

RPKI is Coming of Age

A Longitudinal Study of RPKI Deployment and Invalid Route Origins

Taejoong (Tijay) Chung[§], Emile Aben[†], Tim Bruijnzeels[‡],
Balakrishnan Chandrasekaran[△], David Choffnes^{*}, Dave Levin⁺,
Bruce Maggs^{°♦}, Alan Mislove^{*}, Roland van Rijswijk-Deij^{‡±},
John Rula[♦], Nick Sullivan^{*}

[§]Rochester Institute of Technology, [†]RIPE NCC, [‡]NLNetLabs,
[△] Max Planck Institute for Informatics, ^{*}Northeastern University, ⁺University of Maryland,
[°]Duke University, [±]University of Twente, [♦]Akamai Technologies, [※]Cloudflare

RPKI is Coming of Age

*A Longitudinal Study of RPKI Deployment
and Invalid Route Origins*

Resource PKI (Public Key Infrastructure)

- Public Key Infrastructure framework designed to secure Internet's routing structure; specifically BGP (developed starting in 2008)

(Cryptographically verifiable)
Prefix-to-AS Mapping Database

185.34.56.0/22	AS3356
129.21.128.0/17	AS4385
...	...
...	...
...	...
129.21.0.0/16	AS4385
193.56.235.0/24	AS3549



Router



RIT

Owner

AS 4385
129.21.0.0/16

RPKI: How it works?

What does an resource owner needs to do to protect their IP prefixes?



Router

BGP announcement



RIT

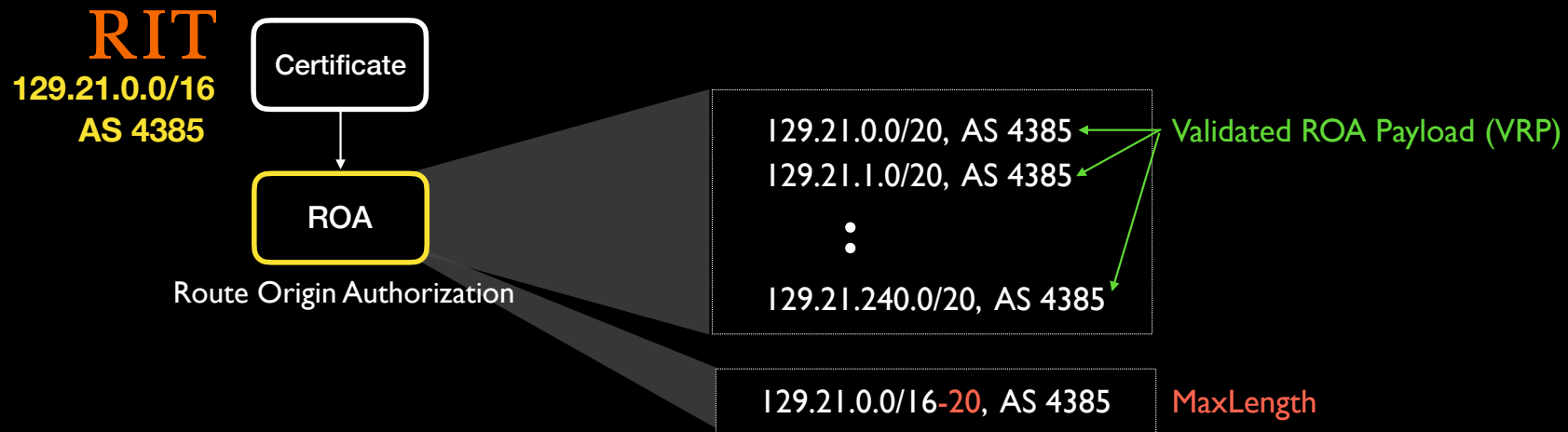
Owner

AS 4385

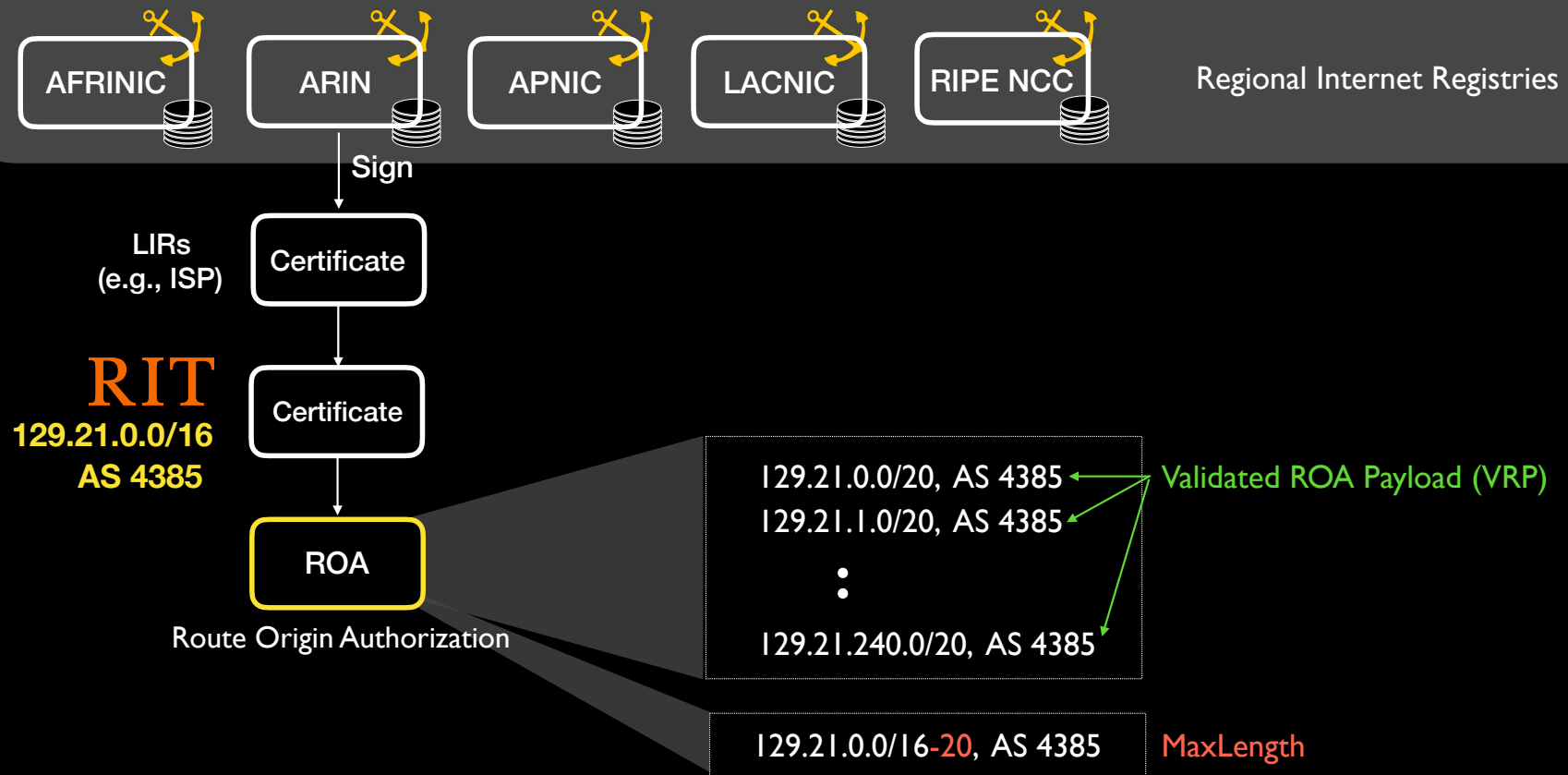
129.21.0.0/16

How can a router verify it using RPKI?

