Problem Statement and Considerations for ROA Mergence

draft-yan-sidr-roa-mergence-00

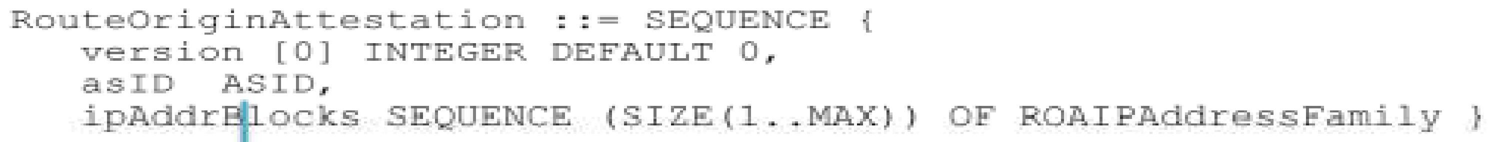
@IETF 96 SIDR meeting

fuyu@cnnic.cn

Background—RFC 6482

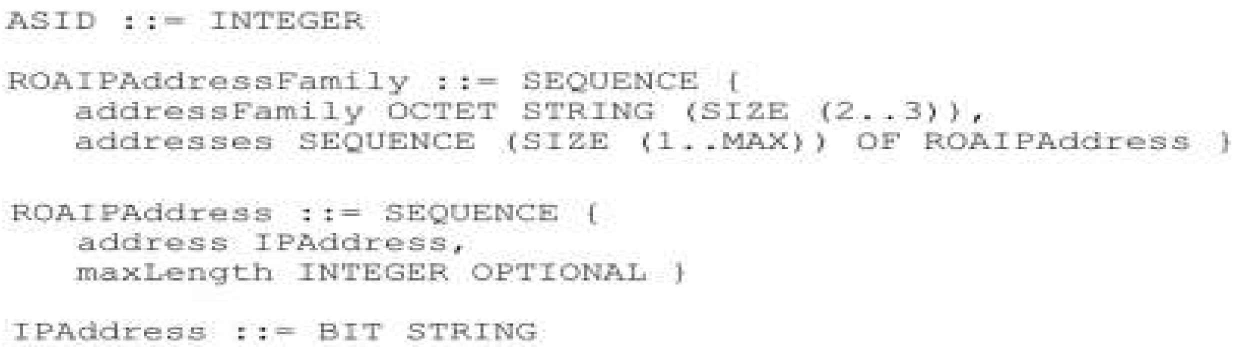
A ROA is a digitally signed object that provides a means of verifying that an IP address block holder has authorized an Autonomous System (AS) to originate routes to one or more prefixes within the address block.

ROAs are digitally signed objects that bind an address to an AS number, and are signed by the address holder.



```
RouteOriginAttestation ::= SEQUENCE {
   version [0] INTEGER DEFAULT 0,
   asID  ASID,
   ipAddrBlocks SEQUENCE (SIZE(1..MAX)) OF ROAIPAddressFamily }
```

The content of a ROA identifies a single AS that has been authorized by the address space holder to originate routes and a list of one or more IP address prefixes that will be advertised.
If the address space holder needs to authorize multiple ASes to advertise the same set of address prefixes, the holder issues multiple ROAs, one per AS number.



```
ASID ::= INTEGER

ROAIPAddressFamily ::= SEQUENCE {
   addressFamily OCTET STRING (SIZE (2..3)),
   addresses SEQUENCE (SIZE (1..MAX)) OF ROAIPAddress }

ROAIPAddress ::= SEQUENCE {
   address IPAddress,
   maxLength INTEGER OPTIONAL }

IPAddress ::= BIT STRING
```

ROA mergence

- What is the ROA mergence?
  - 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.

Statistical analysis

- By the April 19, 2016, the total number of ROA objects issued around the world is about 5027. the number of ROAs containing only one prefix is about 2341 (account for 46.6% of all ROA objects), and the number of ROAs containing two or more prefixes is about 2686 (account for 53.4% of all ROA objects).

