Exploring the Blind Spot of Internet Exchange Point Route Servers

Stefano Servillo.[1], Pietro Spadaccino[1], Stavros Konstantaras[2], Flavio Luciani[3], Franceca Cuomo[1]

1 SAPIENZA UNIVERSITÀ DI ROMA

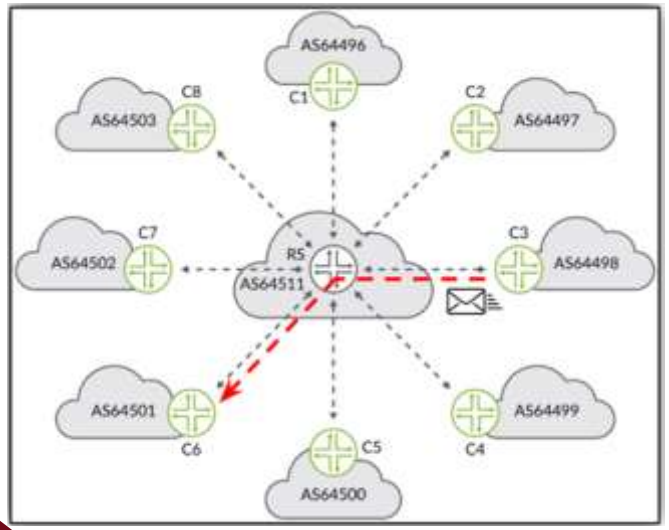
2 amsix

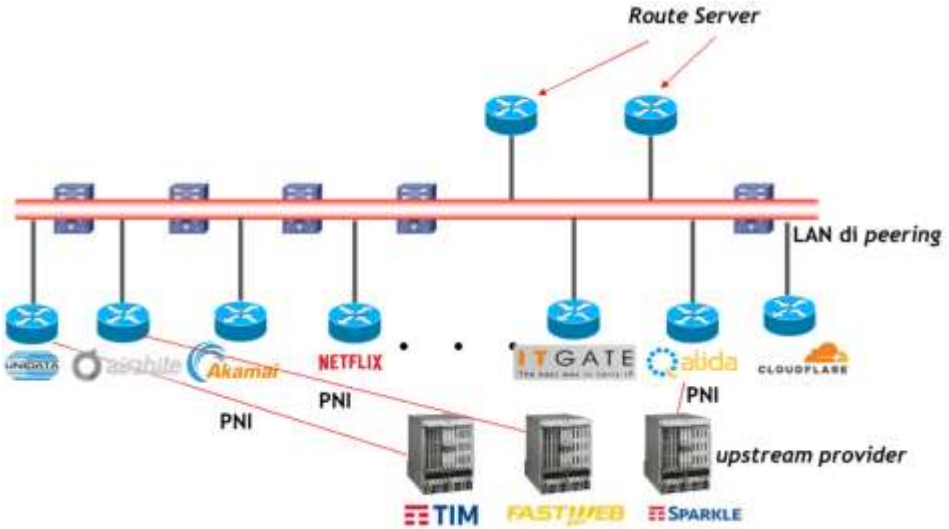
3 NAMEX ROMA INTERNET EXCHANGE POINT

Internet Exchange Points (IXPs)

IXP offer **public peering** through multilateral agreements via **Route Servers (RS)**

Only **one BGP session** with the RS





Peering LAN to interconnect all ASes

IXPs - traffic

LINX Traffic Overview

Traffic

Current	8.895 Tbps
Max	11.532 Tbps

29 APR 2025

IX.br reaches new record, with 40 Tbit/s of aggregate traffic

To avoid large traffic disruptions, IXPs apply BGP **filtering policies** at RS

Route Server filtering policies

Basic filters

- Bogon/Martian - drop invalid/reserved prefixes
- Prefix length - enforce RFC 7454 limits
- Next-hop - must match the peer
- AS path length - reject abnormal paths
- ASN checks - block bogon ASNs, verify leftmost ASN

Commonly **INBOUND**

Advanced filters

- RPKI - drop *Invalid* routes
- IRR - drop *Invalid* routes
- *(ASPA coming soon…)*

