Measuring RPKI adoption and impact

Cecilia Testart

06.11.2023

Georgia Tech

About Me

Assistant Professor
School of Cybersecurity and Privacy &School of Computer Science
Georgia Institute of Technology
Email: ctestart@gatech.edu

Research Area: Internet Security and Policy, Internet Measurements

Teaching: Computer Networks, Internet Security

Motivation: Internet for Society

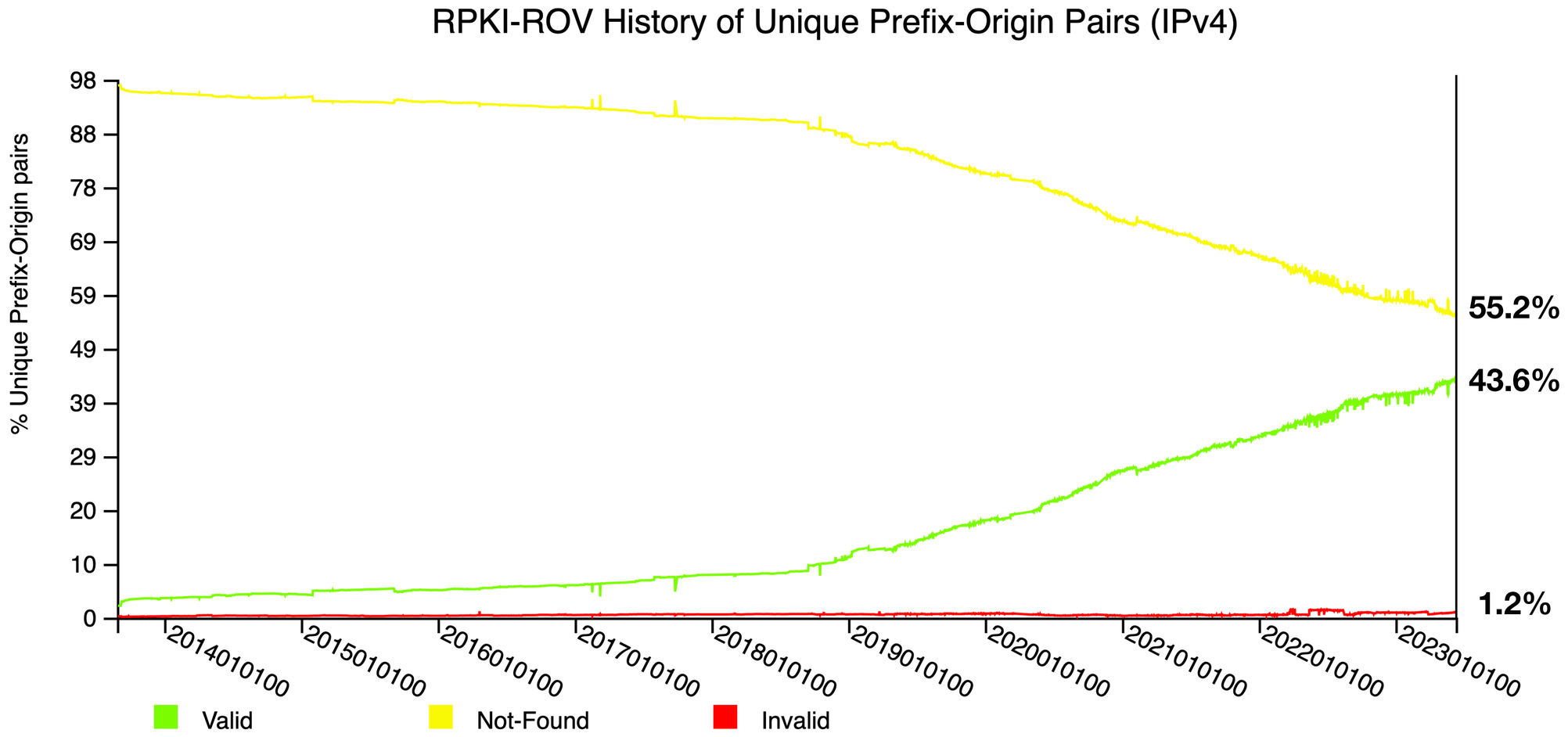
Previously: PhD@MIT, MS Technology and Policy, BSc in Industrial Engineering

Research questions

- How is RPKI adoption evolving over time?
  - Coverage of routed prefixes by ROAs
  - Deployment of ROV
- What is the impact of RPKI adoption?
  - Spread of RPKI-invalid BGP updates
  - BGP hijacking

