RPKI
Resource Public Key Infrastructure
SANOG XXVI | 03-11 August, 2015 | Mumbai, India
Target Audience

• Knowledge of Internet Routing (specially BGP)

• Familiar with any IRR Database

• No need to know Cryptography

• Basic knowledge of PKI (Public Key Infrastructure)
Agenda

- BGP / RPKI
- Configuration
- Hands-on Lab (Juniper)
BGP
Send a packet to 2001:DB8::1

I have 2001:DB8::/32

http://thyme.apnic.net/network/
AS Path

2001:DB8::/32  100  200  300  i

Send a packet to
2001:DB8::1

AS 100

AS 200

AS 300

http://thyme.apnic.net/network/
### AS Path

<table>
<thead>
<tr>
<th>IP Address</th>
<th>AS 100</th>
<th>AS 200</th>
<th>AS 300</th>
<th>AS 420</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:DB8::/32</td>
<td>100</td>
<td>200</td>
<td>300</td>
<td>i</td>
</tr>
<tr>
<td>2001:DB8::/48</td>
<td>100</td>
<td>200</td>
<td>420</td>
<td>i</td>
</tr>
</tbody>
</table>

- Send a packet to 2001:DB8::1
- I have 2001:DB8::/32
- I have 2001:DB8::/48
- AS 100, AS 200, AS 300, AS 420

[More information](http://thyme.apnic.net/network/)
Historical Incident

• April 1997: The "AS 7007 incident" UU/Sprint for 2 days

• February 24, 2008: Pakistan's attempt to block YouTube access within their country takes down YouTube entirely.[6]

• November 11, 2008: The Brazilian ISP CTBC - Companhia de Telecomunicações do Brasil Central leaked their internal table into the global BGP table.

• April 8, 2010: China Telecom originated 37,000 prefixes not belonging to them in 15 minutes, causing massive outage of services globally.

source: http://en.wikipedia.org/wiki/IP_hijacking
Historical Incident

- For theory of positivity let’s call all these as Mis-Origination
- Traffic Hijacking or Prefix Hijacking assumes Negative intent
Current Trend

• Filtering limited to the edges facing the customer

• Filters on peering and transit sessions are often too complex or take too many resources

• Check prefix before announcing it
Filter Where?

- Secure BGP Templates
  - https://www.team-cymru.org/ReadingRoom/Templates/secure-bgp-template.html
Internet Registry (IR)

• Maintains Internet Resources such as IP addresses and ASNs, and publish the registration information
  • Allocations for Local Internet Registries
  • Assignments for end-users

• APNIC is the Regional Internet Registry (RIR) in the Asia Pacific region
  • National Internet Registry (NIR) exists in several economies
The Eco-System

Internet Assigned Numbers Authority

Regional IR (RIR)

National IR (NIR)

Internet Service Provider

End User
Routing Policy Specification Language (RPSL)

- Maintains routing policy database
  - RADB is the most popular service, though some RIRs also provide similar services
  - Routing policy information is expressed in a series of objects
  - On RADB, a registered user can register any object
  - route and route6 objects are used to indicate route origination
    - Prefix and origin AS
Still not enough
IRR is useful, but it’s not perfect
RPKI
Resource Public Key Infrastructure

IP Address & AS Numbers
Digital Certificate
RPKI Origin Validation

2001:DB8::/32 100 200 300 i Valid
2001:DB8::/48 100 200 420 i Invalid

Send a packet to 2001:DB8::1

Only AS300

I have 2001:DB8::/32

I have 2001:DB8::/48
RPKI Deployment

Send a packet to 2001:DB8::1

Phase 2
Path Validation

AS 100
AS 200
AS 300

Phase 1
Origin Validation

I have 2001:DB8::/32
Goals of RPKI

• Able to authoritatively prove who owns an IP Prefix and what AS(s) may Announce It

• Reducing routing leaks

• Attaching digital certificates to network resources (AS Number & IP Address)

• Prefix Ownership Follows the Allocation Hierarchy IANA, RIRs, ISPs, …
RPKI Implementation

• Two RPKI implementation type
  
  • **Delegated**: Each participating node becomes a CA and runs their own RPKI repository, delegated by the parent CA.
  