Different approaches

All inbound

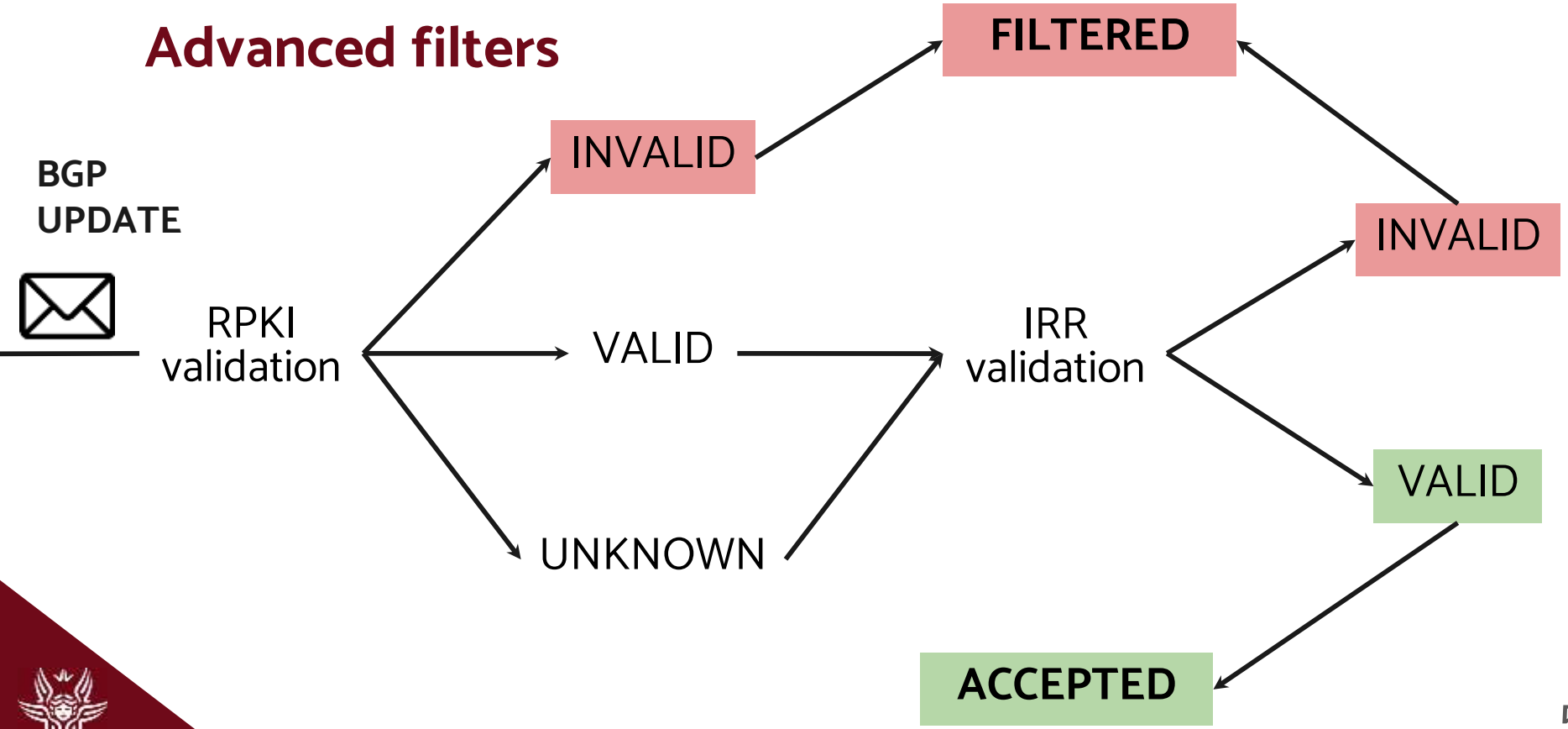
All outbound

Split between in/out

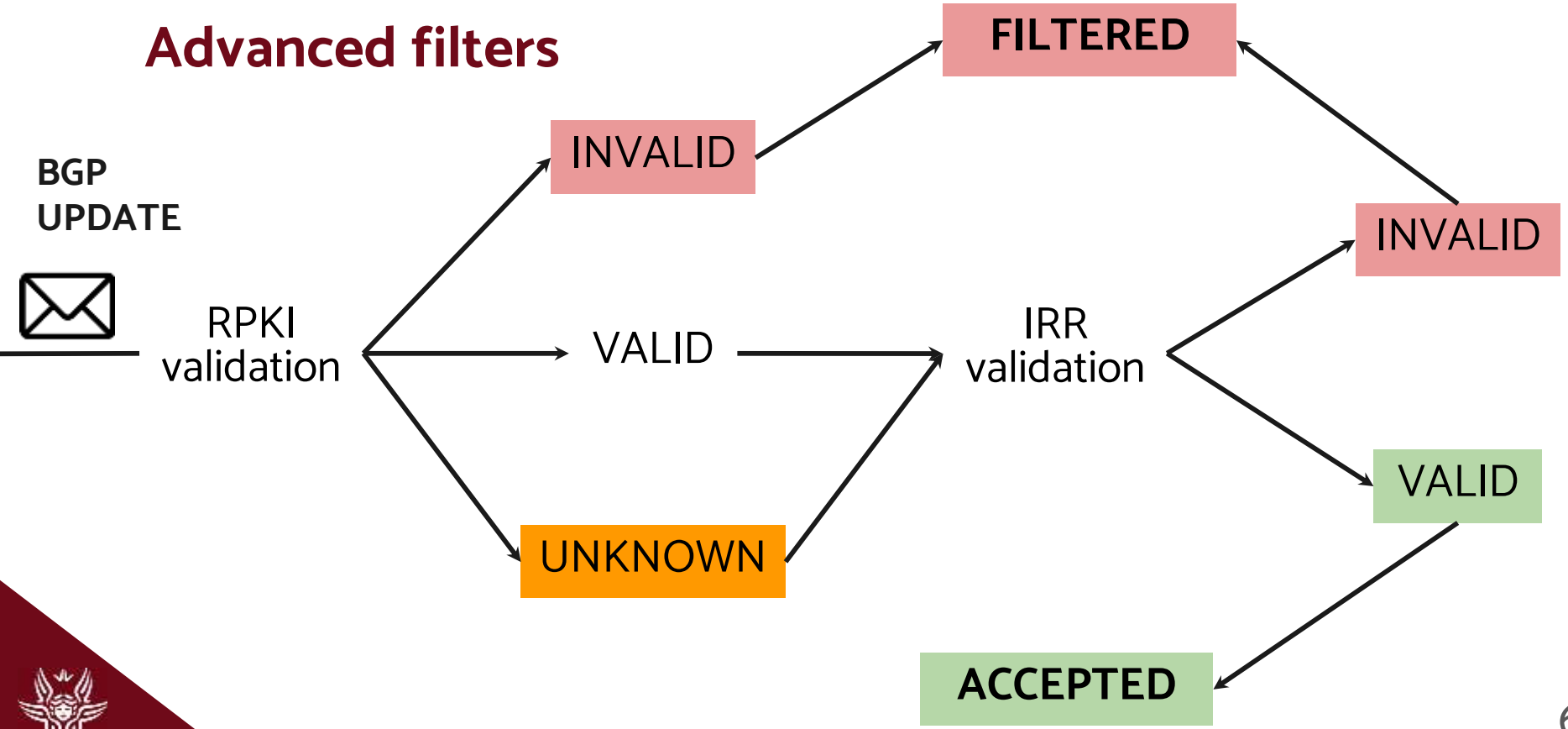
No strict rules

Operators apply filters based on **best practices, needs and clients**

Advanced filters



Advanced filters



AS-SET

Collection of ASNs/AS-SETs used for **route filtering**

RIPE

```
aut-num:        AS137
as-name:        ASGARR
descr:          Consortium GARR
import:         from AS20965 action pref=300; accept ANY
import:         from AS1299 action pref=100; accept ANY
import:         from AS174 action pref=100; accept ANY
mp-import:      afi ipv4.multicast from AS20965 action pref=100; accept ANY
mp-import:      afi ipv6.unicast from AS20965 action pref=100; accept ANY
mp-import:      afi ipv6.multicast from AS20965 action pref=100; accept ANY
export:         to AS20965 announce AS-GARRTOGEANT
export:         to AS1299 announce AS-GARR
export:         to AS174 announce AS-GARR
mp-export:      afi ipv4.multicast to AS20965 announce AS-GARRTOGEANT;
mp-export:      afi ipv6.unicast to AS20965 announce AS-GARRTOGEANT;
mp-export:      afi ipv6.multicast to AS20965 announce AS-GARRTOGEANT;
```

