RPKI Deployment Considerations: Problem Analysis and Alternative Solutions

draft-lee-sidr-rpki-deployment-01

@IETF 95 SIDR meeting

fuyu@cnnic.cn

Background—RPKI in China

- CNNIC deploy a platform to provide RPKI pilot service in China.
- http://v6pilot.cn

Registered identity successfully.


```
<?xml version="1.0"?>
<oob:parent xmlns:oob="http://www.hactrn.net/uris/rpki/myrpki/" versio
BAMTIHJwa2ktdGVzdGJlZC5hcG5pYy5uZXQgQlBLSSBSb290MB4XDTEzMDQyMjAz
MDY0OVoXDTI2MTIzMDAzMDY0OVowKzEpMCcGA1UEAxMgcnBraS10ZXN0YmVkLmFw
bmljLm5ldCBCUEtJIFJvb3QwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALXh
vDUQGQyPyYVRbhE9rsUmLEelHpafPx9DNDO7lV3KlMS6UluN4tXDNzFK3jtuNIyj
723BBSL1sY16TkXrDK6c3ITx+UiWjUXrTlRNtMU6IQNkeESxG+XnTGnQ8zXCHJRZ
X4RUBbo61LqXx0O/U1hsh/w0ehjweYJ/J7OUESbtAgMBAAGjMjAwMA8GA1UdEwEB
/wQFMAMBAf8wHQYDVR0OBBYEFPoYAYoImNSt46XI17GkHCHNgIydMA0GCSqGSIb3
DQEBCwUAA4GBAHNb9tNOot0bUOYz7Ddh9LxX7cfu6YbPZ9Ly9qvIuvhnPK3yjcUX
6rmrnKqsfP1jUPOA1hLN/iC/R67Ui4Za+GatL6N3T7p9RTkFzkqH76OYn6gwBwhN
b04rJwenPhO8XOl4L1vaKT/8LNVAmkKKqnr/UwrX1s4gHkCluMPpEcvS

</oob:bpki_resource_ta><oob:bpki_child_ta>MIIC7zCCAdegAwIBAgIBATANBgkq
YyBCUEtJIHJlc291cmNlIENBMB4XDTE1MDcwMjAzMDEzOFoXDTI1MDcwMTAzMDEz
OFowITEfMB0GA1UEAxMWY25uaWMgQlBLSSByZXNvdXJjZSBDQTCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAPXC17SdQRW0vCpwxv5mmWNXrV1WQ/Pg9Hg/
F1/JxrswatoKy3ljLa/afcZU9KIQ2UbzdHf6ePOl3csTb6ESQkerDfB5zJ/RN7UB
NfdwfaNkF0vFHHTgUVWonVyS8BqX3ePWO5PbEvWlH04NnxAkZtsskV4kT5ZcSwzo
HOt6him3wEcOcrdWueGiA32CkQmi/w9T69nl6JOXE1nX0qm+Kd4x7Sv5cyzpFI0d
JLF39fpQgenPbizzVltplclJfiIO7nanjFSGFLFJ3ezdJ4L7nr3Olmu3Mmb4iMtS
GTvKDzfhNkYU1eQs/vlG0flxcAIIdKR6GCTksQ6CC2sKHE6cpe8CAwEAAaMyMDAw
HQYDVR0OBBYEFBuNwkG0U5SYC2yZJsQ9TZHO/p97MA8GA1UdEwEB/wQFMAMBAf8w
DQYJKoZIhvcNAQELBQADggEBALxHj20DOtDZjKG1KbGhob8VG+OJ0utIF5McsUJ4
eptBd8UVnrDcam3wGoleMqe8zAAO7TVOVKfC/A+6RcyCf/p+MkqHnZQJtwX+ECeM
UJHPGgfiXDSjkvlnGvje+nAwXEGaY15+j6K8f1Zlbe7DE++rq3Rete20SCG+I8yX
xlgUVMJqokwDFpp7vMeE5EzmeS0q6oJDTs3LztZFmhP/xbsJ9VDhcyyQ1qVA/E9g
iupgOSMMEinkldhapM0GV0N3Tjt2VTURgTnUhorSILfFwe34DwKcA8vpzL+QkrHJ
WpTbLlkolv/xvKfvE4kXZXIuwtkw0pXS1E3ulNB/ZXADbGc=

</oob:bpki_child_ta><oob:repository type="none"/></oob:parent>
```


Background—RPKI in world

- Each of the five RIRs has initiated the deployment of RPKI, and each now offers RPKI services to its members. A number of countries (Ecuador, Japan etc.) have also started to test and deploy RPKI internally. In order to promote the deployment of RPKI, ICANN， the five RIRs, many NIRs and companies have making continuous efforts to solve the existing problems and improve the corresponding policies and technical standards.
- However, RPKI is still in its early stages of global deployment. According to the data provided by RPKI Dashboard as of January 2016, the current routing table holds about 628,858 IP prefixes in total, and the RPKI validation state has been determined for 39584 IP prefixes, which means that only 6.29% of the prefixes in the routing table can be validated using the RPKI.

Considerations of RPKI Deployment

- 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
- Solutions
  - The RIRs are trying to continually evolve RPKI, including the migration to a single GTA (Global Trust Anchor) as the root of the RPKI hierarchical structure.
  - With this single root trust anchor deployed, the risks of resource conflicts (at the level of RIR certificates) could be significantly reduced.

Problems of CAs(1/4)

- Operational Errors
  - 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。

Problems of CAs(2/4)

- 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.