  • **Hosted**: The RIR runs the CA functionality for interested participants.
RPKI Building Blocks

• Trust Anchors (RIR’s)

• Route Origination Authorizations (ROA)

• Validators
Let’s discuss these building blocks in details
PKI & Trust Anchors
Public Key Concept

• **Private key**: This key must be known only by its owner.

• **Public key**: This key is known to everyone (it is public)

• **Relation between both keys**: What one key encrypts, the other one decrypts, and vice versa. That means that if you encrypt something with my public key (which you would know, because it's public :-), I would need my private key to decrypt the message.

• Same alike http with SSL aka https
X.509 Certificates 3779 EXT

Certificates are X.509 certificates that conform to the PKIX profile [PKIX]. They also contain an extension field that lists a collection of IP resources (IPv4 addresses, IPv6 addresses and AS Numbers) [RFC3779].
The hierarchy of the RPKI is based on the administrative resource allocation hierarchy, where resources are distributed from the IANA to the RIRs, to Local Internet Registries (LIRs) and end users.
Trust Anchor Locator (TALs)

• In cryptographic systems with hierarchical structure, a Trust anchor is an authoritative entity for which trust is assumed and not derived.

• In X.509 architecture, a root certificate would be the trust anchor from which whole chain of trust is derived. The trust anchor must be in possession of the trusting party beforehand to make any further certificate path validation possible.

• RPKI uses Internet Assigned Numbers Authority (IANA) as the trust anchor, and Regional Internet Registries (RIR) as immediately subordinate nodes to that anchor.
PKI in IRR

- The RIRs hold a self-signed root certificate for all the resources that they have in the registry
  - They are the trust anchor for the system
- That root certificate is used to sign a certificate that lists your resources
- You can issue child certificates for those resources to your customers
  - When making assignments or sub allocations
ROA
Route Origin Authorizations
Route Origination Authorizations (ROA)

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.

With a **ROA**, the **resource holder is attesting** that the **origin AS** number is **authorized to announce** the **prefix(es)**. The attestation can be verified cryptographically using RPKI.
Route Origination Authorizations (ROA)

Next to the prefix and the ASN which is allowed to announce it, the ROA contains:

- A minimum prefix length
- A maximum prefix length
- An expiry date
- Origin ASN

Multiple ROAs can exist for the same prefix
- ROAs can overlap
Validators
Origin Validation

• Router gets ROA information from the RPKI Cache
  • RPKI verification is done by the RPKI Cache
• The BGP process will check each announcement with the ROA information and label the prefix

RPKI to RTR protocol

Validated RPKI Cache
Result of Check

• **Valid** – Indicates that the prefix and AS pair are found in the database.

• **Invalid** – Indicates that the prefix is found, but either the corresponding AS received from the EBGP peer is not the AS that appears in the database, or the prefix length in the BGP update message is longer than the maximum length permitted in the database.

• **Not Found / Unknown** – Indicates that the prefix is not among the prefixes or prefix ranges in the database.

**Valid > Unknown > Invalid**
### ROA Example

**Prefix:** 10.0.0.0/16  
**ASN:** 65420

<table>
<thead>
<tr>
<th>Origin AS</th>
<th>Prefix</th>
<th>Max Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS65420</td>
<td>10.0.0.0/16</td>
<td>/18</td>
</tr>
<tr>
<td>AS65420</td>
<td>10.0.128.0/17</td>
<td></td>
</tr>
<tr>
<td>AS65421</td>
<td>10.0.0.0/16</td>
<td></td>
</tr>
<tr>
<td>AS65420</td>
<td>10.0.10.0/24</td>
<td></td>
</tr>
<tr>
<td>AS65430</td>
<td>10.0.0.0/8</td>
<td></td>
</tr>
</tbody>
</table>
Local Policy

• You can define your policy based on the outcomes

  • Do nothing

  • Just logging

  • Label BGP communities

  • Modify preference values

  • Rejecting the announcement
RPKI Support in Routers

• The RPKI-RTR Protocol is an IETF Internet Draft

• Production Cisco Support:
  • ASR1000, 7600, ASR903 and ASR901 in releases 15.2(1)S or XE 3.5
  • Cisco Early Field Trial (EFT):
    • ASR9000, CRS1, CRS3 and c12K (IOS-XR 4.3.2)

• Juniper has support since version 12.2

• Quagga has support through BGP-SRX
RPKI Caveats

• When RTR session goes down, the RPKI status will be not found for all the bgp route after a while
  
  • Invalid => not found
  
  • we need several RTR sessions or care your filtering policy

• In case of the router reload, which one is faster, receiving ROAs or receiving BGP routes?
  
