RoVista: Measuring and Understanding the Route Origin Validation (ROV) in RPKI

Weitong Li[1], Zhexiao Lin[2], Md. Ishtiaq Ashiq[1], Emile Aben[3], Romain Fontugne[4], Amreesh Phokeer[5], and Tijay Chung[1]

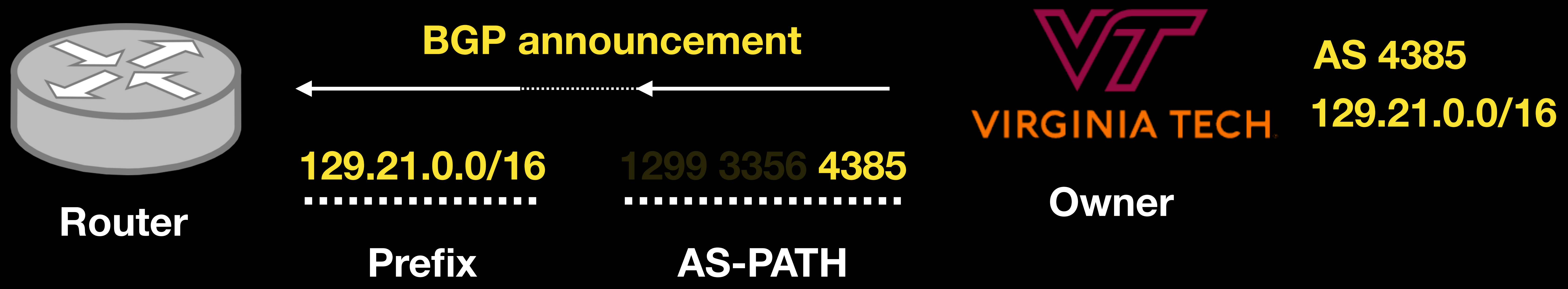
[1]Virginia Tech, [2]UC Berkely, [3]RIPE NCC, [4]IIJ Research Lab, [5]Internet Society

VIRGINIA TECH.

Border Gateway Protocol (BGP)

- Each network resource owner (e.g., VT) announces its IP prefixes to the rest of routers, so that they can learn the path towards VT.

- However, it has NONE of security consideration such as authorization



BGP announcement

AS 4385

129.21.0.0/16

Router

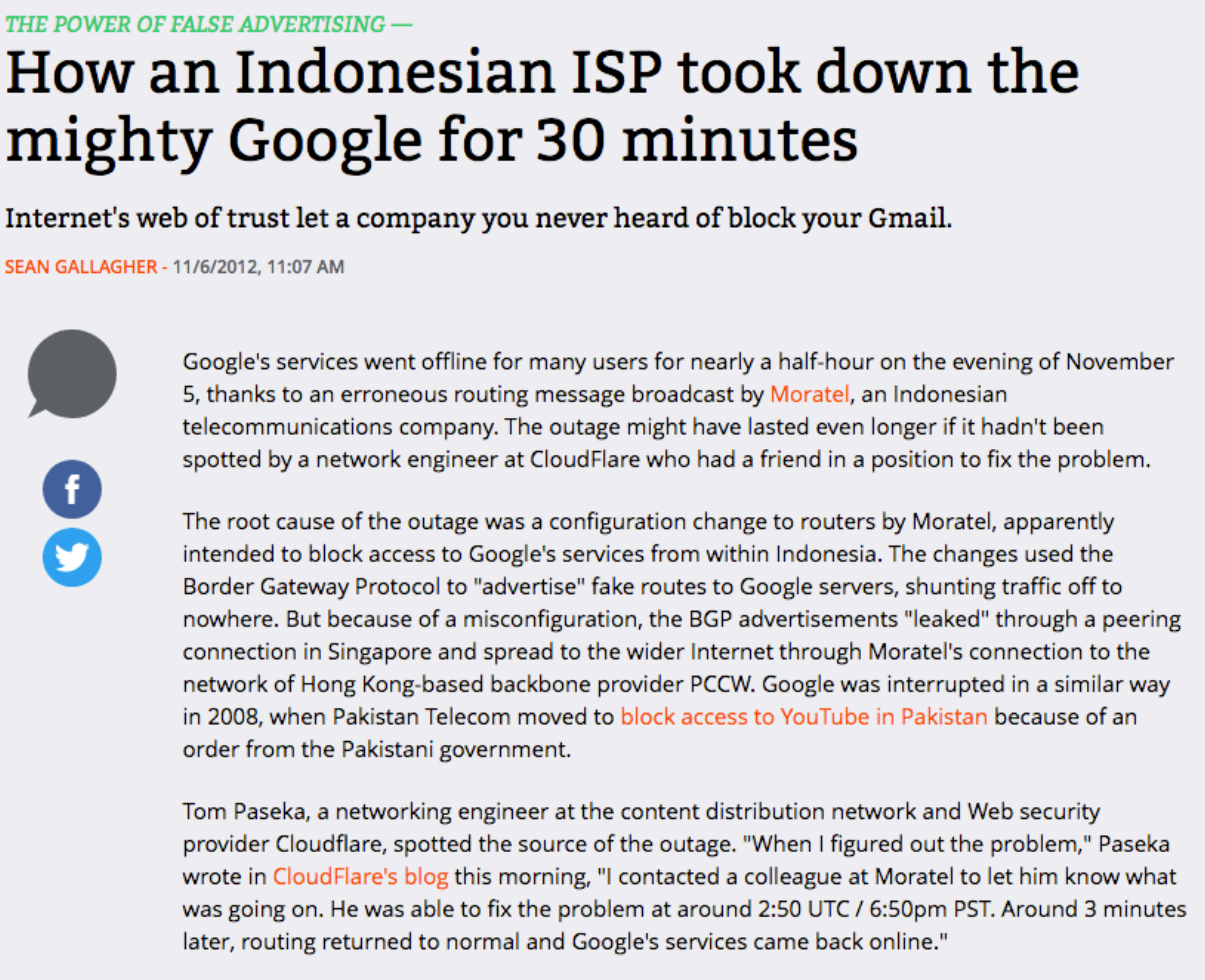
129.21.0.0/16

Prefix

1299 3356 4385

AS-PATH

Owner



THE POWER OF FALSE ADVERTISING —

How an Indonesian ISP took down the mighty Google for 30 minutes

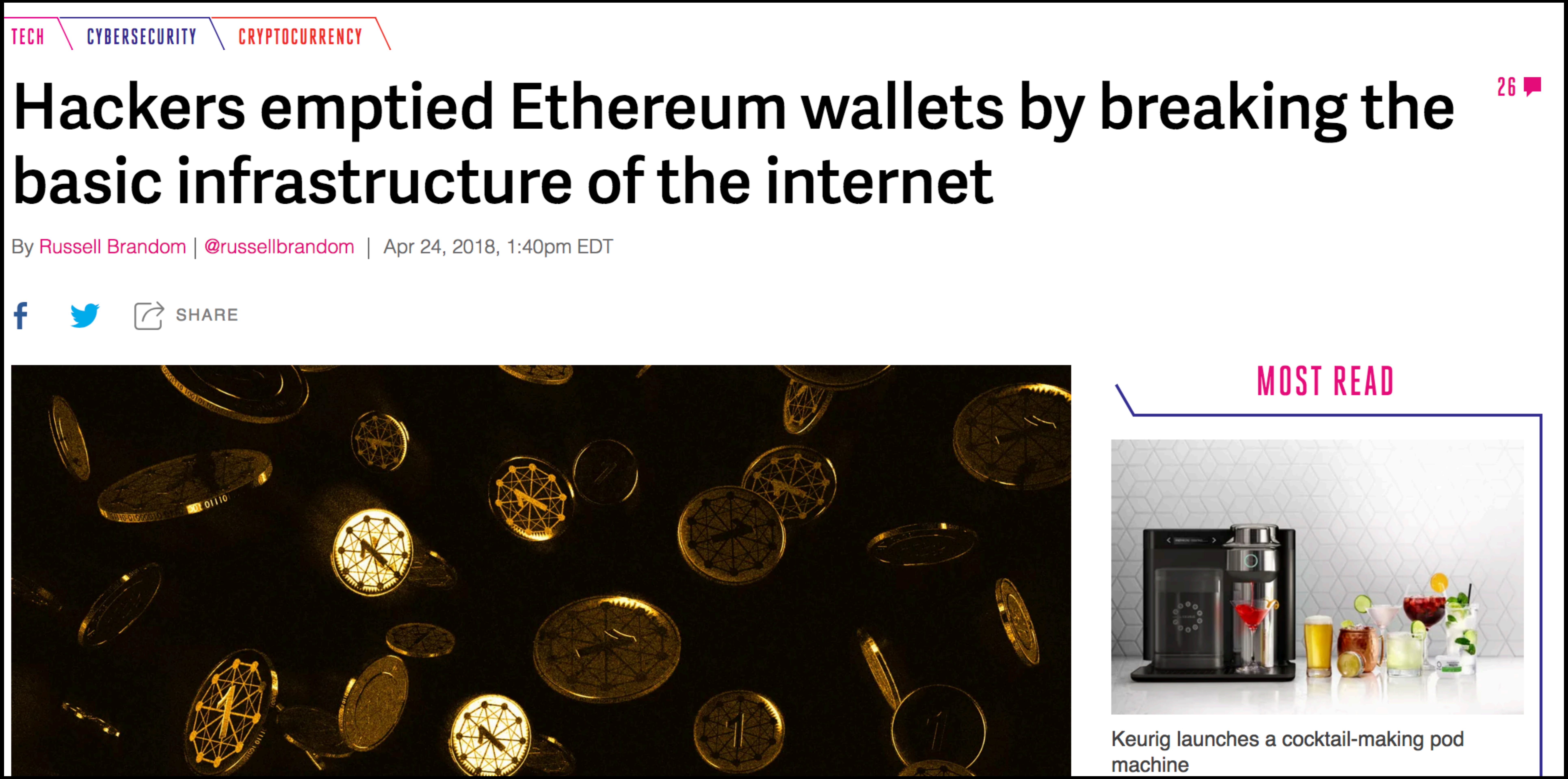
Internet's web of trust let a company you never heard of block your Gmail.

SEAN GALLAGHER - 11/6/2012, 11:07 AM

Google's services went offline for many users for nearly a half-hour on the evening of November 5, thanks to an erroneous routing message broadcast by Moratel, an Indonesian telecommunications company. The outage might have lasted even longer if it hadn't been spotted by a network engineer at CloudFlare who had a friend in a position to fix the problem.

The root cause of the outage was a configuration change to routers by Moratel, apparently intended to block access to Google's services from within Indonesia. The changes used the Border Gateway Protocol to "advertise" fake routes to Google servers, shunting traffic off to nowhere. But because of a misconfiguration, the BGP advertisements "leaked" through a peering connection in Singapore and spread to the wider Internet through Moratel's connection to the network of Hong Kong-based backbone provider PCCW. Google was interrupted in a similar way in 2008, when Pakistan Telecom moved to block access to YouTube in Pakistan because of an order from the Pakistani government.

Tom Paseka, a networking engineer at the content distribution network and Web security provider Cloudflare, spotted the source of the outage. "When I figured out the problem," Paseka wrote in CloudFlare's blog this morning, "I contacted a colleague at Moratel to let him know what was going on. He was able to fix the problem at around 2:50 UTC / 6:50pm PST. Around 3 minutes later, routing returned to normal and Google's services came back online."



Hackers emptied Ethereum wallets by breaking the basic infrastructure of the internet

By Russell Brandom | @russellbrandom | Apr 24, 2018, 1:40pm EDT

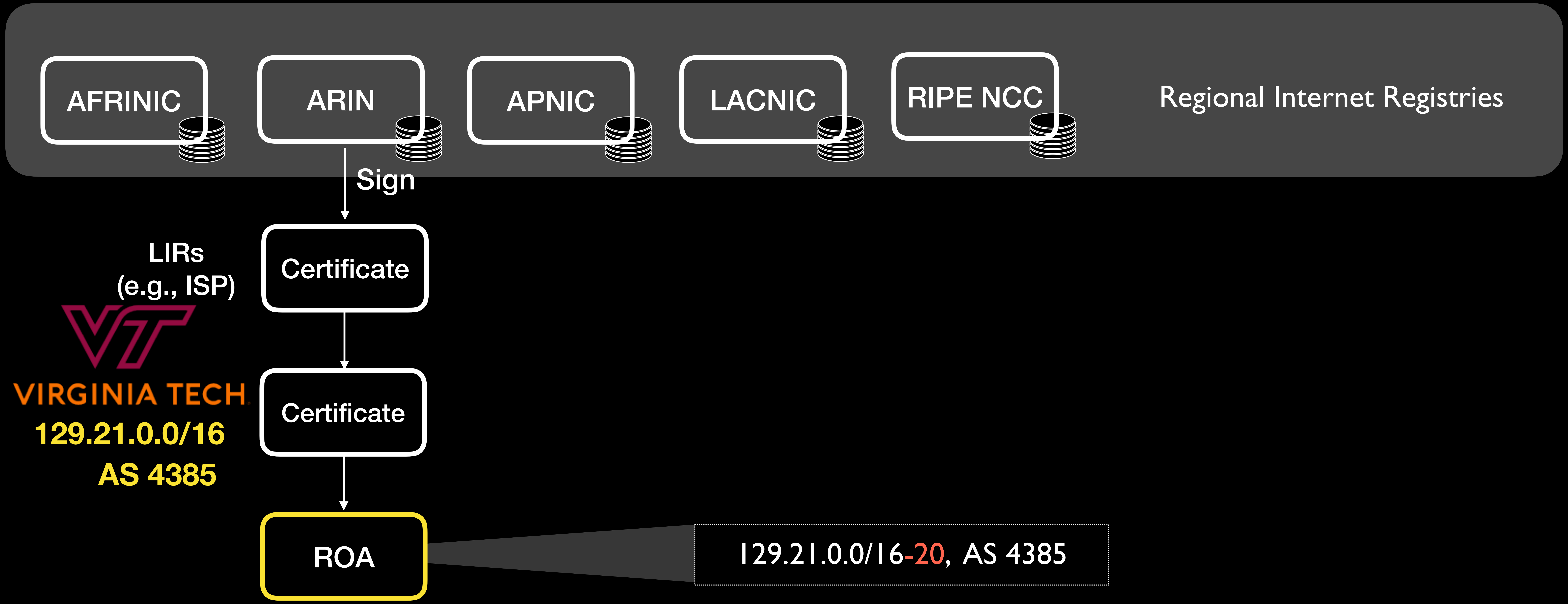
Keurig launches a cocktail-making pod machine

Resource PKI
(Public Key Infrastructure)

