Detecting BGP speakers that announce ROV invalid routes

Kevin Klercq
Security and Network Engineering
University of Amsterdam
kevin.klercq@os3.nl

ABSTRACT – The Border Gateway Protocol (BGP) has not been designed with security in mind. A technology to make BGP safer that sees adoption these days is Route Origin Validation (ROV). ROV can be used to validate if an Autonomous System (AS) is authorized to originate an Internet Protocol (IP) prefix. ROV protects against some BGP weaknesses, but not all. The research aims to show that non-validating routers can be discovered by using traceroutes.

In the experiment a ROV valid and an overlapping more specific ROV invalid route are advertised and traceroutes are performed to addresses in both ranges. When the traceroutes don't take an equal path, a router on the path must have installed the invalid route and thus does not validate routes. The research further identifies the most prevalent non-validating routers, with the aim of pinpointing which parties will have the biggest positive effect on routing security if they would start doing ROV.

1. Introduction

The Border Gateway Protocol (BGP) is the glue of the Internet that interconnects the networks of organizations. Networks of organizations are represented by an Autonomous System Number (ASN) and organizations can use BGP to advertise their IP prefixes to neighboring networks [1][2]. During this exchange of routing information, no checks are performed to validate if the Autonomous System (AS) that advertised the IP prefix(es) is authorized to do so [3].

The BGP protocol is not secure by design and allows anyone with an ASN and a BGP speaker to advertise any IP prefix, even if they don't own the IP prefix or are authorized by the owner of the IP prefix to advertise on their behalf. Unauthorized advertisement of an IP prefix is called a BGP prefix hijack. This event can occur on accident by a misconfigured BGP speaker or intentionally by a malicious actor.

A hijack can arise in multiple ways. By:

- Advertising an IP prefix that you don't own yourself or are not allowed to advertise on behalf of the owner.
- Advertising a more specific prefix. More specific prefixes are preferred over less specific prefixes.
- Advertising a prefix with a different AS_PATH attribute to reroute the traffic.

Multiple proposals have been made to improve the security of BGP. Because of the complicated implementation that some of these proposals require, they see low adoption in the real world [4][5]. A proposal that has the highest adoption rate as of February 2023 is a technology called Resource Public Key Infrastructure (RPKI) [6].

1.1 Resource Public Key Infrastructure

RPKI can be used to cryptographically validate if an AS is authorized to originate a certain prefix [14]. This technology can prevent hijack attacks that are caused by advertising a prefix from a non-authorized AS. The RPKI technology can also prevent hijacks that happen with an unauthorized advertisement of a more specific prefix by a malicious actor. RPKI can prevent this because the maximum prefix length that is allowed for an IP prefix advertisement can be limited. RPKI cannot prevent hijacks where the AS_PATH attribute is changed to reroute traffic through a malicious AS [7][8].

The RPKI is a PKI that has been extended to hold IP prefixes and ASN's in x.509 certificates. [11] Internet numbers like ASN's and prefixes are

assigned to Regional Internet Registries (RIR's) by IANA. The RIR's then assign the internet numbers to organizations that requested the internet numbers. Each RIR has a Trust Anchor its own trust anchor that must be used to validate RPKI signed resources.

1.2 Route origin validation

Route Origin Validation (ROV) is the practice of validating routes that are received by a BGP speaker through the RPKI. The owner of an IP prefix can create a Route Origination Authorization (ROA) which includes the ASN that may originate the prefix(es), the prefix(es) it/themselves and the maximum prefix length [10]. When a route is received by a validating BGP speaker, it can have one of the following three states:

- Valid: A ROA authorizes the AS in the AS_PATH attribute to originate the prefix and the prefix length is not longer than the maximum length specified in the ROA.
- Invalid: The AS advertised is not authorized to originate the prefix or the announcement is more specific than authorized by the ROA.
- Unknown: There is no ROA found for the prefix advertised.

