Misoperation or malicious operation of CA
Scenarios of unexpected resource assignment in RPKI

draft-fu-sidr-unexpected-scenarios-00

@IETF 94 meeting

fuyu@cnnic.cn

Background

- In the RPKI architecture, CA certificates attest to the INR holdings; EE certificates are primarily used for the validation of ROAs. And CAs are responsible for the allocation of these certificates. So CA is very important for the RPKI deployment.
- The misoperation and malicious operation of CA are inevitable and may cause significant impact.
- This draft describes and analyzes some scenarios of the unexpected resource assignment caused by CA in RPKI deployment.

Scenarios: case 1

- Unauthorized resource assignment
  - Completely unauthorized assignment:

    the resources to be allocated to subordinate node are without the ownership of CA.

  - Partially unauthorized assignment:

    the resources to be allocated to subordinate node are with the partially ownership of CA.

Scenarios: case 2

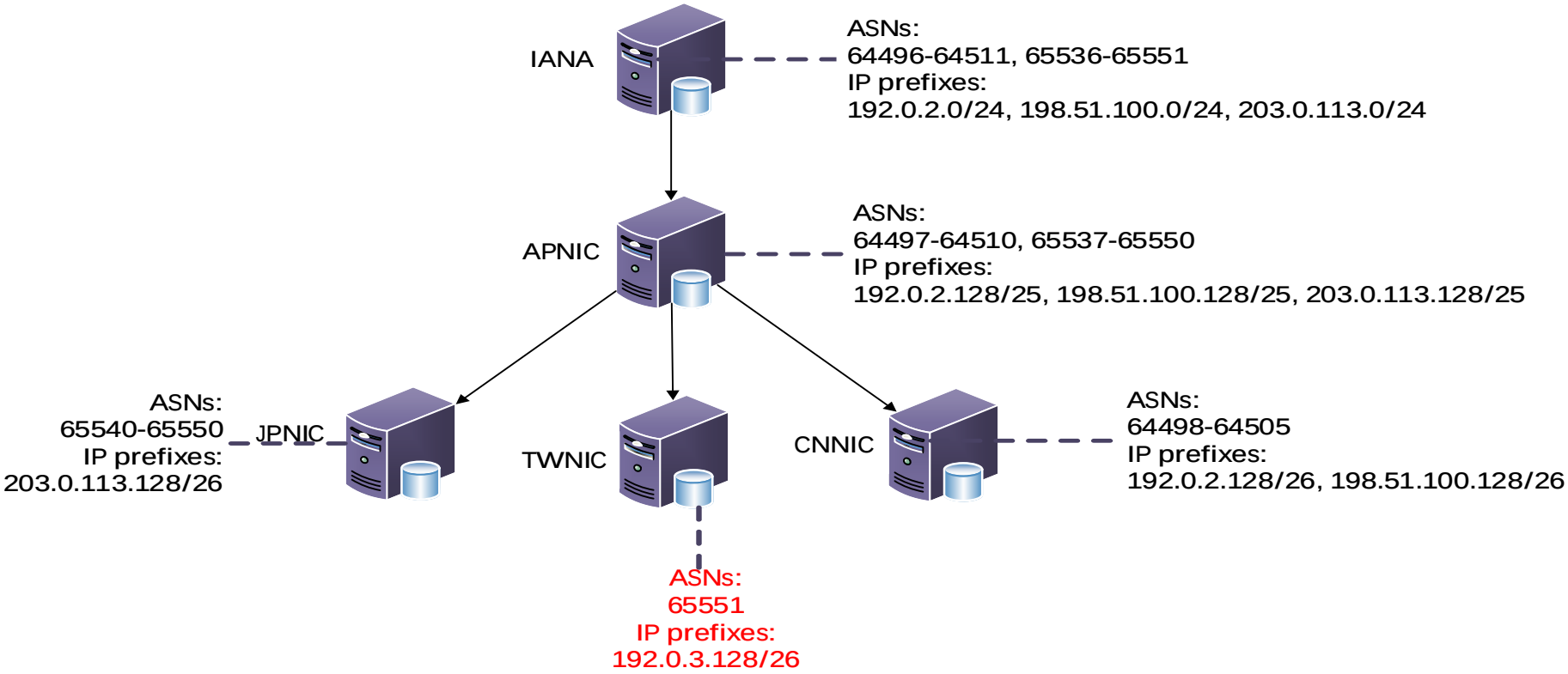
- Resource reassignment
  - Matching: the block of IP address which is reassigned is the same as which has been already assigned to the other sub-node.
  - Subset: The block of IP address which is reassigned is smaller than which has been already assigned to the other sub-node.
  - Intersection: The block of IP address which is reassigned has overlap with which has been already assigned to the other sub-node.