Coverage of Routed Prefixes

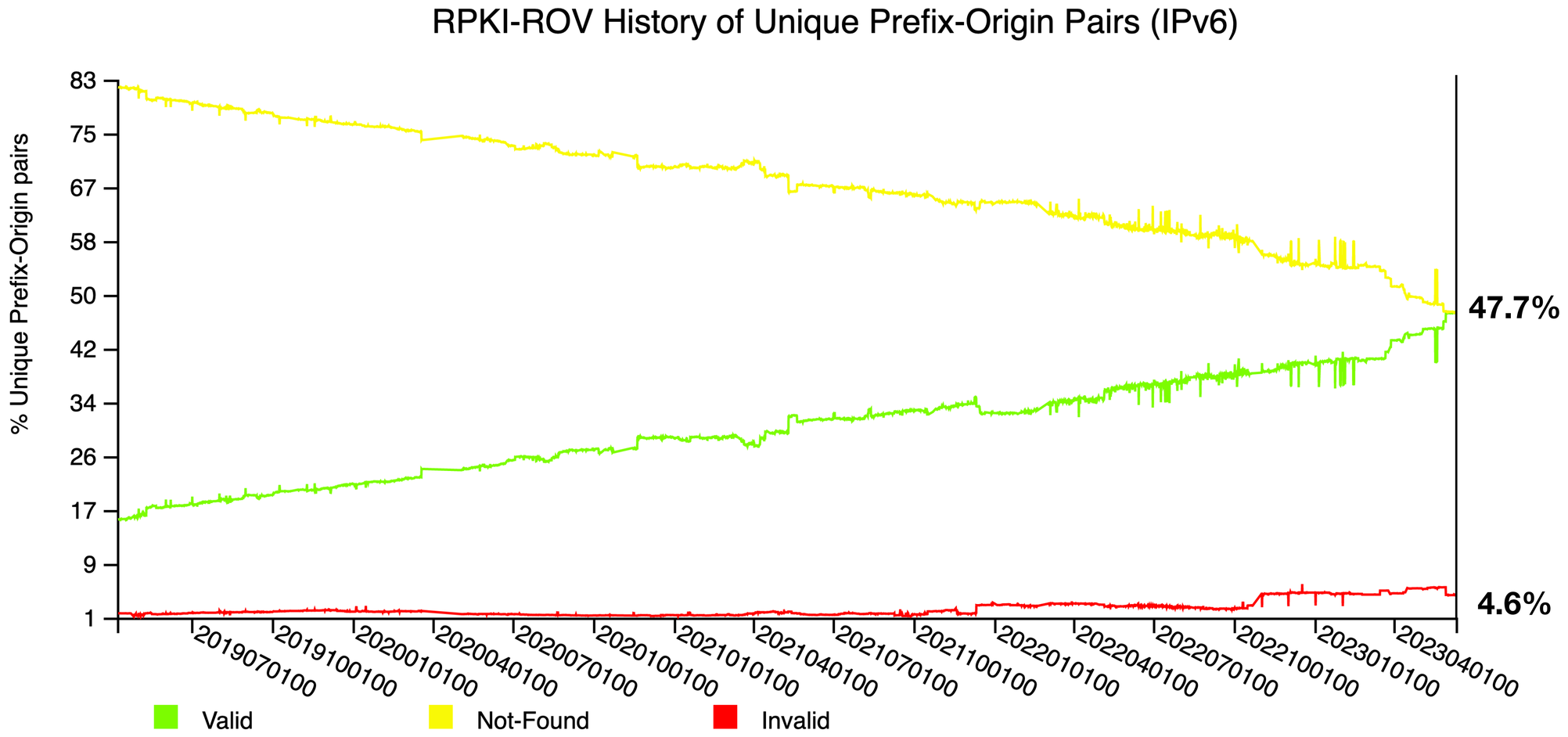
BGP prefixes covered by ROA over time from NIST