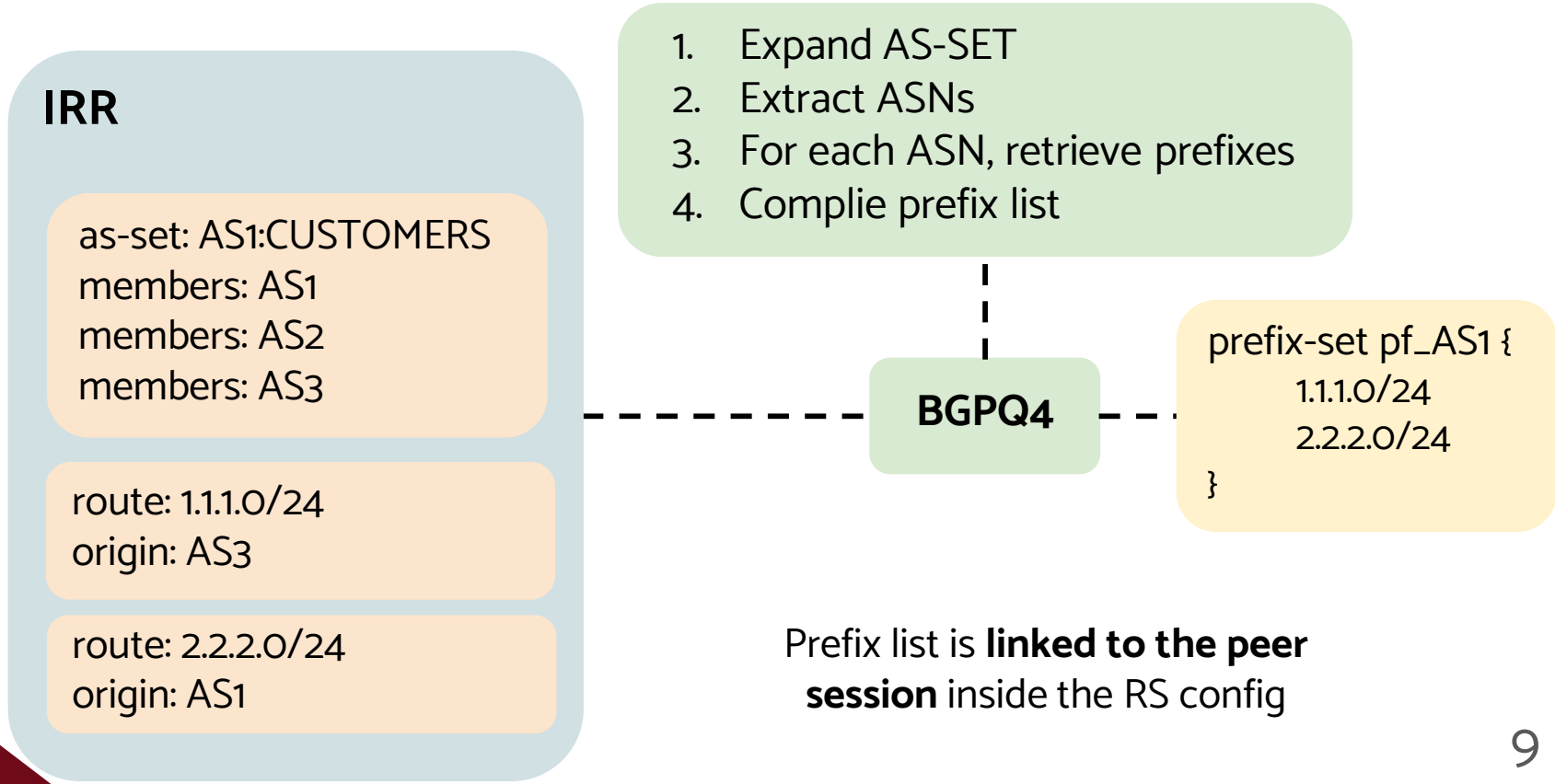
Customer ASes it may providing **transit for**

RIPE

```
as-set:         AS-GARR
descr:          National GARR ASes
members:        AS137
members:        AS24869
members:        AS8978
members:        AS35110
members:        AS42165
members:        AS16004
members:        AS2597
members:        AS50112
members:        AS51708
members:        AS50507
members:        AS29609
members:        AS197440
members:        AS49976
members:        AS31638
members:        AS199342
members:        AS2596
members:        AS2598
members:        AS5502
members:        AS200375
members:        AS6882
members:        AS209631
members:        AS42081
members:        AS20745
members:        AS20697
members:        AS29598
members:        AS21333
members:        AS12
```

How IXPs use AS-SETs for IRR validation?

IRR-based validation



Prefix list is **linked to the peer session** inside the RS config

IRR-based validation

prefix-set pf_AS1 { 1.1.1.0/24, 2.2.2.0/24 }
allow from AS 1 prefix-set pf_AS1

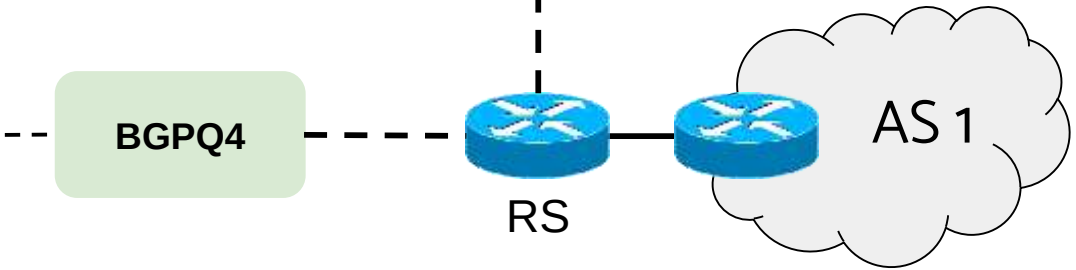
IRR

as-set: AS1:CUSTOMERS
members: AS1
members: AS2
members: AS3

route: 1.1.1.0/24
origin: AS3

route: 2.2.2.0/24
origin: AS1

From AS 1
If prefix in { 1.1.1.0/24, 2.2.2.0/24 }: ACCEPT
Else: DROP



Are RS safe from prefix hijacks/misconfigurations?