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

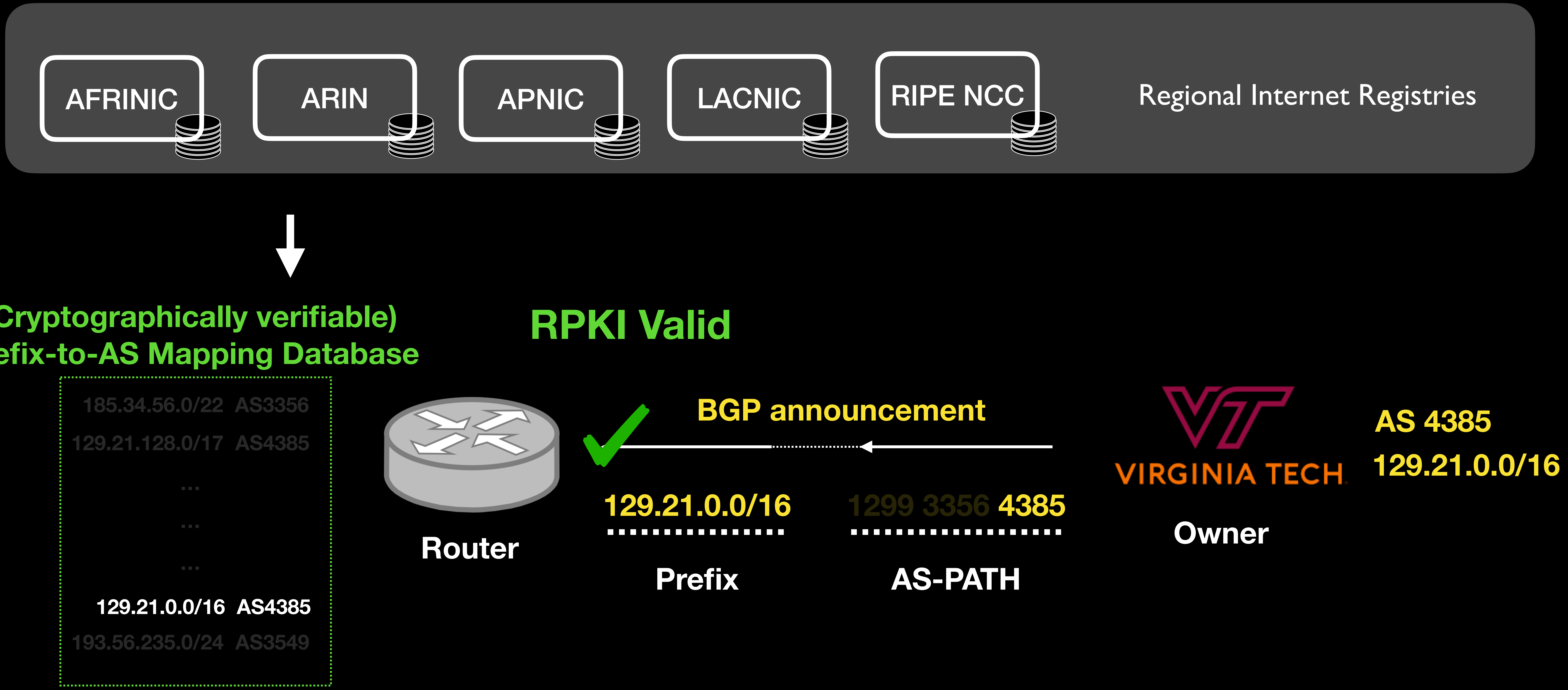
- Currently more than 40% of IP spaces are verifiable with RPKI

RPKI Structure: ROA



Route Origin Authorization

RPKI Structure: ROA



AFRINIC

ARIN

APNIC

LACNIC

RIPE NCC

Regional Internet Registries

(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

RPKI Valid

Router

BGP announcement

129.21.0.0/16

Prefix

1299 3356 4385

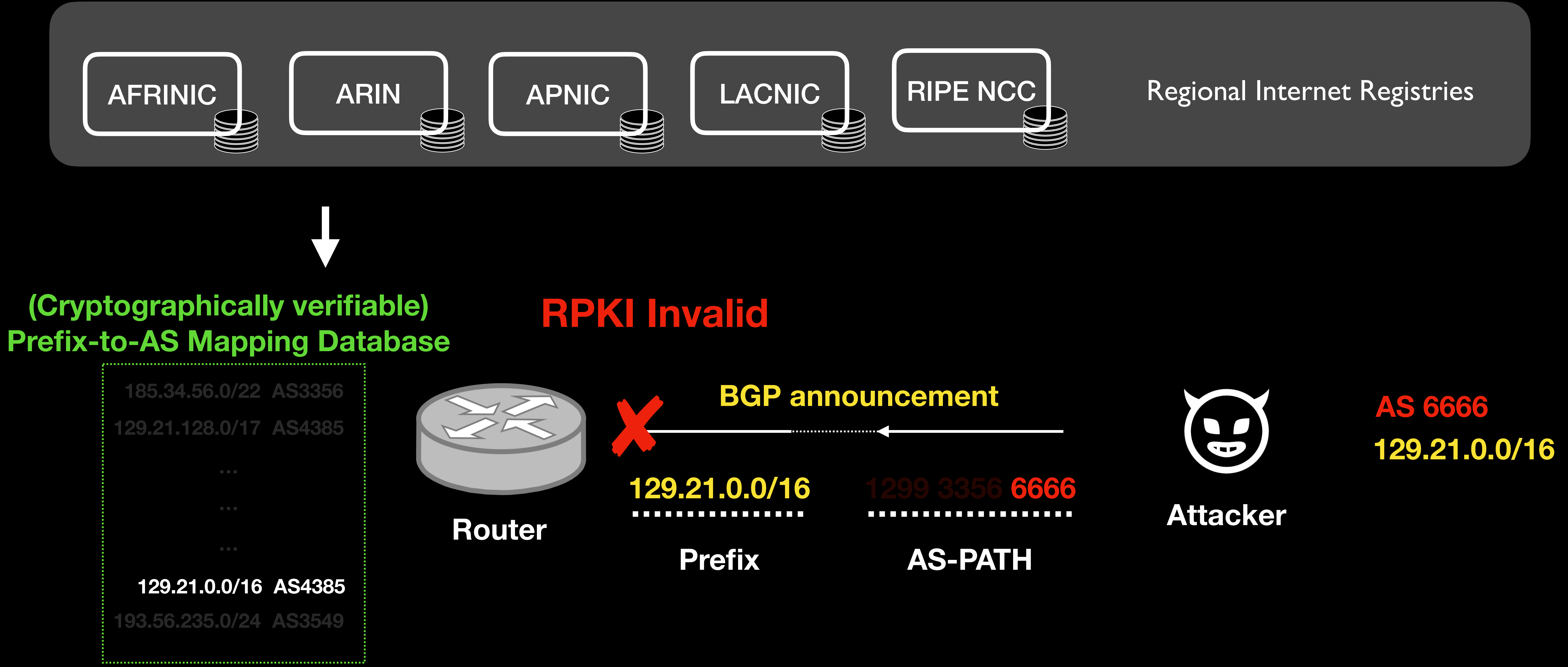
AS-PATH

VIRGINIA TECH

Owner

AS 4385
129.21.0.0/16

RPKI Structure: ROV



AFRINIC

ARIN

APNIC

LACNIC

RIPE NCC

Regional Internet Registries

(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

RPKI Invalid

Router

BGP announcement

129.21.0.0/16

1299 3356 6666

Prefix

AS-PATH

Attacker

AS 6666
129.21.0.0/16

Two questions

- How network operators use RPKI to "claim" their IP addresses? [IMC'19]
- How network operators also use RPKI to "filter" invalid BGP announcements?

Two questions

Answering this question is “relatively” straightforward

- How network operators use RPKI to “claim” their IP addresses? [IMC’19]
- How network operators also use RPKI to “filter” invalid BGP announcements?

Two questions

- How network operators use RPKI to "claim" their IP addresses? [IMC'19]
- How network operators also use RPKI to "filter" invalid BGP announcements?

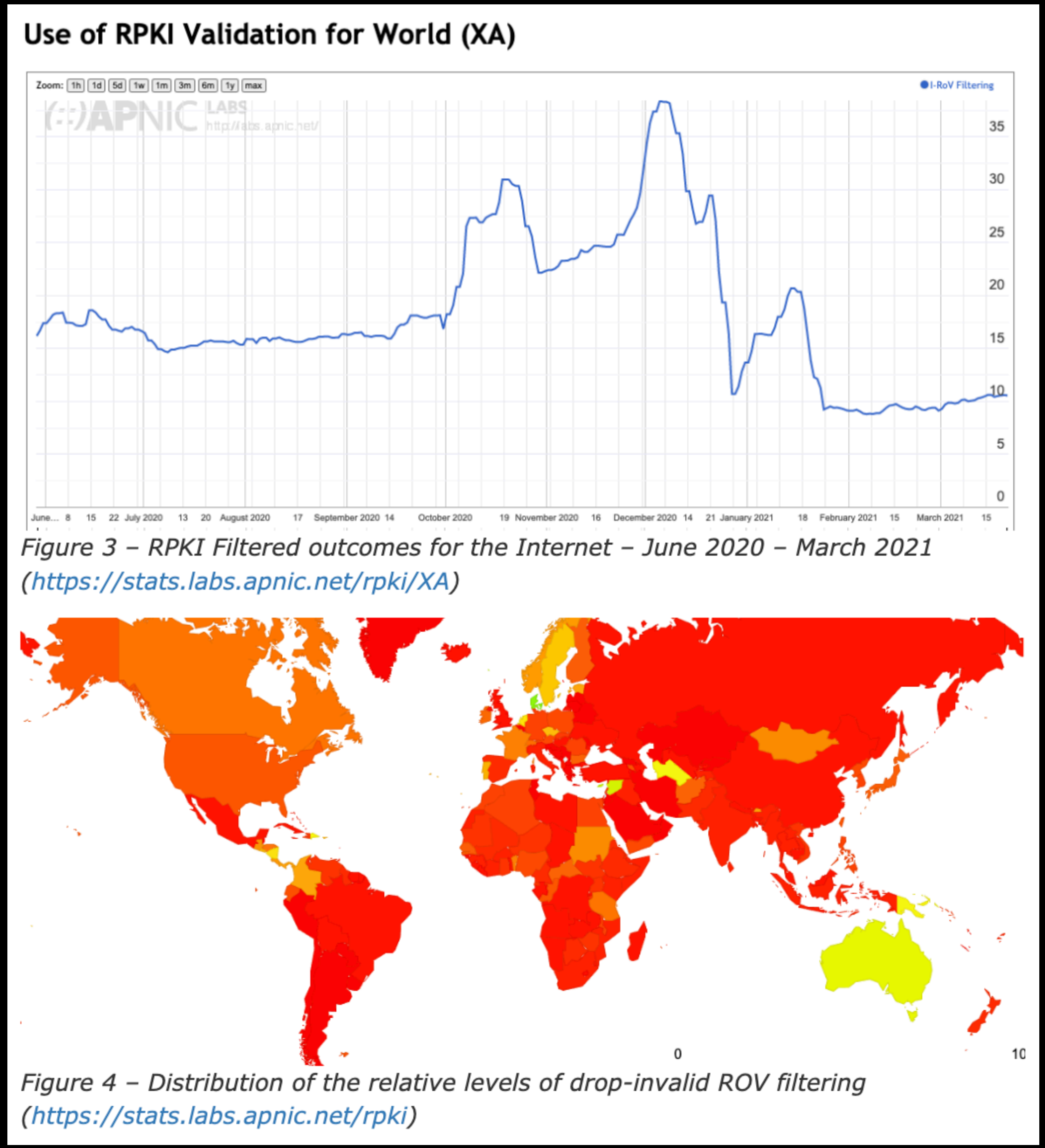
Would it be easy..?

Previous approaches

- Control-plane based methods: like CCR'18
- Data-plane based methods: like DSN'18, TMA'21

Previous approaches

APNIC



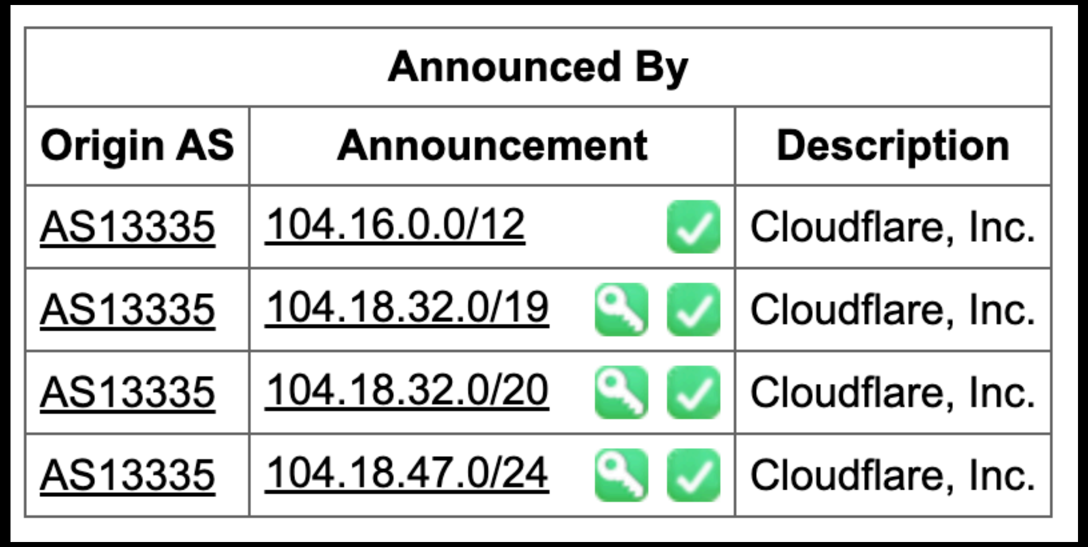
Use of RPKI Validation for World (XA)

Zoom: 1h 1d 5d 1w 1m 3m 6m 1y max
I-RoV Filtering
APNIC LABS
http://labs.apnic.net/
35
30
25
20
15
10
5
0
June... 8 15 22 July 2020 13 20 August 2020 17 September 2020 14 October 2020 19 November 2020 16 December 2020 14 21 January 2021 18 February 2021 15 March 2021 15

Figure 3 – RPKI Filtered outcomes for the Internet – June 2020 – March 2021 (https://stats.labs.apnic.net/rpki/XA)

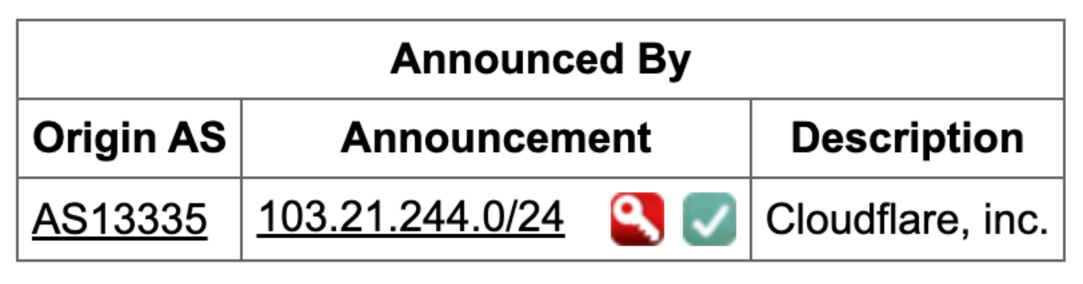
Figure 4 – Distribution of the relative levels of drop-invalid ROV filtering (https://stats.labs.apnic.net/rpki)

valid.rpki.cloudflare.com



Announced By		
Origin AS	Announcement	Description
AS13335	104.16.0.0/12 ✓	Cloudflare, Inc.
AS13335	104.18.32.0/19 🔑 ✓	Cloudflare, Inc.
AS13335	104.18.32.0/20 🔑 ✓	Cloudflare, Inc.
AS13335	104.18.47.0/24 🔑 ✓	Cloudflare, Inc.

invalid.rpki.cloudflare.com



Announced By		
Origin AS	Announcement	Description
AS13335	103.21.244.0/24 🔑 ✓	Cloudflare, inc.

