SIDR Operations
Internet-Draft
Intended status: Informational
Expires: September 11, 2019

Z. Yan
J. Yao
CNNIC
X. Liu
ISCAS
G. Geng
CNNIC
Y. Fu

March 10, 2019

Problem Statement and Considerations for ROAs issued with Multiple Prefixes
draft-yan-sidrops-roa-considerations-02

Abstract

The address space holder needs to issue an ROA object when it authorizes one or more ASes to originate routes to multiple prefixes. During the process of ROA issuance, the address space holder needs to specify an origin AS for a list of IP prefixes. Besides, the address space holder has a free choice to put multiple prefixes into a single ROA or issue separate ROAs for each prefix based on the current specification. This memo analyzes and presents some operational problems which may be caused by the misconfigurations of ROAs containing multiple IP prefixes. Some suggestions and considerations also have been proposed.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Route Origin Authorization (ROA) is a digitally signed object which is used to identify that a single AS has been authorized by the address space holder to originate routes to one or more prefixes within the address space[RFC6482].If the address space holder needs to authorize more than one ASes to advertise the same set of address prefixes, the holder must issue multiple ROAs, one per AS number. However, at present there are no mandatory requirements in any RFCs describing that the address space holders must issue a separate ROA for each prefix or a ROA for multiple prefixes.

Each ROA contains an "asID" field and an "ipAddrBlocks" field. The "asID" field contains one single AS number which is authorized to originate routes to the given IP address prefixes. The "ipAddrBlocks" field contains one or more IP address prefixes to

which the AS is authorized to originate the routes. The ROAs with multiple prefixes is a common case that each ROA contains exactly one AS number but may contain multiple IP address prefixes in the operational process of ROA issuance.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Problem statement and Analysis

3.1. Statistical analysis

As mentioned above, the address space holder needs to issue an ROA object when it authorizes one or more ASes to originate routes to multiple prefixes. During the process of ROA issuance, the address space holder needs to specify an origin AS for a list of IP prefixes. Besides, the address space holder has a free choice to put multiple prefixes into a single ROA or issue separate ROAs for each prefix based on the current specification.

On our RPKI testbed, the Trust Anchor Locator (TAL) files configured by RP correspond to the five RIRs' RPKI Trust Anchors. By using these TAL files, all the ROA objects issued in each region (the five RIRs) around the world are collected and validated with the RPKI Relying Party tools provided by rpki.net. According to the analysis on these data, some statistical results are described in Table. 1.

The total number of ROAs	The number of ROAs with a single prefix	The number of ROAs with multiple prefixes
7166	3307	3859

Table.1 Statistical results of all ROAs

As shown in Table. 1, by the July 4, 2017, the total number of ROA objects issued around the world is about 7166. The result is in accordance with the statistics provided by RIPE NCC and Internet Multifeed Co. (MF). Based on the further analysis on these ROA objects, it is found that: the number of ROAs containing only one prefix is about 3307 (account for 46.1% of all ROA objects), and the number of ROAs containing two or more prefixes is about 3859 (account for 53.9% of all ROA objects).

In the 3859 ROA objects which each one contains two or more prefixes, the number of IP address prefixes are calculated and analyzed. The statistical results are shown in Table. 2.

The number of prefixes	The number of ROAs	The average number of prefixes in each ROA
37367	3859	9.68

Table. 2 Statistical results of the 3859 ROAs

As described in Table. 2, there are 37367 IP address prefixes in the 3859 ROA objects. And the average number of prefixes in each ROA is 9.68 (37367/3859). In addition, four types of ROAs are analyzed and calculated in the 3859 ROAs: ROAs each contains 2-10/11-50/51-100/>100 IP address prefixes. The statistical results are presented in Table. 3.