The invalid state occurs when something happens without the authorization of the owner of the resource. The unknown state occurs when the owner of the resource has not created a ROA for the resource. Network operators should not install any routes that they validated and came out as being an invalid route announcement. Unfortunately, not all network operators on the internet drop invalid routes.

1.3 Problem statement

A BGP prefix hijack can have multiple consequences. When a prefix is hijacked, the IP-addresses in the prefix may become unreachable resulting in a denial-of-service attack. This is something that a user can clearly notice. Another possible consequence of a hijack is that traffic can be eavesdropped if it is rerouted through a malicious AS. If the traffic is only rerouted and reaches its intended destination unchanged, then a user might not notice anything abnormal. This consequence is a reason why a user should care if the routing it is using is secure or not.

The hypothesis of this research is that BGP speakers that installed invalid routes can be discovered by performing traceroutes. An IP prefix with an example length of /23 is advertised via BGP with a valid ROA. Somewhere else in the world a more specific part of that prefix is advertised as well but with an invalid ROA. If traceroutes are performed from a certain source location to both an address in the /23 range that doesn't overlap with the more specific announcement and an address in the more specific announcement, then the traceroutes will take a different path if ROV is not used on that path. By comparing both the traceroutes it can be determined where the non-validating router is located because the next hop on both traceroutes takes a different path. This method works best when the 2 announcements are made from geographically spread-out locations. If the 2 announcements are made from (roughly) the same location then the 2 traceroutes would also take almost similar paths, regardless of whether ROV occurs on the path.

Discovering one non-validating router from one specific source location is nice to know, but it would be more interesting if the test was performed from a wide variety of source locations all over the world. When lots of traceroutes have been performed and (possibly) many non-validating AS's, prefixes or routers have been found, it would be interesting to see if some entities occur multiple times in the results. In theory when those entities enable ROV, it has a bigger positive impact on worldwide routing security. The results of the measurement can also be used to measure the amount of the source locations that are currently protected against invalid announcements. Differences between IPv4 and IPv6 can also be measured.

2. Related work

2.1 Measuring BGP RPKI Route Origin Validation by Cloudflare

Cloudflare measures ROV adoption per AS by letting users visit a website called isbgpsafeyet.com. This website checks if a user can reach a resource that is only reachable via an invalid announcement. If the user can reach the invalid resource, then the AS is marked as not using ROV. Cloudflare announces their invalid prefix from many different locations worldwide using anycast. When the invalid prefix is anycasted closer to the source, it is more likely that the source has a shorter path to the destination. Because of this shorter path, it is less likely that the source could have benefitted from an intermediate AS dropping the invalid route.

The website has received around 70 million requests from 41531 different AS's as of October 2022. According to APNIC's estimates on how many end-users are behind a single AS, this means that the Cloudflare website has representative data for around 96.5% of the internet users. The results were that around 6.5% of the internet users were currently protected from invalid routes [12].

There is only a single, non-overlapping invalid prefix announcement that is used to determine if an AS is safe or not. This means that if there is a single router doing ROV somewhere on the path, the source is not able to reach the invalid prefix and is thus marked as safe by Cloudflare's website. In a more realistic simulation of a prefix hijack, there will also be a route that is valid. This causes the traffic to traverse further to the destination, where it may still encounter a non-validating router that sends the traffic to the invalid destination. This causes Cloudflare's results to give an overly positive image of the protection of end-users by ROV on the internet.

2.2 Where did my packet go? By Koen van Hove

Koen van Hove noticed the shortcomings of the Cloudflare measurements and performed an experiment to prove that doing ROV at the end-point does not have to mean that you are fully protected. Upstream routers that do not validate can still install invalid routes, causing a packet to end up at the wrong (invalid) destination.

An experiment was performed in which Koen advertised a valid and an overlapping more specific invalid announcement and created RPKI publication points at addresses in both prefixes. By checking which addresses (from RPKI validators) contacted which publication points, conclusions could be made on how much of the traffic ended up at the valid and how much of the traffic ended up at the invalid publication point.