Challenges

- C1: We need more invalid prefixes to make the measurement robust
- C2: We need more vantage points to cover more ASes

RoVista:
Measuring and understanding the ROV status

- C1: We need more invalid prefixes to make the measurement robust

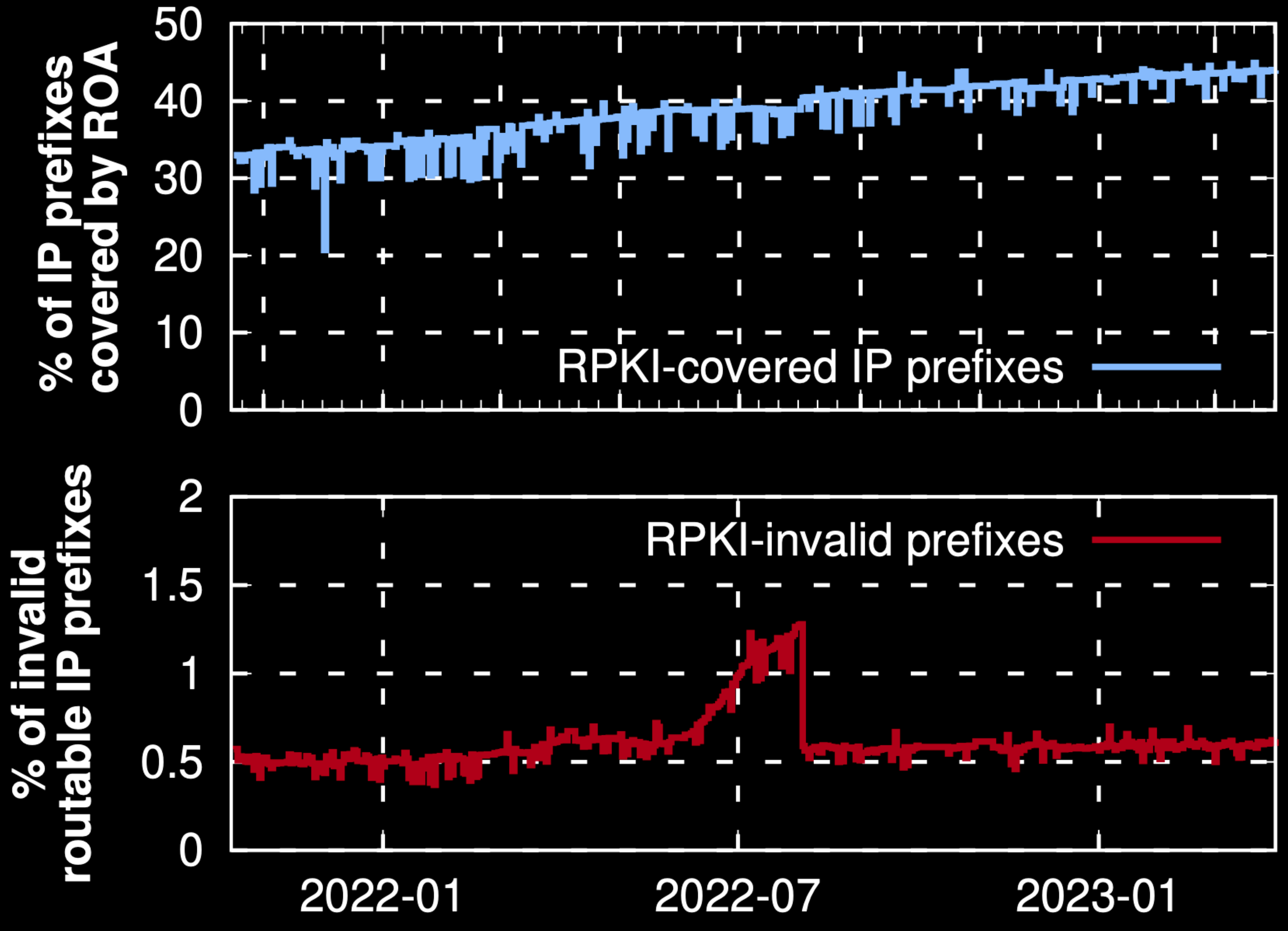
  Use in-the-wild invalid prefixes

- C2: We need more vantage points to cover more ASes

  Use IP-ID side channel

“In-the-wild” invalid prefix

- 0.7% of the RPKI-covered prefixes are invalid



RoVista:
Measuring and understanding the ROV status

- C1: We need more invalid prefixes to make the measurement robust

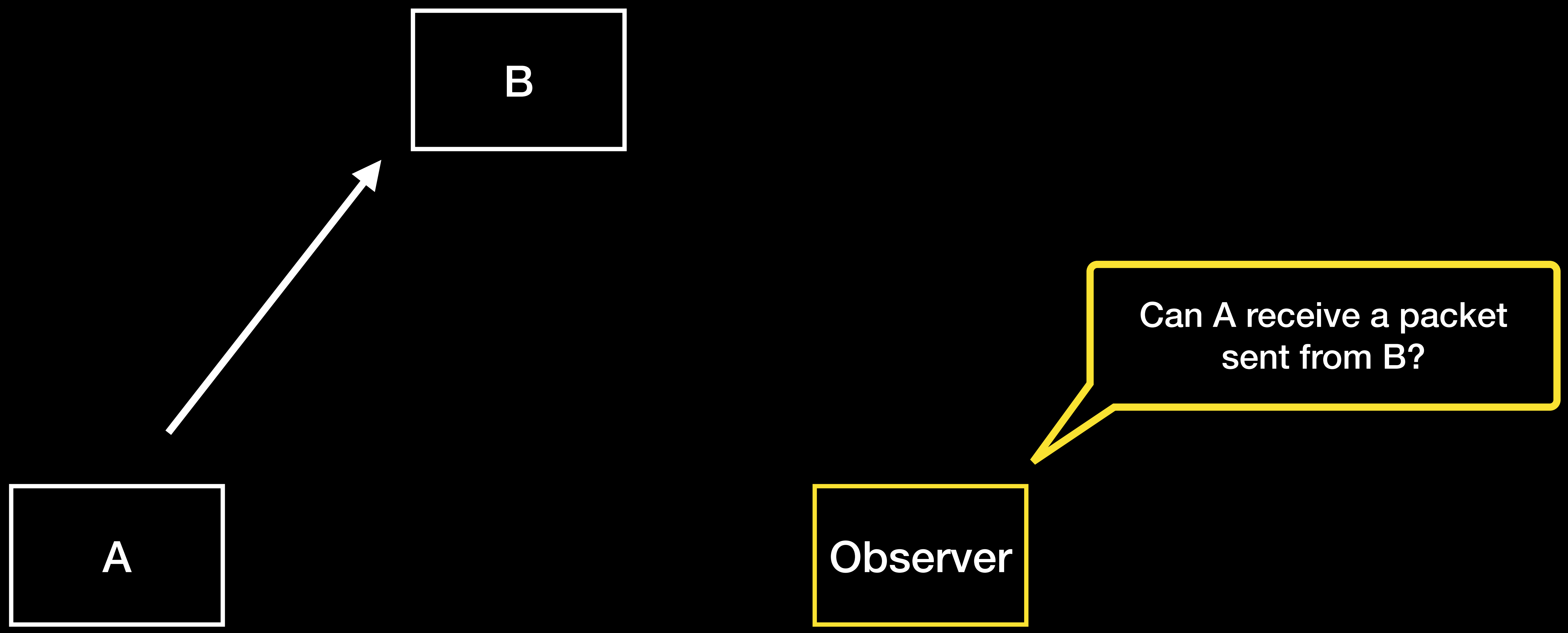
  Use in-the-wild invalid prefixes

- C2: We need more vantage points to cover more ASes

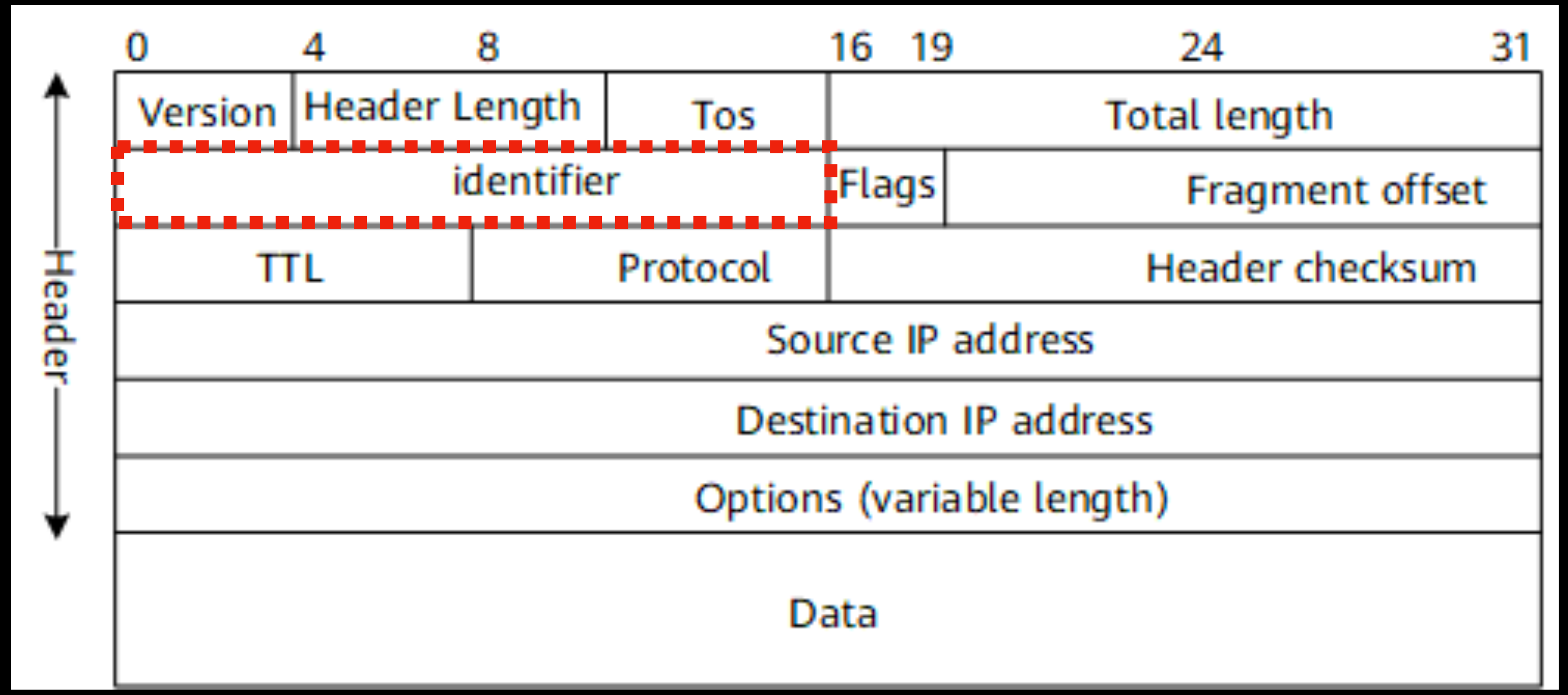
  Use IP-ID side channel

IP-ID side channel

- IP-ID Side-channel technique, which allows to infer the connectivity between two hosts (e.g., whether one host can receive a packet from other host)