ROA types	ROA with 2-10 prefixes	ROA with 11-50 prefixes	ROA with 51-100 prefixes	ROA with >100 prefixes	Total
The number of ROAs	3263	496	60	40	3859
The ratio of ROAs	84.56%	12.85%	1.55%	1.04%	100.00%
The number of prefixes	12442	10365	4125	10435	37367
The ratio of prefixes	33.30%	27.74%	11.04%	27.93%	100.00%

Table. 3 Statistical results of four types of ROAs

As shown in Table. 3, taking the first type of ROA as an example, there are 3263 ROAs (account for 84.56% of the 3859 ROA objects) which each contains 2-10 IP address prefixes, and the total number of IP prefixes in these 3263 ROAs is 12442 (account for 33.29% of the 37367 prefixes).

According to the third row (the ratio of ROAs) in Table. 3, it shows the trend that the address space holders tend to issue each ROA object with fewer IP prefixes (more than 60% of ROAs containing less than 50 prefixes), but they still tend to put multiple prefixes into one single ROA.

It should also be paid more attention that among all the ROAs issued today, a single ROA may contain a large number of IP address prefixes. In the statistical results, it is found that there exists two ROAs (corresponding to ASN 24440 and ASN 23752) which each contains more than 700 IP address prefixes (796 and 892 respectively).

3.2. Experimental analysis

A large number of experiments for the process of ROA issuance have been made on our RPKI testbed, it is found that the misconfigurations during the issuance may cause the ROAs which have been issued to be revoked. The corresponding scenarios are as follows.

AS shown in Fig. 1, an ISP needed to issue two ROA objects respectively to authorize ASN 64500 to originate routes to IP prefixes 192.0.2.128/28 and ASN 64501 to originate routes to IP prefixes 198.51.100.128/28. The operations are simulated on our RPKI testbed.

```
         +-----------+
         |           |      ASNs:
         |   IANA    |----- 0-4294967295
         |           |      IP Prefixes:
         |           |      0.0.0.0/0
         +-----|-----+
               |            ASNs:
         +-----|-----+      64497-64510
         |           |      65537-65550
         |           |      IP Prefixes
         |   APNIC   ------ 192.0.2.118/25
         |           |      198.51.100.128/25
         |           |      203.0.113.128/25
         +-----|-----+
               |
         +-----|-----+      ASNs:
         |           |      64498-64505
         |           |      IP Prefixes
         |           |      192.0.2.128/26
         |  CNNIC    ------ 198.51.100.128/26
         |           |      203.0.113.128/26
         +-----|-----+
               |
         +-----|-----+
         |           |      ASNs:
         |           |      64500-64505
         |           |      IP Prefixes:
         |   ISP     ------ 192.0.2.128/27
         |           |      198.51.100.128/27
         |           |      203.0.113.128/27
         +-----+-----+
               |                     --------------
               |                 ////              \\\\
               |               //    ROA1:             \\
               ---------------| 64500->192.0.2.128/28    |
                             |       ROA2:                 |
                              | 64501->198.51.100.128/28 |
                               \\                      //
                                 \\\\              ////
                                     --------------
```

Fig. 1 Scenario of ROA issuance

The ROA objects issued by ISP could be checked with the "show_published_objects" command. And as shown in Fig. 2, ISP has issued two ROA objects M74Rq1am9m4YUairntkXTRAx6Wg.roa and vulw_jMZBy7-ktn7nyhlpchBKZY.roa to respectively authorize ASN 64500

to originate routes to IP prefixes 192.0.2.128/28 and ASN 64501 to originate routes to IP prefixes 198.51.100.128/28.

```
test@~$cat ISPROA.csv
192.0.2.128/28  64500 Group1
198.51.100.128/28  64501 Group2
test@~$ rpkic -i ISP load_roa_requests ISPROA.csv
test@~$ rpkic -i ISP show_published_objects
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/duPylfF7Hv31rpOa4dVVCZnRkmk.crl
2017-07-19T10:34:04Z 594CB167AF4E81424EBEA7C1A5FD8DDE216D5C69
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/duPylfF7Hv31rpOa4dVVCZnRkmk.mft
2017-07-19T10:34:04Z 17C98CBFB179D60D9D0A6D52C2629B7A8DEA8A9C
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/M74Rq1am9m4YUairntkXTRAx6Wg.roa
2017-07-19T09:20:20Z 0CFD927D1522BF43FC52B748F274646387569222
64500 192.0.2.128/28
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/vulw_jMZBY7-KTN7nyhlpchBKZY.roa
2017-07-19T10:34:04Z 305866D0c4ee5e156ebeda811d3540bf0e094043
64501 198.51.100.128/28
```