NIST RPKI Monitor: RPKI-ROV Analysis **Protocol:** IPv4 **RIR:** All

Georgia Tech

BGP prefixes covered by ROA over time from NIST

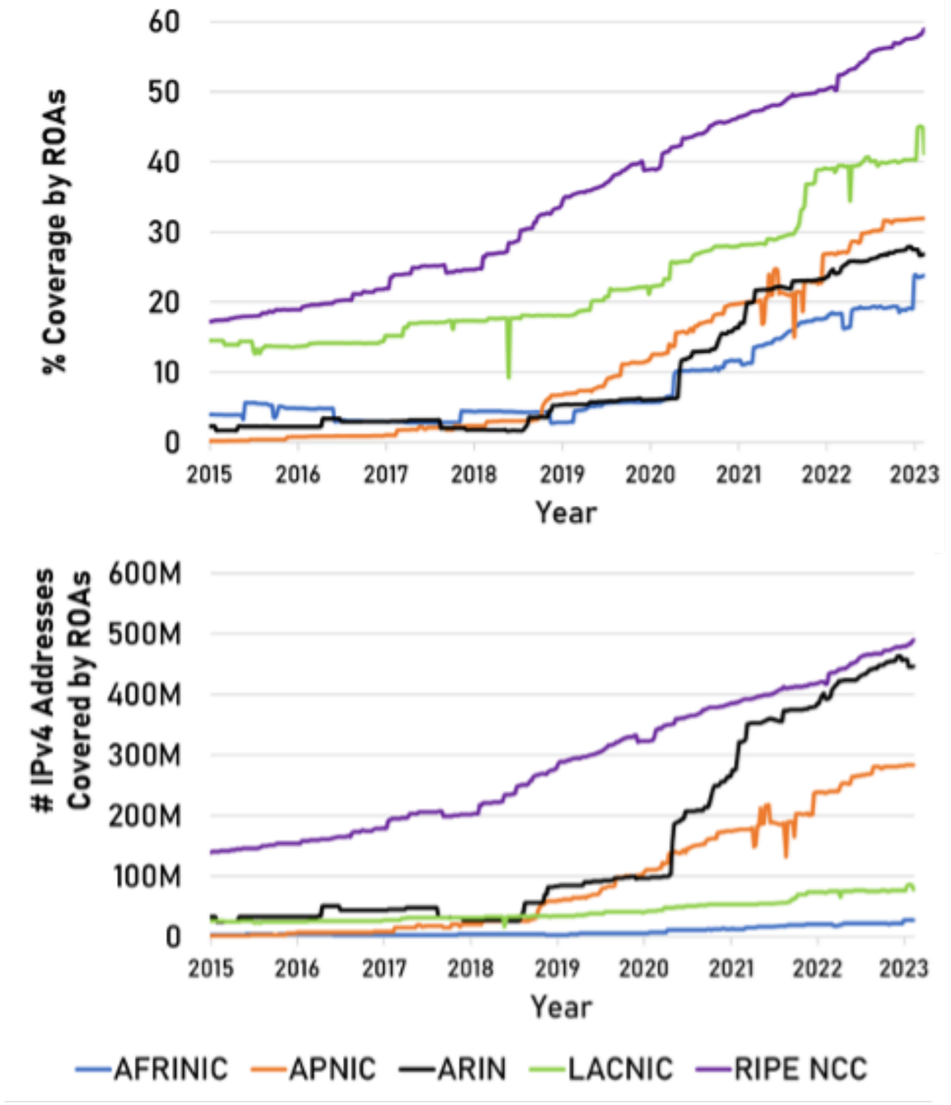


NIST RPKI Monitor: RPKI-ROV Analysis **Protocol:** IPv6 **RIR:** All

Georgia Tech

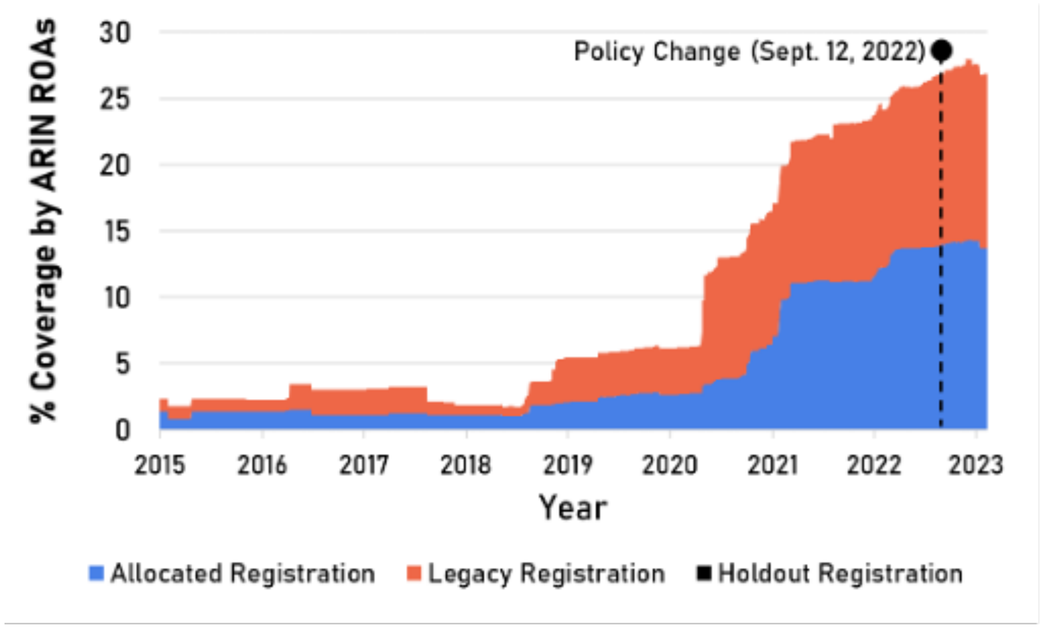
ARIN singularity

- ARIN required legal agreements to:
  - issue ROAs,
  - access ROAs (RPKI TAL),
  - publish ROAs in machine readable way.
- Legacy addresses treated differently.
- Requirements changed in Sept 2022.



Based on work by Noah Craft (MSc Student)

Legacy IP addresses



Organization	/8 legacy holdout count	Other Prefixes covered by ROAs
Apple	1	No
AT&T	1	Yes
Cogent	1	Yes
DISA	12	No
Ford	1	No

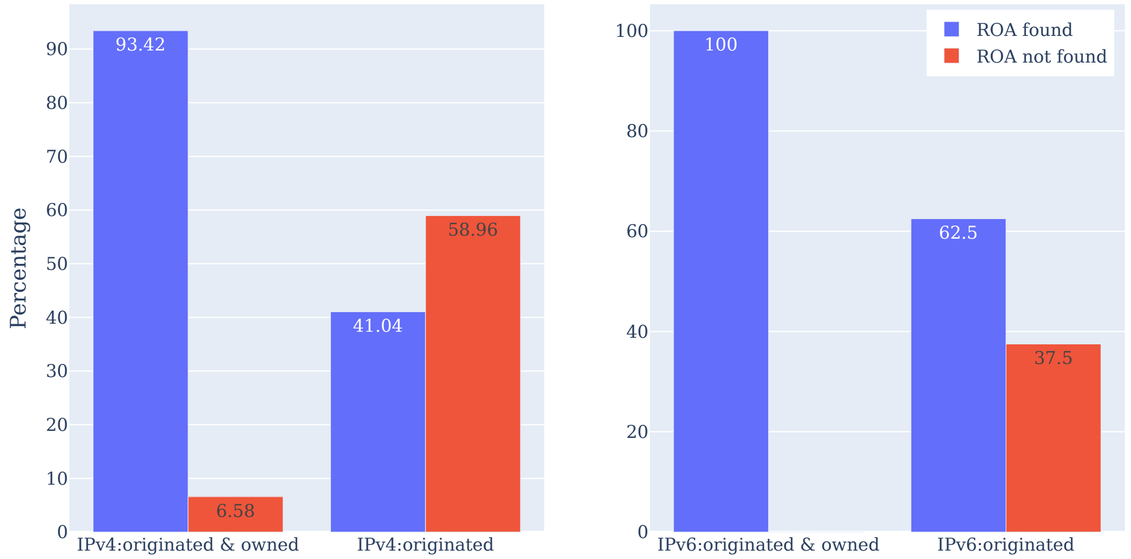
Georgia Tech

Based on work by Noah Craft (MSc Student)

ROA coverage by organization vs. by ASN

Case study of IIJ ROA Coverage

- Originated prefixes ~ 41%
- Originates & Owned ~ 93%



Based on work by Deepak Gouda (MSc Student)

ROA coverage by organization vs. by ASN

Org by prefix origination	% Prefixes	# Orgs	ROA Coverage (%)	
No AS	13.53	29765	47.23	← Should be easy but org. challenges
Originates only by own AS	10.12	23737	35.28	← Should be easy but org. challenges (?)
Originates by self & others	10.61	8906	33.65	← Afraid of mess
Originates self & others	12.38	10641	50.58	← Less afraid of mess
Originates self & others by self & others	53.36	5594	42.98	← Messy but large orgs