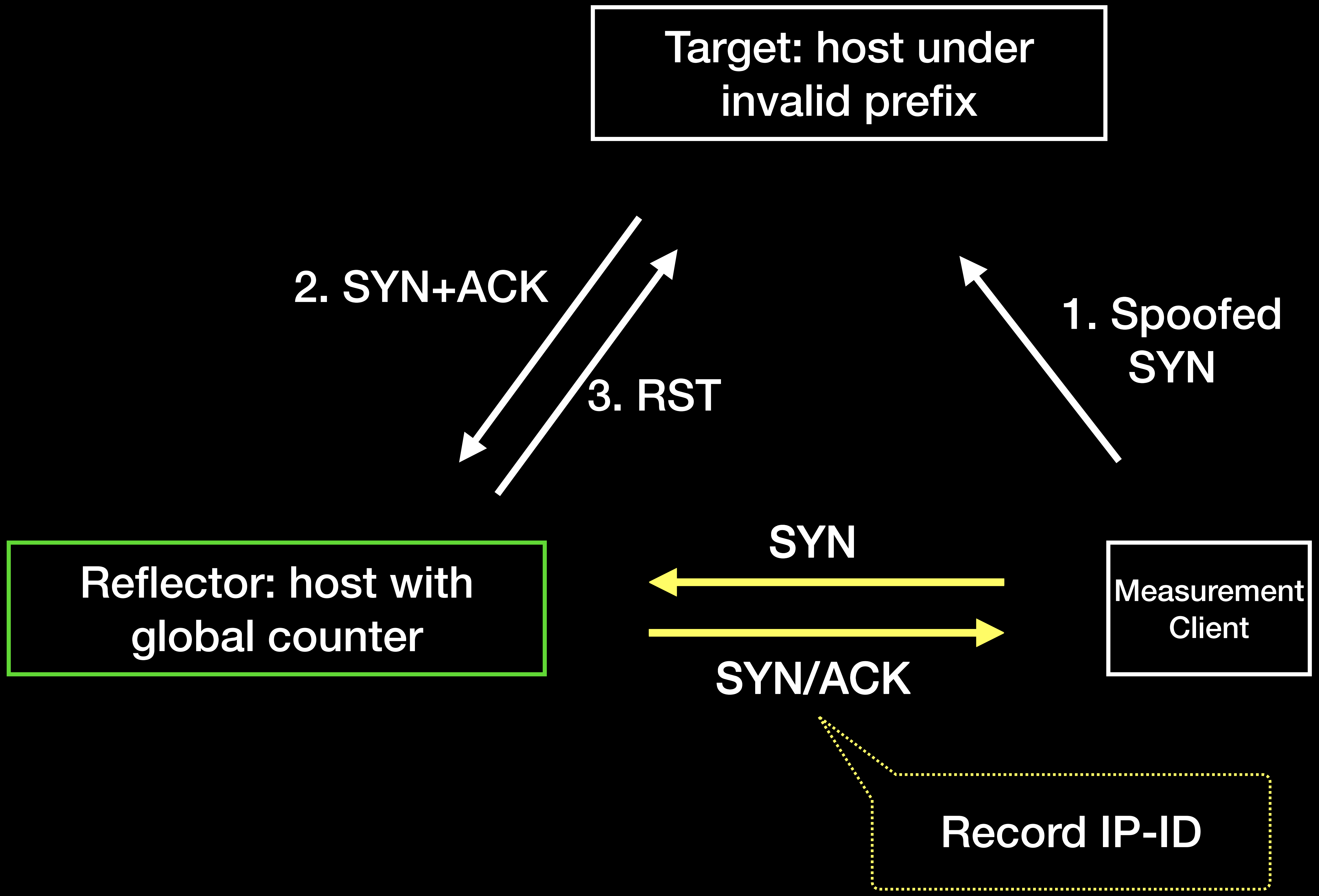


IP-ID

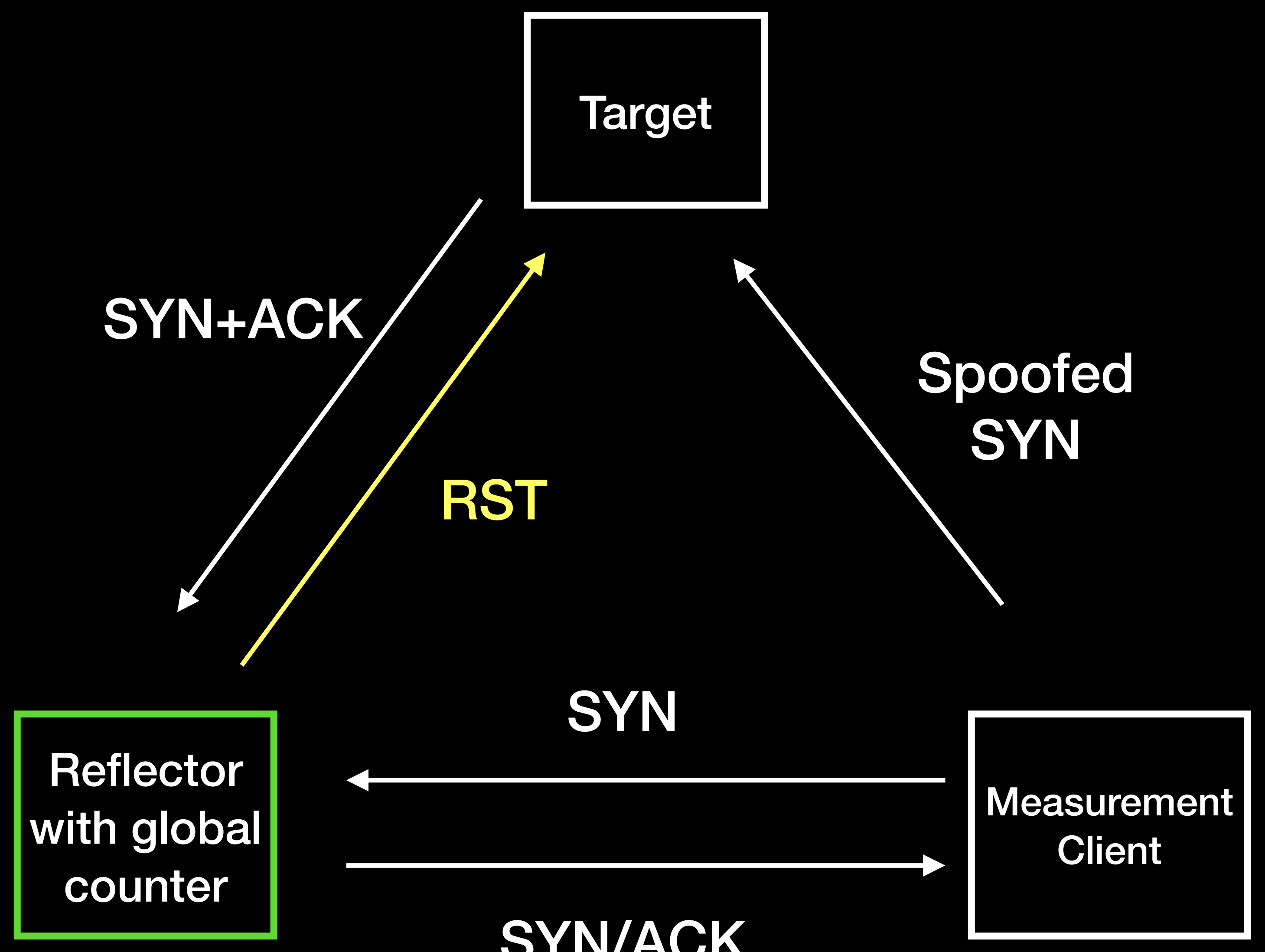


- IP ID was first introduced by RFC 791
    - originally designed to assist packet fragmentation and reassembly by assigning an unique identifier for each packet
- How to assign IPID?
    - Global counter
        - increments the IP-ID by 1 unit whenever it sends a new packet regardless of the destination IP address
    - Local counter
        - manages a unique counter for each destination IP address
    - Random counter
    - …