Problems of CAs(3/4)

- 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
  - When these deceived RPs offer their validation results to BGP routers, the routers may abandon the legitimate routes that are considered to be invalid according to the erroneous validation results they have received

Problems of CAs(4/4)

- Solution
  - "Suspenders" is designed to address the adverse effects on INR holders which were caused by CAs' accidental or deliberate misbehavior or attacks on CAs and repositories. This mechanism imports two new objects: an INRD (Internet Number Resource Declaration) file and a LOCK object.
  - The INRD file is external to the RPKI repository, and it contains the most recent changes that were made by the INR holder. Whenever the RPs detect the inconsistencies between the actual changes and the INRD file, they can determine individually whether to accept these changes or not.

Data Synchronization

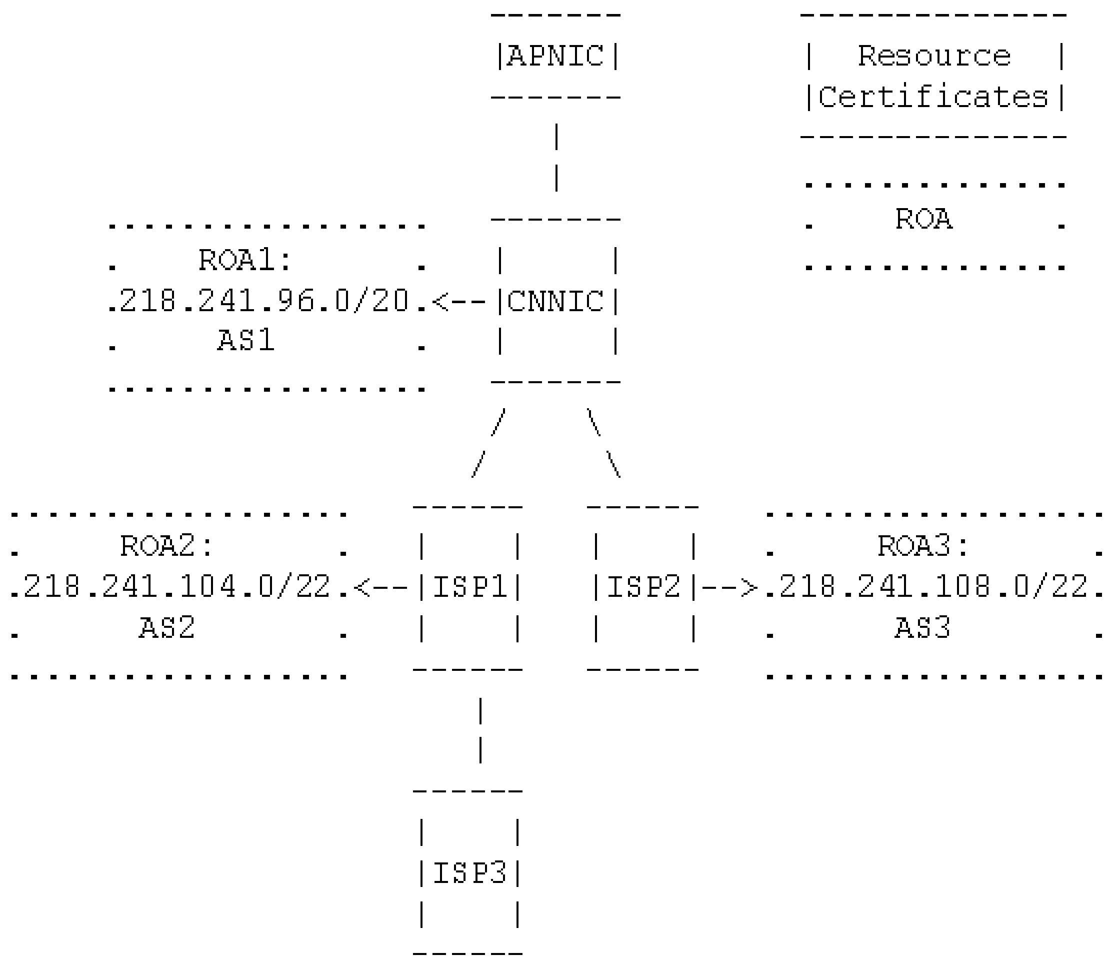
- It is required in [RFC6480] that all repositories must be accessible via rsync protocol which is used by RPs to get the RPKI objects in the global distributed repositories.
  - Lack of standards and non-modular implementation.
  - Not good enough in efficiency, scalability and security.
  - Underlying overhead caused by repository updates during active data transmissions

Data Synchronization

- Solution
  - RRDP, (RPKI Repository Delta Protocol) for RPs to keep their local caches in sync with the repository system [I-D.ietf-sidr-delta-protocol]. This new protocol is based on notification, snapshot and delta files. Compared with rsync protocol, RRDP is considered to be effective to eliminate a number of consistency related issues, help to reduce the load on publication servers, and have higher scalability.
  - Improve Rsync Protocol: CNNIC also proposed an improved rsync mechanism which transfers the work of checksums calculation to RPs in order to reduce the computation load on the rsync server side. The mechanism also offered a NOTIFY method that send NOTIFY message to make some important RPs to actively fetch the updated RPKI objects in time.

Problems of Staged and Incomplete Deployment

Since the global deployment of RPKI is an incremental and staged process, unexpected problems may appear during this process. It may cause legitimate routes to be misclassified into invalid



Does this work make sense?

Join us ?

Comments?

Thank you