Scenarios: case 3

- Resource transfer
  - a block of IP addresses will be transferred from one sub-node to the other. This scenario is described in [I-D.ymbk-sidr-transfer] in more detail. The resource reassignment may happened in this scenario by the misoperation of the CA.

Test Result: case 1

- A CA (eg. APNIC) allocates a block of "IP Address" to subordinate node (eg. TWNIC). However, this CA doesn't own this block of IP Prefixes actually. So the TWNIC cannot use these addresses. This may be caused by mistake or misconfiguration.



Test Result: case 1

APNIC allocates the resource which doesn't belong to him to the TWNIC successfully . But the TWNIC could not see(receive) the resource as below

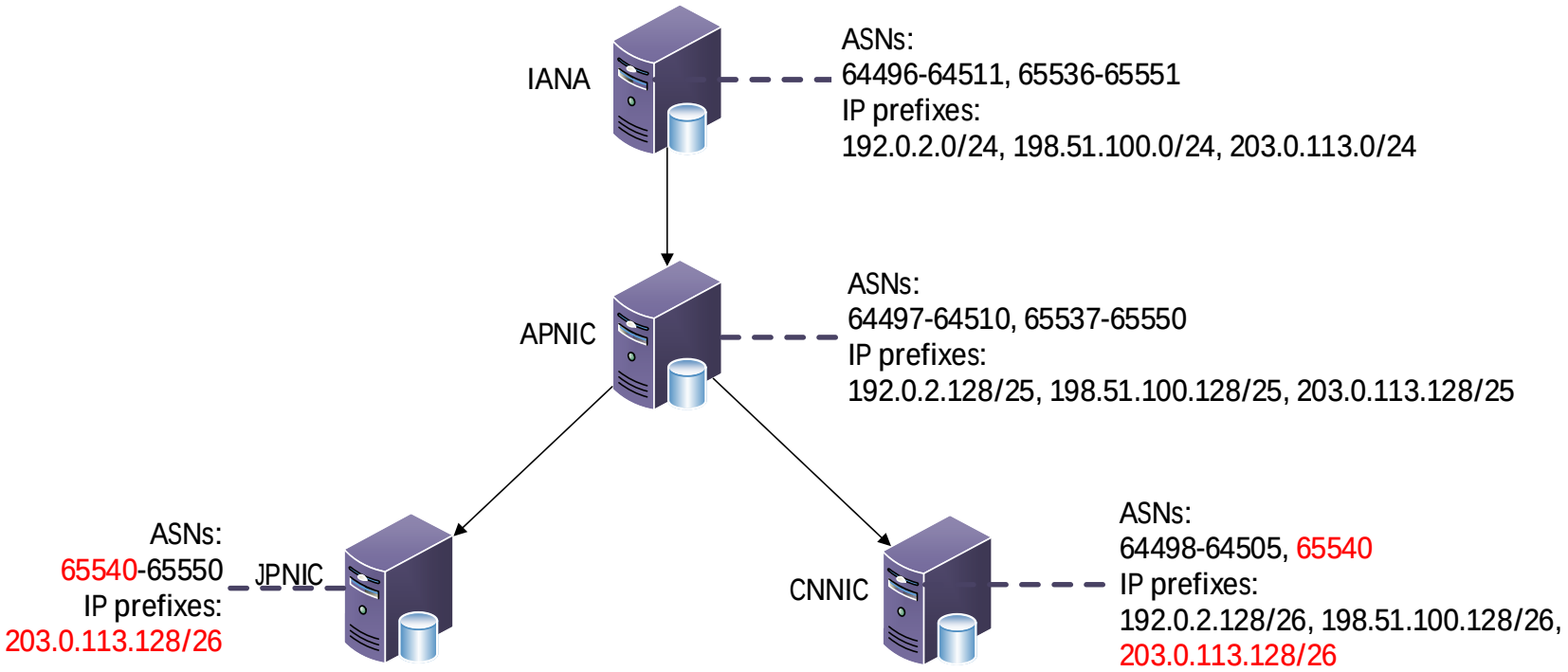
```
root@ubuntu:~# rpkic -i apnic load_asns apnic2cnnicjpnictwnic_asns.csv
root@ubuntu:~# rpkic -i apnic load_prefixes apnic2cnnicjpnictwnic_prefix.csv
```

```
root@ubuntu:~# cat apnic2cnnicjpnictwnic_asns.csv
cnnic    64498-64505
jpnic    65540-65550
twnic    65551
root@ubuntu:~# cat apnic2cnnicjpnictwnic_prefix.csv
cnnic    192.0.2.128/26
cnnic    198.51.100.128/26
jpnic    203.0.113.128/26
twnic    192.0.3.128/26
```

```
root@ubuntu:~# rpkic -i cnnic show_received_resources
Parent:       apnic
  notBefore:  2015-07-15T15:53:25Z
  notAfter:   2016-07-14T15:36:05Z
  URI:        rsync://localhost/rpki/iana/apnic/BqHiZw8I7JRhXby5cljW-Iy75c4.cer
  SIA URI:    rsync://localhost/rpki/iana/apnic/cnnic/