The conclusion of the article is that merely doing ROV (and dropping invalids) does not mean your traffic goes to the intended location. A non-validating routing along the path can still steer the packet to the invalid location [13].

Because Koen's tests were performed with RPKI publication points, it is reasonable to assume that validators that try to reach RPKI publication points validate routes themselves. Nonetheless roughly 25% of the contacting addresses ended at the invalid location. It would have added value to perform a similar experiment but with random sources across the world.

Koen's tests showed that ROV at an endpoint does not necessarily protect that endpoint from route hijacks, but it did not identify the routes that caused the traffic to be steered to the invalid locations. Furthermore, the measurements involved Internet supportive infrastructure and not end-users' networks

3. Methodology

A test environment was set up to test the hypothesis that non-validating routers can be discovered using traceroutes.

The test environment consists of a BGP speaker located in Amsterdam that announces the prefixes 185.49.142.0/24 and 2a04:b907::/48. Another BGP speaker located in Singapore is set up that announces the prefixes 185.49.142.0/23 and 2a04:b907::/47. ROA's are set up to authorize the BGP speaker in Singapore to announce the 185.49.142.0/23 and 2a04:b907::/47 prefixes. The

max-length attribute in the ROA is set to /23 for the IPv4 prefix and to /47 for the IPv6 prefix. This makes the more specific announcements made from Amsterdam invalid.

Validating routers should mark the advertised routes as invalid because they are more specific than the ROA allows. If all the routers on the internet did ROV, all the traffic destined for addresses in the prefixes should go to Singapore. A non-validating router will prefer the route towards the invalid more specific announcements in Amsterdam for addresses in those prefixes, since more specific announcements take precedence over less specific.

At both sites machines are installed that can respond to traceroutes. The IP-addresses of the machine in Amsterdam are 185.49.142.16 and 2a04:b907::16. The IP-addresses of the machine that is set up in Singapore are 185.49.143.16 and 2a04:b907:1::16, as well as 185.49.142.16 and 2a04:b907::16.

Traceroutes are being sent to 185.49.142.16 and 185.49.143.16 for IPv4 and to 2a04:b907::16 and 2a04:b907:1::16 for IPv6. If both traceroutes to the valid and the IP address that also has an invalid announcement are the same, then all routers on the path did not have the more specific prefix that was advertised from Amsterdam. This could be because the routers on the path never received the more specific route because it was dropped out earlier by other validating routers, or because the router on the path checked it itself and disregarded the invalid prefix.

If the 2 traceroutes are not the same, then 2 things could have happened. The packet was load-balanced and took another path and still reached the valid destination, or a router on the path installed the invalid, more specific route and routed the packet to Amsterdam. By comparing the traceroutes to the valid and the invalid IP-addresses, and checking where the path starts to be different, it can be determined where a router lives that installed the invalid route.

The point from which the traceroutes are performed matters. If traceroutes are performed from a wide variety of points on the internet, more non-validating routers can be discovered. Then it can also be checked if some routers occur multiple times in the results. The routers that occur more often in the results, will have a bigger positive impact on routing security if they implemented ROV.

The 2 BGP speakers should be geographically far apart. If the 2 prefixes were advertised from the same location or from nearby locations, then the traceroutes that are performed would take the same or roughly the same path to the 2 destinations. Then only non-validating routers in the vicinity of the place where the advertisements are made could be determined. If the 2 locations are far apart from a network perspective, and tests are performed, then the chance that the 2 traceroutes will take a completely different path if the invalid route is installed is higher.

To determine if a source reached the invalid announcement made in Amsterdam, a DNS TXT record name lookup is done for the domain rpkitest.nlnetlabs.nl directly from the authoritative nameserver. This authoritative nameserver is served from both sites using the same prefixes. The nameserver in Amsterdam returns a TXT record that says “`NO - Your resolver reached the RPKI Invalid announcement :(`". The nameserver in Singapore returns a TXT record that says "`HOORAY - Your resolver reached the RPKI Valid announcement :)!`".