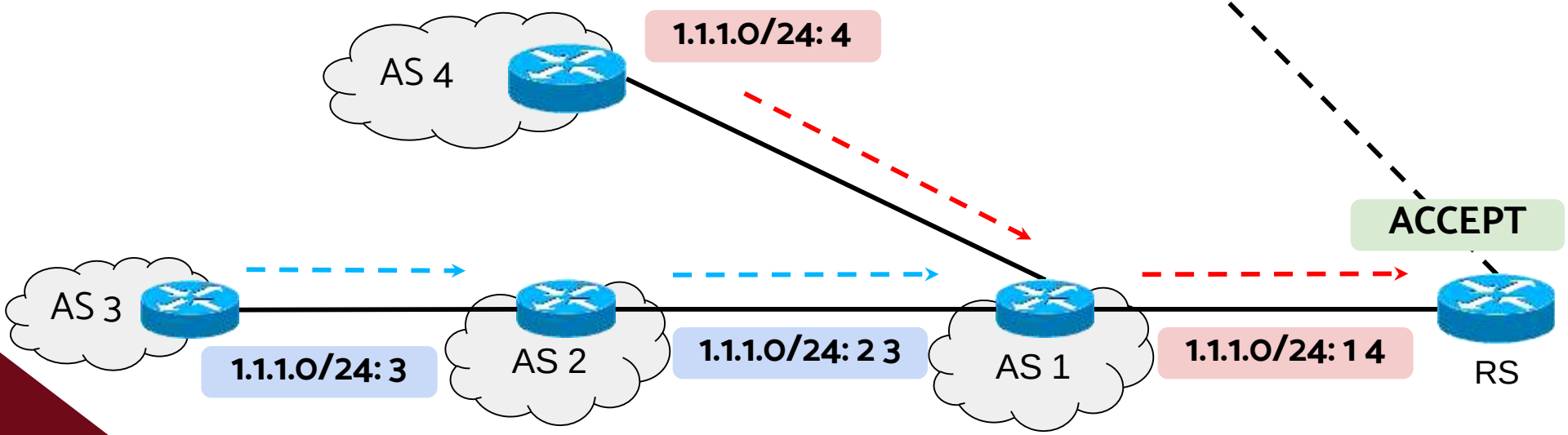
Are RS safe from prefix hijacks/misconfigurations?

Not completely

Blind Spot

NO INFORMATION regarding the real owner

From AS 1
If prefix in { 1.1.1.0/24, 2.2.2.0/24 }: ACCEPT
Else: DROP



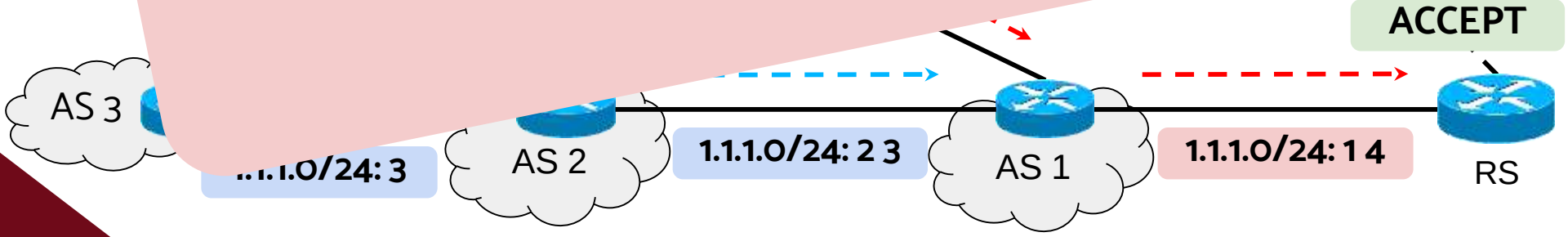
Blind Spot

NO INFORMATION regarding th…
real ow…

From AS…

…CCEPT

PREFIX HIJACKING/ MISCONFIGURATION



Are your prefixes safe?

AS-SET – not maintained

AS-SETs grow with **unallocated, private and inactive** ASes

~130k allocated ASes by RIR

~77,000 active ASes

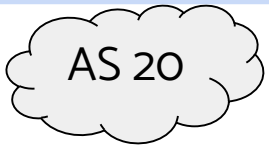
AS-SET	ASes	IPv4	IPv6
AS39533:AS-PEERS	104,491	2,232,229	955,918
AS214292:AS-DECIX-L3-SERVICES...	104,266	2,231,371	955,732
AS-ST1-IXPS	104,059	2,230,016	955,623
AS3326:AS-PEERS-DEE	103,864	2,229,607	955,575
AS-CLOUD-IX-PRO	103,856	2,229,582	955,555
AS-MERKEL-PEERS	103,856	2,229,594	955,567
AS12732:AS-UPSTREAMS	103,843	2,229,584	955,554
AS39533:AS-SET:AS6695	103,842	2,229,580	955,553
AS6695:AS-DECIX-FRA	103,842	2,229,580	955,553
AS-DECIX	103,842	2,229,580	955,553