  • If receiving BGP is match faster than ROA, the router propagate the invalid route to others
  
  • We need to put our Cache validator within our IGP scope
Who do we trust?

- Can we trust the *IR for hosting our Private Keys?

Two digital certificates have been mistakenly issued in Microsoft's name that could be used by virus writers to fool people into running harmful programs, the software giant warned Thursday.

According to Microsoft, someone posing as a Microsoft employee tricked VeriSign, which hands out so-called digital signatures, into issuing the two certificates in the software giant's name on Jan. 30 and Jan. 31.

Such certificates are critical for businesses and consumers who download patches, updates and other pieces of software from the Internet, because they verify that the software is being supplied from a particular company, such as Microsoft.
RPKI Further Reading

• RFC 5280: X.509 PKI Certificates

• RFC 3779: Extensions for IP Addresses and ASNs

• RFC 6481-6493: Resource Public Key Infrastructure
RPKI Configuration
Topology for Origin Validation

1. Create ROA
2. Setup validator & check the prefix

- AS 132442
- Cache Server rpki.df-h.net
- AS 23956
  - 103.12.176.0/22
- AS 58656
  - 202.4.96.0/19
  - 2404:D9000::/32
Phase I - Publishing ROA

- Login to your MyAPNIC portal
- Required valid certificate
- Go to Resources > Certification Tab
Phase I - Publishing ROA

1. Select the Certification tab.

2. Enable Resource Certification.
   - Option 1: I want to operate in the MyAPNIC RPKI portal.
   - Option 2: I want to host my own certification authority and run an RPKI engine myself.
   
3. Click the button to create your Certification Authority.
### Phase I - Publishing ROA

#### RPKI

**BGP Route Validity**

<table>
<thead>
<tr>
<th>Origin AS</th>
<th>Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>23956</td>
<td>118.179.192.0/19</td>
</tr>
<tr>
<td>23956</td>
<td>202.4.96.0/19</td>
</tr>
<tr>
<td>23956</td>
<td>2405:7600::/32</td>
</tr>
</tbody>
</table>

- Show available prefix for which you can create ROA
Phase I - Publishing ROA - IPv4

ROA Configuration

1. Write your ASN
2. Your IP Block
3. Subnet
4. Click Add

- Create ROA for smaller block.
Phase I - Publishing ROA - IPv6

ROA Configuration

1. Write your ASN
2. Your IP Block
3. Subnet
4. Click Add

• ROA for your IPv6 prefix
Phase I - Check your ROA

fakrul@access ~> whois -h whois.bgpmon.net 202.4.96.0/24

Prefix: 202.4.96.0/24
Prefix description: APT (Dhakacom)
Country code: BD
Origin AS: 23956
Origin AS Name: DHAKACOM-BD-AS dhakaCom Limited,BD
RPKI status: ROA validation successful
First seen: 2013-12-23
Last seen: 2015-07-10
Seen by #peers: 221
Phase I - Check your ROA

fakrul@access ~> whois -h whois.bgpmon.net " --roa 23956 202.4.96.0/24"

0 - Valid

------------------------
ROA Details
------------------------
Origin ASN:       AS23956
Not valid Before: 2014-10-21 02:40:16
Not valid After:  2015-12-30 00:00:00  Expires in 172d6h6m23s
Trust Anchor:     rpki.apnic.net
Prefixes:         202.4.96.0/19 (max length /24)
                    2405:7600::/32 (max length /32)
Phase II - RPKI Validator

