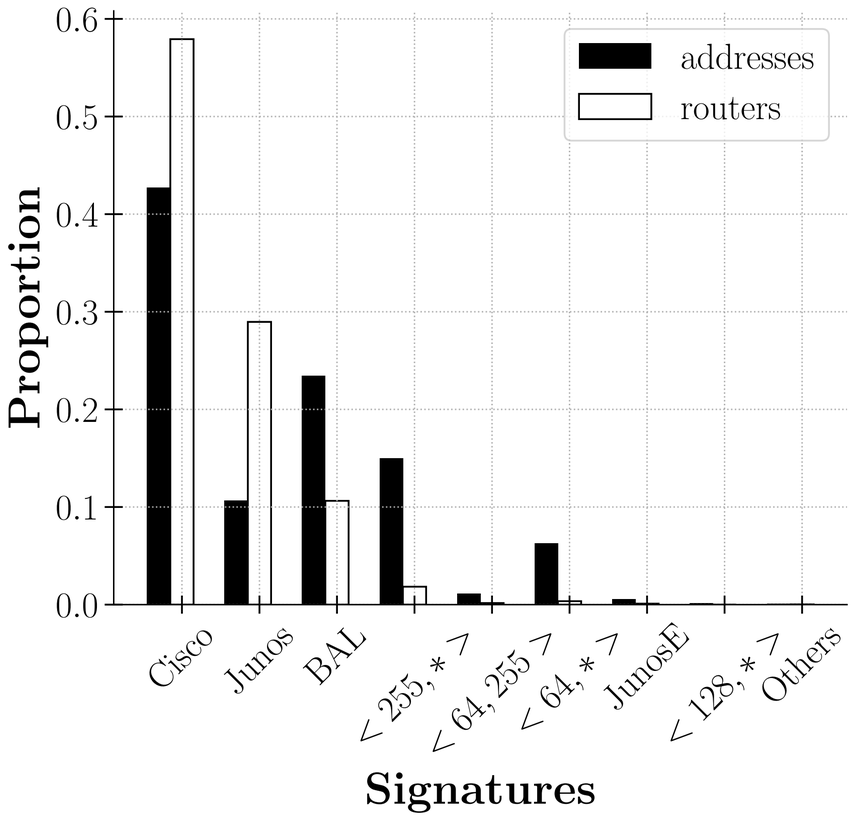
ROUTER OWNERSHIP

BDRMAPIT [17]

- *Annotate routers with ownership*
- *Allows to study the Internet on a per-AS scale*