3.1 Result gathering

For the best measurements, traceroutes and name lookups from as much and as diverse points as possible should be performed. To do this, the NLNOG RING and RIPE ATLAS were used.

The NLNOG RING is a set of Ubuntu machines that are located all over the world, coordinated by the Dutch network operator group (NLNOG). The machines can be used to confirm if resources that are published by network administrators are propagated throughout the entire internet the way the network administrator intended. Everyone with access to the NLNOG RING has access to the Ubuntu machine and can execute commands on all

the machines. The NLNOG RING works on a trust base, organizations and network administrators make a machine available to the network so all the members can use it, and by doing so the operator that makes the machine available gets access to all the other members' machines. Although the NLNOG RING network is coordinated by mainly Dutch entities, the machines are very widespread across the globe. This can be confirmed because the physical location of the machine is also registered.

RIPE ATLAS is a similar internet measurement system that can be used by organizations and network operators to perform experiments and measurements across the internet. RIPE ATLAS doesn't work on a trust base, users must spend credits to perform measurements like traceroutes and DNS lookups. Measurements can be executed using a web interface or through the API.

Python scripts were written to schedule measurements and gather and process results. The scripts first perform a name lookup to determine if the source can reach the invalid prefix. If a source can reach the invalid prefix, traceroutes are performed to determine which router causes the source to reach the invalid prefix. If a source reaches the valid prefix, it is marked as safe and no traceroute is performed.

When performing traceroutes, the traceroute relies on a router sending an ICMP message back that the packet that was sent was dropped. Not all routers reply to this, and packets can also be load balanced, causing the traceroute to return multiple paths on multiple tries. To reduce this behavior, 10 queries per hop are sent. The value in which a reply from a hop should be received (timeout value) is also changed from 3 to 5 seconds to give routers on the path more time to reply.

Traceroute measurements performed via RIPE ATLAS are done using paris-traceroute instead of regular traceroute. Paris-traceroute tries to keep the checksum of the ICMP packet consistent so routers on the internet that apply a per-flow load balancing algorithm keep forwarding the traceroute over the same path. Paris-traceroute doesn’t provide a solution to a router that implements a per-packet load-balancing algorithm. The per-packet load-balancing algorithm problem is tried to suppress by sending 10 queries per-hop. Unfortunately, it was not possible to use paris-traceroute for the tests performed via the NLNOG ring. Results from the NLNOG ring might be more error prone because of this.

4. Results

Gathering the test results is like making a snapshot of the internet. When the results are gathered, they represent the state of the network for a specific time. The results gathered from the NLNOG ring network were gathered on the 24th of February 2023. The results from RIPE ATLAS were gathered on the 27th of January 2023.

The traceroutes provides the IP-address of a router. Because of load-balancing and time-outs, a lot of false positives occurred where the script detected an unequal path which was in fact just a timeout or load-balancing taking place. To reduce false positives, entities are looked at at AS or prefix level. The IP-address of a router is part of a prefix that is announced via BGP. Usually, a set of routers handle the same traffic, this set of routers are usually part of the same prefix. For all the IP-addresses in the traceroutes, the corresponding prefix and AS was looked up.

4.1 NLNOG Ring

A total of 556 sources were tested using IPv4. Of those sources, 335 (60.25%) sources reached the valid announcement and 221 sources (39.75%) reached the invalid announcement.

A total of 556 sources were tested using IPv6. Of those sources, 401 (72.12%) sources reached the valid announcement and 155 sources (27.88%) reached the invalid announcement.

The table below displays how many unique AS's, prefixes or IP-addresses occur in the results that reached the invalid announcement based on the IP version used. A lot of unique IP addresses can be seen, which are part of fewer prefixes which are part of even fewer AS’s.