IP-ID Side-Channel Basic Idea

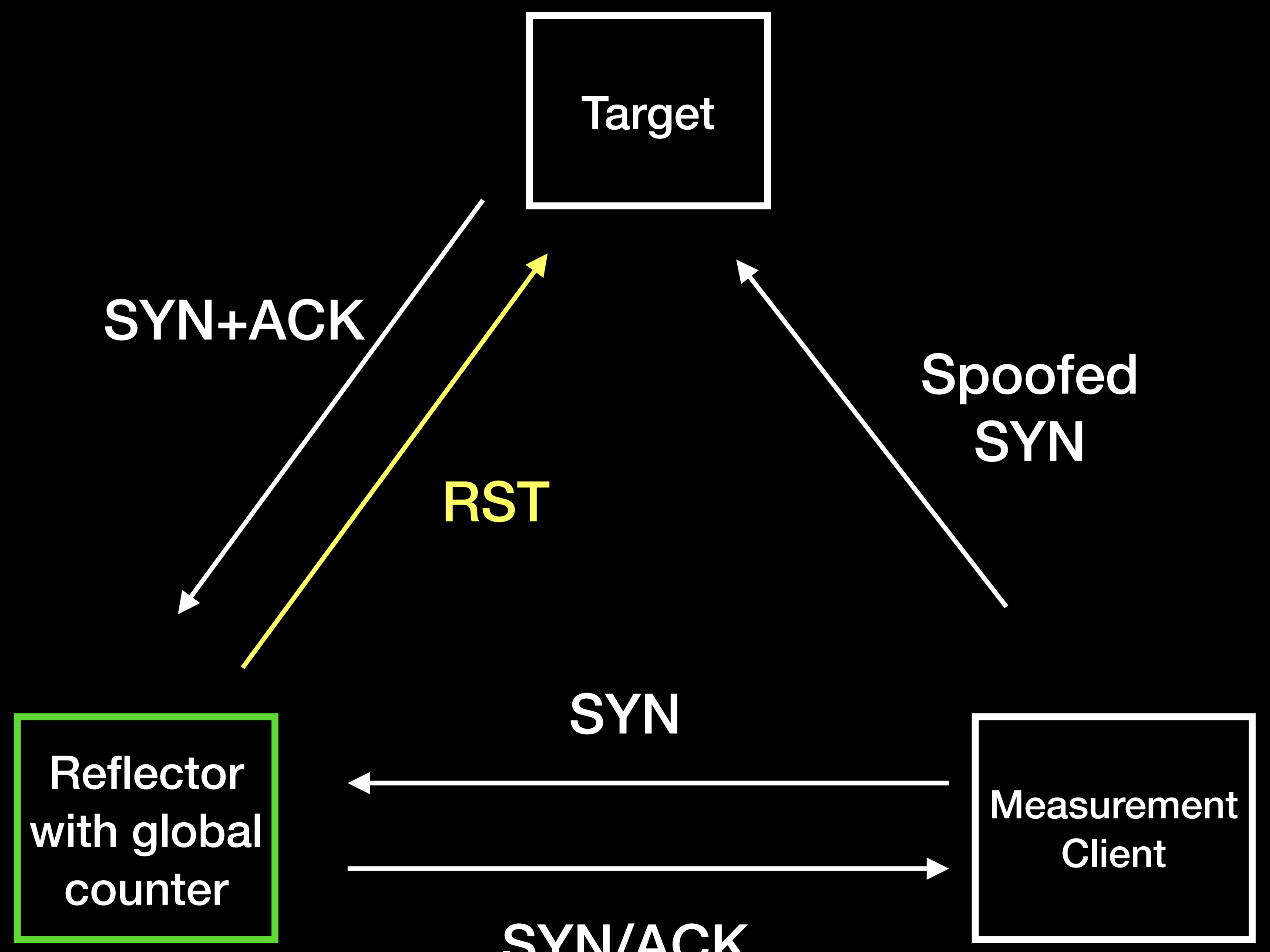


IP-ID Side-Channel Possible Scenarios

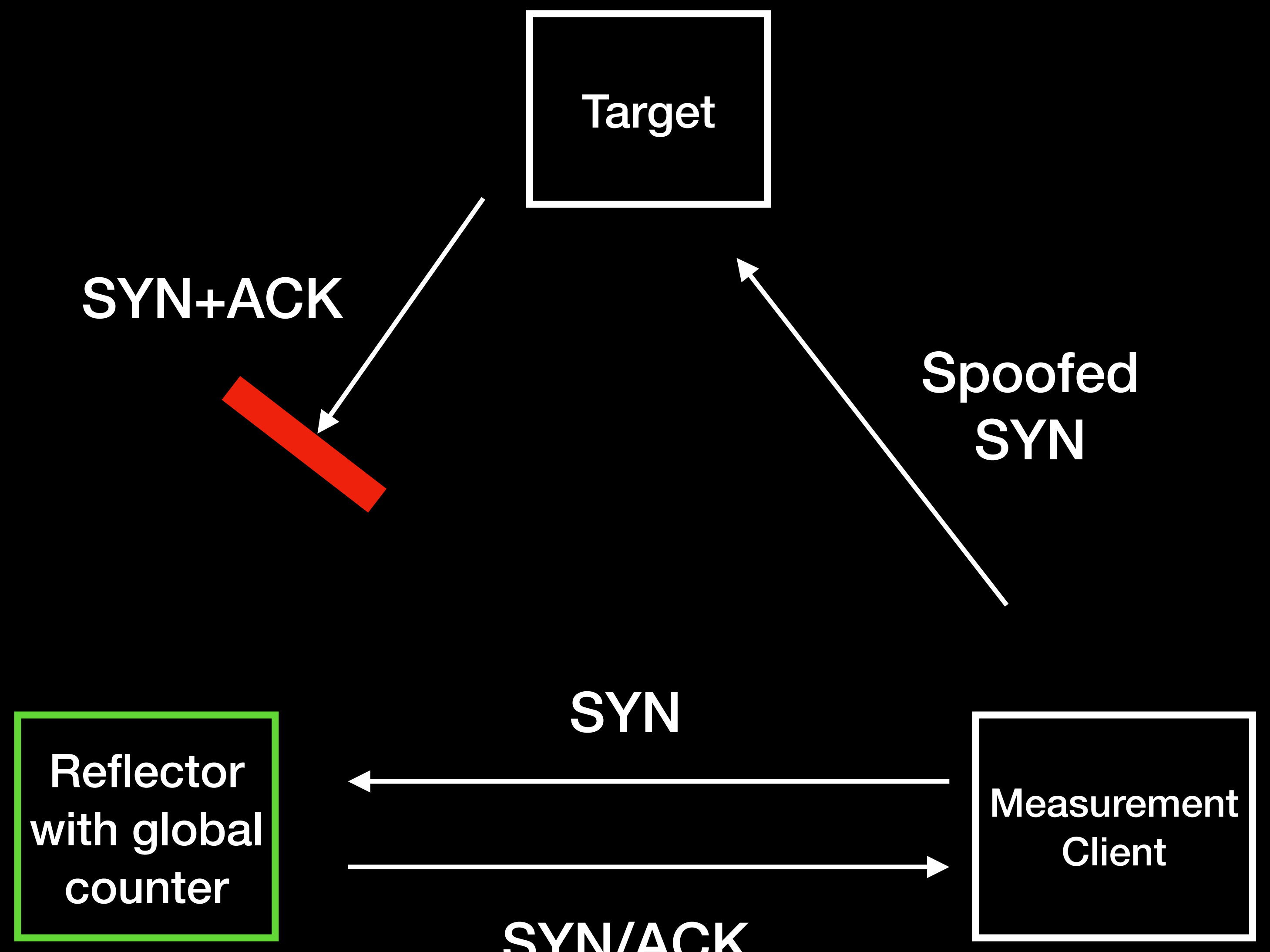


No filtering

IP-ID Side-Channel

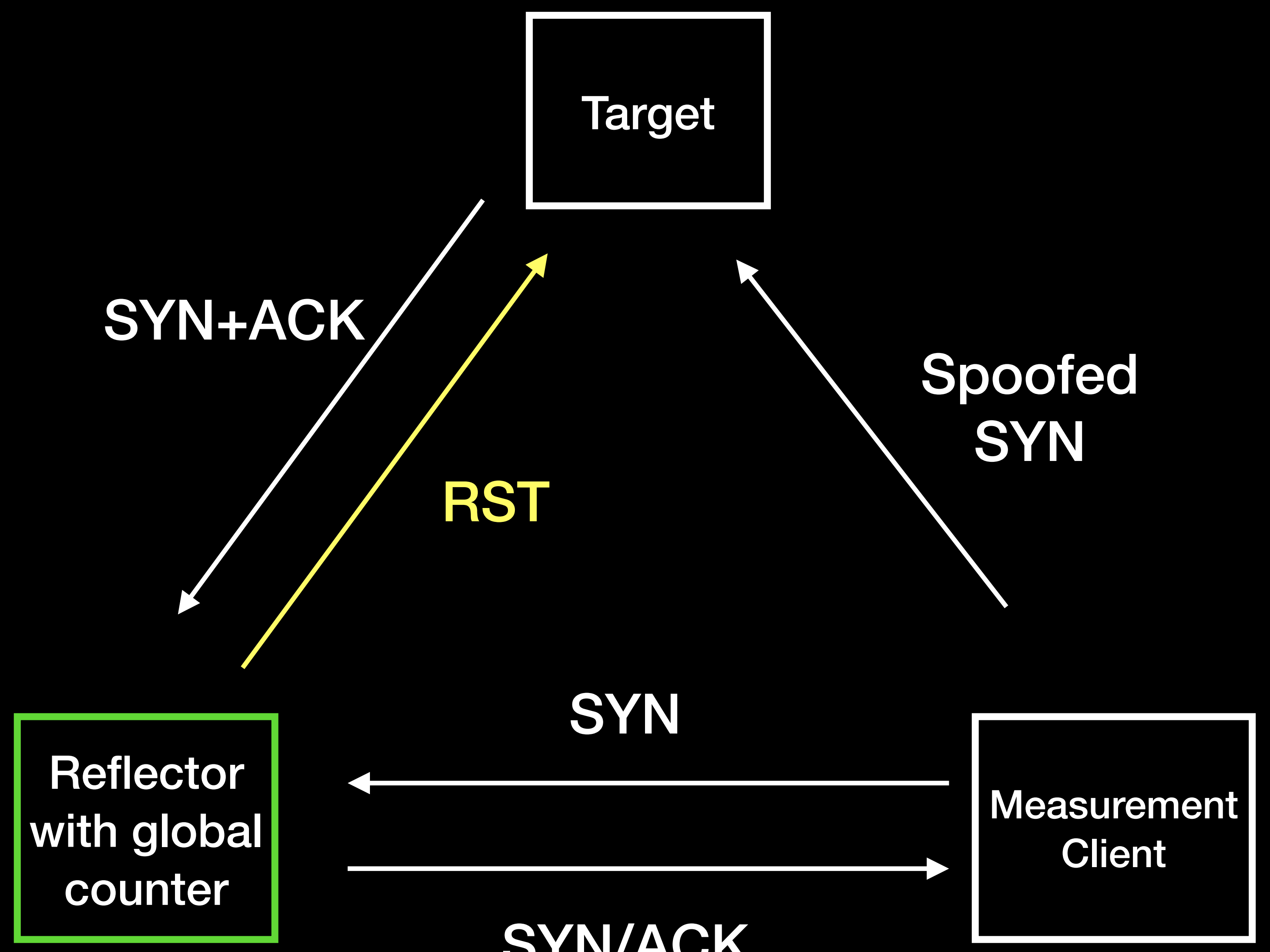


No filtering

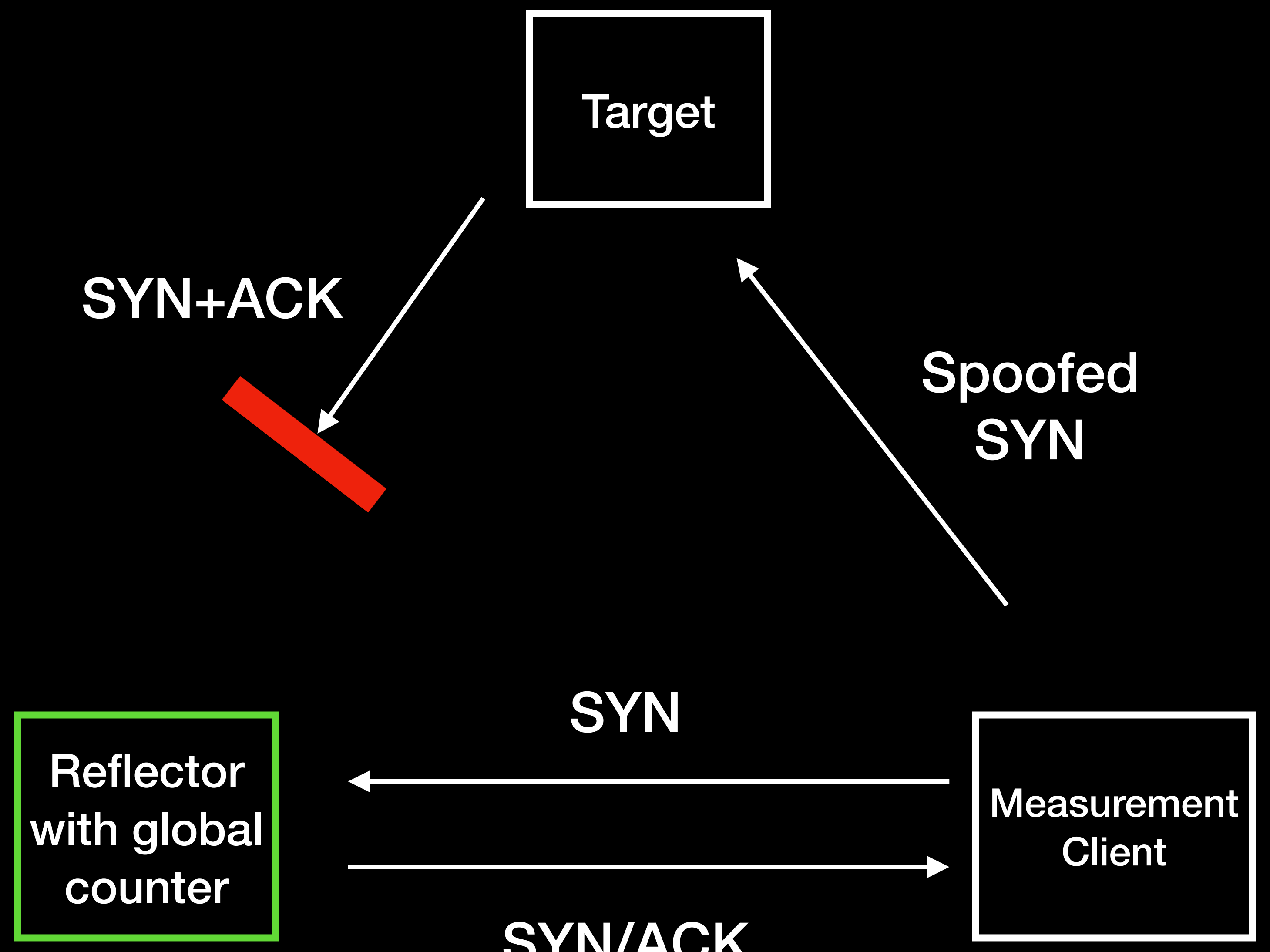


Inbound filtering

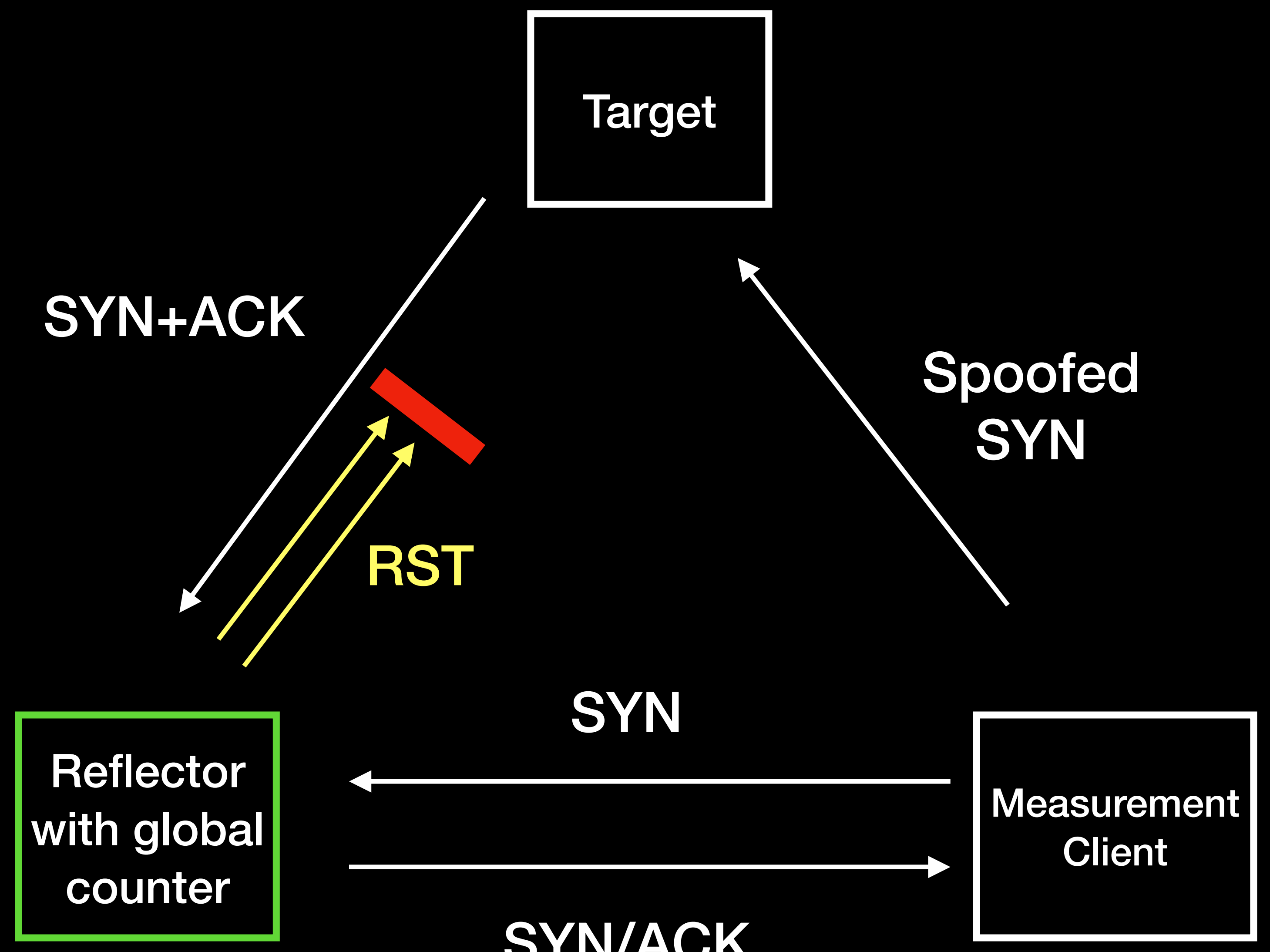
IP-ID Side-Channel



No filtering

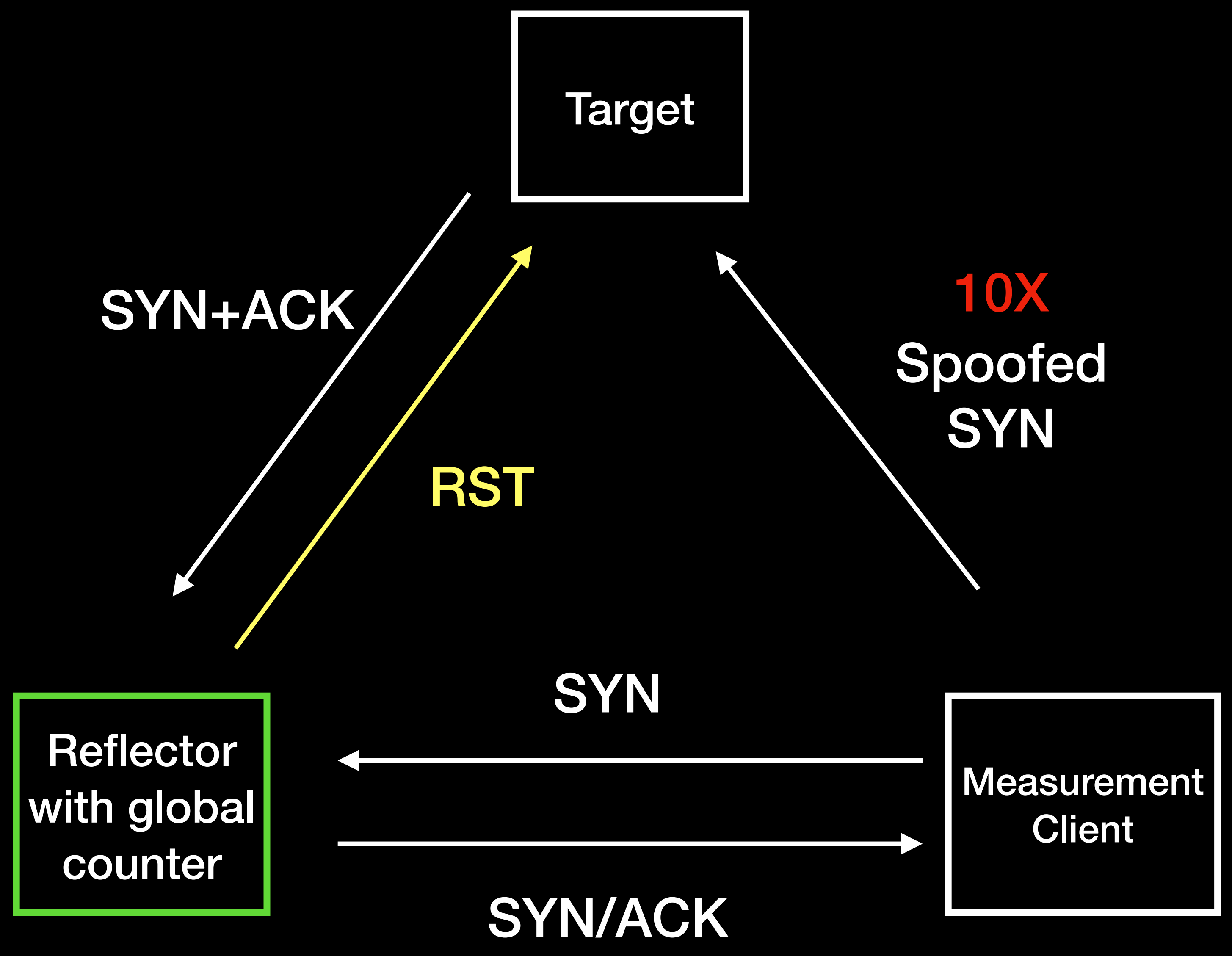


Inbound filtering

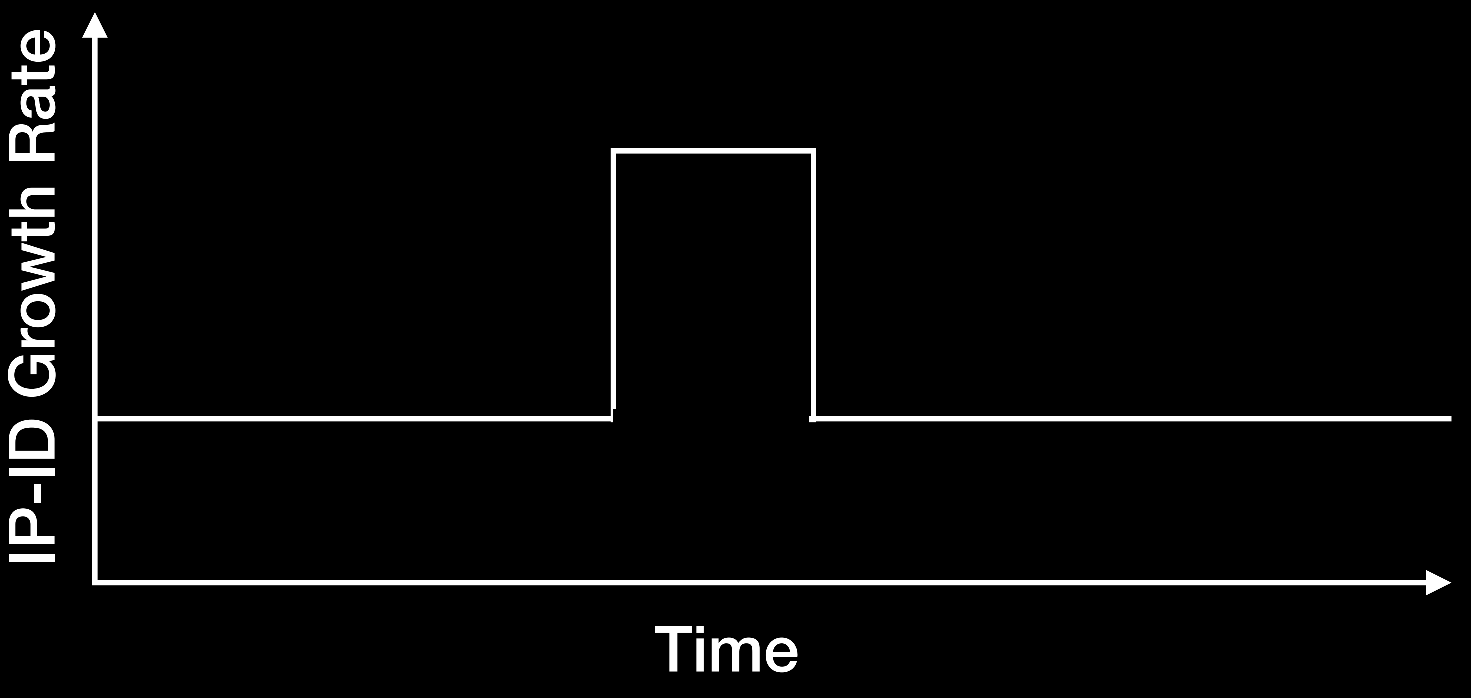


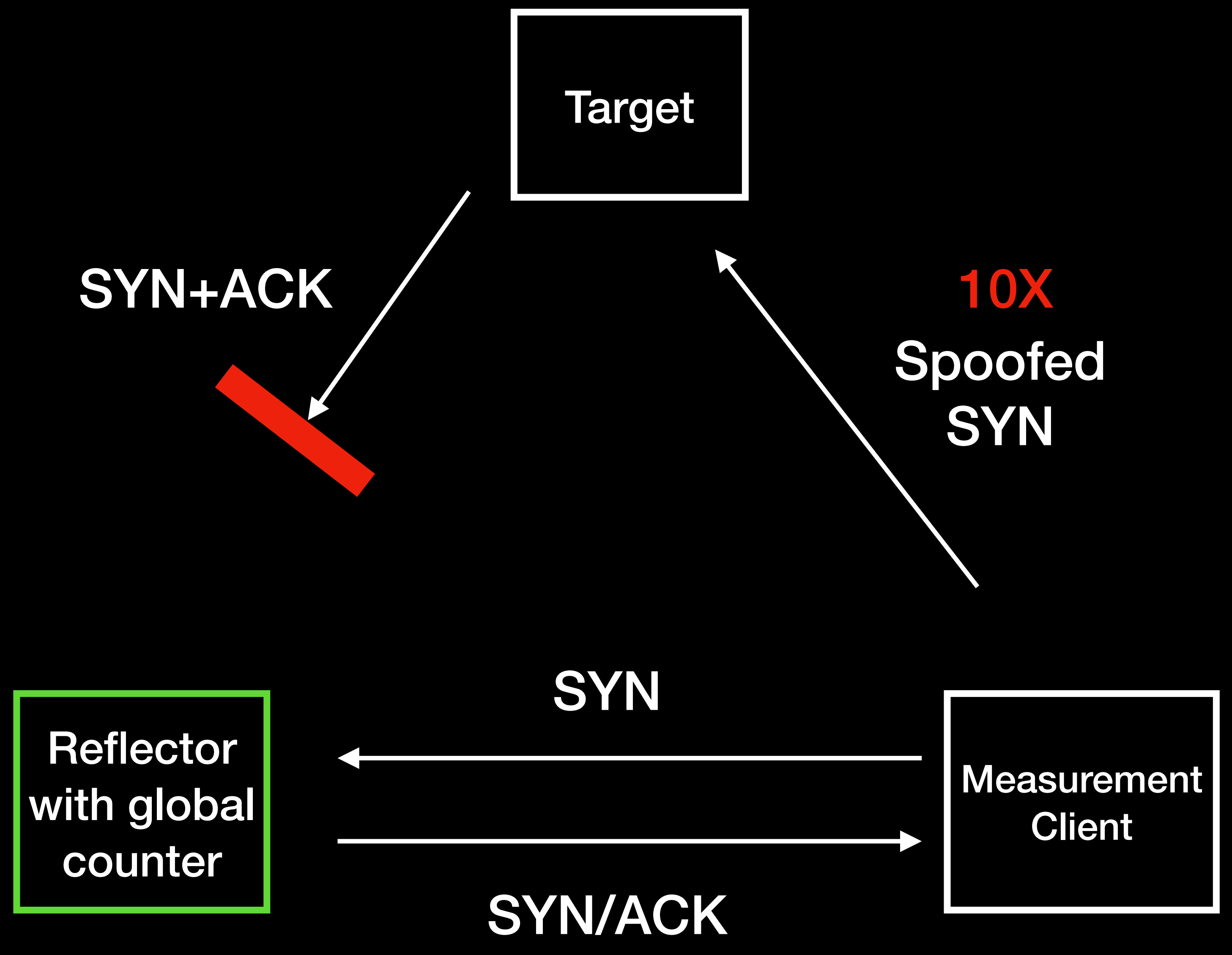
Outbound filtering

IP-ID Side-Channel

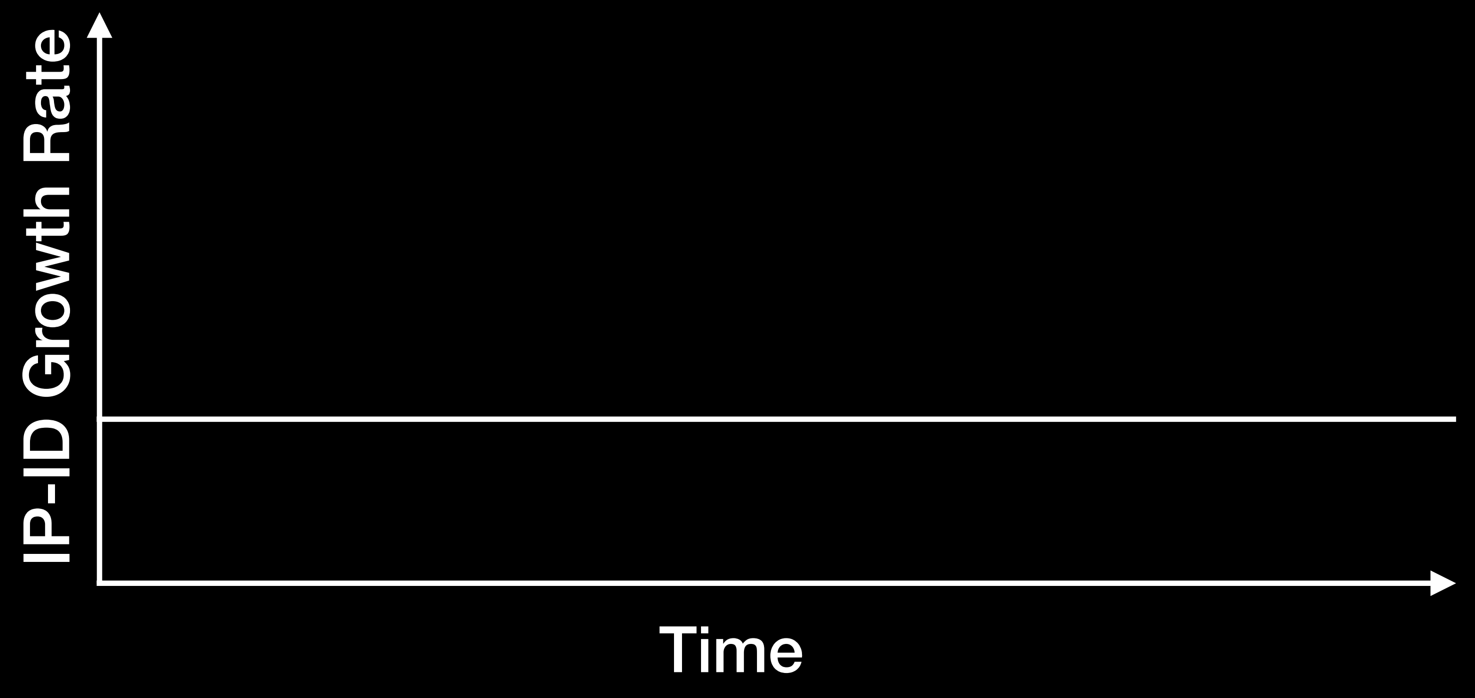


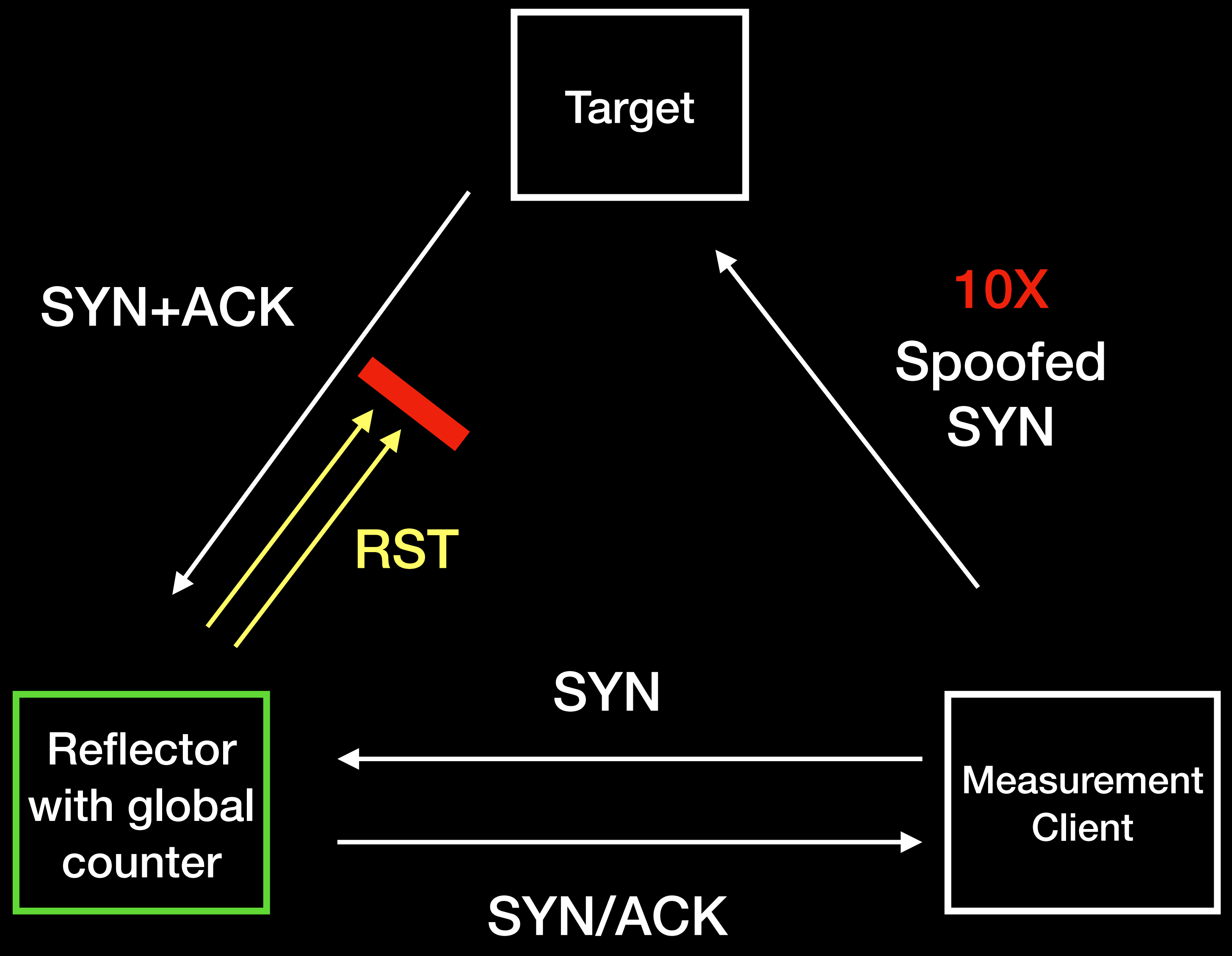
No filtering