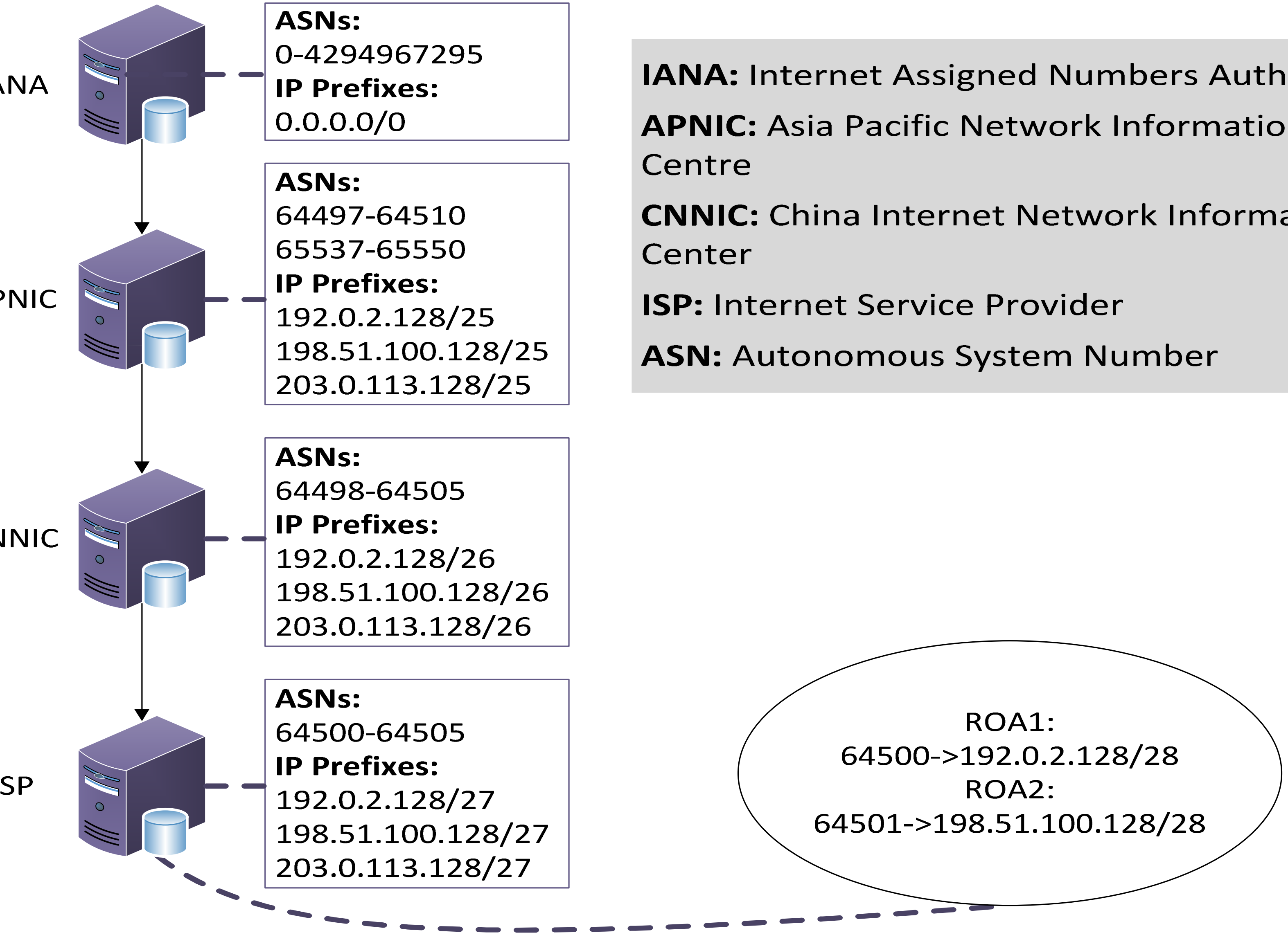
The total number of ROAs	The number of ROAs with a single prefix	The number of ROAs with multiple prefixes
5027	2341	2686