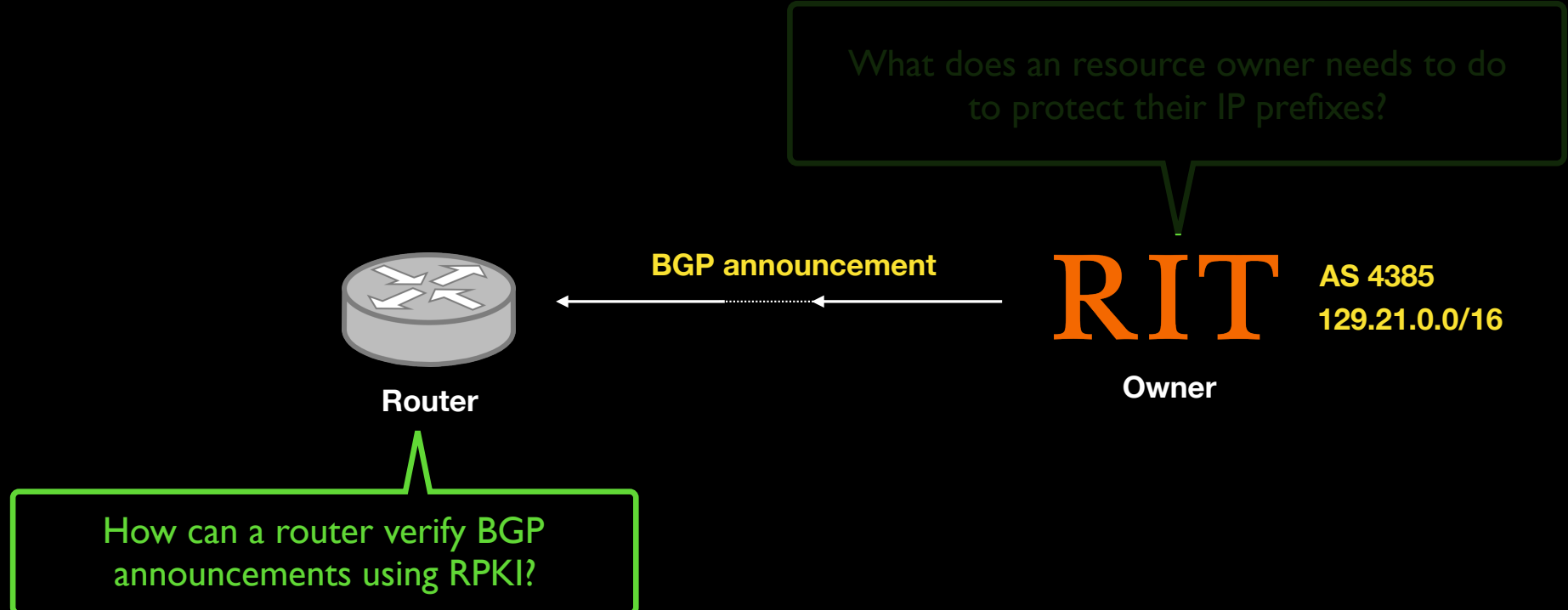
RPKI Structure



RPKI Structure



RPKI: How it works?



RPKI: How it works?

Validation process: Valid

Prefix-to-AS Mapping Database

1.1.0.0/16 AS 111
2.0.0.0/8-16 AS 222
3.3.0.0/16 AS 333
4.4.4.0/24 AS 444



Router

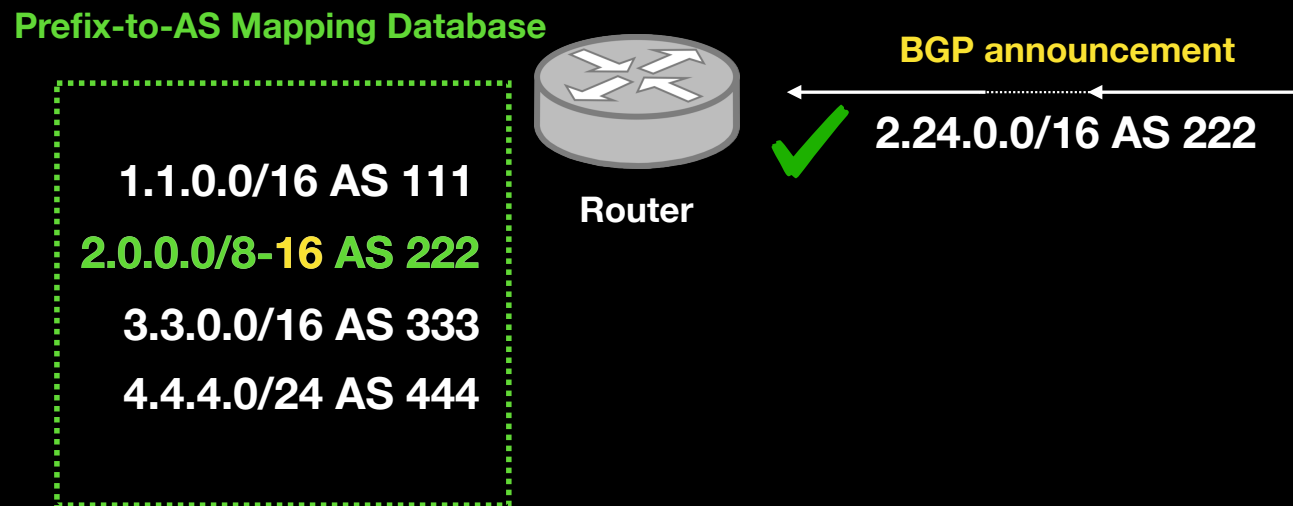
BGP announcement



1.1.0.0/16 AS 111

RPKI: How it works?

Validation process: Valid (w/ MaxLength)



RPKI: How it works?

Validation process: **Invalid** (too-specific)

Prefix-to-AS Mapping Database

1.1.0.0/16 AS 111
2.0.0.0/8-16 AS 222
3.3.0.0/16 AS 333
4.4.4.0/24 AS 444



Router

BGP announcement

← 3.3.3.0/24 AS 333



Covered, but the announcement is too specific

RPKI: How it works?

Validation process: **Invalid** (wrong ASN)

Prefix-to-AS Mapping Database

1.1.0.0/16 AS 111
2.0.0.0/8-16 AS 222
3.3.0.0/16 AS 333
4.4.4.0/24 AS 444



Router

BGP announcement

← 4.4.4.0/24 AS 555 ←



IP prefix is matched,
but the ASN is different.

RPKI: How it works?