Top 10 AS-SETs ranked by number of ASes

A prefix **may be vulnerable** due to a route object for an unallocated, private or inactive AS

AS-SET – not maintained

Route: 3.3.3.0/24
Origin: AS20



AS-SET – not maintained

Route: 3.3.3.0/24
Origin: AS20

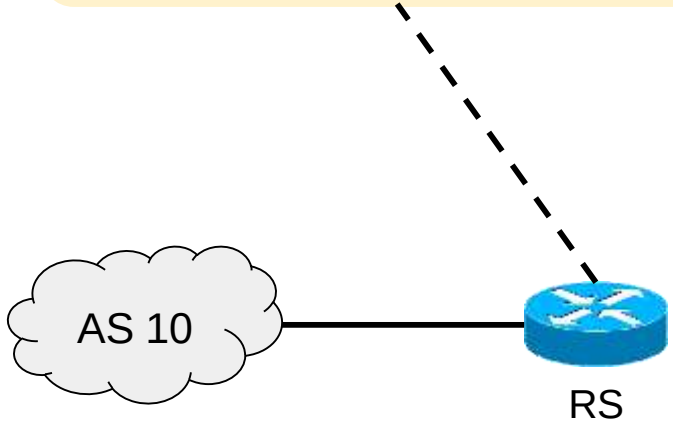
AS 20

IRR

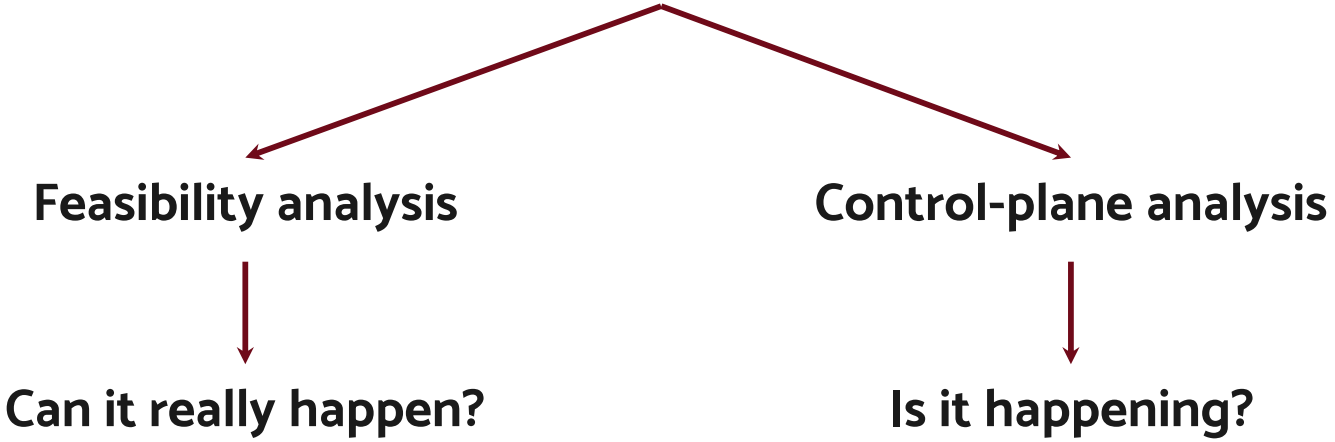
as-set: AS10:CUSTOMERS
members: AS10
members: AS65512

route: 3.3.3.0/24
origin: AS65512

From AS 10
If prefix in { 3.3.3.0/24 }: ACCEPT
Else: DROP



Data analysis



NAMEX
ROMA INTERNET EXCHANGE POINT

amsix

Can it really happen?

1) Prefix must **not be covered** by a ROA
2) Update must **not be filtered** by intermediate ASes
3) Update must reach RS **through Member Y**
4) Origin AS **not required** to be in Member Y's AS-SET
5) Prefix **in a route object** with AS X
6) AS X **in the AS-SET** of a Member Y

Can it really happen?

1) Prefix must **not be covered** by a ROA - - - - - - - - - - - - - → **32%** are *NotFound*

2) Update must **not be filtered** by intermediate ASes - - - - - - → **9%** are *Invalid*

3) Update must reach RS **through Member Y**

4) Origin AS **not required** to be in Member Y's AS-SET

5) Prefix **in a route object** with AS X

6) AS X **in the AS-SET** of a Member Y

Can it really happen?

1) Prefix must **not be covered** by a ROA

2) Update must **not be filtered** by intermediate ASes

3) Update must reach RS **through Member Y** ⟶ **52%** via *auth-member*, **28%** via *two or more*

4) Malicious AS **not required** to be in Member Y's AS-SET ⟶ **5.4%** are *Not in as-set*

5) Prefix **in a route object** with AS X

6) AS X **in the AS-SET** of a Member Y

Can it really happen?

