IRRegularities in the Internet Routing Registry

Ben Du, Katherine Izhikevich, Sumanth Rao,
Gautam Akiwate^, Cecilia Testart*, Alex C. Snoeren, kc claffy

UC San Diego ^Stanford *Georgia Tech

ACM Internet Measurement Conference
Oct 24, 2023

UC San Diego

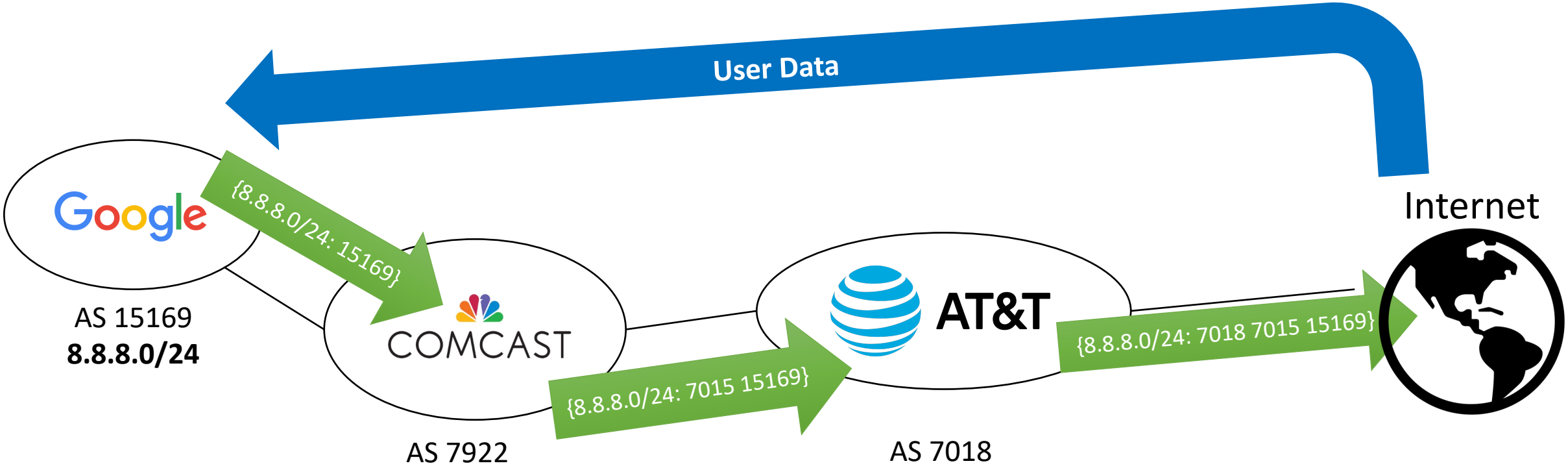
Georgia Tech

Stanford University

caida

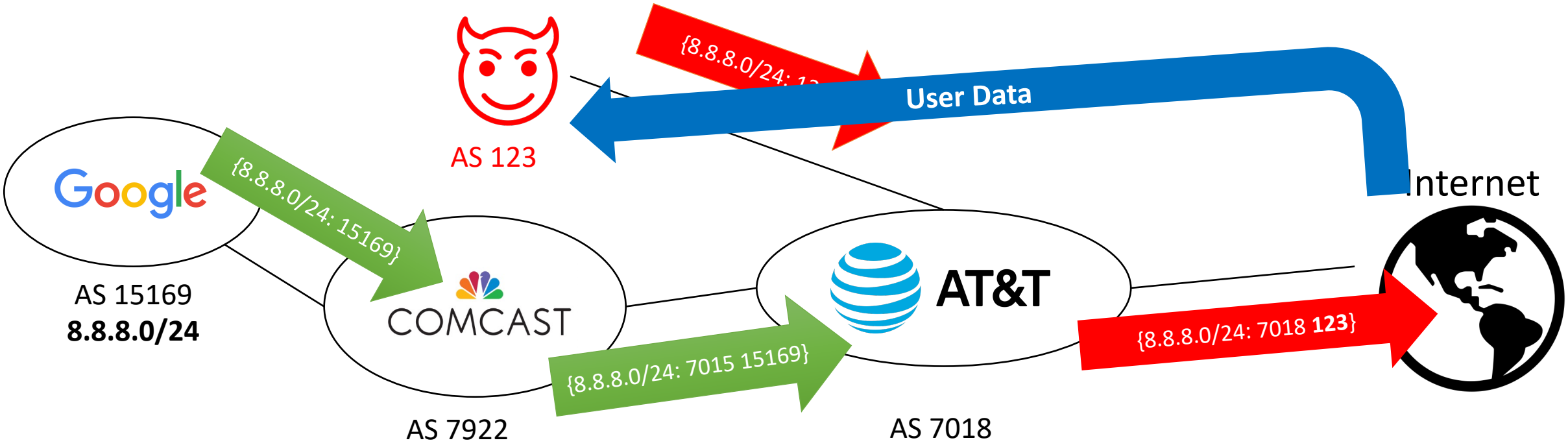
Attack on the Internet routing system

- The Border Gateway Protocol allows networks to share reachability information.