  AIA URI:    rsync://localhost/rpki/iana/RAseYE67qlpBd34u5UqhMjwq8c0.cer
  ASN:        64498-64505
  IPv4:       192.0.2.128/26,198.51.100.128/26
  IPv6:
root@ubuntu:~# rpkic -i jpnic show_received_resources
Parent:       apnic
  notBefore:  2015-07-15T15:25:54Z
  notAfter:   2016-07-14T15:20:04Z
  URI:        rsync://localhost/rpki/iana/apnic/NSt9KXs-a2py_OGZlOl4fipm1lQ.cer
  SIA URI:    rsync://localhost/rpki/iana/apnic/jpnic/
  AIA URI:    rsync://localhost/rpki/iana/RAseYE67qlpBd34u5UqhMjwq8c0.cer
  ASN:        65540-65550
  IPv4:       203.0.113.128/26
  IPv6:
root@ubuntu:~# rpkic -i twnic show_received_resources
root@ubuntu:~#
```

Test Result: case 2

- A CA(eg.APNIC) reassigns the resource to one sub-node (JPNIC) which has been already assigned to another sub-node(eg.CNNIC) by misoperation.



Test Result: case 2

Before allocation: APNIC shows the child node

```
root@ubuntu:~# rpkic -i apnic show_child_resources
Child: cnnic
Child: jpnic
```

After allocation: APNIC allocates the resource to the JPNIC and CNNIC

```
root@ubuntu:~# rpkic -i apnic load_asns apnic2cnnicjpnic_asns.csv
root@ubuntu:~# rpkic -i apnic load_prefixes apnic2cnnicjpnic_prefix.csv
```

```
root@ubuntu:~# cat apnic2cnnicjpnic_asns.csv
cnnic    64498-64505
cnnic    65540
jpnic    65540-65550
root@ubuntu:~# cat apnic2cnnicjpnic_prefix.csv
cnnic    192.0.2.128/26
cnnic    198.51.100.128/26
cnnic    203.0.113.128/26
jpnic    203.0.113.128/26
```