1) Prefix must **not be covered**
2) Update must **not be filtered**
3) Update must reach RS **throu**
4) Origin AS **not required** to be

AS-SET	# ASes	# IPv4 No ROAs	# IPv6 no ROAs
AS-TELIANET	99,677	936,517	292,035
AS-GTT	88,331	915,268	289,253
AS-GLOBEINTERNET	86,740	900,248	289,045
AS-NETIX-INT	82,610	872,404	287,856
AS-SEABONE	76,434	863,144	286,162
AS-UNITAS	68,678	810,917	282,942
AS-CTGNet	66,791	792,108	281,870
AS-1031-PEER1	52,228	623,434	235,373
AS-RTD	44,973	546,078	214,810
AS-OTEGLOBE	44,238	557,762	214,463

5) Prefix **in a route object** with AS X
6) AS X **in the AS-SET** of a Member Y

Is it happening?

Step	Announcements	Unique Prefixes	Unique Origins
Initial data	492,543	288,314	38,246
Public ASN	492,418	288,223	38,201
RPKI unknown	158,134	98,284	18,937
AS-SET Valid	64,901	45,592	10,723
Blind spot	1,426	1,343	513
High-level analysis			
Cust-Prov	807	750	285
Siblings	104	97	36
AS path	34	30	19
Supernet	242	242	68
Allocation	38	36	26
No relationship	201	188	79

Valid for RS, but Origin AS has **no route object**

Most cases are **business agreements**

Suspicious

What happen to correct announcements?

Origin AS has a **valid route object** for the prefix

Filtered due to **outdated AS-SET or non-auth (65,5%)**

Step	Announcements	Unique Prefixes	Unique Origins
Correct	133,658	81,779	18,110
AS-SET invalid	69,616	51,938	12,189
No route available	55,650	43,266	10,316
AS-SET valid	64,042	45,095	10,737
Propagated	47,012	45,091	10,736
Not propagated	17,030	10,514	2,813

All announcement are filtered

Valid but not propagated because of BGP selection process

Multiple Origin AS (MOAS)

Same prefix announced by two or more ASes

Same prefix announced by both an **invalid and a valid** AS

MOAS type	Announcements	Unique Origins	Unique Prefixes
ALL MOAS	446	143	155
Special MOAS	8	8	6
Correct adv.	0	0	0
Incorrect adv.	8	8	6

RS propagates the route via the **illegitimate AS**

Only AMS-IX and NAMEX?

Checked IRR-based filtering descriptions

Verified prefixes via looking glass

If prefixes considered valid, IXP marked as **not protected**

22 are not protected
Only 4 IXPs protected
8 no information

IXP	AS-SET usage	Looking glass check	Protected
AMSIX	✓	✓	X
BCIX	✓	✓	X
BIX	✓	✓	X
BNIX	✓	✓	X
BKNIX	✓	?	?
CIX	✓	✓	X
DECIX	✓	X	✓
FRANCE-IX	✓	✓	X
GRIX	✓	✓	X
GIGAPIX	✓	✓	X
HKIX	✓	?	?
IX Australia	✓	✓	X
IX.br	✓	✓	X
INEX	✓	✓	X
INTERLAN	?	?	?
JPNAP	?	?	?
LINX	✓	✓	X
LONAP	✓	✓	X
MINAP	✓	✓	X
MEGAPORT	✓	✓	X
MSK-IX	✓	✓	X
NAMEX	✓	✓	X
NETNOD	✓	✓	X
NLIX	✓	✓	X
NIXI	?	?	?
PIT CHILE	?	?	?
SGIX	✓	✓	X
SIX	✓	X	✓
STUTTGART	✓	✓	X
SOX	?	?	?
SWISSIX	✓	X	✓
TOP-IX	✓	✓	X
UAE-IX	✓	X	✓
VIX	?	?	?

Only AMS-IX and NAMEX?

Checked IRR-based fil

IXP	AS-SET usage	Looking glass check	Protected
AMSIX	✓	✓	X
BCIX	✓	✓	X
BIX	✓	✓	X
BNIX	✓	✓	X
BKNIX	✓		?
CIX	✓		
DECIX			
			X
		✓	X
		✓	X
	✓	✓	X
	✓	✓	X
NIXI	?	?	?
PIT CHILE	?	?	?
SGIX	✓	✓	X
SIX	✓	X	✓
STUTTGART	✓	✓	X
SOX	?	?	?
SWISSIX	✓	X	✓
TOP-IX	✓	✓	X
UAE-IX	✓	X	✓
VIX	?	?	?