	IPv4	IPv6
AS	83	95
Prefix	94	103
IP	240	182

NLNOG RING top 20 IPv4 AS

Count	**ASN**
32	7473
31	8283
13	8455
4	34984
4	24961
3	6461
3	31027
3	16276
2	50304
2	48635
2	47605
2	42695
2	34762
2	31122
2	197731
2	16302
2	16097
2	13030
1	9112
1	9009

NLNOG RING top 20 IPv4 prefixes

Count	**Prefix**
32	203.208.128.0/17
31	94.142.240.0/21
11	95.142.96.0/20
4	195.66.224.0/21
3	64.124.0.0/15
3	194.182.96.0/21
2	92.63.168.0/21
2	89.163.128.0/17
2	87.236.152.0/21
2	5.180.132.0/22
2	185.49.142.0/24
2	109.104.32.0/19
1	95.214.17.0/24
1	93.92.96.0/22
1	91.90.40.0/21
1	91.212.242.0/24
1	91.205.212.0/22
1	91.205.184.0/22
1	91.201.164.0/22
1	91.123.204.0/22

NLNOG RING top 20 IPv4 IP’s

Count	**IP**
30	203.208.153.246
26	80.249.211.217
20	203.208.158.186
5	203.208.166.242
4	203.208.182.250
3	95.142.106.62
3	94.142.244.32
3	203.208.182.253
3	185.49.142.16
2	92.63.170.192
2	87.236.154.212
2	82.195.67.90
2	195.66.227.118
2	193.239.117.111
2	185.96.186.118
2	168.209.201.28
2	145.145.128.4
2	10.95.81.8
2	10.95.81.10
2	109.104.61.53

NLNOG RING top 20 IPv6 AS

Count	**ASN**
5	8455
4	42525
4	202053
4	16276
3	3741
3	13030
2	8365
2	48635
2	42695
2	30844

2	29838
2	24961
2	20860
2	197731
1	8717
1	8648
1	8560
1	8468
1	8283
1	7642

NLNOG RING top 20 IPv6 prefixes

Count	**Prefix**
5	2a00:1188::/29
4	2a01:7e8::/32
3	2c0f:fc00::/27
3	2a04:3540::/32
2	2a05:1500:ff00::/40
2	2a03:7900::/32
2	2a00:5641::/32
2	2001:4ba0::/32
2	2001:41d0::/32
2	2001:41b8::/32
2	2001:1b40::/32
1	2c0f:fe40::/32
1	2a10:fc40::/29
1	2a10:b880::/32
1	2a0f:9200::/48
1	2a0e:46c7::/48
1	2a0d:3e80::/29
1	2a0b:a700::/29
1	2a0b:8f80::/48
1	2a09:d380::/30

NLNOG RING top 20 IPv6 IP’s

Count	**IP**
3	2a04:b907::16
2	2a00:5641:12e::7
2	2a00:1188:4::3c01
1	ffff:185.96.186.60
1	fc00:c:0:1:e::16
1	fc00:10:44:0:36::1
1	2c0f:fe40:2::81
1	2c0f:fe40:2::3f
1	2c0f:fc00:2:72::2
1	2c0f:fc00:2:70::2
1	2c0f:fc00:2:63::2
1	2c0f:fc00:2:62::2
1	2c0f:fc00:2:53::1
1	2c0f:fc00:2:48::1
1	2c0f:fc00:2:37::2
1	2c0f:fc00:0:8::4
1	2c0f:fc00:0:8::26
1	2c0f:fc00:0:7::4
1	2c0f:fc00:0:7::26
1	2c0f:fc00:0:6::94

4.2 RIPE ATLAS

A total of 11428 sources were tested using IPv4. Of those sources, 5479 (47.94%) sources reached the valid announcement and 5949 (52.06%) sources reached the invalid announcement.

A total of 5365 sources were tested using IPv6. Of those sources, 2939 (54.78%) sources reached the valid announcement and 2426 (45.22%) sources reached the invalid announcement.