Statistical analysis

- There are 20379 IP address prefixes in the 2686 ROA objects. And the average number of prefixes in each ROA is 7.59

ROA types	Number of ROAs	ratio of ROAs	Number of prefixes	ratio of prefixes
ROA with 2-10 prefixes	2316	86.22%	8849	43.42%
ROA with 11-50 prefixes	325	12.10%	6563	32.20%
ROA with 51-100 prefixes	29	1.08%	1917	9.41%
ROA with >100 prefixes	16	0.60%	3050	14.97%
Total	2686	100.00%	20379	100.00%

Experimental analysis



ANA

ASNs:
0-4294967295
IP Prefixes:
0.0.0.0/0

PNIC

ASNs:
64497-64510
65537-65550
IP Prefixes:
192.0.2.128/25
198.51.100.128/25
203.0.113.128/25

NNIC

ASNs:
64498-64505
IP Prefixes:
192.0.2.128/26
198.51.100.128/26
203.0.113.128/26

SP

ASNs:
64500-64505
IP Prefixes:
192.0.2.128/27
198.51.100.128/27
203.0.113.128/27

IANA: Internet Assigned Numbers Authority

APNIC: Asia Pacific Network Information Centre

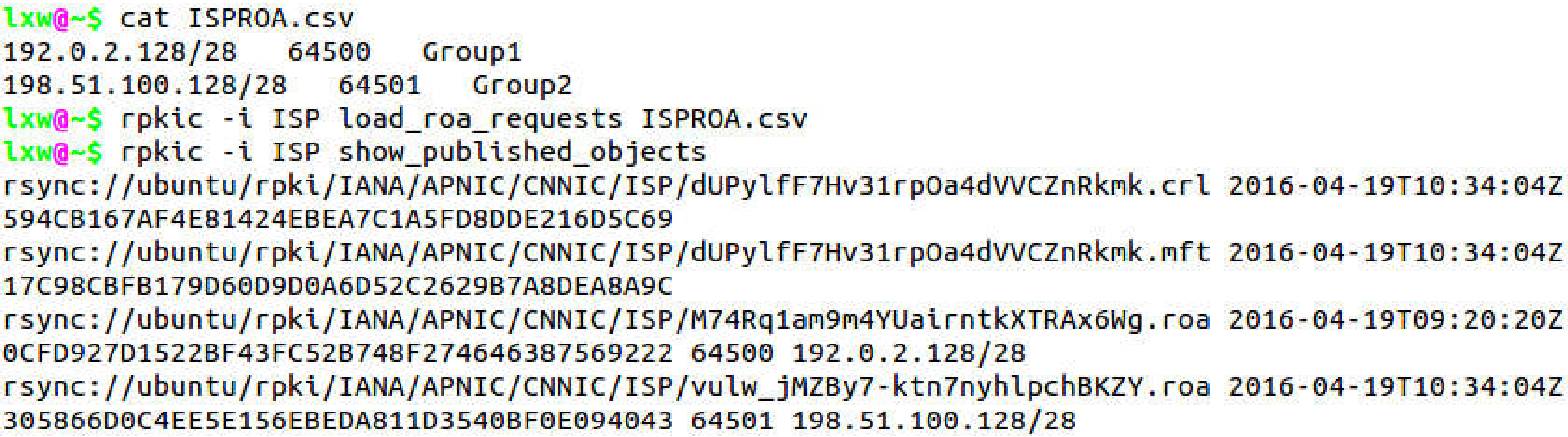
CNNIC: China Internet Network Information Center