We could look into your RIB ;)

are not protected

Only 4 IXPs protected

8 no information

Solutions

Perform **origin validation** against route objects (ROs)

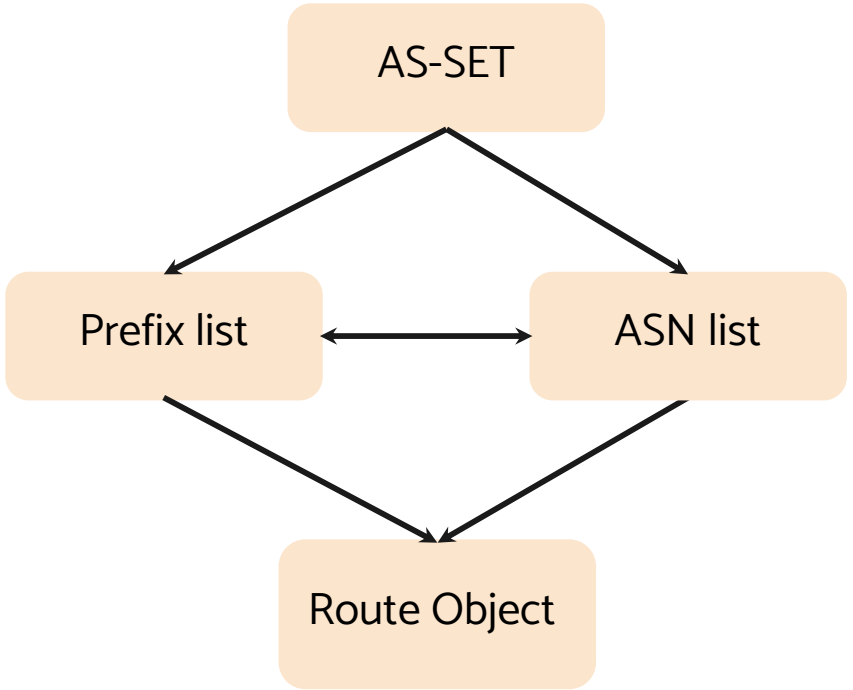
- **RO**

Route Object

Mitigations

Perform **origin validation** against route objects (ROs)

- **RO**
- **Prefix -> RO**
- **ASN -> RO**
- **Prefix-> ASN -> RO**
- **ASN -> Prefix -> RO**



Recommendations

Network Operators

Creates ROAs for each prefix, following the **RFC 9319**

Keep IRR AS-SET objects **up to date** and use **authoritative IRR DBs**

* After removal of unallocated, private, and inactive ASes

Recommendations

Network Operators

Creates ROAs for each prefix, following the **RFC 9319**

Keep IRR AS-SET objects **up to date** and use **authoritative IRR DBs**

BEFORE

AS-SET	ASes	IPv4	IPv6
AS39533:AS-PEERS	104,491	2,232,229	955,918
AS214292:AS-DECIX-L3-SERVICES...	104,266	2,231,371	955,732
AS-ST1-IXPS	104,059	2,230,016	955,623
AS3326:AS-PEERS-DEE	103,864	2,229,607	955,575
AS-CLOUD-IX-PRO	103,856	2,229,582	955,555
AS-MERKEL-PEERS	103,856	2,229,594	955,567
AS12732:AS-UPSTREAMS	103,843	2,229,584	955,554
AS39533:AS-SET:AS6695	103,842	2,229,580	955,553
AS6695:AS-DECIX-FRA	103,842	2,229,580	955,553
AS-DECIX	103,842	2,229,580	955,553

AFTER CLEANUP*

AS-SET	ASes	IPv4	IPv6
AS39533:AS-PEERS	77,289	2,171,351	906,575
AS214292:AS-DECIX-L3-SERVICES...	77,252	2,170,569	906,409
AS-ST1-IXPS	77,134	2,169,482	906,306
AS3326:AS-PEERS-DEE	77,009	2,169,119	906,259
AS-CLOUD-IX-PRO	77,002	2,169,105	906,252
AS-MERKEL-PEERS	77,001	2,169,104	906,252
AS12732:AS-UPSTREAMS	77,002	2,169,108	906,253
AS39533:AS-SET:AS6695	77,001	2,169,104	906,252
AS6695:AS-DECIX-FRA	77,001	2,169,104	906,252
AS-DECIX	77,001	2,169,104	906,252

* After removal of unallocated, private, and inactive ASes

Recommendations

Network Operators

Creates ROAs for each prefix, following the **RFC 9319**

Keep IRR AS-SET objects **up to date** and use **authoritative IRR DBs**

IXP Operators

Review filtering policy

Check prefixes in RIB

If affected, **apply** one of the proposed **solutions**

Conclusions and future work

Exposed a **blind spot** in IXP route server filtering, showing how i**nvalid announcements can still be accepted** and propagated, and even preferred over legitimate routes.

Our findings show that his is not an isolated issue but a **widespread challenge** for interconnection security and can impact **all ASes** performing such filtering

- Extend analysis to **IPv6**
- Implement proposed solutions -> **measure RS performance**
- **Is the juice worth the squeeze?**

Thank you for your attention!

Questions?

stefano.servillo@uniroma1.it