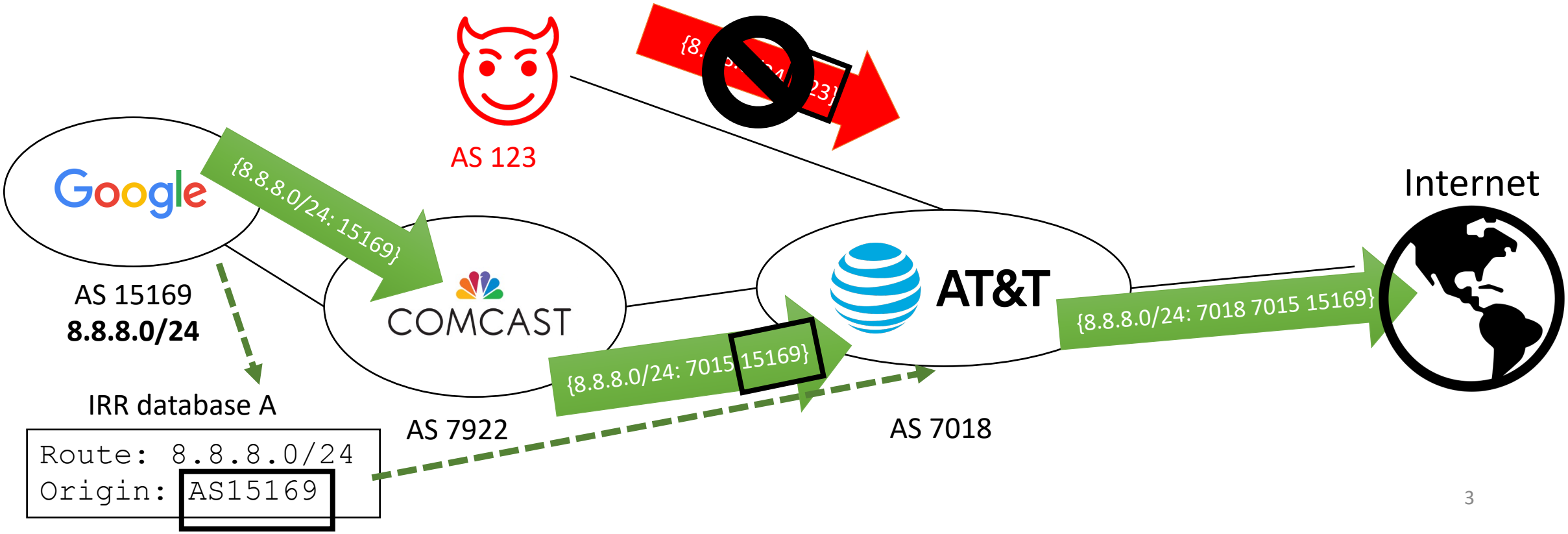
Attack on the Internet routing system

- The Border Gateway Protocol allows networks to share reachability information.
- Attackers can redirect Internet traffic without authorization (**BGP hijacking**).



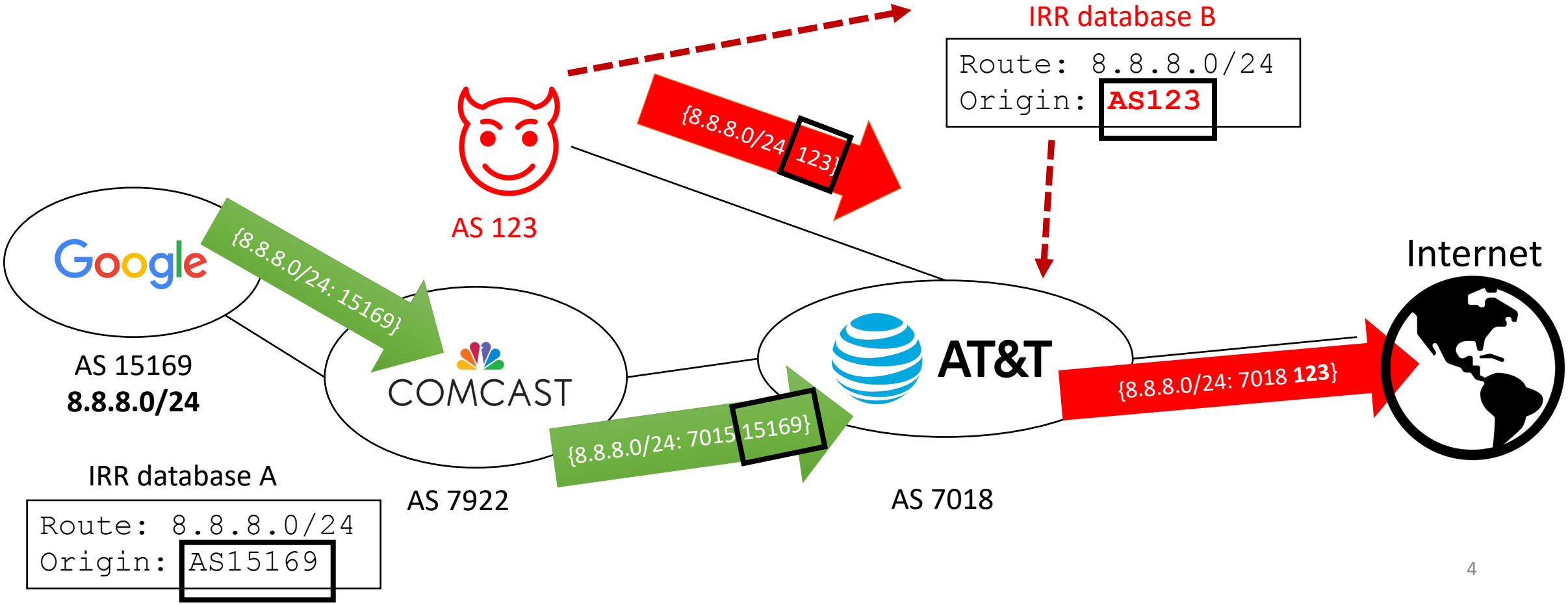
Using IRR to defend against BGP hijacking