- Download RPKI Validator

http://www.ripe.net/lir-services/resource-management/certification/tools-and-resources
Phase II - RPKI Validator

# tar -zxvf rpki-validator-app-2.17-dist.tar.gz

# cd rpki-validator-app-2.17

# ./rpki-validator.sh start
Phase II - RPKI Validator

http://ip-address:8080
1. Establish session with RPKI Validator

### JunOS

```plaintext
routing-options {
  validation {
    group RPKI {
      session 103.21.75.10 {
        refresh-time 120;
        hold-time 180;
        port 8282;
        local-address 103.12.75.1;
      }
    }
  }
}
```

### Cisco IOS

```plaintext
router bgp 64500
  bgp log-neighbor-changes
  bgp rpki server tcp 103.21.75.10 port 8282 refresh 120
```
Phase III - Router Configuration (JunOS)

2. Configure policy to tag ROA

```conf
policy-options {
    policy-statement ROUTE-VALIDATION {
        term valid {
            from {
                protocol bgp;
                validation-database valid;
            }
            then {
                local-preference 110;
                validation-state valid;
                accept;
            }
        }
        term invalid {
            from {
                protocol bgp;
                validation-database invalid;
            }
            then {
                local-preference 90;
                validation-state invalid;
                accept;
            }
        }
        term unknown {
            from {
                protocol bgp;
                validation-database unknown;
            }
            then {
                local-preference 100;
                validation-state unknown;
                accept;
            }
        }
    }
}
```
Phase III - Router Configuration (Cisco IOS)

2. Configure policy to tag ROA

! route-map ROUTE-VALIDATION permit 10
   match rpki invalid
   set local-preference 90
!
route-map ROUTE-VALIDATION permit 20
   match rpki not-found
   set local-preference 100
!
route-map ROUTE-VALIDATION permit 30
   match rpki valid
   set local-preference 110
Phase III - Router Configuration

3. Push policy to the BGP neighbour

<table>
<thead>
<tr>
<th>protocols {</th>
<th>protocols {</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp {</td>
<td>bgp {</td>
</tr>
<tr>
<td>log-updown;</td>
<td>log-updown;</td>
</tr>
<tr>
<td>import ROUTE-VALIDATION;</td>
<td>import ROUTE-VALIDATION;</td>
</tr>
<tr>
<td>group EBGP {</td>
<td>group EBGP {</td>
</tr>
<tr>
<td>type external;</td>
<td>type external;</td>
</tr>
<tr>
<td>! other configurations</td>
<td>! other configurations</td>
</tr>
<tr>
<td>}</td>
<td>}</td>
</tr>
<tr>
<td>}</td>
<td>}</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>JunOS</th>
<th>Cisco IOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>router bgp 64500</td>
<td>router bgp 64500</td>
</tr>
<tr>
<td>bgp log-neighbor-changes</td>
<td>bgp log-neighbor-changes</td>
</tr>
<tr>
<td>! other neighbour related configuration</td>
<td>! other neighbour related configuration</td>
</tr>
<tr>
<td>neighbor 10.1.1.2 route-map ROUTE-VALIDATION in</td>
<td>neighbor 10.1.1.2 route-map ROUTE-VALIDATION in</td>
</tr>
</tbody>
</table>
Check your prefix

fakrul@core01.bdhub.com> show route protocol bgp 202.4.96.0/24

inet.0: 549862 destinations, 549874 routes (549862 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

202.4.96.0/24     *[BGP/170] 2d 07:54:43, localpref 110
    AS path: 58587 58656 23956 I, validation-state: valid
    > to 103.229.83.9 via ge-1/0/1.0
fakrul@core01.bdhub.com> show validation session detail

Session 103.21.75.10, State: up, Session index: 2
Group: RPKI, Preference: 100
Local IPv4 address: 103.21.75.1, Port: 8282
Refresh time: 120s
Hold time: 180s
Record Life time: 3600s
Serial (Full Update): 6717
Serial (Incremental Update): 6717
    Session flaps: 0
    Session uptime: 1w1d 11:36:48
Last PDU received: 00:00:40
IPv4 prefix count: 14755
IPv6 prefix count: 2153
fakrul@core01.bdhub.com> show validation statistics