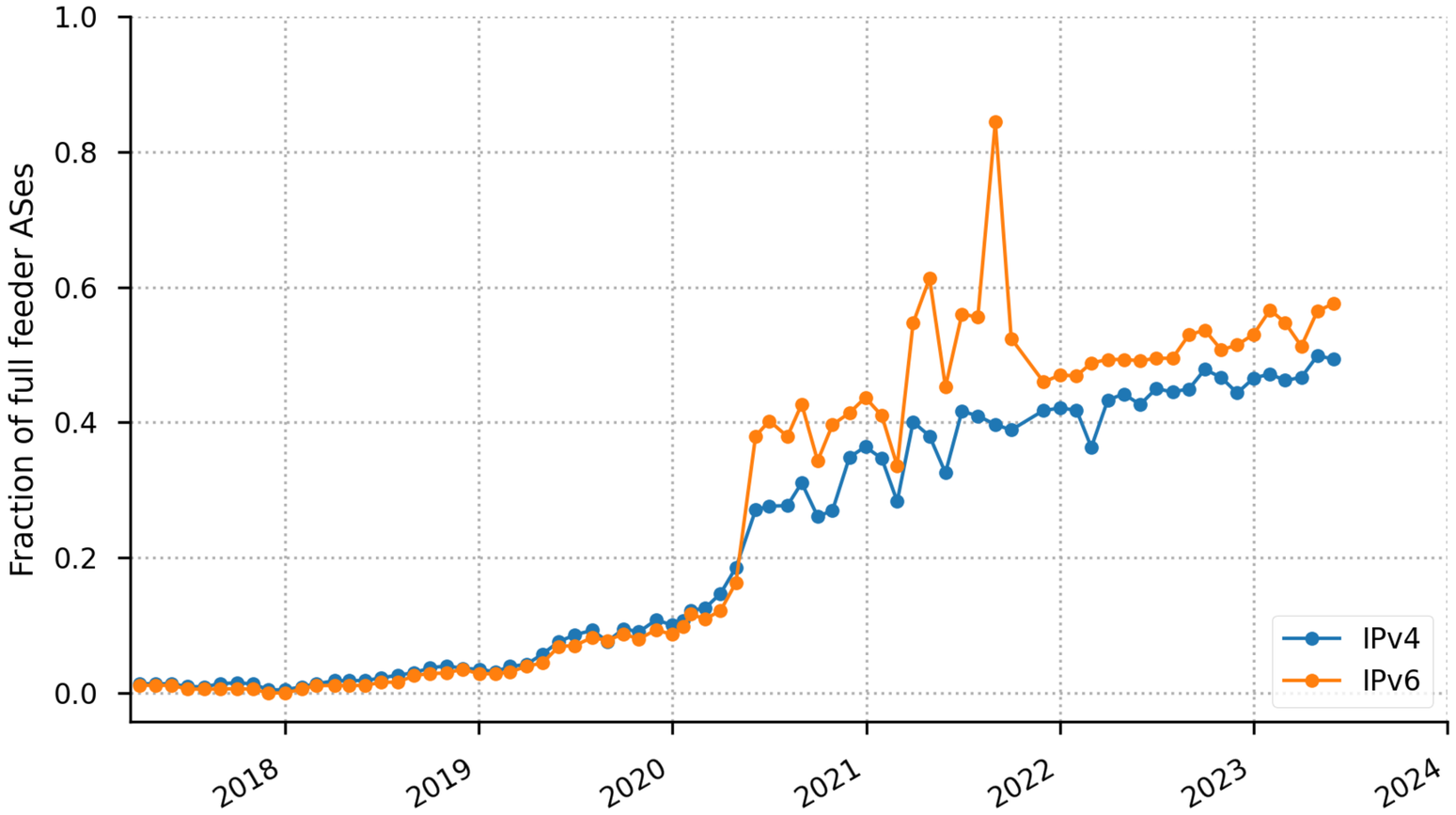
Georgia Tech

Based on work by Deepak Gouda (MSc Student)

ROV Deployment

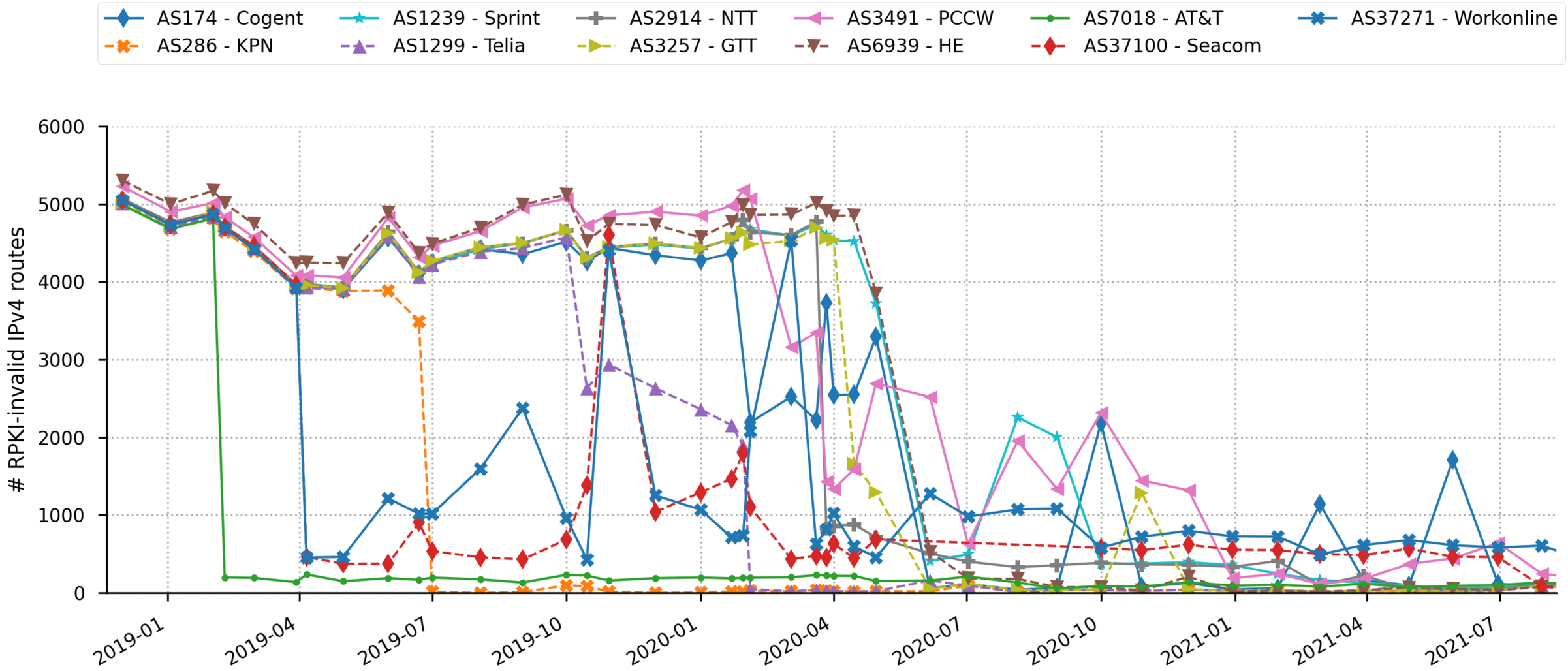
ROV deployment in ASes peering with BGP collectors

- BGP collectors peers in 2023:
  - IPv4: 315-320 ASNs
  - IPv6: 280-290 ASNs
- ROV ASNs 06/2023
  - IPv4: 155
  - IPv6: 163
- Unique ROV ASNs: 303