- **The Internet Routing Registry (IRR)** provides external reference information for networks to filter received messages through the Border Gateway Protocol (BGP).



Threat model: attacker registers false IRR records

- Circumventing the route filters used by the attacker's upstream providers.



IRR data may not be accurate

Authoritative IRR databases

Validated Records

- Also manage the Resource Public Key Infrastructure (RPKI), a more secure alternative of the IRR.

Non-authoritative IRR databases

RADb
THE INTERNET ROUTING REGISTRY

Largest, Oldest, and Most Popular

AltDB

FREE

IRR is widely used by networks

- Large cloud providers, Internet Exchange Points (IXPs), and transit providers require their customers/peers to register in an IRR database.

Cloudflare Docs

Route registry	URL
AFRINIC	https://afrinic.net/internet-routing-registry#guide
APNIC	https://www.apnic.net/manage-ip/apnic-services/routing-registry/
ARIN	https://www.arin.net/resources/manage/irr/quickstart/
NTT	https://www.gin.ntt.net/support-center/policies-procedures/routing-registry/
RADB	https://www.radb.net/support/
RIPE	https://www.ripe.net/manage-ips-and-asns/db/support/managing-route-objects-in-the-irr

Updating Internet Routing Registry (IRR) data to peer with Google

Which IRRs can I use?

We currently use:

- ALTDB
- AFRINIC
- APNIC
- ARIN
- BBOI
- BELL Canada
- CANARIE
- EASYNET
- HOST
- JPIRR
- Level3
- LACNIC
- NESTEGG
- NTT
- OPENFACE
- OTTIX
- PANIX
- REACH
- RADB
- RGNET
- RIPE
- RISQ
- ROGERS,
- TC

False IRR record of UCSD-originated prefix

- In 2020, gohosted.eu registered 4 UCSD-originated prefixes in RADB.
- gohosted.eu originated those prefixes in BGP until early 2021 (BGP hijacking) .
- The hijacker’s upstream providers accepted the BGP announcements because they matched RADB records.

```
route:      44.190.131.0/24
origin:     AS207427
descr:      NLVIX
mnt-by:     MAINT-213282
changed:    info@webdiensten.nu 20201216  #18:41:36Z
source:     RADB
```