Validation process: Unknown (Uncovered)

Prefix-to-AS Mapping Database

1.1.0.0/16 AS 111
2.0.0.0/8-16 AS 222
3.3.0.0/16 AS 333
4.4.4.0/24 AS 555



Router

BGP announcement

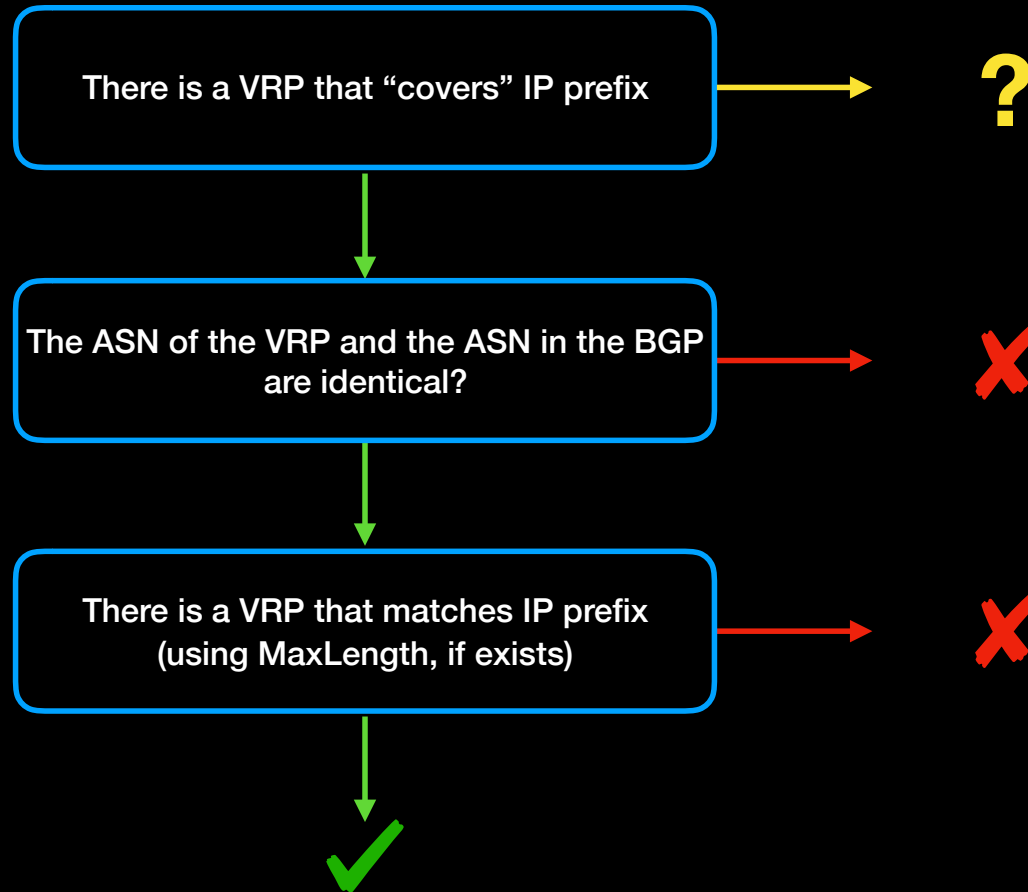
5.5.0.0/16 AS 555



Uncovered, thus unknown

RPKI: How it works?

Validation Process



Alright, so in this talk..

RPKI is Coming of Age

*A Longitudinal Study of RPKI Deployment
and Invalid Route Origins*

Why do we study RPKI?

It is relatively new

It works differently

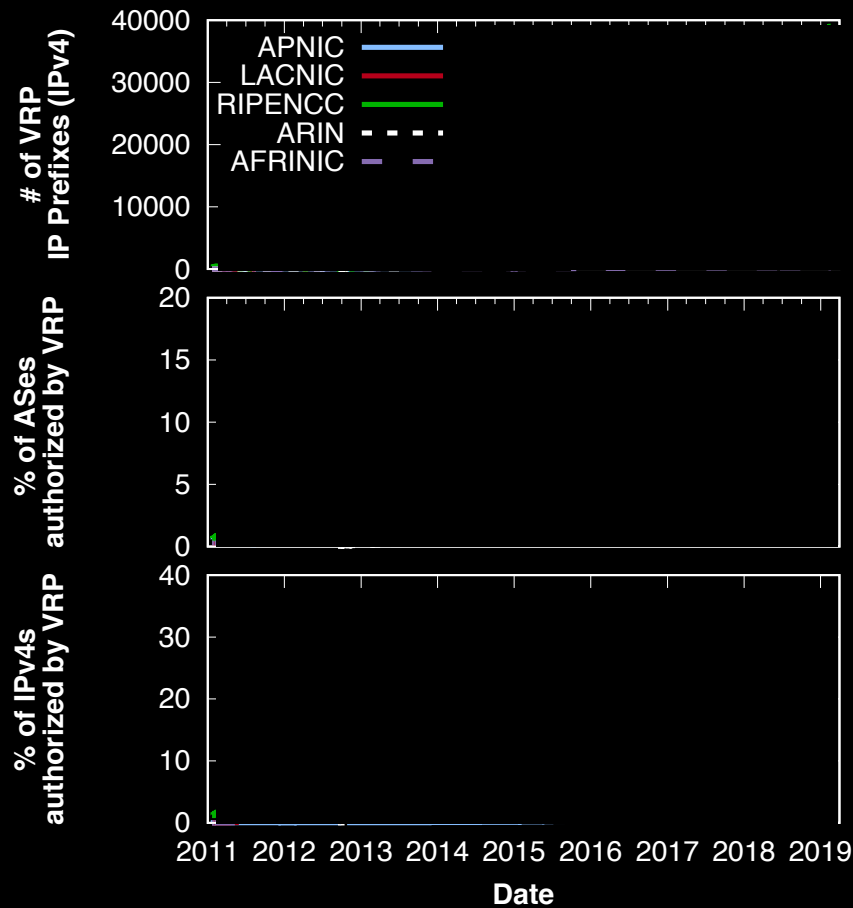
It is easy to deploy

Datasets (I)

RPKI Objects

	Measurement Period*	VRPs (from the latest snapshot)	
		Number	Percent of ASes
APNIC	2011-01 ~ 2019-02	14,025	8.14%
LACNIC	2011-01 ~ 2019-02	4,510	9.33%
RIPENCC	2011-01 ~ 2019-02	40,830	16.04%
ARIN	2012-09 ~ 2019-02	4,575	1.47%
AFRINIC	2011-01 ~ 2019-02	176	3.30%

Deployment: VRPs



A general increasing trend in adoption of RPKI!

It varies significantly between RIRs:
1.38% (ARIN) ~ 15.11% (RIPENCC) of ASes and
2.7% (AFRINIC) ~ 30.6% (RIPENCC) of IPv4
addresses are authorized by VRPs

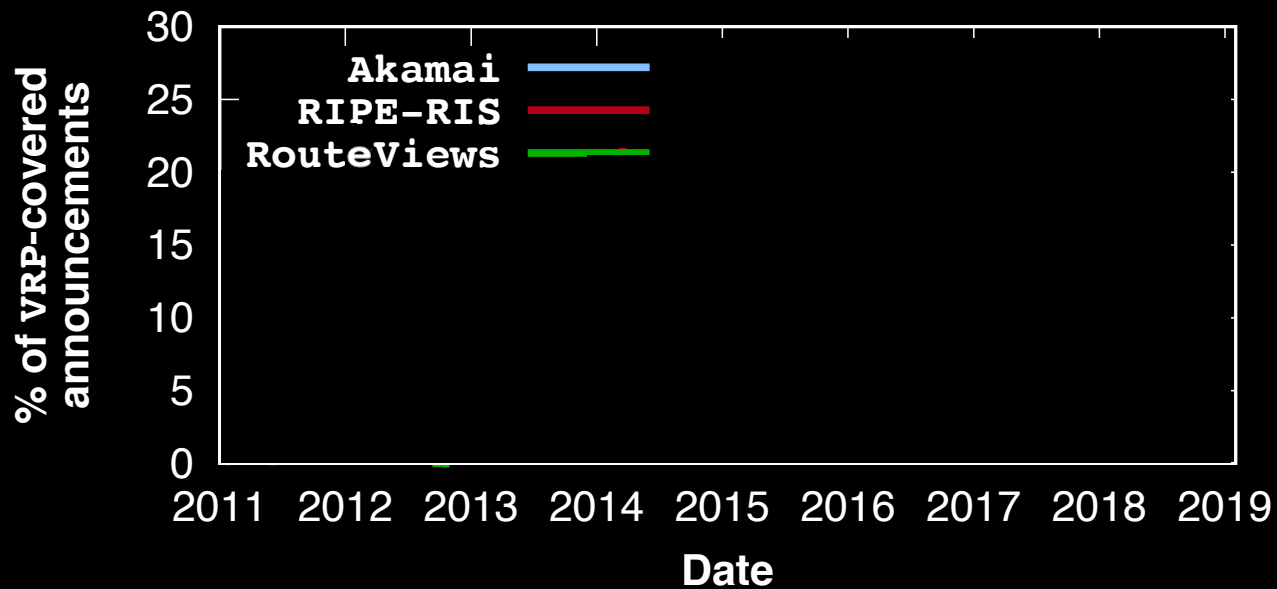
Datasets (2)