ISP: Internet Service Provider

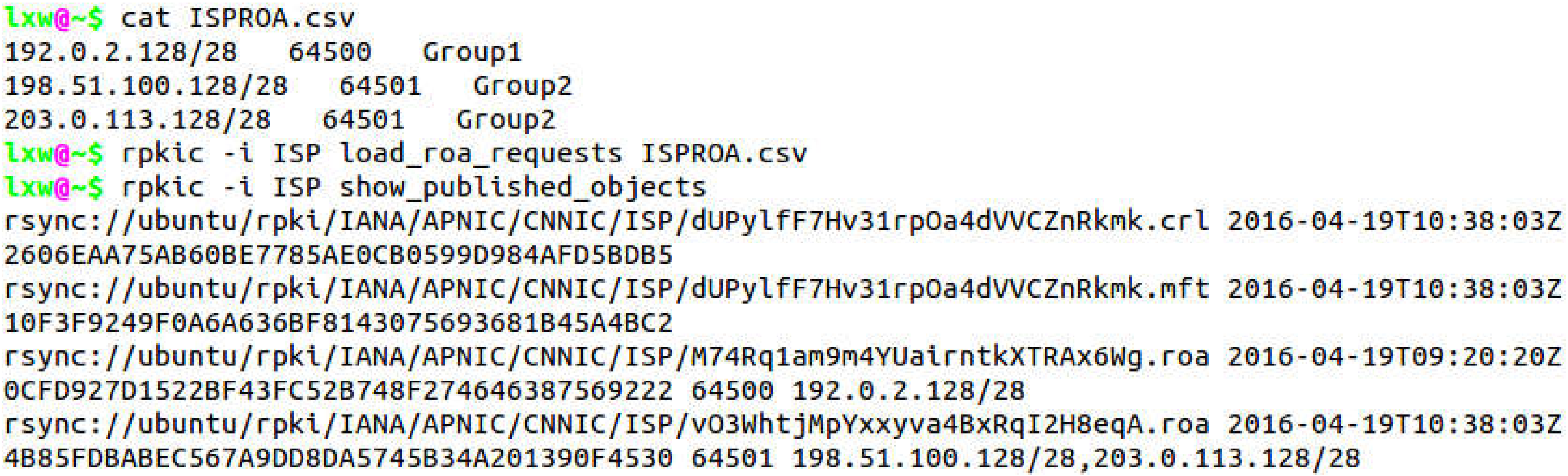
ASN: Autonomous System Number

ROA1:
64500->192.0.2.128/28
ROA2:
64501->198.51.100.128/28

Experimental analysis

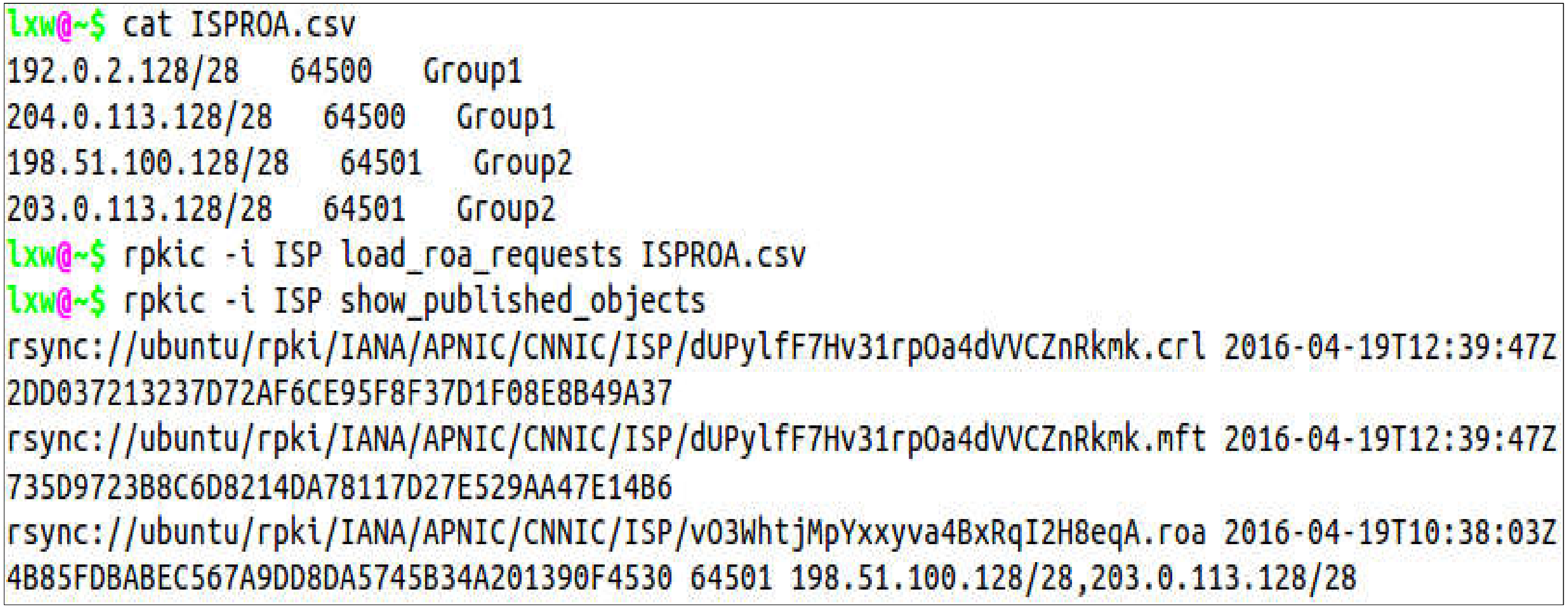


```
lxw@~$ cat ISPROA.csv
192.0.2.128/28    64500    Group1
198.51.100.128/28    64501    Group2
lxw@~$ rpkic -i ISP load_roa_requests ISPROA.csv
lxw@~$ rpkic -i ISP show_published_objects
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/dUPylfF7Hv31rpOa4dVVCZnRkmk.crl 2016-04-19T10:34:04Z
594CB167AF4E81424EBEA7C1A5FD8DDE216D5C69
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/dUPylfF7Hv31rpOa4dVVCZnRkmk.mft 2016-04-19T10:34:04Z
17C98CBFB179D60D9D0A6D52C2629B7A8DEA8A9C
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/M74Rq1am9m4YUairntkXTRAx6Wg.roa 2016-04-19T09:20:20Z
0CFD927D1522BF43FC52B748F274646387569222 64500 192.0.2.128/28
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/vulw_jMZBy7-ktn7nyhlpchBKZY.roa 2016-04-19T10:34:04Z
305866D0C4EE5E156EBEDA811D3540BF0E094043 64501 198.51.100.128/28
```



```
lxw@~$ cat ISPROA.csv
192.0.2.128/28    64500    Group1
198.51.100.128/28    64501    Group2
203.0.113.128/28    64501    Group2
lxw@~$ rpkic -i ISP load_roa_requests ISPROA.csv
lxw@~$ rpkic -i ISP show_published_objects
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/dUPylfF7Hv31rpOa4dVVCZnRkmk.crl 2016-04-19T10:38:03Z
2606EAA75AB60BE7785AE0CB0599D984AFD5BDB5
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/dUPylfF7Hv31rpOa4dVVCZnRkmk.mft 2016-04-19T10:38:03Z
10F3F9249F0A6A636BF8143075693681B45A4BC2
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/M74Rq1am9m4YUairntkXTRAx6Wg.roa 2016-04-19T09:20:20Z
0CFD927D1522BF43FC52B748F274646387569222 64500 192.0.2.128/28
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/vO3WhtjMpYxxyva4BxRqI2H8eqA.roa 2016-04-19T10:38:03Z
4B85FDBABEC567A9DD8DA5745B34A201390F4530 64501 198.51.100.128/28,203.0.113.128/28
```