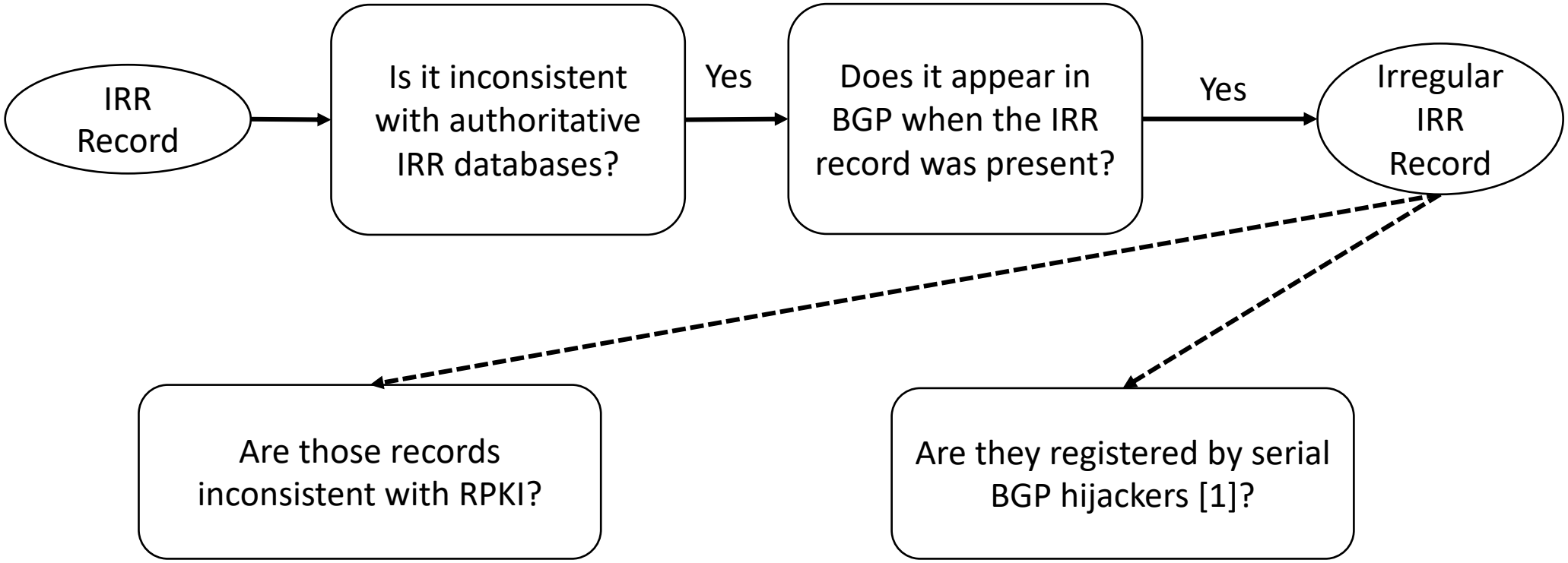
Looking for false IRR records

- We propose a methodology to identify IRR records collected over 1.5 years that may be registered by hijackers – *a.k.a* **irregular** IRR records.
- We use results from previous papers to validate our results.

Profiling BGP Serial Hijackers: Capturing Persistent Misbehavior in the Global Routing Table — IMC 2019

IRR Hygiene in the RPKI Era — PAM 2020

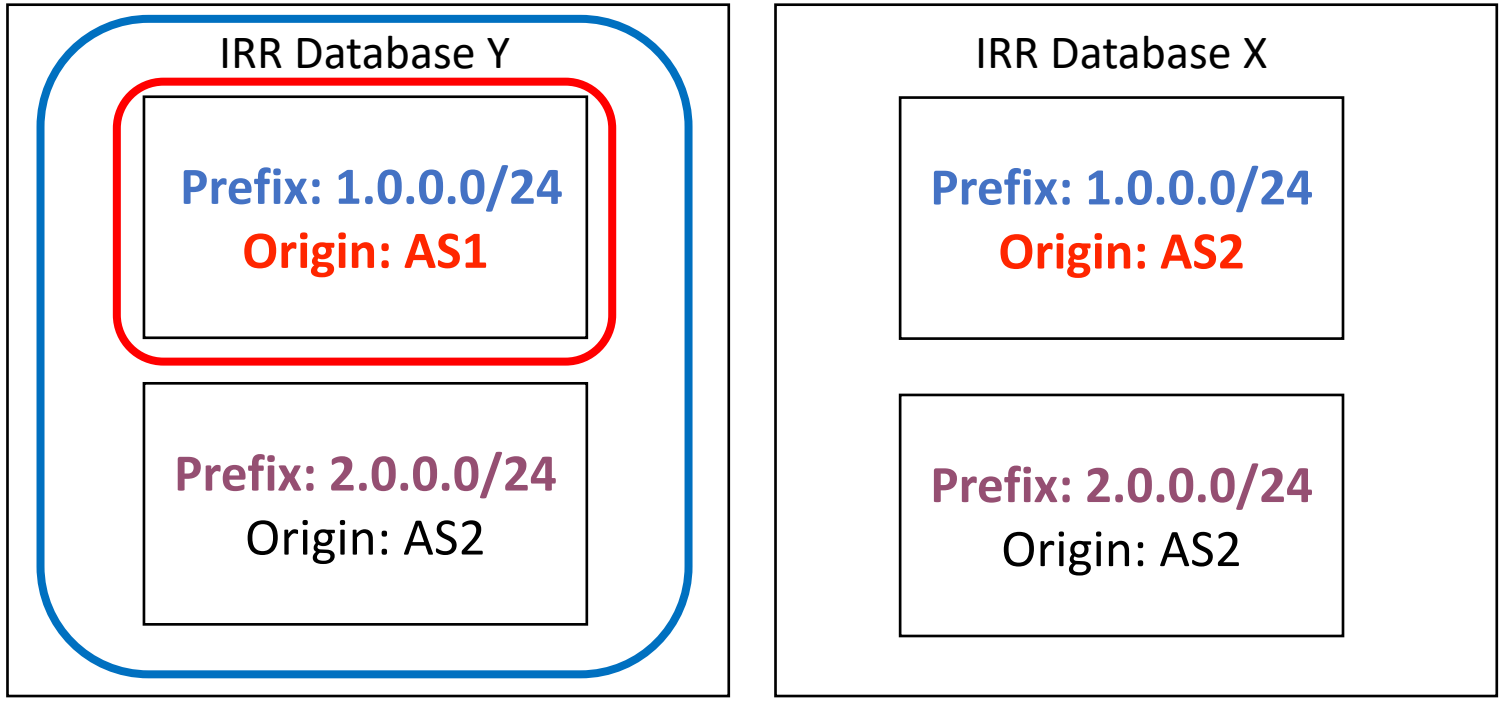
Workflow to identify irregular route objects



[1] Cecilia Testart et al. 2019. Profiling BGP Serial Hijackers: Capturing Persistent Misbehavior in the Global Routing Table. In Proceedings of the Internet Measurement Conference (IMC '19).