BGP Announcements

	Measurement Period	# of	
		VPs	Prefixes
RIPE-RIS	2011-01 ~ 2018-12	24	905K
RouteViews	2011-01 ~ 2018-12	23	958K
Akamai	2017-01 ~ 2018-12	3,300	1.94M

More than 46 Billion BGP announcements

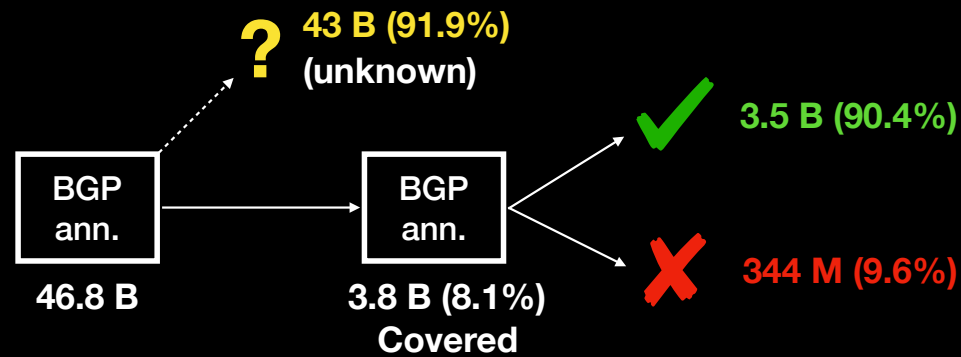
Deployment: BGP announcements w/ RPKI



Deployment

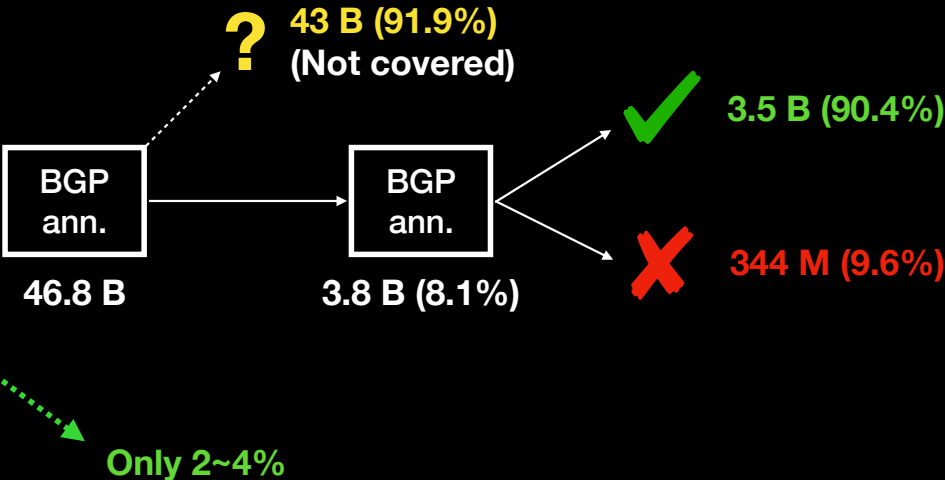
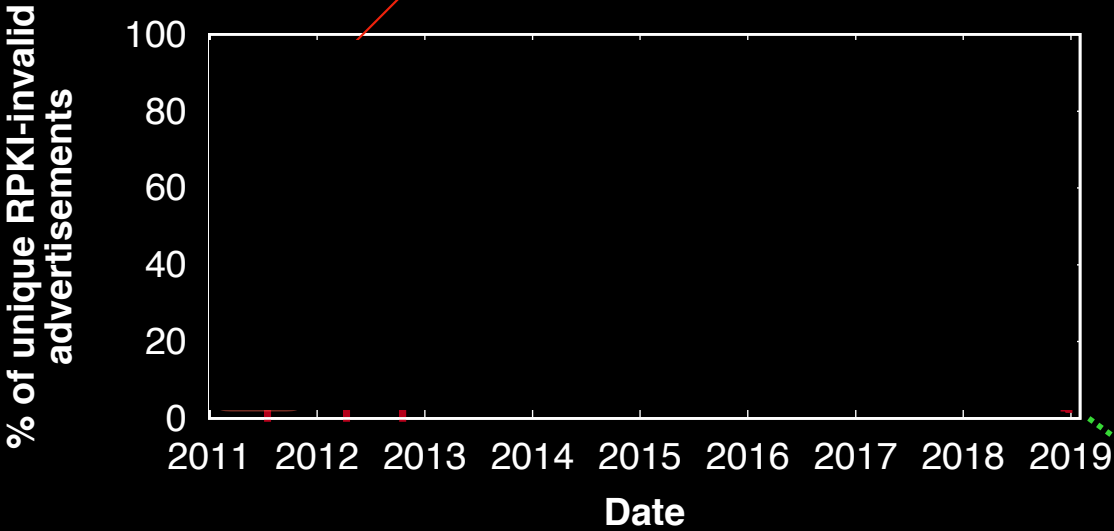
RPKI-enabled BGP announcements are consistently increasing

RPKI validation over BGP announcements



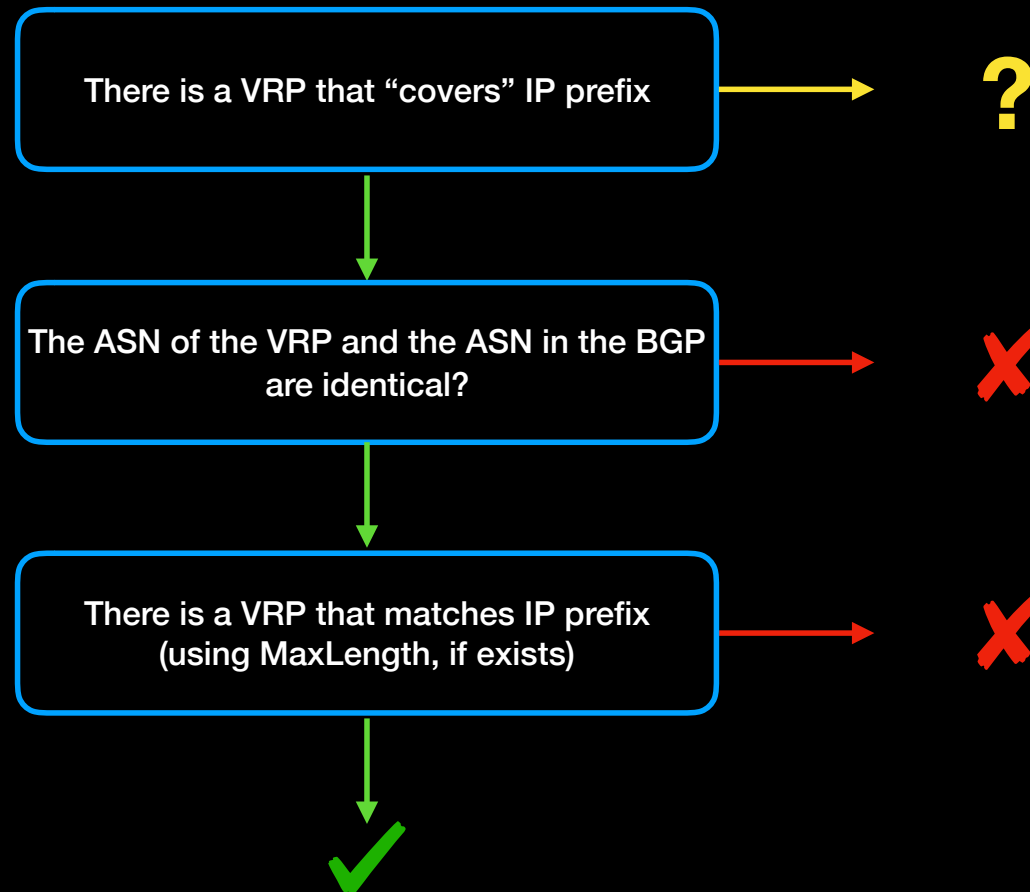
RPKI validation over BGP announcements

During 2011, 48.92% covered announcements were invalid;
 27.47% of invalid were due to announced IP prefixes being covered, but not matched with VRPs