Experimental analysis



```
lxw@~$ 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
lxw@~$ rpkic -i ISP load_roa_requests ISPROA.csv
lxw@~$ rpkic -i ISP show_published_objects
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/dUPylfF7Hv31rpOa4dVVCZnRkmk.crl 2016-04-19T12:39:47Z
2DD037213237D72AF6CE95F8F37D1F08E8B49A37
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/dUPylfF7Hv31rpOa4dVVCZnRkmk.mft 2016-04-19T12:39:47Z
735D9723B8C6D8214DA78117D27E529AA47E14B6
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/vO3WhtjMpYxxyva4BxRqI2H8eqA.roa 2016-04-19T10:38:03Z
4B85FDBABEC567A9DD8DA5745B34A201390F4530 64501 198.51.100.128/28,203.0.113.128/28
```

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 "invalid")

Problem statement

- The misconfigurations of ROAs containing multiple IP address prefixes may lead to much more serious consequences than ROAs with fewer IP address prefixes.

- 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 convergence time of BGP routers and reduce their performance obviously

Suggestions and Considerations

- 1) The issuance of ROAs containing a large number of IP prefixes may lead to misconfigurations more easily than ROAs with fewer IP 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.
- 3) A safeguard scheme is essential to protect the process of ROA issuance

Does this work make sense?

Join us ?

Comments?

Thank you

RPKI Deployment Considerations: Problem Analysis and Alternative Solutions

draft-lee-sidr-rpki-deployment-02

@IETF 96 SIDR meeting

fuyu@cnnic.cn

Background

- Our original intention is to write a informational draft for a guidance to introduce the ISP, NIR and etc. to deploy the RPKI, share the experience of our deployment, and include some considerations for the issues which they may encounter during the deployment process.
- We had a presentation at IETF 95 meeting. It has some feedback from the sidr WG during the IETF meeting.

Considerations of RPKI Deployment

RP issues

CA issues

Data Synchronization

Other issues

Considerations of RPKI Deployment

- **RP issues**

1) TA issues in RP-----More than One TA

  - there is no technical mechanism to prevent two or more TAs from asserting control over the same set of INRs accidentally or maliciously.
  - This kind of problem obviously may cause resource conflicts on the Internet

2) Data management---How to manage these signed objects after downloading them from repository

Considerations of RPKI Deployment

- **CA issues**
  1) Operational issues of CA behavior
     - Operational errors by CAs are inevitable and may cause significant impact on Internet routing. For example, an error in using a ROA (adding a new erroneous ROA or whacking an existing ROA) may cause all routes covered by the original ROA to become invalid or to assume an “unknown” security status.

Considerations of RPKI Deployment

- **CA issues**

2) Unilateral Resource Revocation

- In the RPKI architecture, there is a risk that CAs have the power to unilaterally revoke the INRs which have been allocated to their descendants, just by revoking corresponding CA certificates.
- The results can be significant. Specifically, all RPs will view the origin assertions by the CA (and its descendants) to be invalid. This may cause ISPs to de-preference routes to the affected prefixes.

Considerations of RPKI Deployment

- **Data Synchronization**

1) between the CA and repository

- A Publication Protocol for the Resource Public

Key Infrastructure (RPKI) **(**draft-ietf-sidr-publication-08 **)**

2) between the RP and repository

- rsync protocol
- RRDP protocol

3) Between the RP and BGP routers

RFC 6810: The Resource Public Key Infrastructure (RPKI) to Router Protocol

Considerations of RPKI Deployment

- **Other issues**
- Mirror World Attacks
  - In mirror world attacks, a malicious CA presents one view of the RPKI repository (that it manages) to some RPs, and a different view to others. (Because repository data may be cached by ISPs, it may not be possible for a malicious CA to provide erroneous results to a narrowly targeted set of RPs.)
- Staged and Incomplete deployment
- Low validation Coverage

Comments?

Call for adoption ?

Thank you