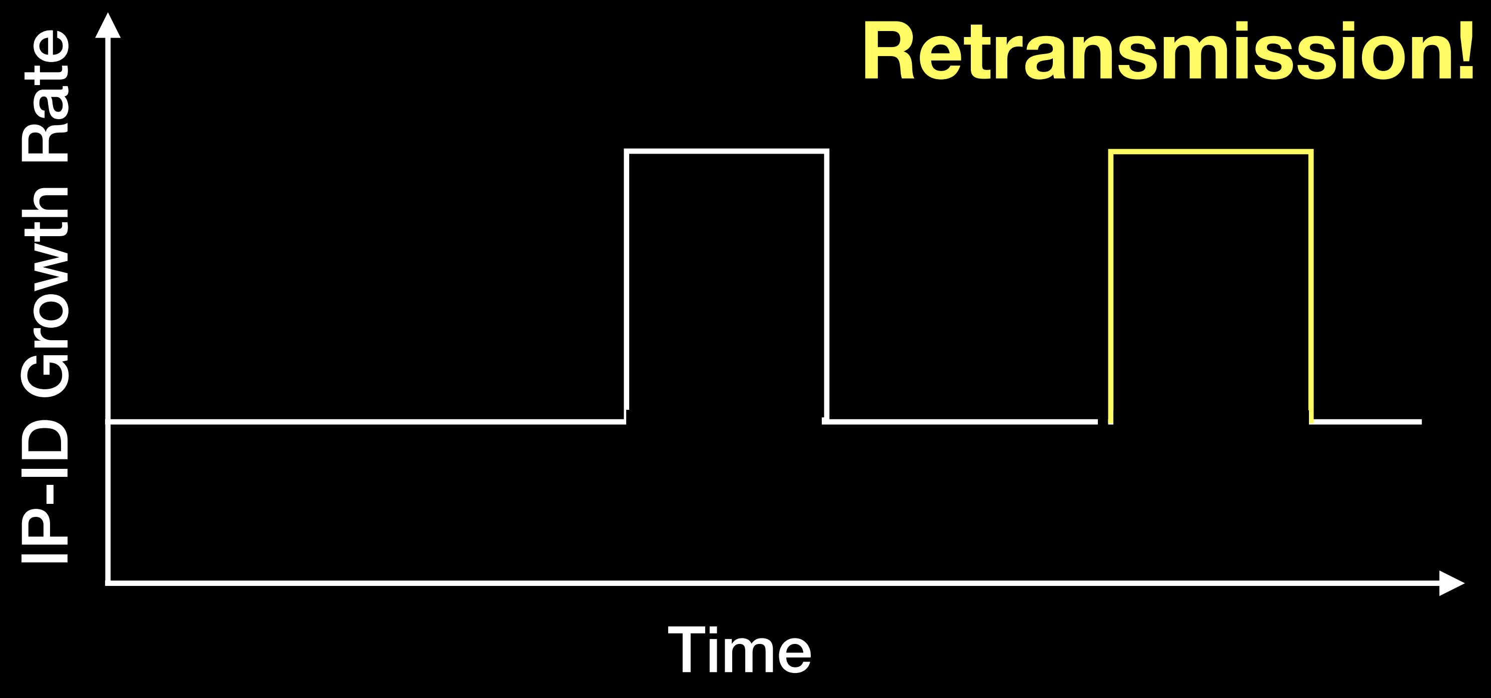


Inbound filtering





Outbound filtering



RoVista:
Measuring and understanding the ROV status

- C1: We need more invalid prefixes to make the measurement robust

  Use in-the-wild invalid prefixes

- C2: We need more vantage points to cover more ASes

  Use IP-ID side channel

ROV Scores

- In order to infer the ROV status. we calculate the percentage of target that all reflectors under the same AS cannot reach to, which will be the ROV Score of that AS

- But, high ROV score does not mean "ROV deployment"

Experiments

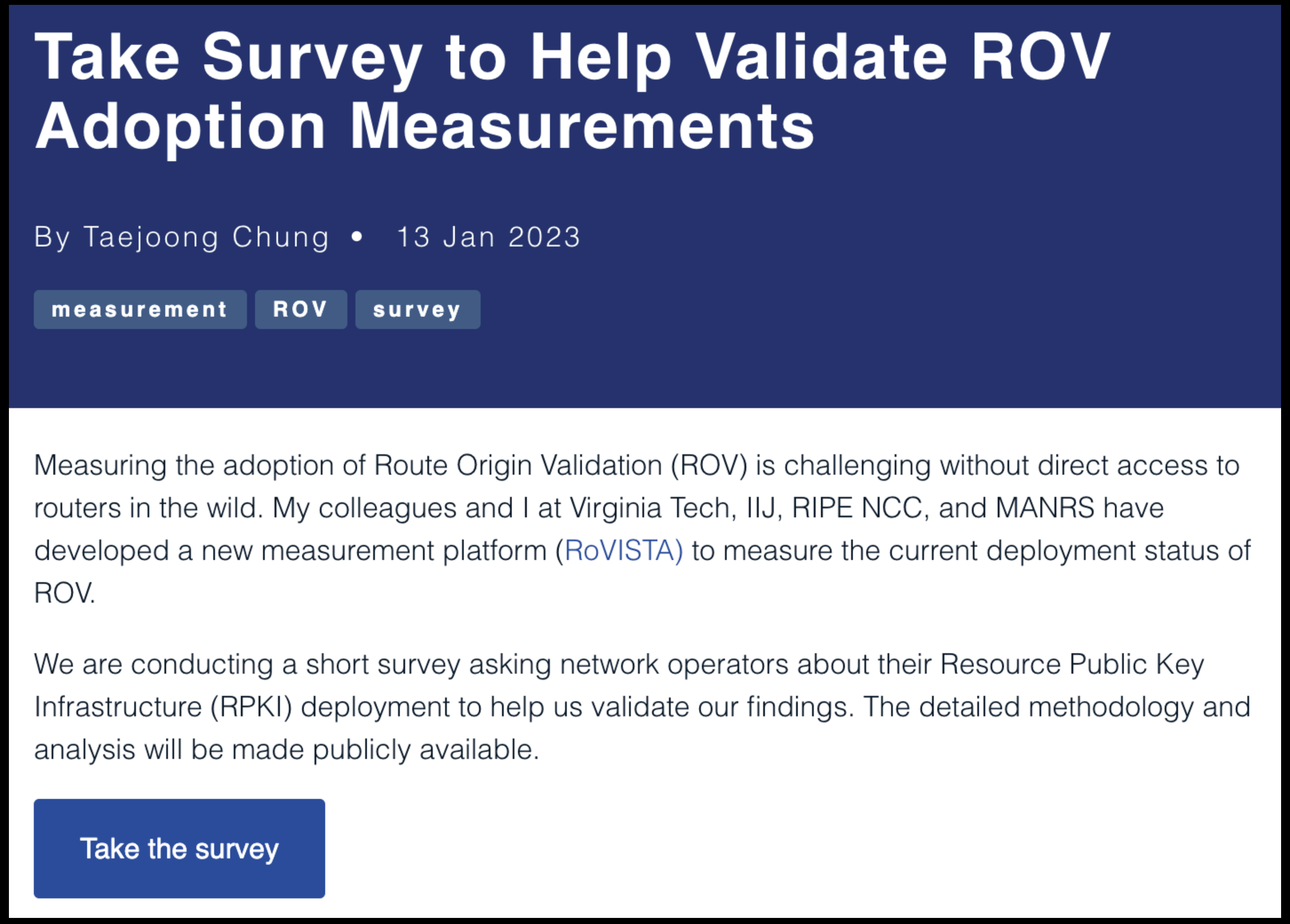
Measurement Period	12/24/2021 ~ now
# of ASes	28K
# of countries	231