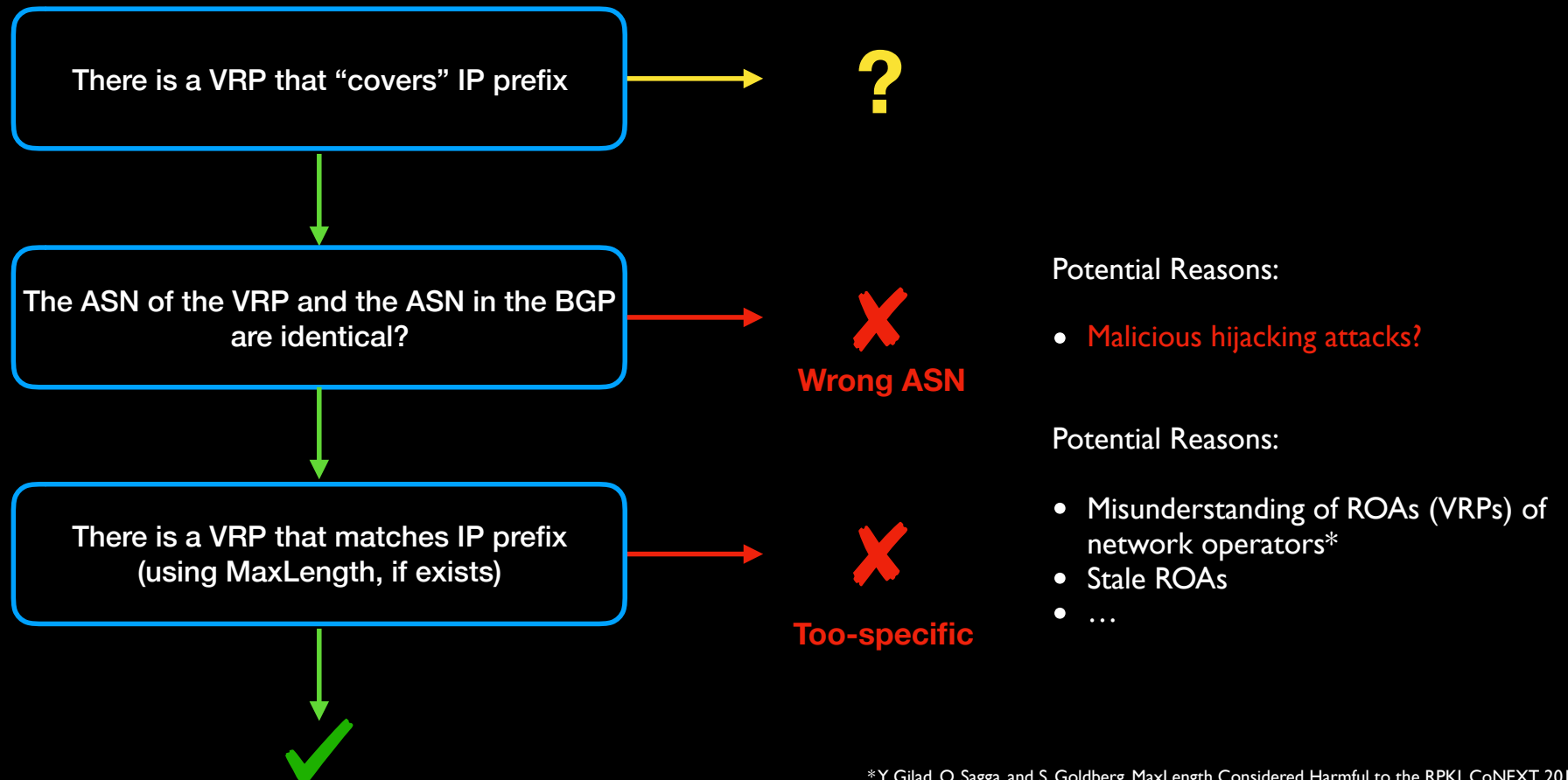


Only 2~4%

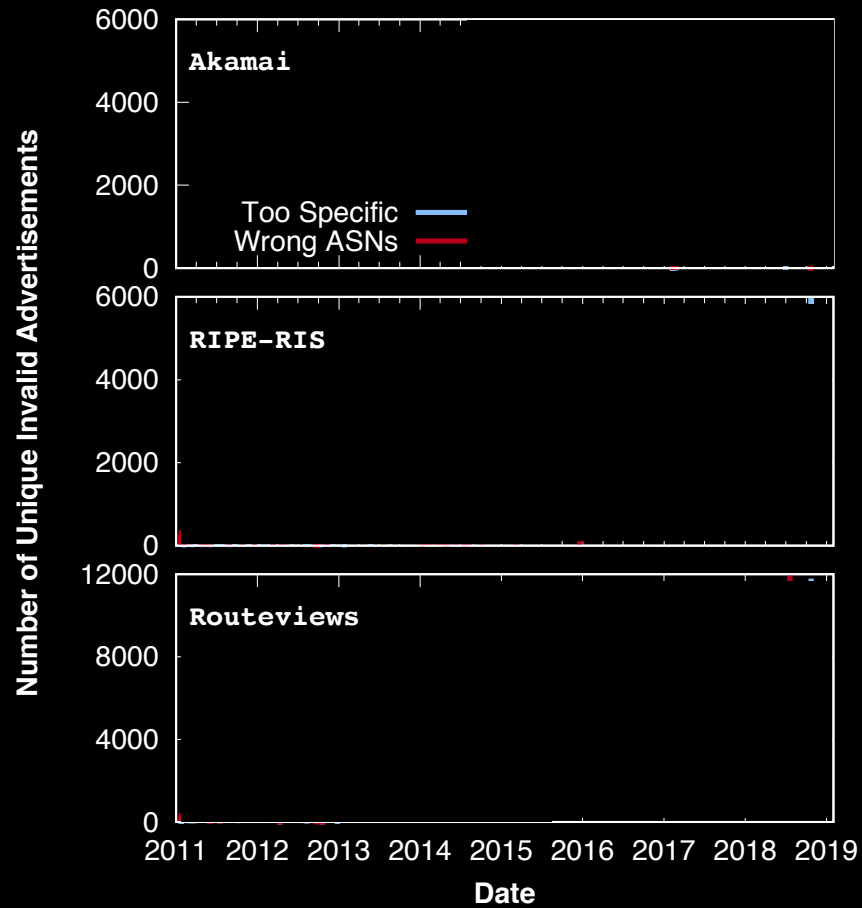
Then, why are they invalid?



Then, why are they invalid?