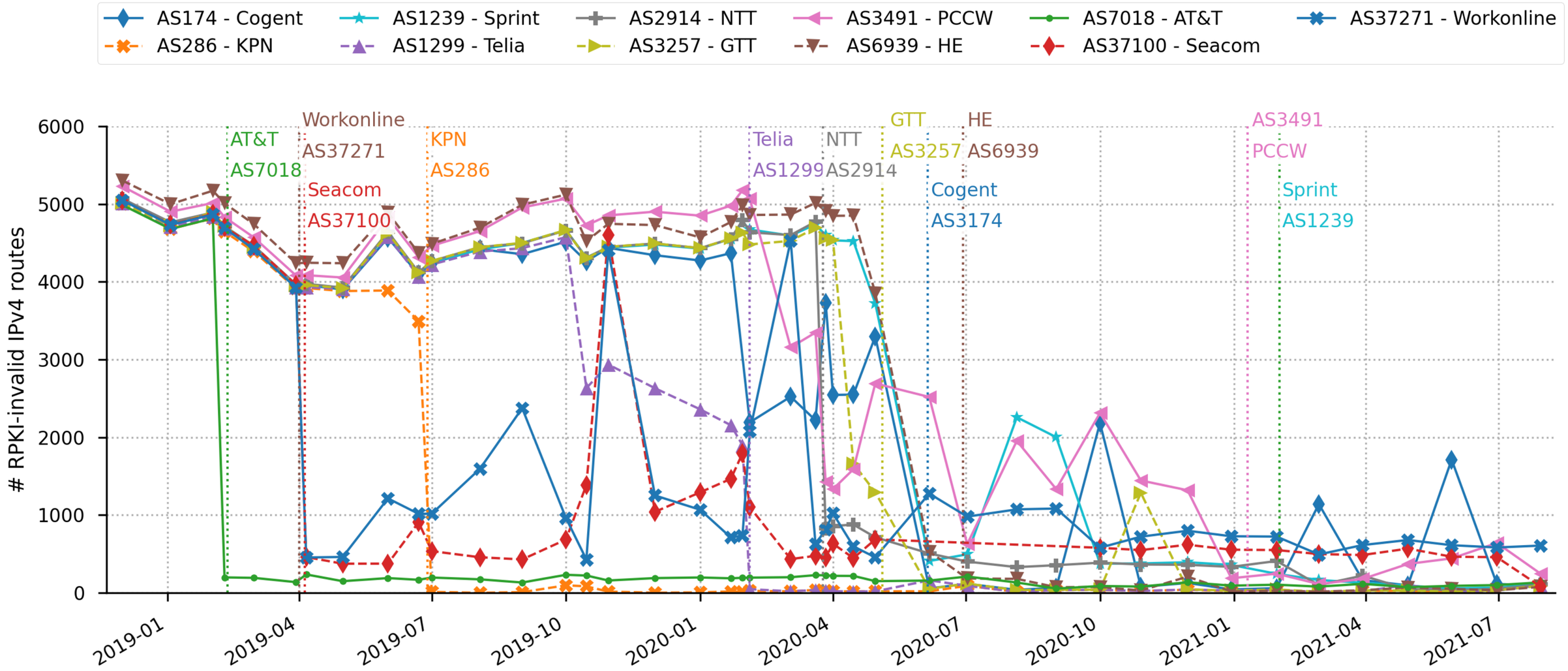
Georgia Tech

RPKI-invalid prefix count over time 2019-2021



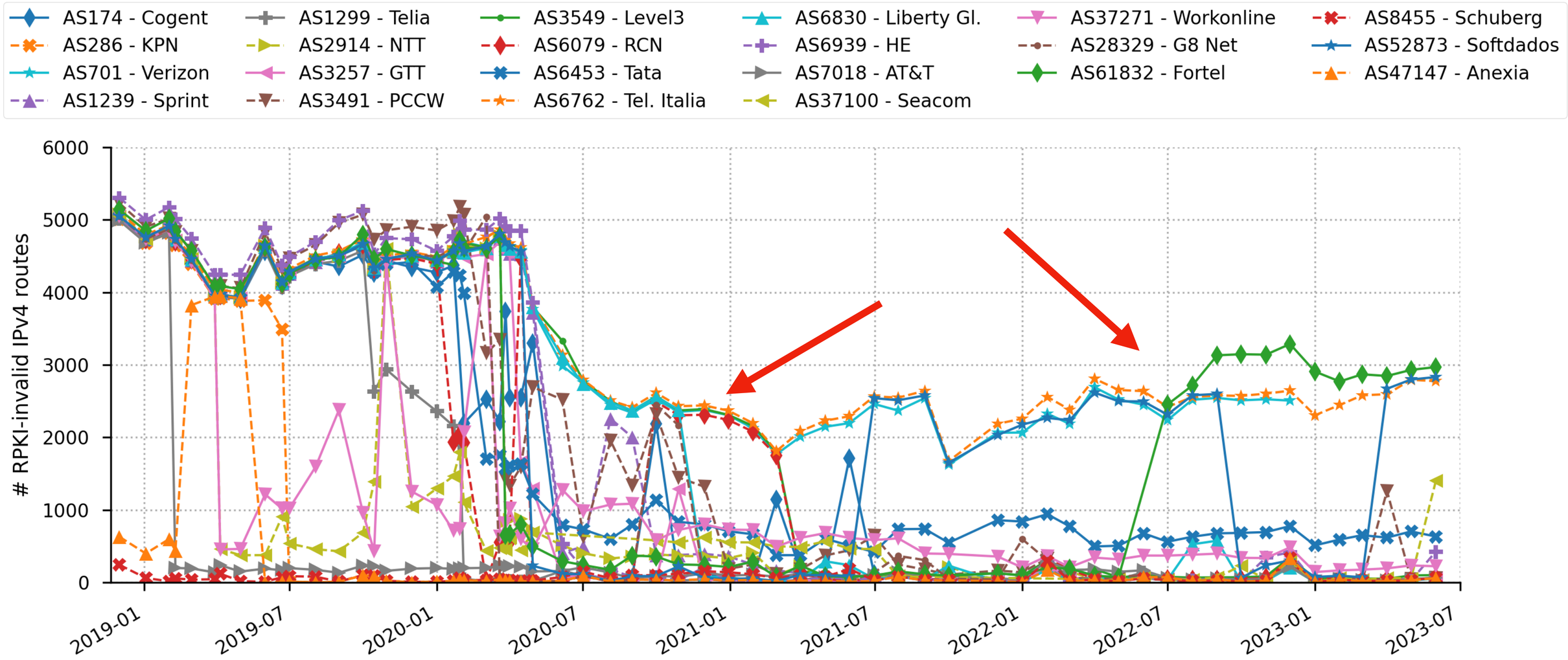
Georgia Tech