We have released our results at https://rovista.netsecurelab.org/ with APIs

Cross-validation
Comparison with the official sources

Personal communication: 10 ASes

Survey: 31 ASes



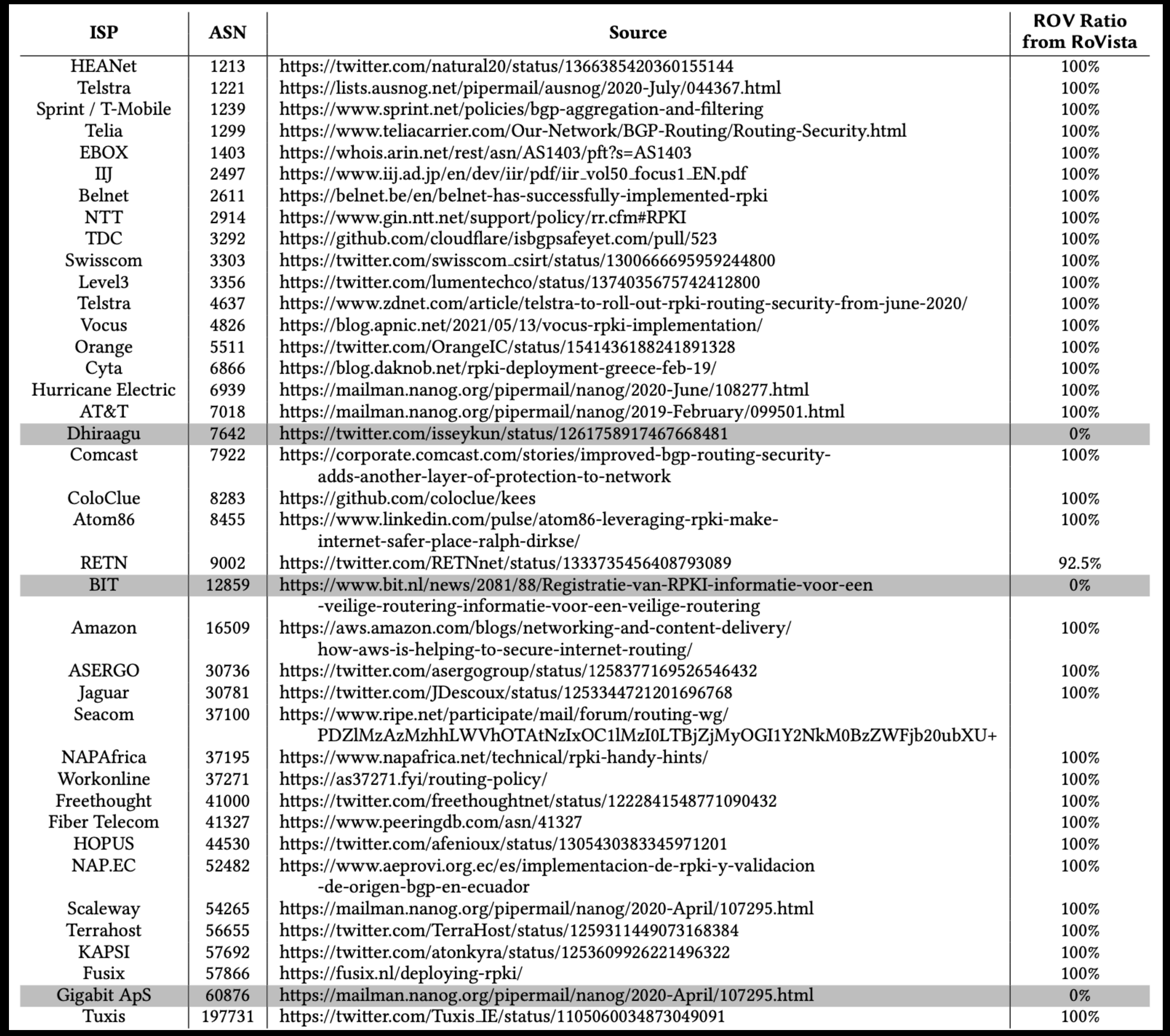
Take Survey to Help Validate ROV Adoption Measurements

By Taejoong Chung • 13 Jan 2023

Measuring the adoption of Route Origin Validation (ROV) is challenging without direct access to routers in the wild. My colleagues and I at Virginia Tech, IIJ, RIPE NCC, and MANRS have developed a new measurement platform (RoVISTA) to measure the current deployment status of ROV.

We are conducting a short survey asking network operators about their Resource Public Key Infrastructure (RPKI) deployment to help us validate our findings. The detailed methodology and analysis will be made publicly available.

Post : 40 ASes

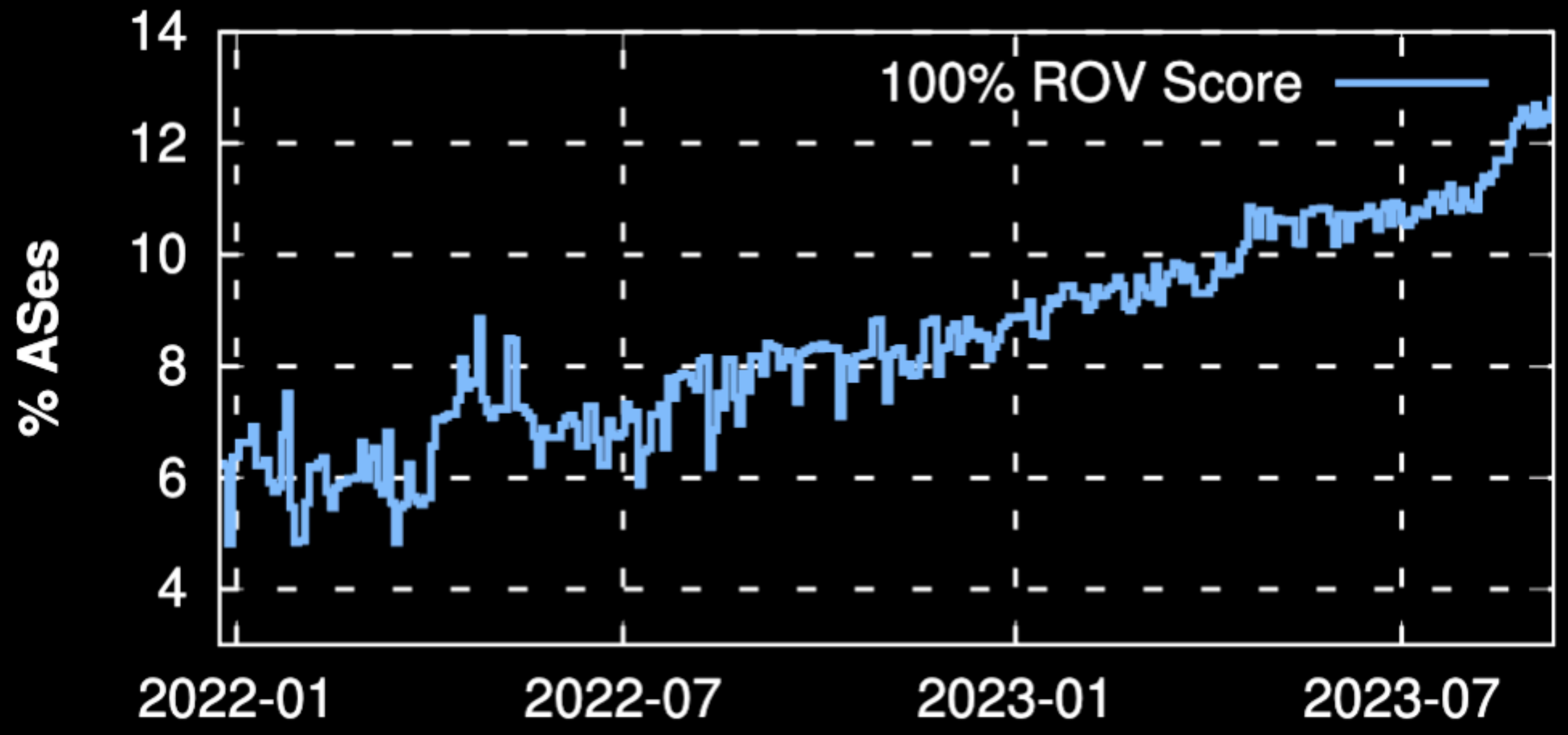


ISP	ASN	Source	ROV Ratio from RoVista
HEANet	1213	https://twitter.com/natural20/status/1366385420360155144	100%
Telstra	1221	https://lists.ausnog.net/pipermail/ausnog/2020-July/044367.html	100%
Sprint / T-Mobile	1239	https://www.sprint.net/policies/bgp-aggregation-and-filtering	100%
Telia	1299	https://www.teliacarrier.com/Our-Network/BGP-Routing/Routing-Security.html	100%
EBOX	1403	https://whois.arin.net/rest/asn/AS1403/pft?s=AS1403	100%
IIJ	2497	https://www.iij.ad.jp/en/dev/iir/pdf/iir_vol50_focus1_EN.pdf	100%
Belnet	2611	https://belnet.be/en/belnet-has-successfully-implemented-rpki	100%
NTT	2914	https://www.gin.ntt.net/support/policy/rr.cfm#RPKI	100%
TDC	3292	https://github.com/cloudflare/isbgpsafeyet.com/pull/523	100%
Swisscom	3303	https://twitter.com/swisscom_csirt/status/1300666695959244800	100%
Level3	3356	https://twitter.com/lumentechco/status/1374035675742412800	100%
Telstra	4637	https://www.zdnet.com/article/telstra-to-roll-out-rpki-routing-security-from-june-2020/	100%
Vocus	4826	https://blog.apnic.net/2021/05/13/vocus-rpki-implementation/	100%
Orange	5511	https://twitter.com/OrangeIC/status/1541436188241891328	100%
Cyta	6866	https://blog.daknob.net/rpki-deployment-greece-feb-19/	100%
Hurricane Electric	6939	https://mailman.nanog.org/pipermail/nanog/2020-June/108277.html	100%
AT&T	7018	https://mailman.nanog.org/pipermail/nanog/2019-February/099501.html	100%
Dhiraagu	7642	https://twitter.com/isseykun/status/1261758917467668481	0%
Comcast	7922	https://corporate.comcast.com/stories/improved-bgp-routing-security-adds-another-layer-of-protection-to-network	100%
ColoClue	8283	https://github.com/coloclue/kees	100%
Atom86	8455	https://www.linkedin.com/pulse/atom86-leveraging-rpki-make-internet-safer-place-ralph-dirkse/	100%
RETN	9002	https://twitter.com/RETNnet/status/1333735456408793089	92.5%
BIT	12859	https://www.bit.nl/news/2081/88/Registratie-van-RPKI-informatie-voor-een-veilige-routering-informatie-voor-een-veilige-routering	0%
Amazon	16509	https://aws.amazon.com/blogs/networking-and-content-delivery/how-aws-is-helping-to-secure-internet-routing/	100%
ASERGO	30736	https://twitter.com/asergogroup/status/1258377169526546432	100%
Jaguar	30781	https://twitter.com/JDescoux/status/1253344721201696768	100%
Seacom	37100	https://www.ripe.net/participate/mail/forum/routing-wg/PDZlMzAzMzhhLWVhOTAtNzIxOC1lMzI0LTBjZjMyOGI1Y2NkM0BzZWFjb20ubXU+	
NAPAfrica	37195	https://www.napafrica.net/technical/rpki-handy-hints/	100%
Workonline	37271	https://as37271.fyi/routing-policy/	100%
Freethought	41000	https://twitter.com/freethoughtnet/status/1222841548771090432	100%
Fiber Telecom	41327	https://www.peeringdb.com/asn/41327	100%
HOPUS	44530	https://twitter.com/afenioux/status/1305430383345971201	100%
NAP.EC	52482	https://www.aeprovi.org.ec/es/implementacion-de-rpki-y-validacion-de-origen-bgp-en-ecuador	100%
Scaleway	54265	https://mailman.nanog.org/pipermail/nanog/2020-April/107295.html	100%
Terrahost	56655	https://twitter.com/TerraHost/status/1259311449073168384	100%
KAPSI	57692	https://twitter.com/atonkyra/status/1253609926221496322	100%
Fusix	57866	https://fusix.nl/deploying-rpki/	100%
Gigabit ApS	60876	https://mailman.nanog.org/pipermail/nanog/2020-April/107295.html	0%
Tuxis	197731	https://twitter.com/Tuxis_IE/status/1105060034873049091	100%