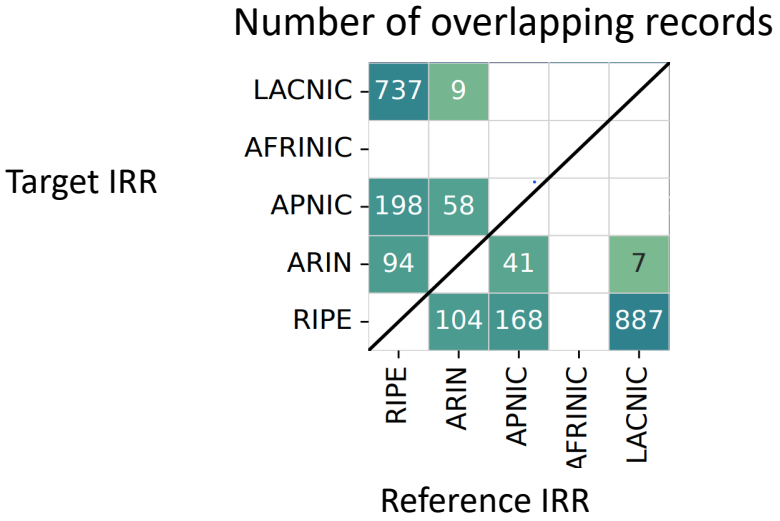
Calculating inconsistent records

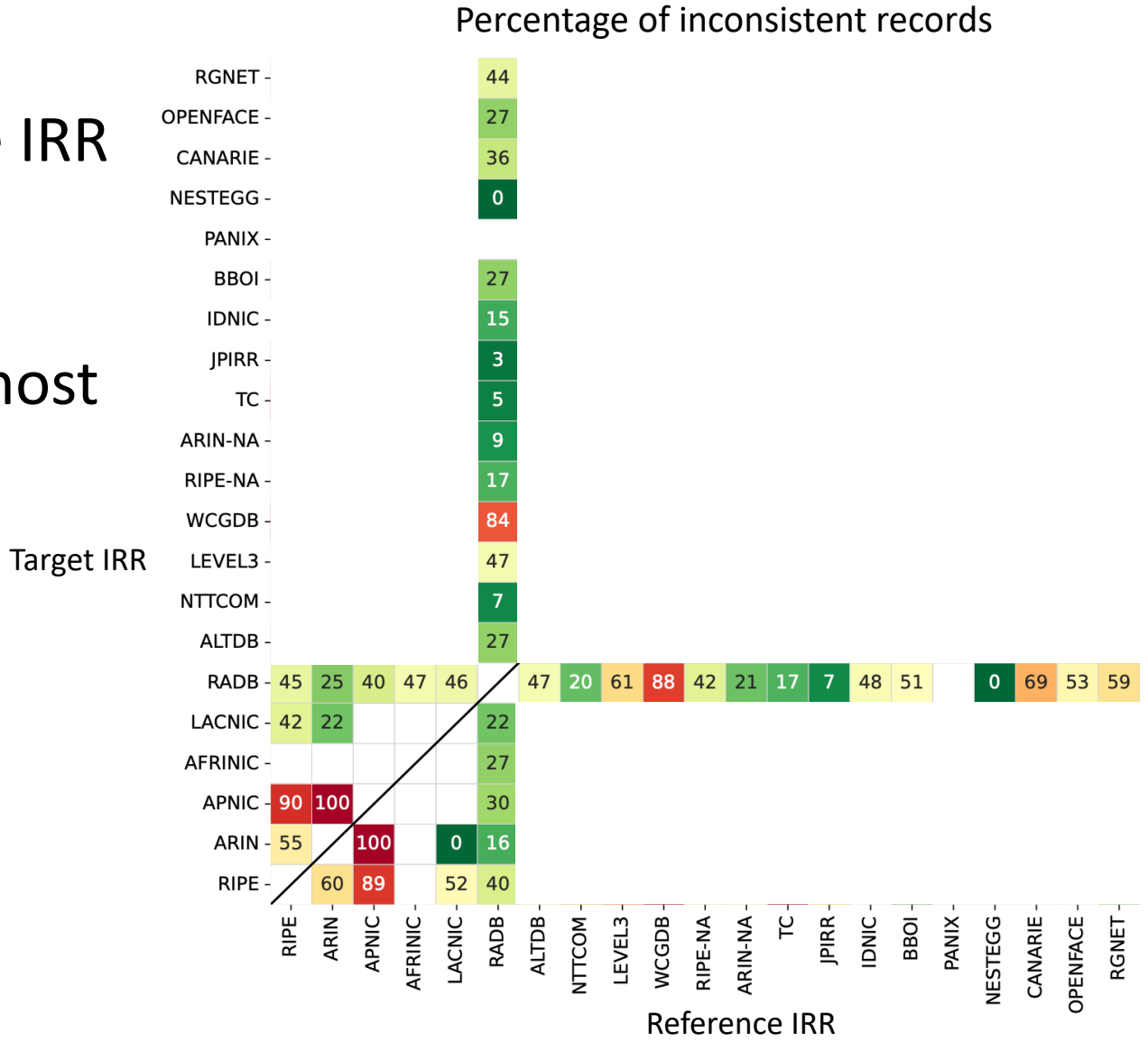
- How inconsistent is IRR Y compared to IRR X?
  - 2 records in IRR Y have the same prefix in IRR X.
  - 1 of the 2 records has a different origin AS.
- Inconsistency (Y, X) = 1 / 2 = 50%