RPKI-invalid prefix count over time 2019-2021



Georgia Tech

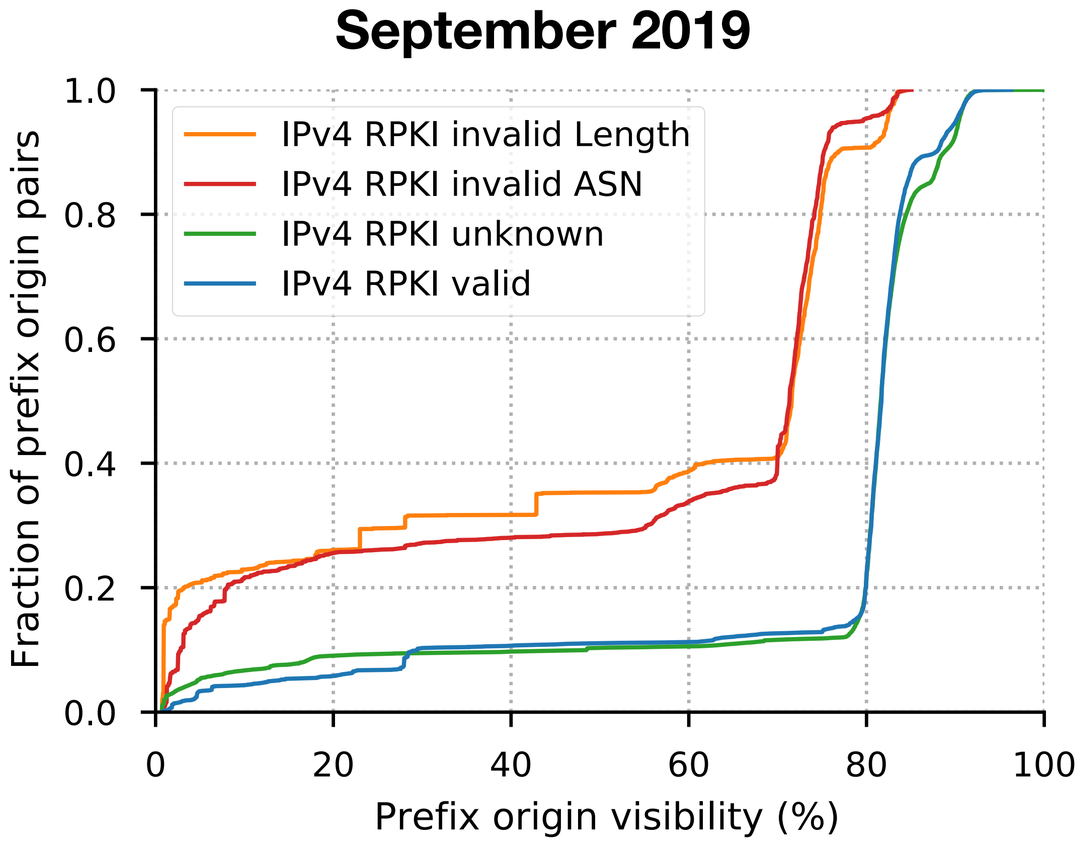
RPKI-invalid prefix count over time 2019-2023