Verification by parent node: APNIC shows the child's resource

```
root@ubuntu:~# rpkic -i apnic show_child_resources
Child: cnnic
  ASN: 64498-64505,65540
 IPv4: 192.0.2.128/26,198.51.100.128/26,203.0.113.128/26
Child: jpnic
  ASN: 65540-65550
 IPv4: 203.0.113.128/26
```

Test Result: case 2

Verification by CNNIC: CNNIC shows his resources

```
root@ubuntu:~# rpkic -i cnnic show_received_resources
Parent:       apnic
  notBefore:  2015-07-15T15:37:58Z
  notAfter:   2016-07-14T15:36:05Z
  URI:        rsync://localhost/rpki/iana/apnic/BqHiZw8I7JRhXby5cljW-Iy75c4.cer
  SIA URI:    rsync://localhost/rpki/iana/apnic/cnnic/
  AIA URI:    rsync://localhost/rpki/iana/RAseYE67qlpBd34u5UqhMjwq8c0.cer
  ASN:        64498-64505,65540
  IPv4:       192.0.2.128/26,198.51.100.128/26,203.0.113.128/26
  IPv6:
```

Verification by JPNIC: JPNIC shows his resource

```
root@ubuntu:~# rpkic -i jpnic show_received_resources
Parent:       apnic
  notBefore:  2015-07-15T15:25:54Z
  notAfter:   2016-07-14T15:20:04Z
  URI:        rsync://localhost/rpki/iana/apnic/NSt9KXs-a2py_OGZlOl4fipm1lQ.cer
  SIA URI:    rsync://localhost/rpki/iana/apnic/jpnic/
  AIA URI:    rsync://localhost/rpki/iana/RAseYE67qlpBd34u5UqhMjwq8c0.cer
  ASN:        65540-65550
  IPv4:       203.0.113.128/26
  IPv6:
```

CNNIC and JPNIC could see the same resource assigned by the APNIC at the same time.

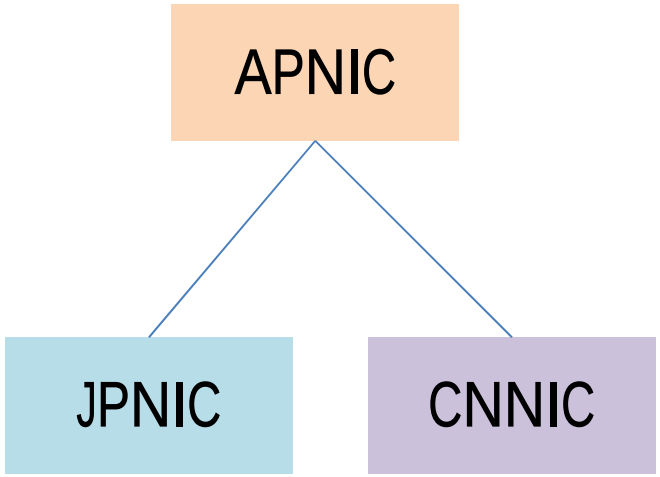
So the same resource could be allocated to the different sub-node simultaneously.

Test Result: case 3

A block of “ IP address ” will be transferred from the JPNIC to CNNIC.

This scenario has been described in draft-ymbk-sidr-transfer-01.

Some additional problems
will be caused, such as reassignment.



Solutions

- Safeguard of CA function
  - We have designed a mechanism to enhance the CA function to avoid the above misoperation or malicious operation. The detail information will be given in the future.

- The RP function enhancement
  - The enhancement of RP function is needed to discover these resource assignment errors.

Does this work make sense?

Join us ?

Comments?

Thank you