The table below displays how many unique AS's, prefixes or IP-addresses occur in the results that reached the invalid announcement based on the IP version used. A lot of unique IP addresses can be seen, which are part of fewer prefixes which are part of even fewer AS’s.

	IPv4	IPv6
AS	957	505
Prefix	1505	591
IP	3597	1657

RIPE ATLAS top 20 IPv4 AS

Count	ASN
433	3320
367	7473
145	1273
127	3209
110	6762
103	6830

95	8881
94	12389
90	5400
89	15557
87	20965
80	9498
77	34984
67	13030
58	16276
52	6805
52	6461
52	5410
43	24940
40	8359

RIPE ATLAS top 20 IPv4 prefixes

Count	ASN	Prefix
358	7473	203.208.128.0/17
293	3320	62.154.0.0/15
131	1273	195.2.0.0/19
119	3209	145.254.0.0/20
103	6830	84.116.0.0/16
90	6762	195.22.192.0/19
85	8881	62.214.0.0/16
82	20965	62.40.96.0/19
72	34984	195.66.224.0/21
65	13030	5.180.132.0/22
52	6805	62.52.0.0/14
49	6461	64.124.0.0/15
43	3320	62.156.0.0/14
43	12389	87.226.128.0/17
40	24940	213.239.192.0/18
38	8359	212.188.0.0/17
38	5410	212.194.0.0/15
35	8657	195.8.0.0/19
35	20712	90.155.0.0/18
33	5432	91.183.0.0/16

RIPE ATLAS top 20 IPv6 ASN's

Count	ASN
303	3320
205	12322
126	2860
93	1273
74	8881
57	3209
45	13030
41	5400
35	6805
31	8657
30	9498
29	20712
28	24940
25	8422
24	9198
24	47583
24	15557
23	60294
23	5432
21	8447

RIPE ATLAS top 20 IPv6 prefixes

Count	**ASN**	**Prefix**
303	3320	2003::/19
124	2860	2a01:8::/29
93	1273	2001:5000::/21
74	8881	2001:1438::/32
44	13030	2a00:5641::/32
41	5400	2a00:2000::/22
41	12322	2a01:e00::/32
35	6805	2a02:3000::/23
35	12322	2a01:e03::/32
35	12322	2a01:e02::/32
32	3209	2a00::/22
31	8657	2001:15d8::/32
30	9498	2404:a800::/48
29	20712	2001:8b0::/32
28	24940	2a01:4f8::/32
28	12322	2a01:e34::/32
27	12322	2a01:e01::/32
26	12322	2a01:e05::/32
25	8422	2001:4dd0::/32
24	9198	2a00:12f8::/32

5. Analysis

5.1 NLNOG

Results from the tests performed on the NLNOG RING show that for both IPv4 and IPv6 more than half of all the sources end up at the valid destination. IPv6 also has a bit higher percentage of sources that reach the valid destination compared to IPv4.

Something that is also interesting is that the top IPv4 ASN is AS 7473. This is the top AS for IPv4 but the AS does not occur in the last at all in the IPv6 results. This might be because AS7473 does not provide IPv6 services, or that AS7473 has implemented ROV for their IPv6 network.

5.2 RIPE ATLAS

Results from the tests performed show that a lot of sources are vulnerable for reaching prefixes that are advertised in an invalid way. IPv6 is a little bit less vulnerable than IPv4 as can be seen in the results. With IPv4, 52.06% of the sources reached the invalid announcement versus 45.22% for IPv6. This can have a few causes. One of the possible causes is that operators that deployed IPv6 are a bit more technological advanced and see the positives of implementing ROV and the need for dropping invalid routes. Another reason could be that operators are worried that dropping invalid routes on their networks breaks their networks. These operators see IPv6 as something that is a little less important than IPv4 because it is not used as often, and all services are still reachable over IPv4 if IPv6 breaks. This mindset causes them to dare to implement ROV for IPv6 but not for IPv4.