Current ROV status

- ROV deployment is increasing over the last 2 years

- But, still not enough to secure the Internet

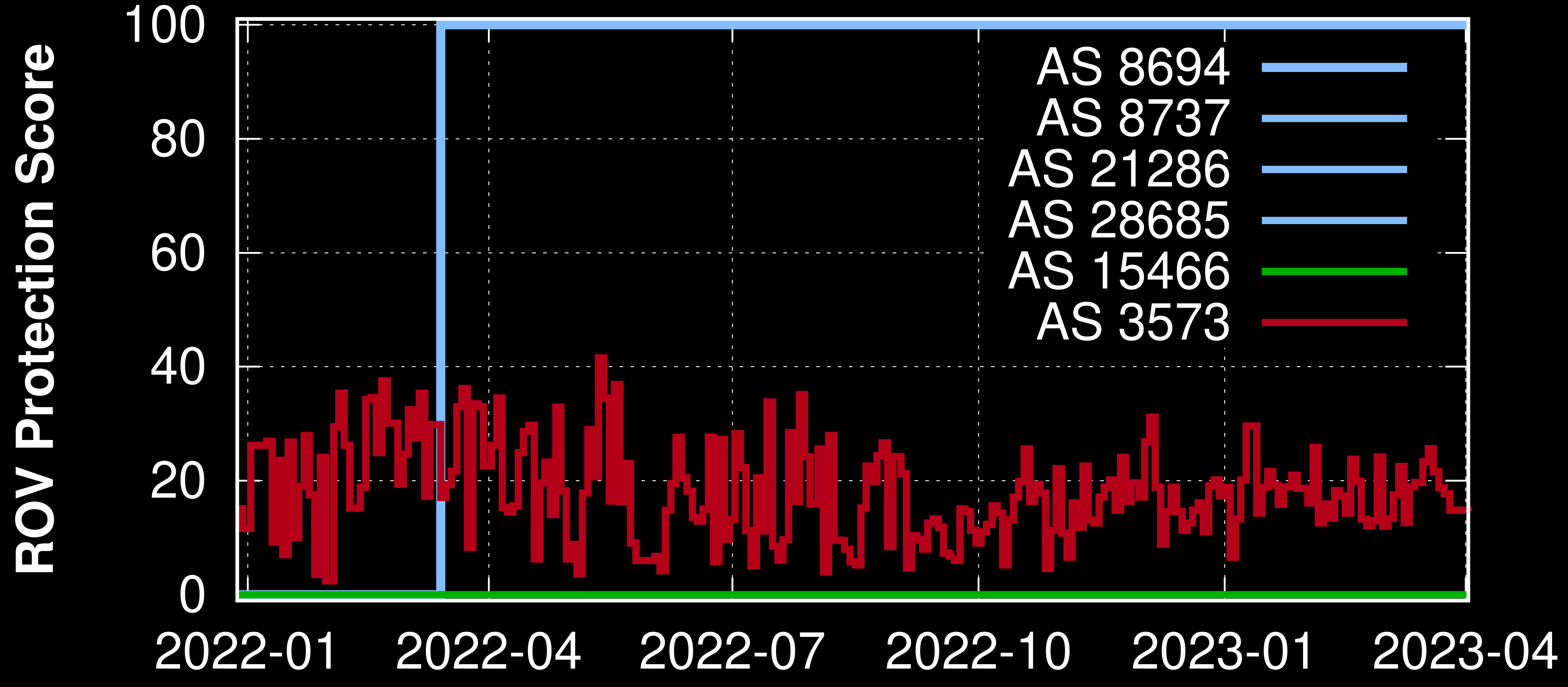


Current ROV status

- Large network are more likely to deploy ROV
- Tier-1 ASes are doing a good job

Rank	ASN	ISP	ROV Score	Rank	ASN	ISP	ROV Score
1	3356	Level 3	100	15	12956	Telefonica Global Solutions	100
2	1299	Telia	100	18	701	Verizon	94
3	174	Cogent Communications	100	21	7018	AT&T	100
4	3257	GTT Communications	100	22	3320	Deutsche Telekom AG	0
6	2914	NTT America	100	31	6830	Liberty Global B.V.	100
8	6461	Zayo Bandwidth	100	32	1239	Sprint	100
9	6453	TATA Communications	100	36	209	CenturyLink Communications	100
10	3491	PCCW Global	100	72	2828	Verizon	94
14	5511	Orange	100				

Case-Study:
Collateral Benefits of ROV



Limitations & Conclusion

- We present ROVista, a new platform to measure the protection of ROV

- With 2 years running, we successfully measure the ROV status of more than 28,000 ASes

- We publish all dataset and source codes in: rovista.netsecurelab.org

- There's a need of future study to distinguish ROV deployment and ROV protection in a larger scale

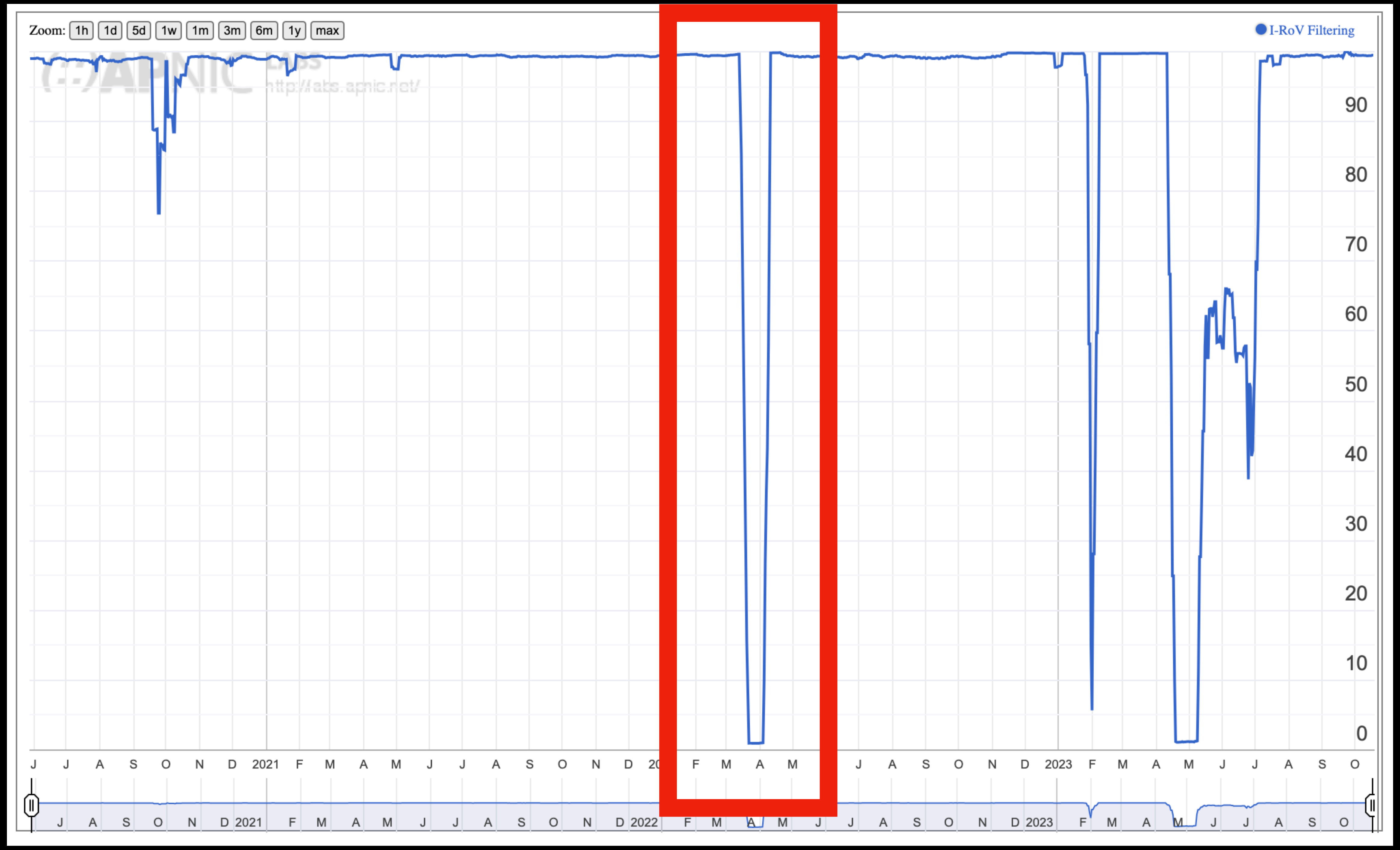
Questions

Previous approaches

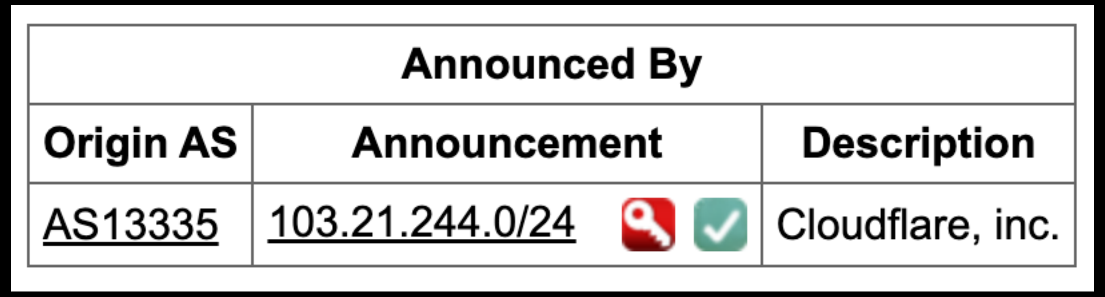
ROV Measurement result for AT&T from APNIC

Fully ROV →

Non ROV →

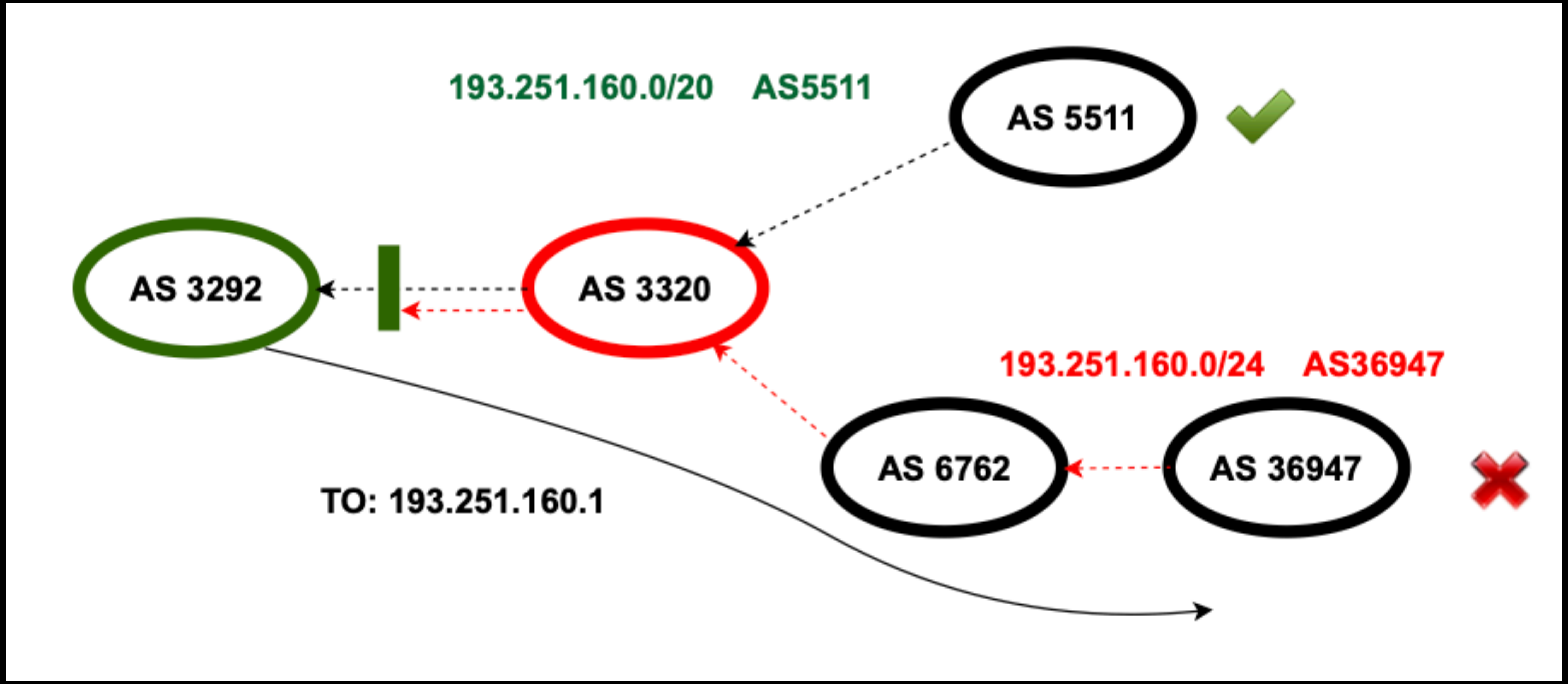


invalid.rpki.cloudflare.com

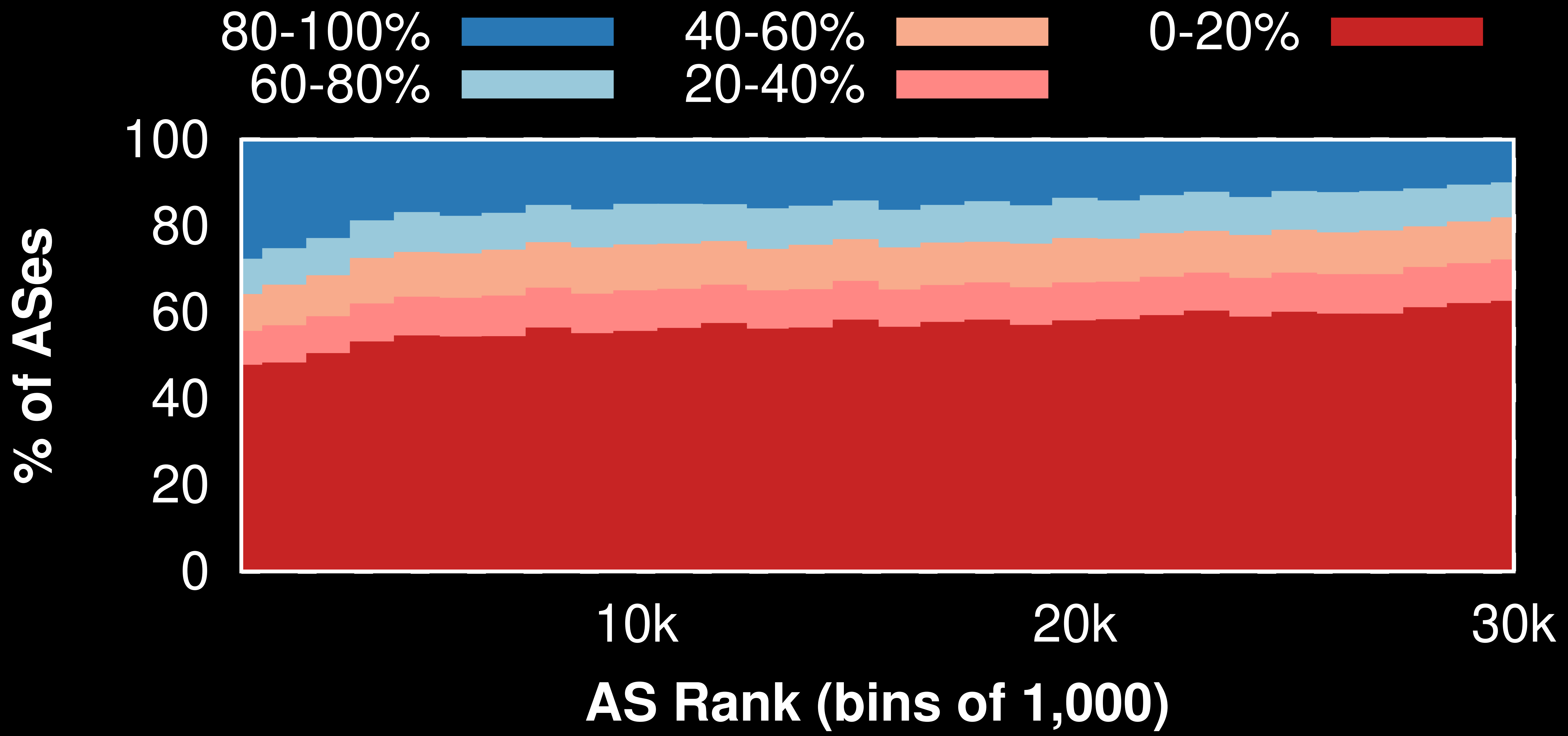


Announced By		
Origin AS	Announcement	Description
AS13335	103.21.244.0/24 ✓	Cloudflare, inc.

Collateral damage



AS Rank vs ROV score


% of ASes
10k
20k
30k
AS Rank (bins of 1,000)