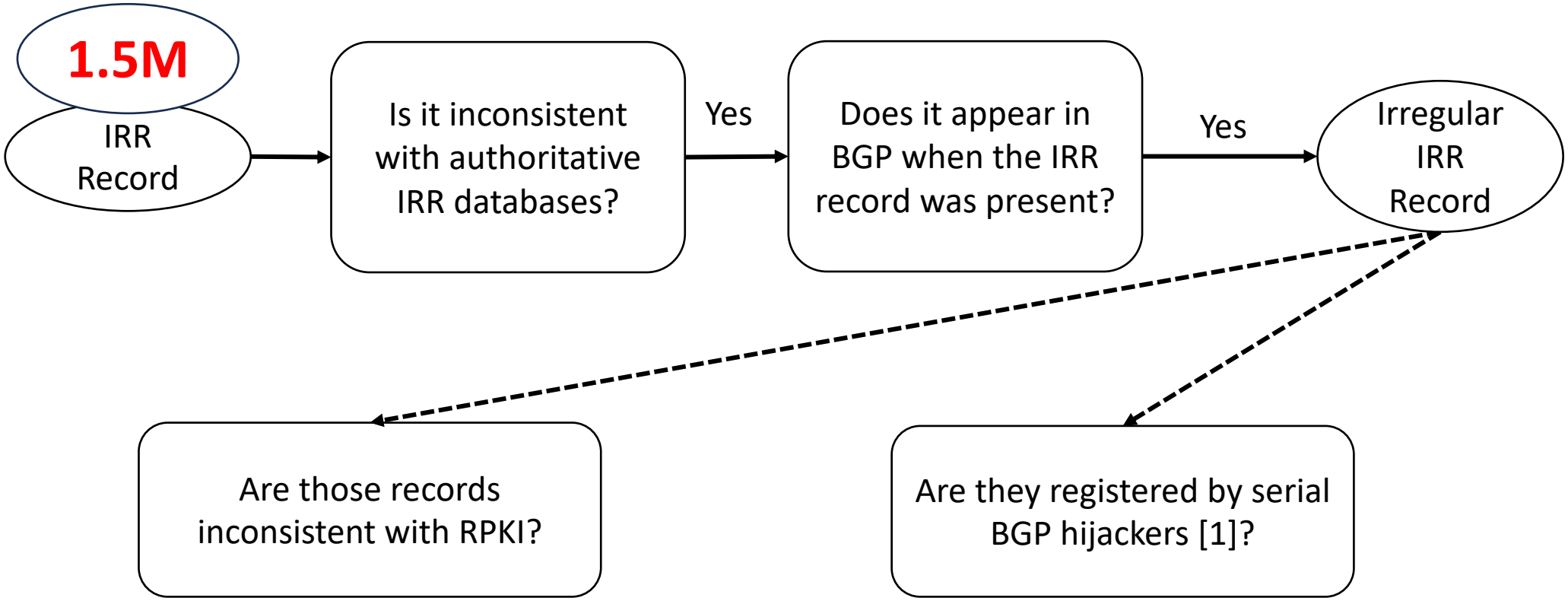
Inconsistency among IRR databases

- Overlap between authoritative IRR databases.
  - Inter-RIR address space transfer
- RADB has inconsistency with most other IRR databases.