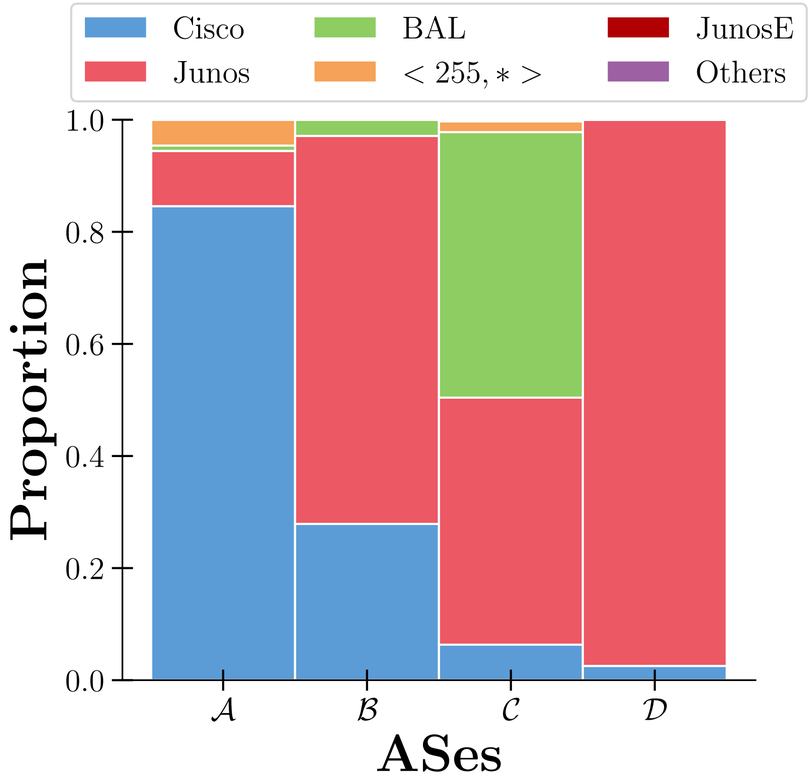
RQ-1: HARDWARE ECOSYSTEM

- *Globally*



Cisco largely dominates the overall market

- *Per AS*

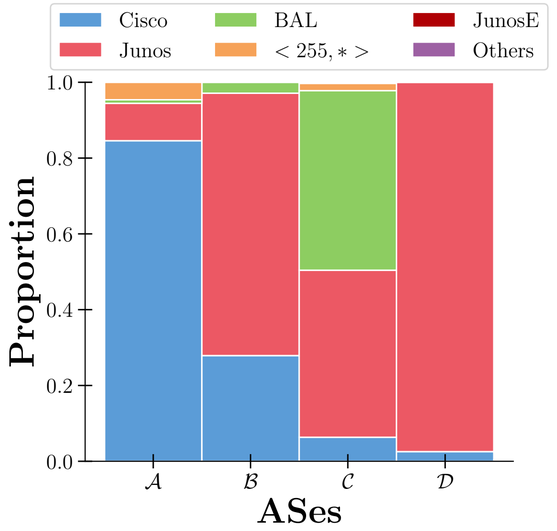


Hardware distribution greatly varies depending on the AS

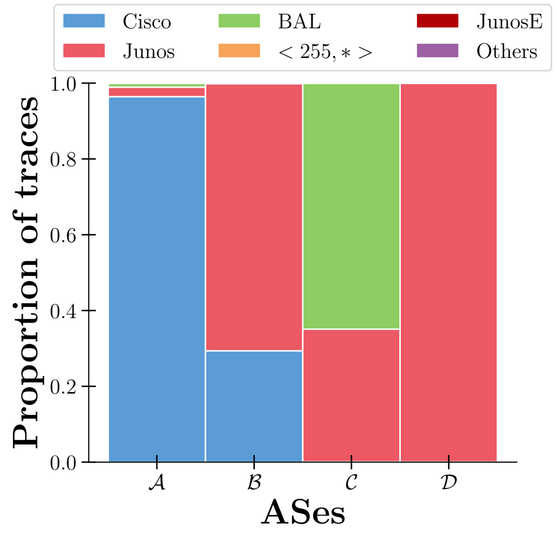
RQ-2: ATTACKS ON ROUTERS

- *Not all routers contribute equally to forwarding*
  - *Some routers with a lot of forwarding power, some others not*
  - *Target of interest for attackers*
- *Hardware popularity*
  - *Proportion of traces crossing each hardware brand*
  - *Reflects the topological importance of a brand in terms of **connectivity** and **amount of traffic** [18]*