The results show which AS's and prefixes are marked as non-validating most often. If these entities would implement ROV and drop invalid routes they would make a bigger impact on global routing security than entities that occur less frequently.

Something interesting from the results is that the top ASN at the IPv4 results does not match the top ASN at the prefix results. This is caused by AS 3320 (Deutsche Telekom AKA T-Mobile) announcing more routes, which individually occur multiple times while AS 7473 (Singapore telecommunications) announces one big prefix. This could be explained by the sources from which the tests were performed using AS3320 a lot. Deutsche Telekom has a huge European network which is probably used a lot by many source locations. The single big prefix from Singtel can also be explained by all the sources trying to reach the valid announcement in Singapore via Singtel which steered them right back to Amsterdam!

6. Conclusion

BGP is the protocol that enables the internet to work. However, the protocol is prone to a set of attacks that can harm internet users. Traffic can be rerouted or eavesdropped on by malicious actors or by misconfigured network equipment. RPKI is a technique to help to prevent these attacks which has seen increasing adoption. RPKI enables the owner of a prefix to cryptographically sign how their owned resources will be announced on the Internet. When other network operators receive a prefix advertised by a neighbor, a check is performed to validate if the originating AS in the advertisement is also authorized to originate the prefix. ROV can help with detecting and preventing route hijacks. ROV does not protect against rerouting attacks.

Which of the routers on a path to the invalid announcement is not validating, can be discovered by advertising two prefixes from two locations. One of the prefixes has a valid ROA, the other prefix is more specific and does not have a valid ROA. When performing traceroutes to IP-addresses in the valid and the invalid, more specific prefix, a non-validating router can be discovered. When the two traceroutes both take the same path to both IP-addresses in both prefixes, this proves that no routers on the path installed the more-specific invalid route. If both traceroutes start to take a different path somewhere, this may mean that a router on the path installed the invalid route.

Tests were performed to analyze if some non-validating routers occur multiple times. This turned out to be the case. In theory, when the routers that occur a lot of times in the test results implement

ROV, they have a bigger impact on improving resistance against invalid announcements and thus improving routing security. In the results, differences between IPv4 and IPv6 can also be observed. ROV has a higher adoption rate for IPv6 compared to IPv4 if looking at the results.

7. Future work

The research didn't look into combining the results from the tests performed on the NLNOG ring and RIPE ATLAS. It could be that there is an overlap between the list of non-validating routers that were discovered using NLNOG ring and RIPE ATLAS.

Another thing that could be done with this research is running the script weekly or monthly to monitor the adoption rate of ROV.

Something that would also make the research better is using more sources to perform traceroutes from, and announcing more prefixes from more geographically diverse regions to see if there are differences or similarities.

8. References

[1] Hawkinson, J. and Bates, T. (1996) *Guidelines for creation, selection, and registration of an autonomous system (AS)*, *Guidelines for creation, selection, and registration of an Autonomous System (AS)*. Available at: https://www.rfc-editor.org/rfc/rfc1930.html (Accessed: February 22, 2023).

[2] *What is BGP? | BGP routing explained | cloudflare* (no date) *What is BGP? | BGP routing explained*. Cloudflare. Available at: https://www.cloudflare.com/learning/security/glossary/what-is-bgp/ (Accessed: February 22, 2023).

[3] Tofoni, T., Luciani, F. and Eltigani, H. (2020) *What is BGP prefix hijacking? (Part 1)*. MANRS. Available at: https://www.manrs.org/2020/09/what-is-bgp-prefix-hijacking-part-1/ (Accessed: February 22, 2023).

[4] van Rossum, T. (2020) *BGP security and the future: A meta-analysis of BGP threats and security to provide a new direction for practical BGP security*, *BGP security and the future*. TU Delft. Available at: https://repository.tudelft.nl/islandora/object/uuid:794ce56f-3cd3-46a9-98a0-023e911c856d/datastream/OBJ/download (Accessed: February 22, 2023).