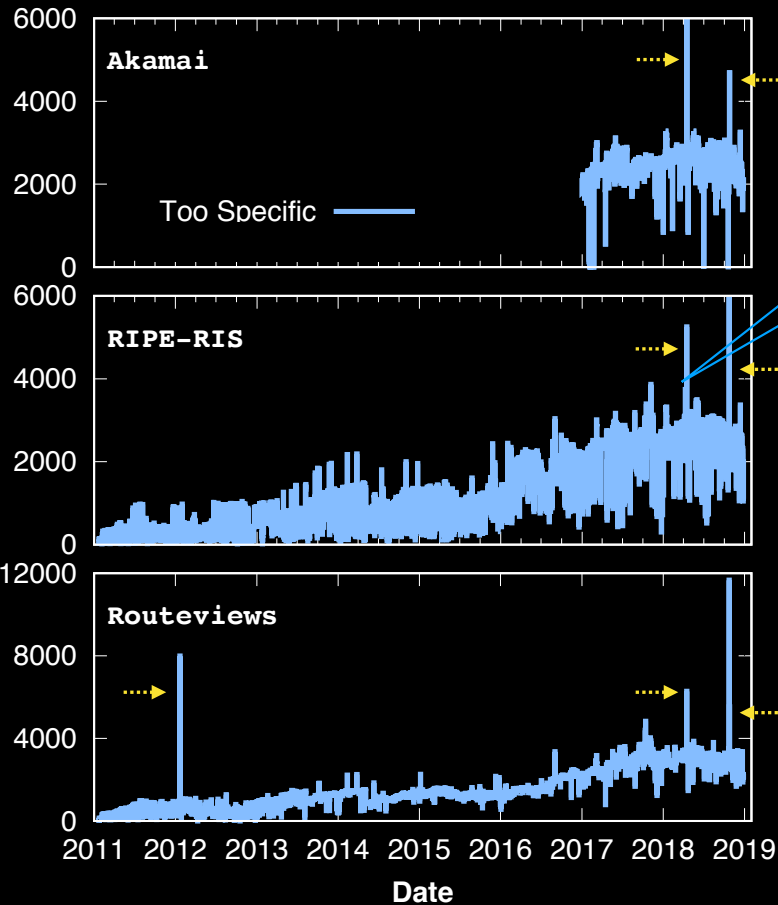


Too specific vs. Wrong ASNs



Too specific vs. Wrong ASNs

Number of Unique Invalid Advertisements



AS 5089 (Virgin Media Limited)

On April 16, 2018,
3,200 IP prefixes are more specific than the
VRPs; none of them specified MaxLength

AS12322 (Free SAS)

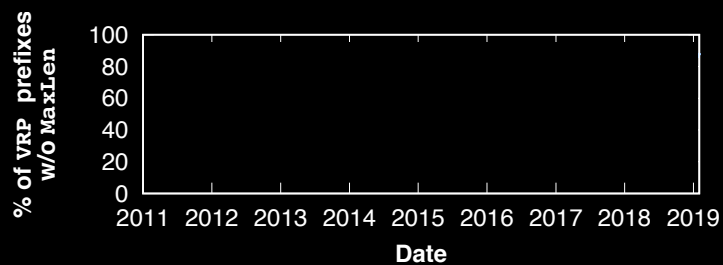
6 ROAs for 7,671 (96.0%) IP prefixes
are more specific than the VRPs (w/o
MaxLength)

8,800 IP prefixes went invalid failing to
specify a proper value for MaxLength

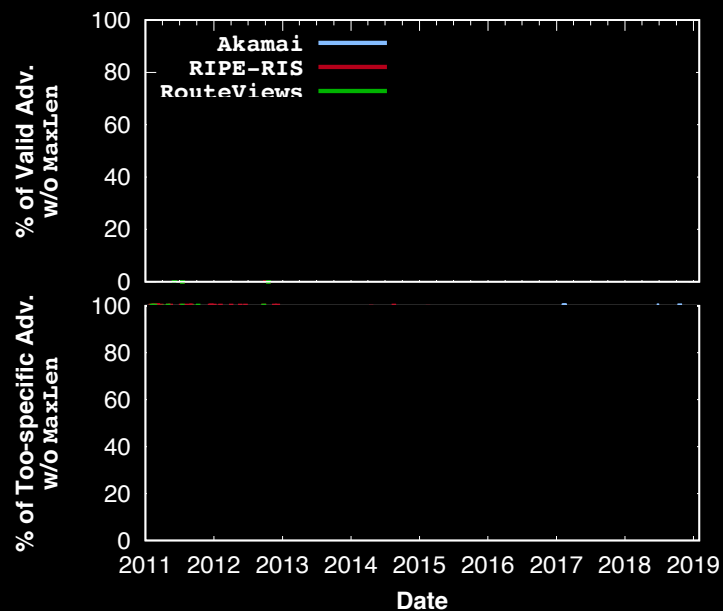


Added the MaxLength to include
more specific IP prefixes

Too-specific and MaxLength attribute



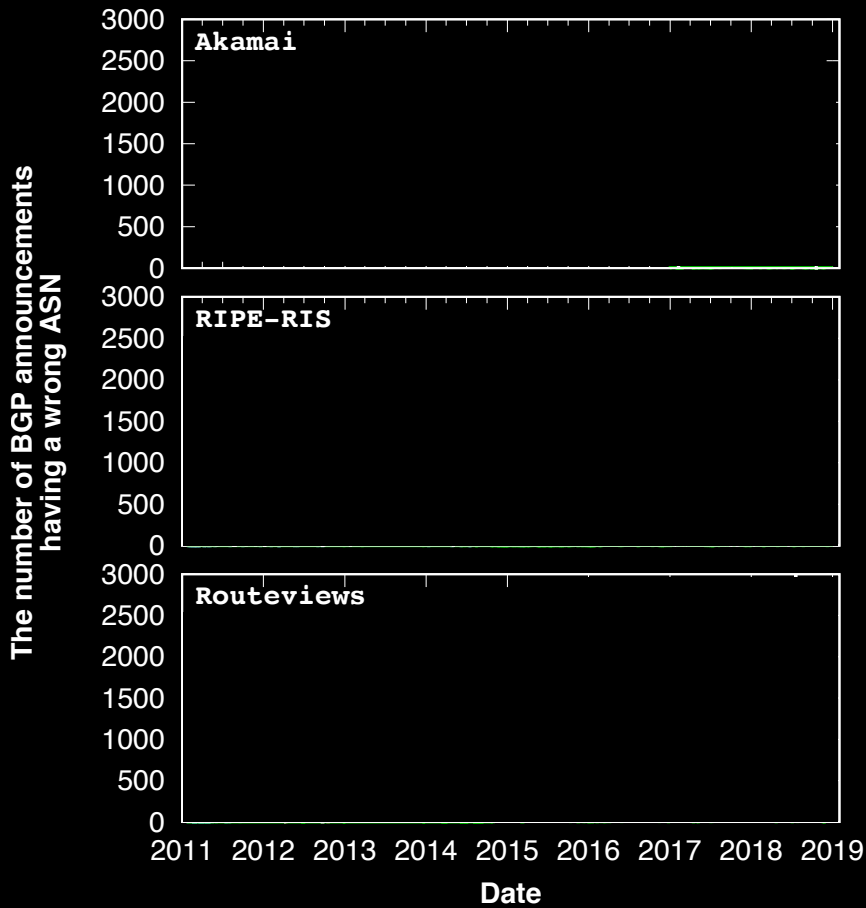
The use of MaxLength has been decreasing



52.3% of the valid IP prefixes are validated through VRPs with the MaxLength attribute