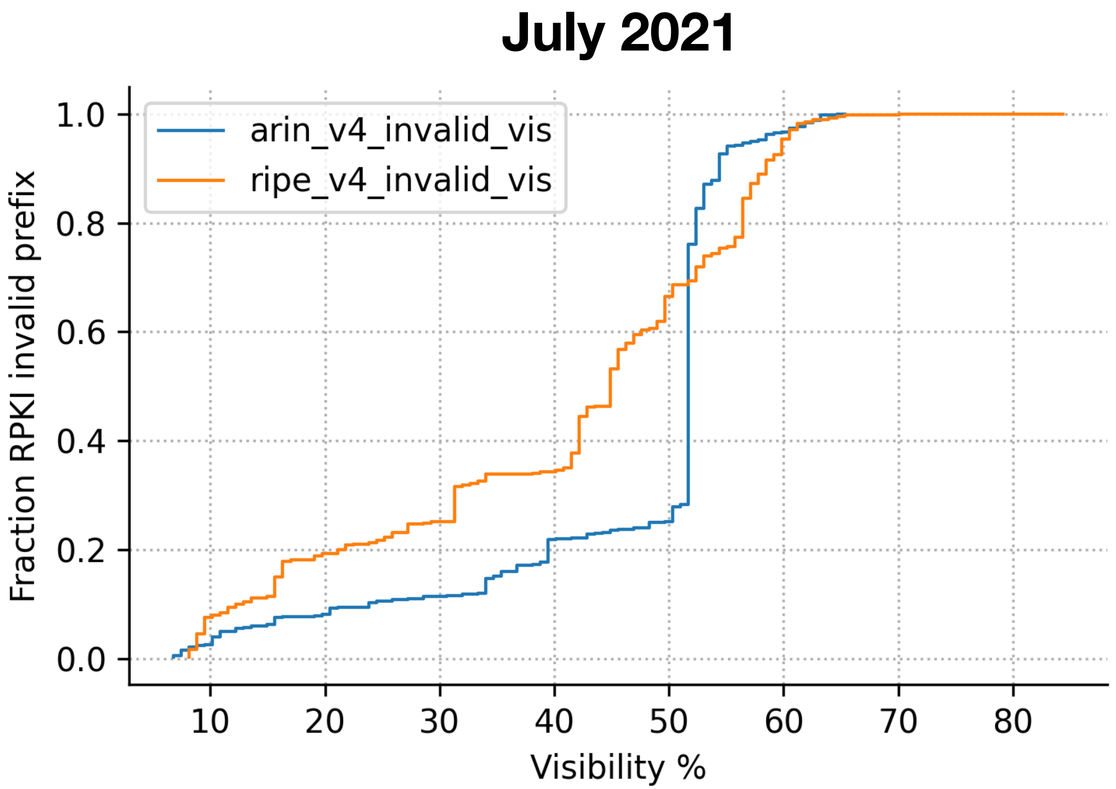
ROV Impact - RPKI Invalid visibility

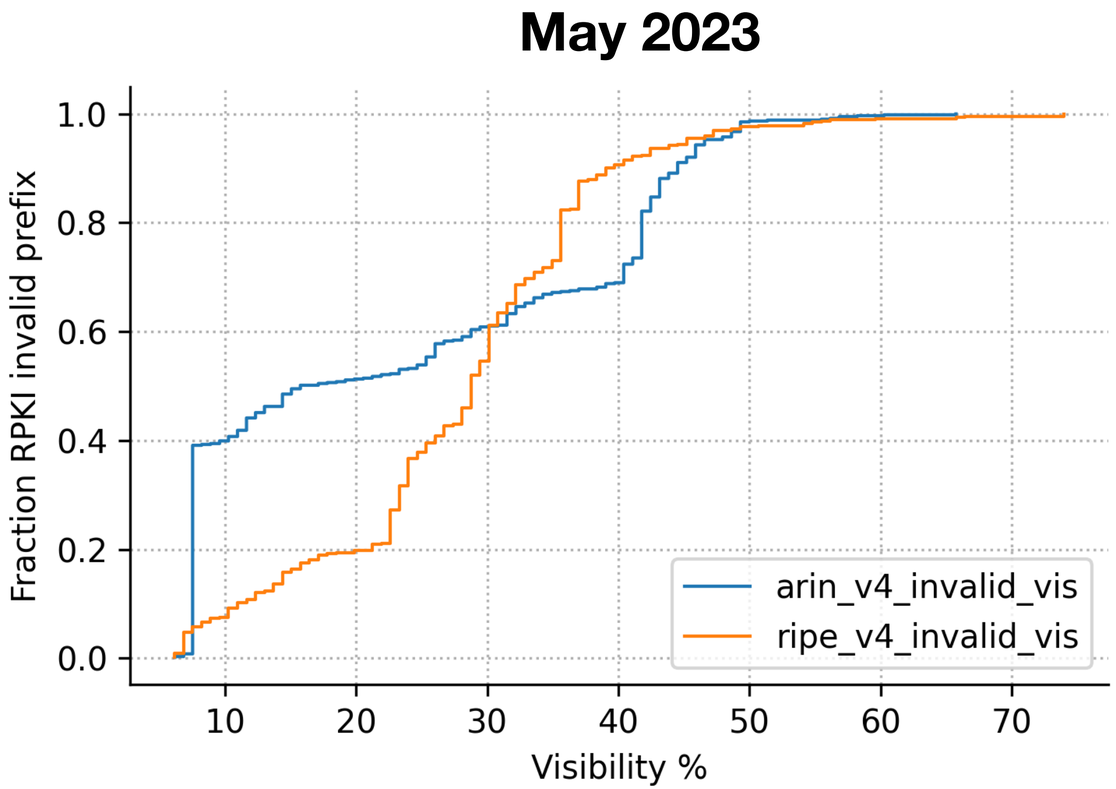
ROV impact in prefix visibility

- ROAs impact prefix visibility.
- Most prefixes are either high visibility or low visibility
- Natural experiment option: each RIR defines its own RPKI-related policies.



ROV impact in RPKI invalid prefix visibility ARIN & RIPE





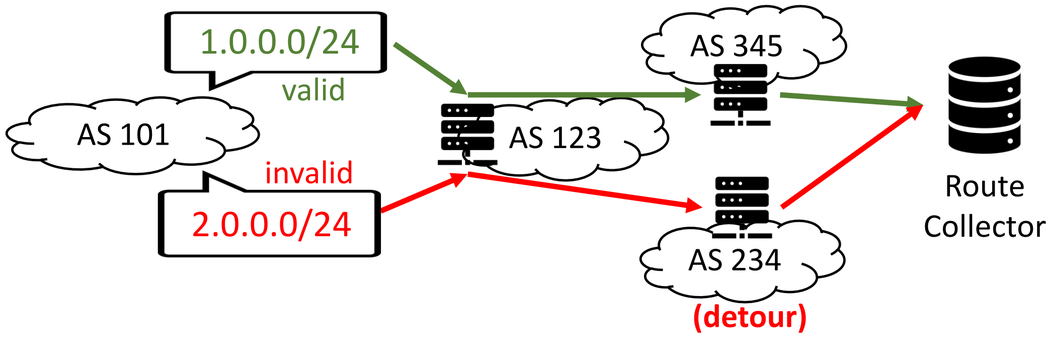
- Arin still has more high-visibility RPKI-invalid prefixes

ARIN RPA

Validator	Auto download ARIN repo	Date of ARIN Update
FORT Validator	No, requires agreement	N/A
Routinator	Yes	11/10/22
RPKI Prover	Yes	11/22/22
Octo RPKI	Yes	4/5/23
RPSTIR2	Yes	3/4/21

ROV Impact - RPKI Invalid detour

Detour of RPKI invalid BGP announcements



- 160 detour ASNs
- Limitations: ROV depends on AS relationships (Hegemony score may help)

Transit ASN	Company	# AS	# Invalid Pfx
AS 6762	Telecom Italia	301	1,125
AS 6461	Zayo	59	147
AS 7473	Singapore Telecom	54	135
AS 6453	TATA America	38	78
AS 1273	Vodafone	13	18