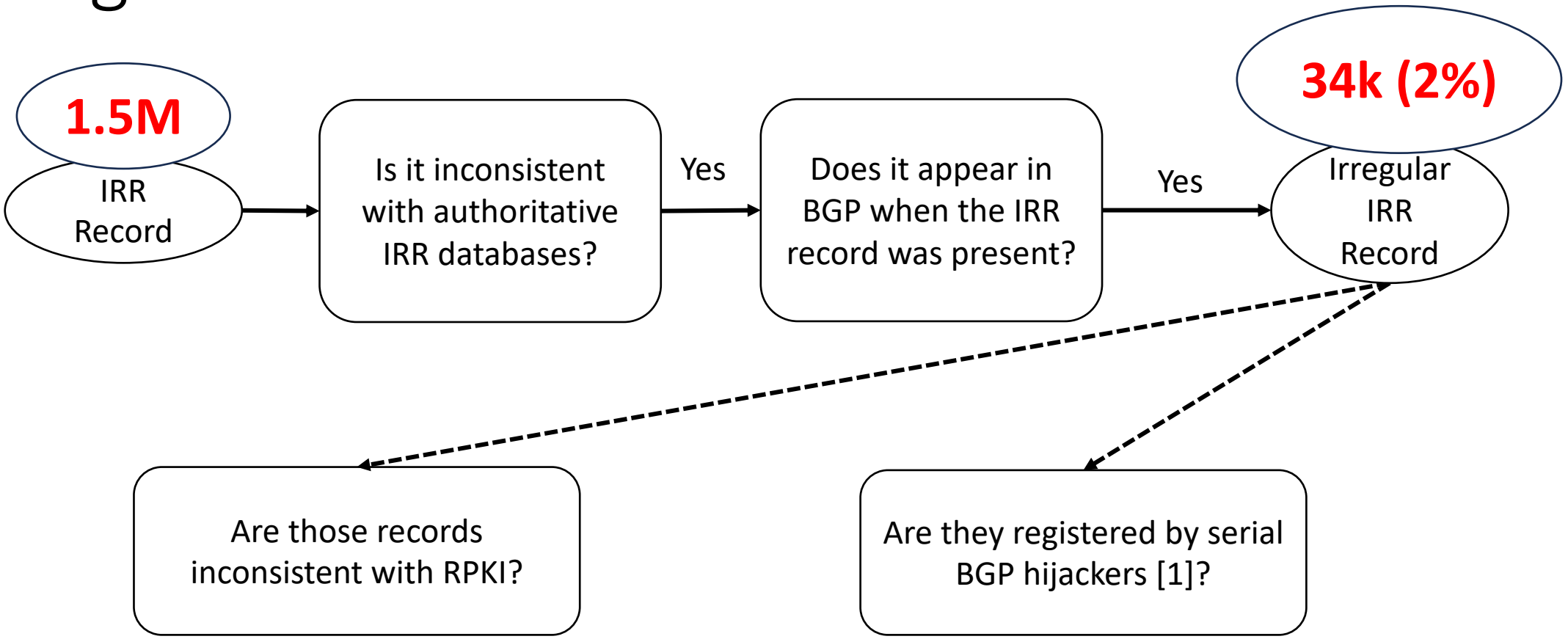


Irregular RADB records



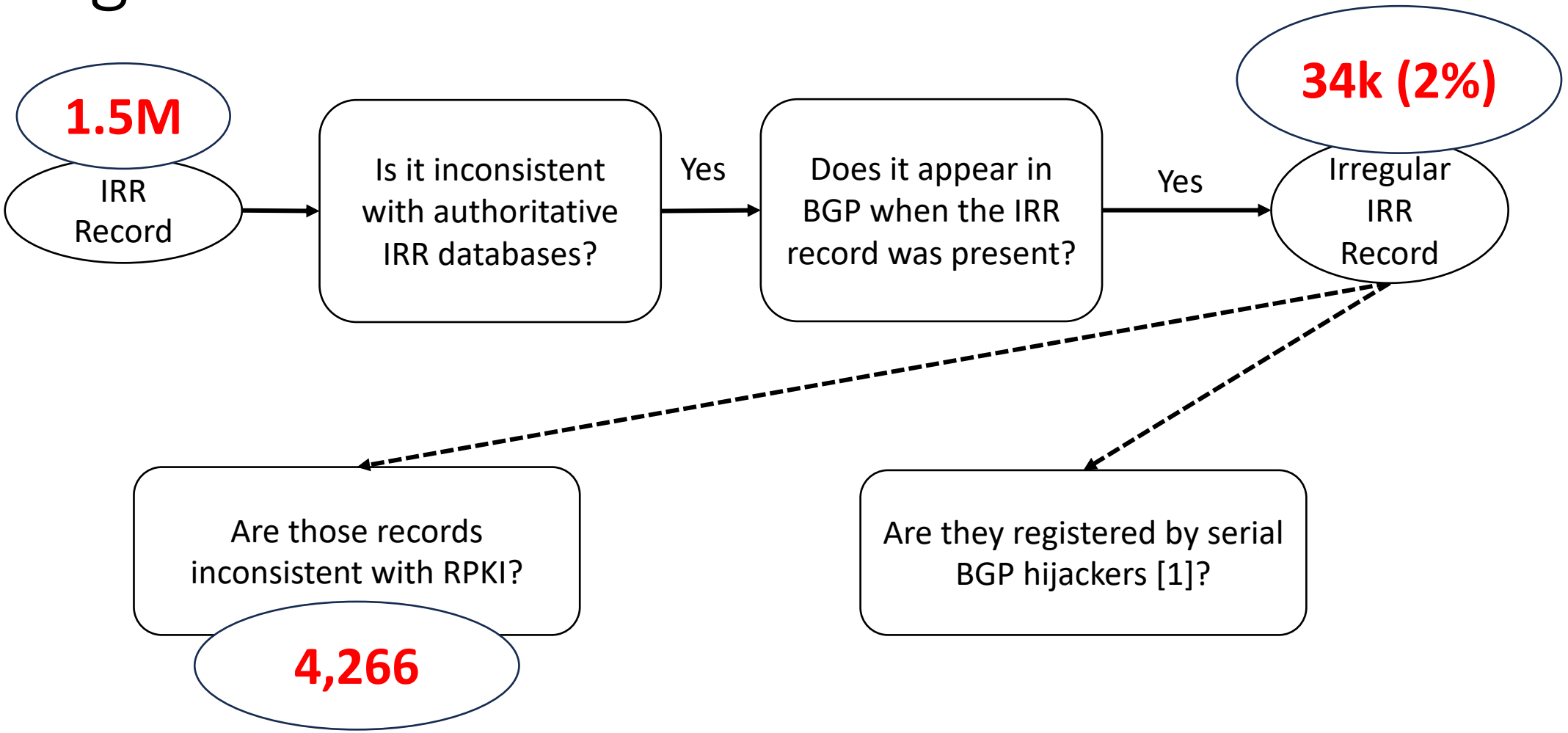
[1] Cecilia Testart et al. 2019. Profiling BGP Serial Hijackers: Capturing Persistent Misbehavior in the Global Routing Table. In Proceedings of the Internet Measurement Conference (IMC '19).