Fig. 2 Check the ROAs issued by ISP

Then, ISP wanted to authorize ASN 64501 to originate routes to another IP prefixes 203.0.113.128/28, so it modified the ISPROA.csv file and operated the "load_roa_requests" command again.

```
test@~$cat ISPROA.csv
192.0.2.128/28  64500 Group1
198.51.100.128/28  64501 Group2
203.0.113.128/28  64501 Group2
test@~$ rpkic -i ISP load_roa_requests ISPROA.csv
test@~$ rpkic -i ISP show_published_objects
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/duPylfF7Hv31rpOa4dVVCZnRkmk.crl
2017-07-19T10:38:03Z 2606EAA75AB60BE7785AE0CB0599D984AFD5BDB5
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/duPylfF7Hv31rpOa4dVVCZnRkmk.mft
2017-07-19T10:38:03Z 10F3F9249F0A6A636BF8143075693681B45A4BC2
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/M74Rq1am9m4YUairntkXTRAx6Wg.roa
2017-07-19T09:20:20Z 0CFD927D1522BF43FC52B748F274646387569222
64500 192.0.2.128/28
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/vO3whtjMpYxxyva4BxRqI2H8eqA.roa
2017-07-19T10:38:03Z 4B85FDBABEC567A9DD8DA5745B34A201390F4530
64501 198.51.100.128/28,203.0.113.128/28
```

Fig. 3 Add a new authorization

As shown in Fig. 3, so a new ROA object vO3WhtjMpYxxyva4BxRqI2H8eqA.roa which contained two IP prefixes was issued. It should be noticed that in the ISPROA.csv file the third column of the last two lines (with respect to ASN 64501) are set as

the same label "Group2" to make sure that the authorizations to the two IP prefixes will be issued into a single ROA.

Now, ISP wants to authorize ASN 64500 to originate routes to IP prefixes 203.0.113.128/28 as well, but when it modifies the ISPROA.csv file, it appends 204.0.113.128/28 (or any prefixes that do not belong to ISP) instead of 203.0.113.128/28 into the ISPROA.csv file by mistake. And then, when it operates the "load_roa_requests" command, something unexpected happened.

```
test@~$cat ISPROA.csv
192.0.2.128/28  64500 Group1
204.0.113.128/28 64500 Group1
198.51.100.128/28  64501 Group2
203.0.113.128/28  64501 Group2
test@~$ rpkic -i ISP load_roa_requests ISPROA.csv
test@~$ rpkic -i ISP show_published_objects
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/duPylfF7Hv31rpOa4dVVCZnRkmk.crl
2017-07-19T12:39:47Z 2DD037213237D72AF6CE95F8F37D1F08E8B49A37
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/duPylfF7Hv31rpOa4dVVCZnRkmk.mft
2017-07-19T12:39:47Z 735D9723B8C6D8214DA78117D27E529AA47E14B6
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/vO3whtjMpYxxyva4BxRqI2H8eqA.roa
2017-07-19T10:38:03Z 4B85FDBABEC567A9DD8DA5745B34A201390F4530
64501 198.51.100.128/28,203.0.113.128/28
```

Fig. 4 Add an incorrect authorization by mistake

As shown in Fig. 4, a legitimate ROA object was revoked because of ISP's misconfiguration. Obviously, this misconfiguration may lead to some serious consequences to RPKI (such as legitimate BGP routes are misclassified as "not found").

3.3. Problem statement

It shows that the misconfigurations of ROAs containing multiple IP address prefixes may lead to much more serious consequences than ROAs with fewer IP address prefixes. According to the above statistical and experimental analysis, misconfigurations of the ROAs which contain more than 300 IP address prefixes may cause a large-scale network interruption.