92% of too-specific announcements are due to VRPs that do not have the MaxLength attribute

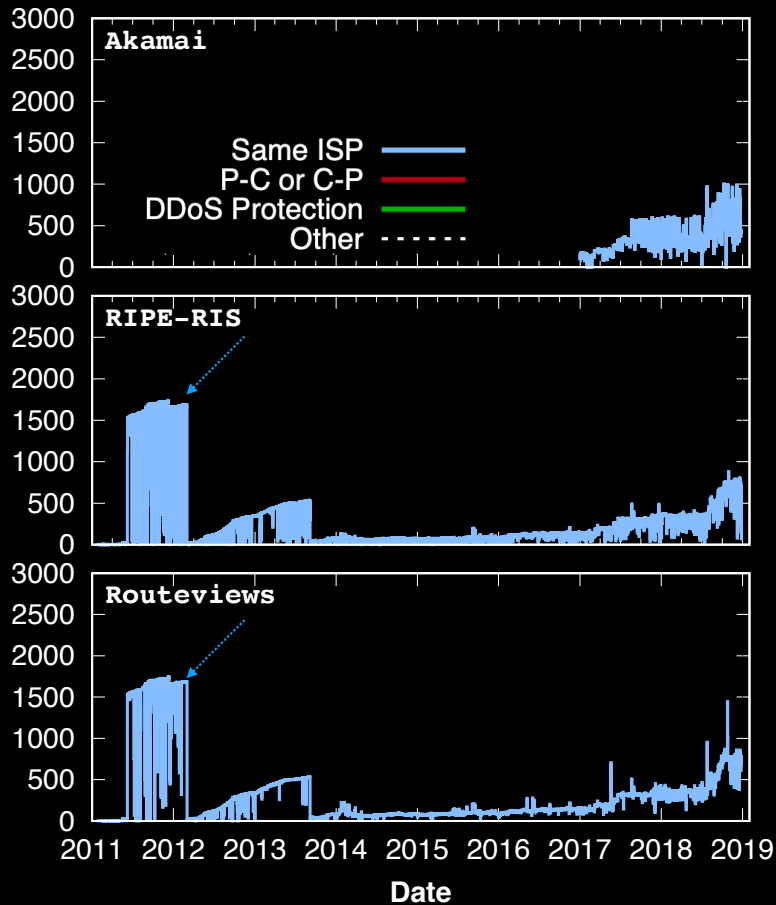
Wrong ASN



Same ISP	Two different ASNs are managed by the same operator
Provider—Customer Relationship	An AS can sub-allocate part of its IP prefixes to its customer
DDoS Protection	Origin ASes may outsource “scrubbing” of their traffic by using traffic diversion to a DDoS protection service (DPS)
Other	We don’t know, but it could be malicious (e.g., hijacking)

Wrong ASN: Same ISP

The number of BGP announcements having a wrong ASN

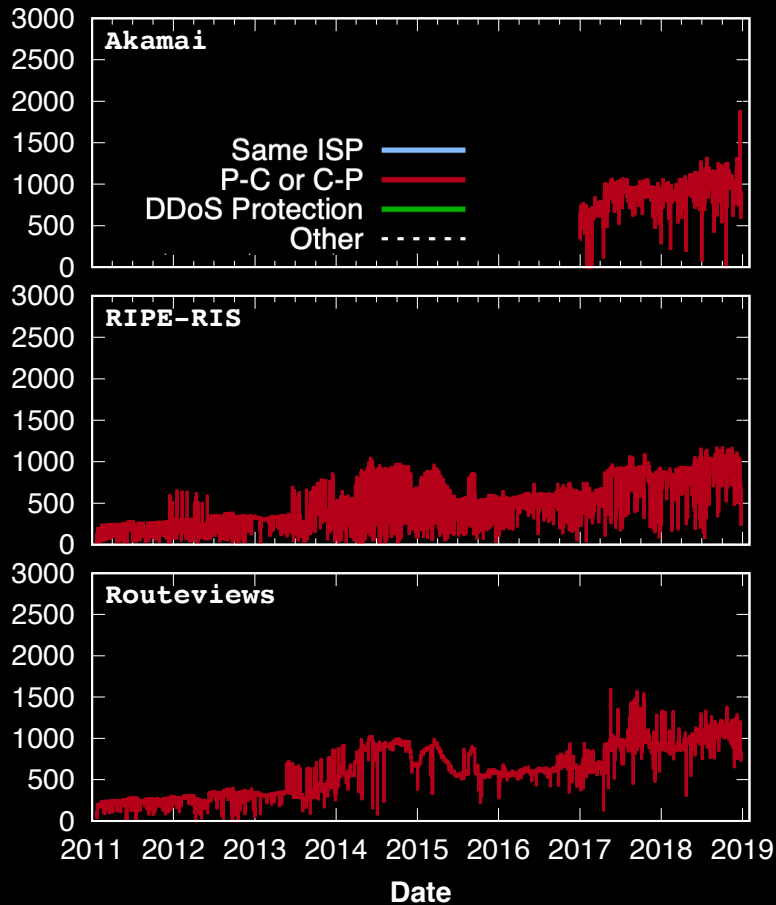


Same ISP	Two different ASNs are managed by the same operator
Provider—Customer Relationship	An AS can sub-allocate part of its IP prefixes to its customer
DDoS Protection	Origin ASes may outsource “scrubbing” of their traffic by using traffic diversion to a DDoS protection service (DPS)
Other	We don’t know, but it could be malicious (e.g., hijacking)

Telmex Columbia S.A. manages two ASes (AS 10620, 14080)
 AS 10620 announced 1,500 prefixes supposed to be from AS 14080
 for 9 months

Wrong ASN: Provider — Customer Relationship

The number of BGP announcements having a wrong ASN



Same ISP

Two different ASNs are managed by the same operator

Provider—Customer Relationship

An AS can sub-allocate part of its IP prefixes to its customer

DDoS Protection

Origin ASes may outsource “scrubbing” of their traffic by using traffic diversion to a DDoS protection service (DPS)

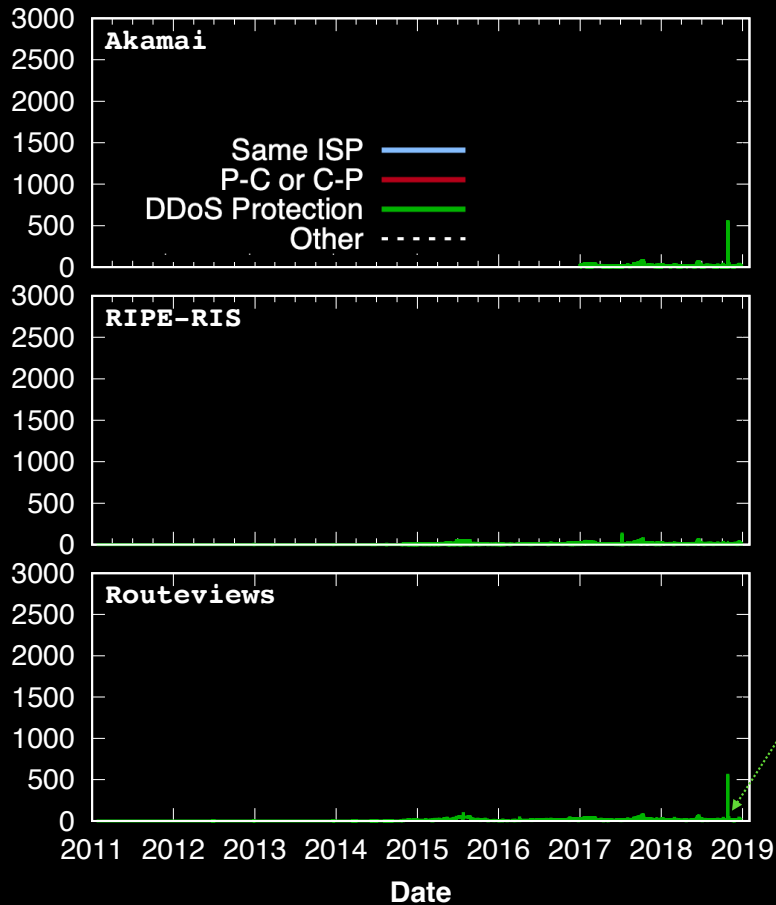
Other

We don't know, but it could be malicious (e.g., hijacking)