Hardware distribution

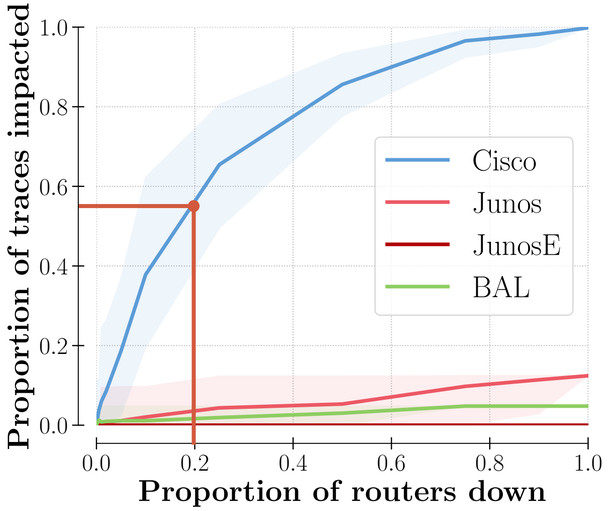


Hardware popularity

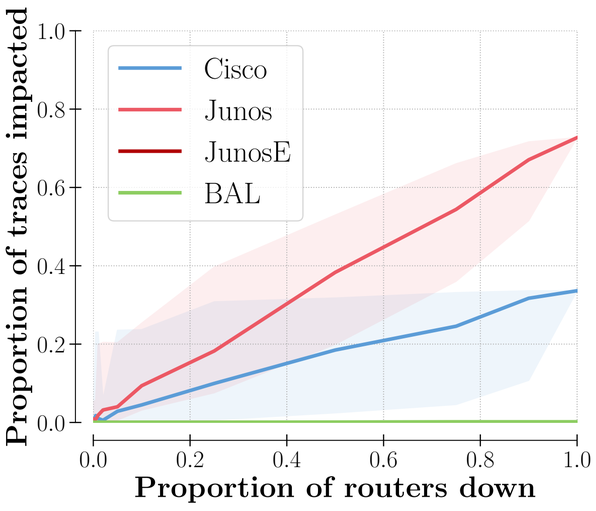


RQ-2: ATTACKS ON ROUTERS

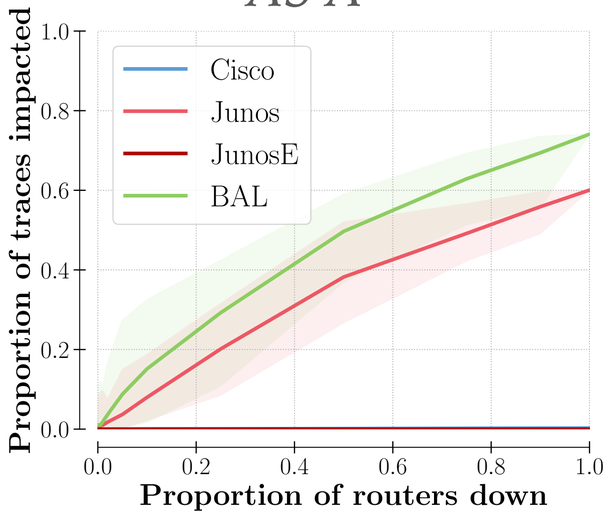
- *Methodology*
  - *For each brand, kill a given percentage of routers*
  - *Results averaged over 30 simulations*
- *Key findings*
  - *Not all router brands contribute equally to network connectivity*
  - *Different ASes are vulnerable to different targeted attacks*



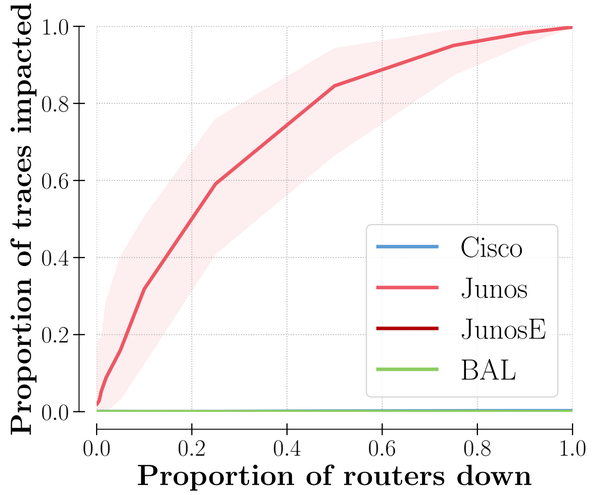
AS A



AS B



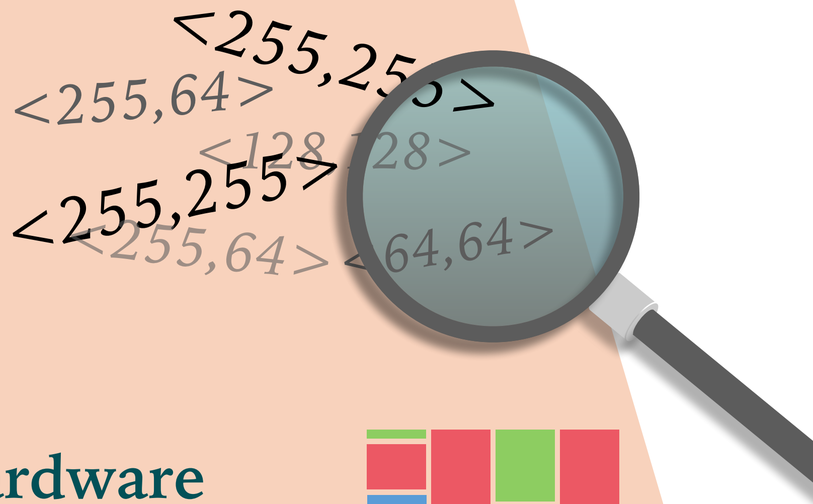
AS C



AS D

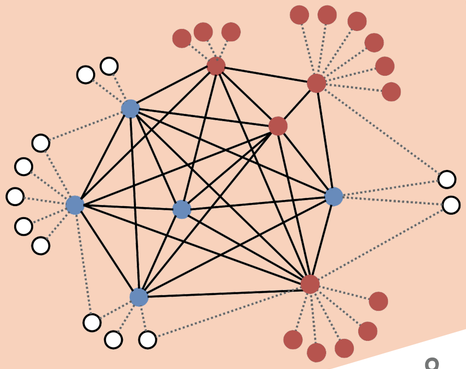
CONCLUSION

- One can easily retrieve router brands with a **lightweight fingerprinting** technique.



- Although Cisco dominates the overall market share, the **hardware distribution greatly varies** between ASes.

- An attacker can cause **great damage with little effort**, depending on the AS hardware infrastructure.



contact: emeline.marechal@uliege.be