Another potential influence of misconfigurations of ROAs containing multiple IP prefixes on BGP routers may be considered. For the ROA containing multiple prefixes, once increase or delete one <AS, ip_prefix> pair in it, this ROA will be reissued. Through sychronization with repository, RPs fetch a new ROA object and then notify and send all the <AS, ip_prefix> pairs in this ROA to BGP routers. That is to say, the update of the ROA containing multiple

IP address prefixes will lead to redundant transmission between RP and BGP routers . So frequent update of these ROAs will increase the convergency time of BGP routers and reduce their performance obviously.

4. Suggestions and Considerations

Based on the statistical and experimental analysis, following suggestions should be considered during the process of ROA issuance:

1) The issuance of ROAs containing a large number of IP prefixes may lead to misconfigurations more easily than ROAs with fewer IP prefixes.

A ROA which contains a large number of IP prefixes is more vulnerable to misconfigurations, because any misconfiguration of these prefixes may cause the legitimate ROA to be revoked. Besides, since the misconfigurations of ROAs containing a larger number of IP address prefixes may lead to much more serious consequences (a large-scale network interruption) than ROAs with fewer IP address prefixes, it is suggested to avoid issuing ROAs with a large number of IP address prefixes.

So it is also recommended in the last paragraph of the section 4.2.5 of [I-D.ietf-sidr-rpki-validation-reconsidered] that opterators MAY issue separate ROAs for each IP address prefix, so that the loss of on IP address prefix from the VRS-IP of any certificate along the path to the trust anchor would not invalidate authorizations for other IP address prefixes.

2) The number of ROAs containing multiple IP prefixes should be limited and the number of IP prefixes in each ROA should also be limited.

The extreme case (a single ROA can only contain one IP address prefix) may lead to too much ROA objects globally, which may in turn become a burden for RPs to synchronize and validate all these ROA objects with the fully deployment of RPKI. So a tradeoff between the number of ROAs and the number of IP prefixes in a single ROA should be considered.

3) A safeguard scheme is essential to protect the process of ROA issuance

Considering the misconfigurations during the process of ROA issuance are inevitable and the serious consequences they may lead to, a safeguard scheme to protect and monitor the process of ROA issuance should be considered.

5. Security Considerations

TBD.

6. IANA Considerations

This document does not request any IANA action.

7. Acknowledgements

The authors would like to thanks the valuable comments made by members of sidrops WG.

This document was produced using the xml2rfc tool [RFC2629].

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", RFC 6482, DOI 10.17487/RFC6482, February 2012, <https://www.rfc-editor.org/info/rfc6482>.

8.2. Informative References

[I-D.ietf-sidr-rpki-validation-reconsidered]
Huston, G., Michaelson, G., Martinez, C., Bruijnzeels, T., Newton, A., and D. Shaw, "RPKI Validation Reconsidered", draft-ietf-sidr-rpki-validation-reconsidered-10 (work in progress), December 2017.

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, DOI 10.17487/RFC2629, June 1999, <https://www.rfc-editor.org/info/rfc2629>.

Authors' Addresses

Zhiwei Yan
CNNIC
No.4 South 4th Street, Zhongguancun
Beijing, 100190
P.R. China

Email: yanzhiwei@cnnic.cn

Jiankang Yao
CNNIC
4 South 4th   Street,Zhongguancun,Haidian   District
Beijing, Beijing 100190
China

Phone: +86 10   5881 3007
Email: yaojk@cnnic.cn

Xiaowei Liu
ISCAS
Institute of Software Chinese Academy of Sciences
Beijing, 100190
P.R. China

Email: liuxiaowei@iscas.ac.cn

Guanggang Geng
CNNIC
No.4 South 4th Street, Zhongguancun
Beijing, 100190
P.R. China

Email: gengguanggang@cnnic.cn

Yu Fu

Email: eleven711711@foxmail.com