P-C and C-P are quite prevalent; mainly due to providers that have not updated after leasing to the IP prefixes customers (up to 89.45%) such as AS 6128 (CableVision Systems) allocating to 9 different ASes

Wrong ASN: DDoS Protection

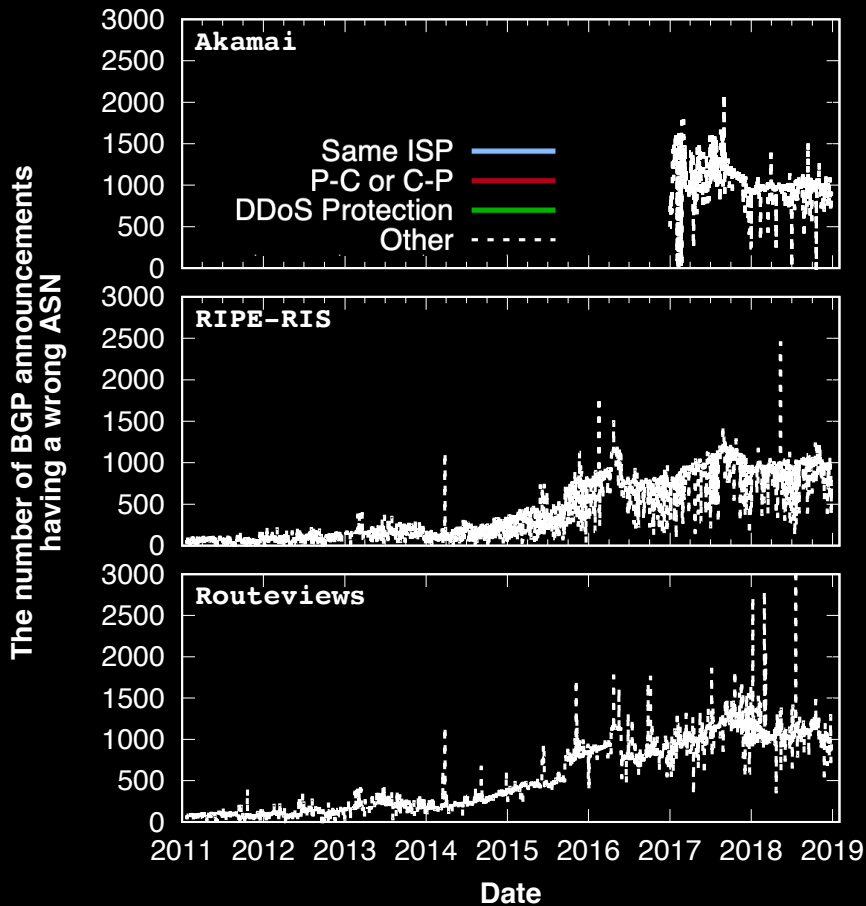
The number of BGP announcements having a wrong ASN



Same ISP	Two different ASNs are managed by the same operator
Provider—Customer Relationship	An AS can sub-allocate part of its IP prefixes to its customer
DDoS Protection	Origin ASes may outsource “scrubbing” of their traffic by using traffic diversion to a DDoS protection service (DPS)
Other	We don’t know, but it could be malicious (e.g., hijacking)

We rarely see announcements from DDoS protection services
 AS 26415 (Verisign) announced 6 IP prefixes of AS 13285 (TalkTalk)
 AS 19905 (Neustar) announced 1 IP prefix of AS 21599

Wrong ASNs: The others (possibly suspicious)

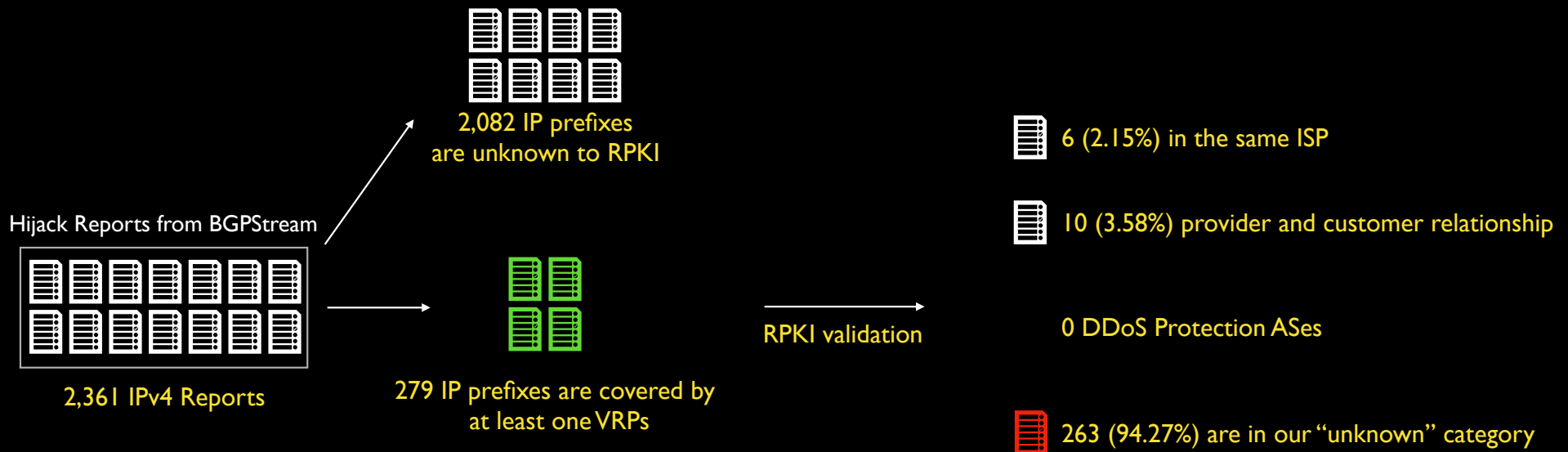


(1) AS 37468 (Angola Cables) announced more than 2,500 IP prefixes owned by 82 ASes on May 11, 2018 and 15,000 IP prefixes owned by 1,554 ASes on July 19, 2018

(2) Targeted attack: AS 55649 (a private ISP in Hong Kong) announced 1,091 IP prefixes owned by 12 ASes, 10 of which are in China on February 28, 2018

(3) Targeted attack: 401 IP prefixes owned by AS 27738 (Ecuador Telecom S.A.) are announced by 743 ASes on January 7, 2018?

Case-study: BGPStream



Conclusion and Discussion

- RPKI has been widely deployed
 - RPKI Objects: 2.7% (AFRINIC) ~ 30.6% (RIPENCC) of the total IPv4 space is covered
 - BGP announcements: 8.1% of BGP announcements are covered
- 2~4 % of (verifiable) BGP announcements are invalid!
 - Too specific announcements
 - Wrong ASNs
- Open Question: how can we identify hijacking attempt with high confidence?

Thanks!

<https://rpki-study.github.io>
(and <https://securePKI.org>)

Datasets, code, figures, and instructions are available!

tjc@cs.rit.edu