[5] Patel, H.B. and Patel, D.R. (2009) *Performance Analysis of BGP Security Proposals*. Available at: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=44378bcac48392cad9820783aa5e4fac4fc65b0b (Accessed: February 22, 2023).

[6] Crone, M. (2021) *Analyzing adoptability of secure BGP routing proposals*. KTH Royal Institute of Technology. Available at: https://maxcrone.org/assets/docs/2021-02-01-secure-bgp-adoption.pdf (Accessed: February 22, 2023).

[7] (2019) *What is RPKI?* RIPE NCC. Available at: https://www.ripe.net/manage-ips-and-asns/resource-management/rpki/what-is-rpki (Accessed: February 22, 2023).

[8] (no date) *Resource Certification (RPKI)*. ARIN. Available at: https://www.arin.net/resources/manage/rpki/ (Accessed: February 22, 2023).

[9] Lepinski, M. and Kent, S. (2012) *An infrastructure to support secure internet routing*, *An Infrastructure to Support Secure Internet Routing*. rfc-editor.org. Available at: https://www.rfc-editor.org/rfc/rfc6480 (Accessed: February 22, 2023).

[10] Datta, A. and Khan, Z. (2020) *What is route origin validation?* MANRS. Available at: https://www.manrs.org/2020/10/what-is-rov/ (Accessed: February 22, 2023).

[11] Lepinski, M., Kent, S. and Kong, D. (2012) *A profile for route origin authorizations (roas)*, *RFC Editor*. BBN Technologies. Available at: https://www.rfc-

editor.org/rfc/rfc6482.html#section-3.2 (Accessed: February 22, 2023).

[12] Rodrigues, C., & Giotsas, V. (2022, December 16). *Helping build a safer internet by measuring BGP RPKI route origin validation*. Helping build a safer Internet by measuring BGP RPKI Route Origin Validation. Retrieved February 23, 2023, from https://blog.cloudflare.com/rpki-updates-data/

[13] Van Hove, K. (2022, July 19). *Where did my packet go? measuring the impact of Rpki Rov*. Where Did My Packet Go? Measuring the Impact of RPKI ROV. Retrieved February 23, 2023, from https://labs.ripe.net/author/koen-van-hove/where-did-my-packet-go-measuring-the-impact-of-rpki-rov/

[14] Mohapatra, P. *et al.* (2013) *BGP prefix origin validation*, *BGP Prefix Origin Validation*. Available at: https://www.rfc-editor.org/rfc/rfc6811 (Accessed: February 23, 2023).

9. Acknowledgements

This research wouldn't have been possible without the support from Willem Toorop and Koen van Hove from NLnet Labs. They supported me during the research and provided me with the necessary infrastructure (BGP speakers, AS numbers etc.) to perform the research. I would like to thank them for their support.

Appendix A: Scripts and raw results

All the scripts that were used in this report can be found in the Gitlab repository hosted by OS3, which is only available for authorized personnel. The repository also contains all the tables and raw results that were used in this report. The repository can be found here: https://gitlab.os3.nl/kklercq/rp1-scripts

Appendix B: RIPE ATLAS Measurements

The RIPE ATLAS measurements are publicly available at the following locations for IPv4 measurements:

- DNS Check: https://atlas.ripe.net/measurements/49174309
- Traceroute to 185.49.142.16 (Invalid) https://atlas.ripe.net/measurements/49174310
- Traceroute to 185.49.143.16 (Valid) https://atlas.ripe.net/measurements/49174311

The measurements made over IPv6 can be found here:

- DNS Check: https://atlas.ripe.net/measurements/49174306
- Traceroute to 2a04:b907::16 (Invalid) https://atlas.ripe.net/measurements/49174307
- Traceroute to 2a04:b907:1::16 (Valid) https://atlas.ripe.net/measurements/49174308