Irregular RADB records



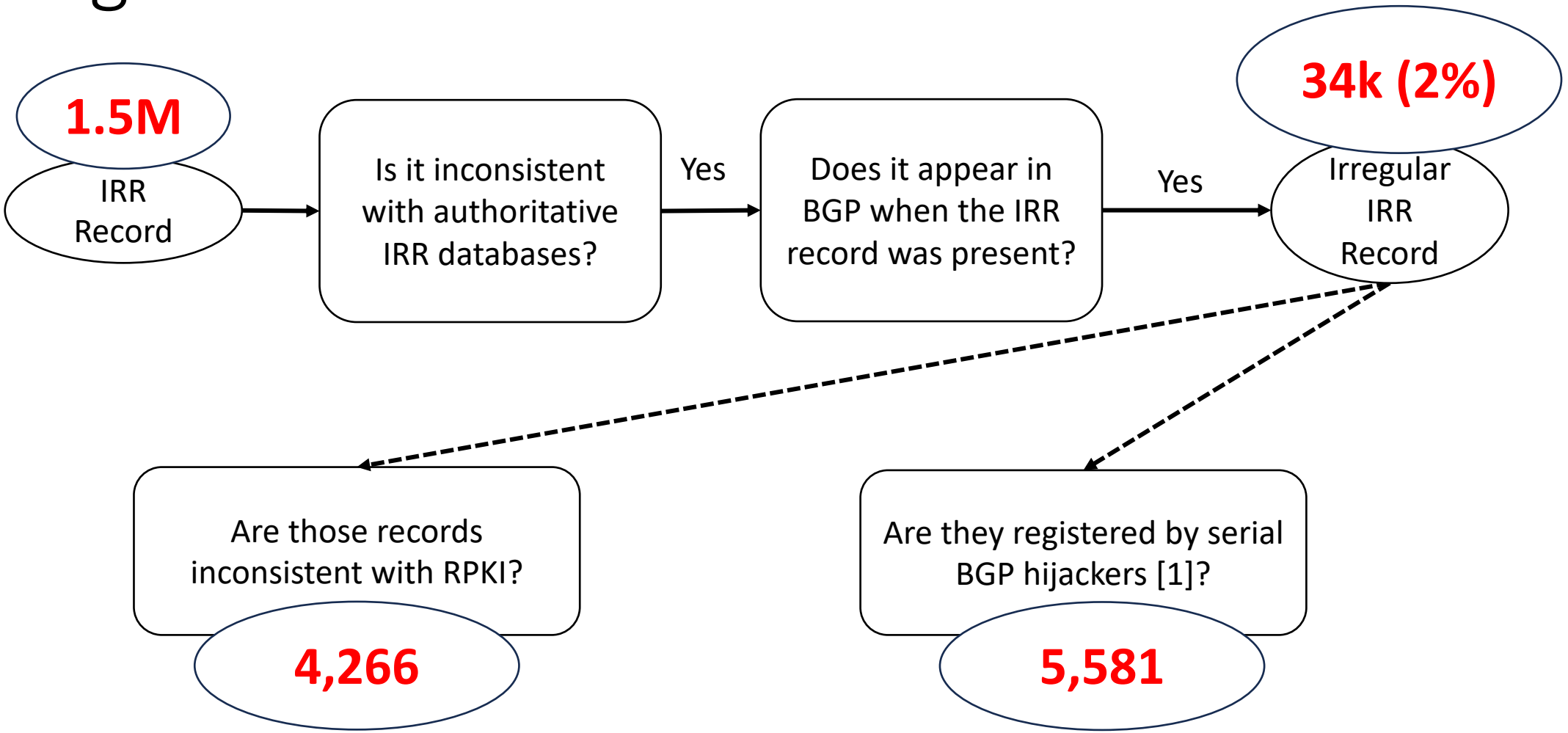
[1] Cecilia Testart et al. 2019. Profiling BGP Serial Hijackers: Capturing Persistent Misbehavior in the Global Routing Table. In Proceedings of the Internet Measurement Conference (IMC '19).

Irregular RADB records



[1] Cecilia Testart et al. 2019. Profiling BGP Serial Hijackers: Capturing Persistent Misbehavior in the Global Routing Table. In Proceedings of the Internet Measurement Conference (IMC '19).

Irregular RADB records



[1] Cecilia Testart et al. 2019. Profiling BGP Serial Hijackers: Capturing Persistent Misbehavior in the Global Routing Table. In Proceedings of the Internet Measurement Conference (IMC '19).

Case Study: IP Leasing Company

- We found 30.4% (10,408 / 34,199) were registered by ipxo.com, an IP leasing company.
- They register IRR records for their customers.
- Some of their IRR records existed in RADB for only 5 days.

- Further analysis needed to check whether their customers are using leased IP address space maliciously.

Summary

- Inconsistency is common between IRR databases.
  - 13% (~200k) of all RADB records were inconsistent compared to NTTCOM.
  - Future work is needed to resolve such inconsistency.
- 34k irregular IRR records need further attention from the community.
  - Non-authoritative IRR records need validation.

Questions? bendu@ucsd.edu