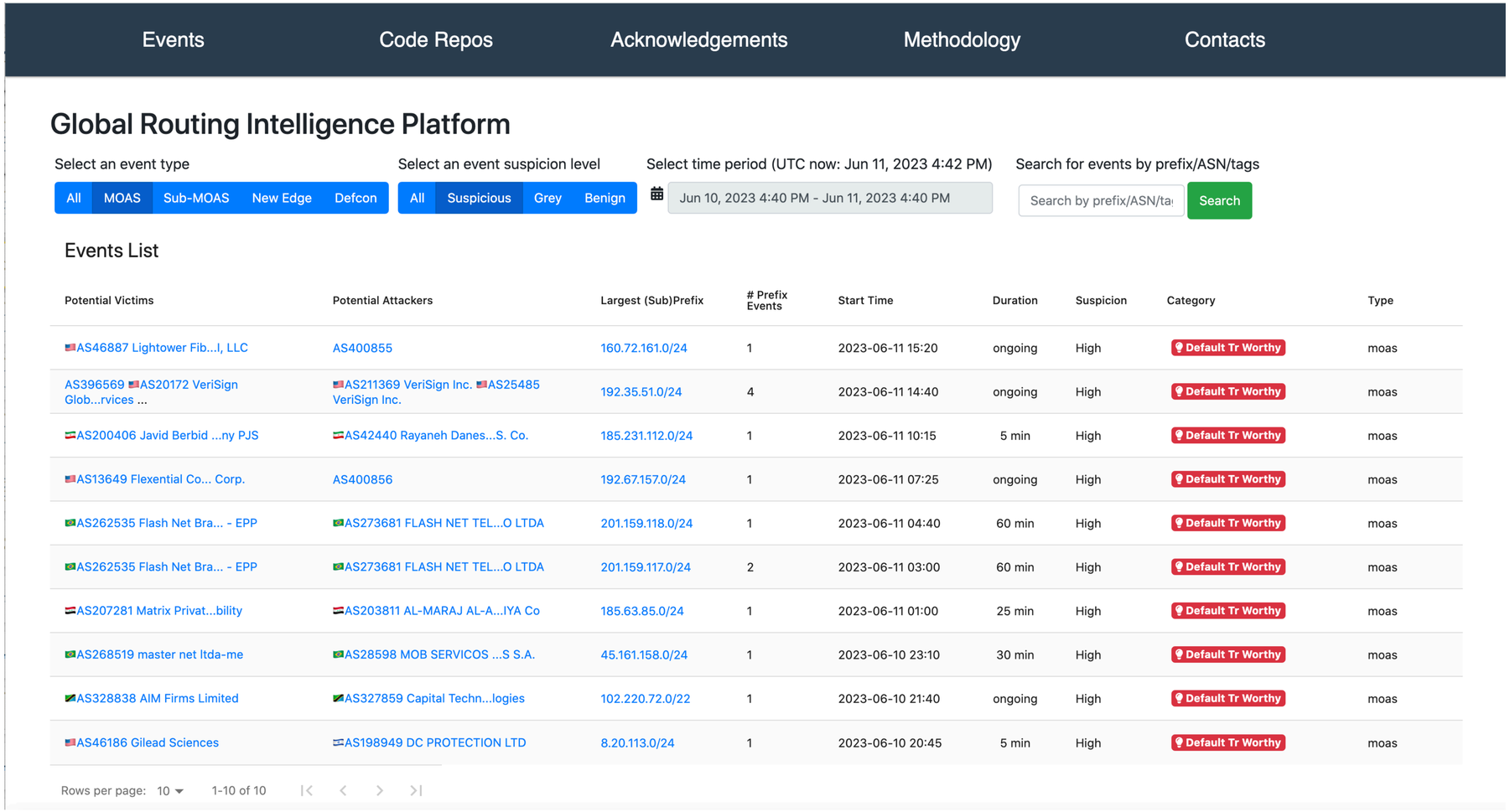
Georgia Tech

Based on work by Ben Du (PhD candidate UCSD)

BGP Hijacks

Global Routing Internet Platform (GRIP)

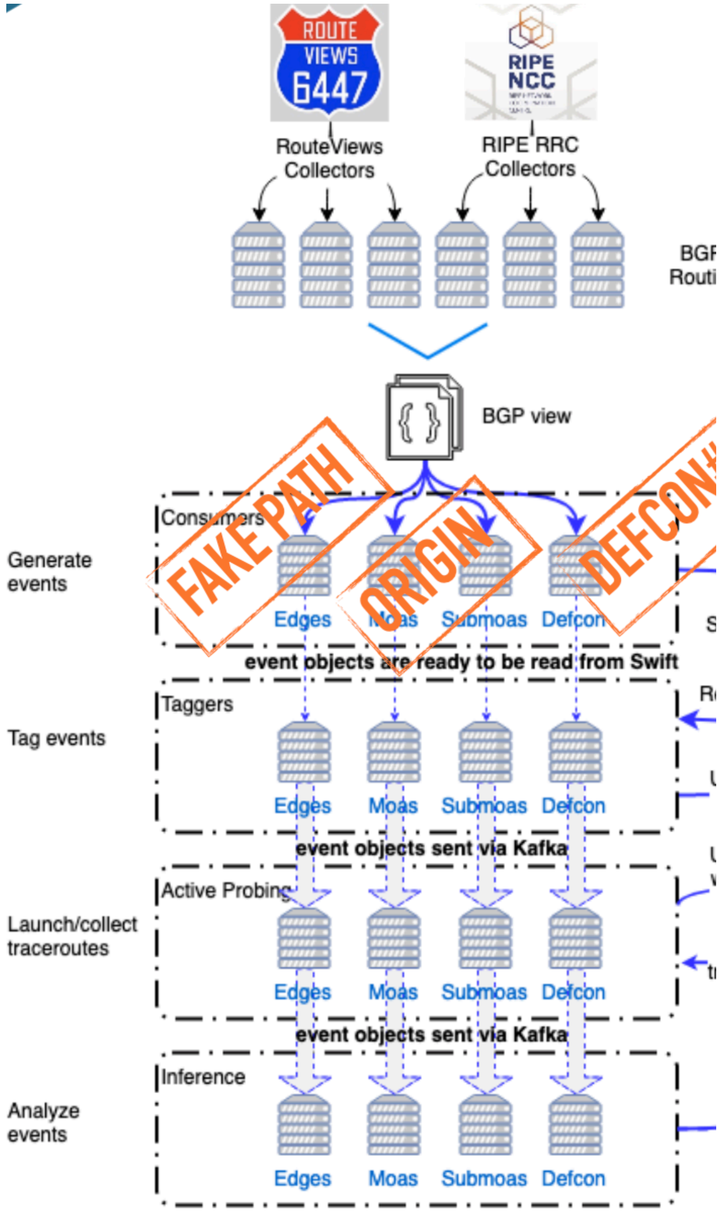
- All types of hijacks:
  - Origin
  - Fake path
  - Not preferred path (Defcon #16)
- In use by MANRS Observatory



Collaboration with Alberto Dainotti et al.

GRIP Infrastructure

- Gathers all potential events
- Tags based on routing behavior and additional data (RPKI, IRR, AS type, etc)
- Inference engine to weed out false positive cases
- Allows to gather feedback



Thanks