Total RV records: 16908
Total Replication RV records: 16908
  Prefix entries: 16304
  Origin-AS entries: 16908
Memory utilization: 3280312 bytes
Policy origin-validation requests: 31825409
  Valid: 784332
  Invalid: 677941
  Unknown: 30363136
BGP import policy reevaluation notifications: 85447
  inet.0, 85447
  inet6.0, 0
fakrul@core01.bdhub.com> show validation database

RV database for instance master

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Origin-AS</th>
<th>Session</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>41.73.32.0/19-24</td>
<td>37105</td>
<td>103.21.75.10</td>
<td>valid</td>
</tr>
<tr>
<td>41.77.152.0/22-22</td>
<td>32653</td>
<td>103.21.75.10</td>
<td>valid</td>
</tr>
<tr>
<td>41.77.156.0/23-23</td>
<td>32653</td>
<td>103.21.75.10</td>
<td>valid</td>
</tr>
<tr>
<td>41.77.158.0/23-23</td>
<td>37394</td>
<td>103.21.75.10</td>
<td>valid</td>
</tr>
<tr>
<td>41.78.188.0/22-22</td>
<td>37271</td>
<td>103.21.75.10</td>
<td>valid</td>
</tr>
<tr>
<td>41.79.148.0/22-22</td>
<td>37403</td>
<td>103.21.75.10</td>
<td>valid</td>
</tr>
<tr>
<td>41.86.32.0/19-19</td>
<td>36958</td>
<td>103.21.75.10</td>
<td>valid</td>
</tr>
<tr>
<td>2001:43f8:90::/48-128</td>
<td>37708</td>
<td>103.21.75.10</td>
<td>valid</td>
</tr>
<tr>
<td>2001:43f8:92::/48-128</td>
<td>37301</td>
<td>103.21.75.10</td>
<td>valid</td>
</tr>
<tr>
<td>2001:43f8:110::/48-128</td>
<td>37181</td>
<td>103.21.75.10</td>
<td>valid</td>
</tr>
</tbody>
</table>
Command

fakrul@core01.bdhub.com> show route protocol bgp validation-state valid

inet.0: 549890 destinations, 549902 routes (549890 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

2.0.0.0/16         *[BGP/170] 1d 06:25:16, localpref 110
    AS path: 58587 6453 5511 3215 I, validation-state: valid
    > to 103.229.83.9 via ge-1/0/1.0

2.1.0.0/16         *[BGP/170] 1d 06:25:16, localpref 110
    AS path: 58587 6453 5511 3215 I, validation-state: valid
    > to 103.229.83.9 via ge-1/0/1.0

2.2.0.0/16         *[BGP/170] 1d 06:25:16, localpref 110
    AS path: 58587 6453 5511 3215 I, validation-state: valid
    > to 103.229.83.9 via ge-1/0/1.0

2.3.0.0/16         *[BGP/170] 1d 06:25:16, localpref 110
    AS path: 58587 6453 5511 3215 I, validation-state: valid
    > to 103.229.83.9 via ge-1/0/1.0
fakrul@core01.bdhub.com> show route protocol bgp validation-state invalid

inet.0: 549895 destinations, 549907 routes (549895 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

5.152.160.0/24  *[BGP/170] 4d 07:18:39, localpref 90
    AS path: 58587 9498 20804 59472 I, validation-state: invalid
    > to 103.229.83.9 via ge-1/0/1.0

5.152.161.0/24  *[BGP/170] 4d 07:18:40, localpref 90
    AS path: 58587 9498 20804 59472 ?, validation-state: invalid
    > to 103.229.83.9 via ge-1/0/1.0

5.152.163.0/24  *[BGP/170] 4d 07:18:40, localpref 90
    AS path: 58587 9498 20804 59472 ?, validation-state: invalid
    > to 103.229.83.9 via ge-1/0/1.0

5.152.164.0/24  *[BGP/170] 4d 07:18:39, localpref 90
    AS path: 58587 9498 20804 59472 I, validation-state: invalid
    > to 103.229.83.9 via ge-1/0/1.0
!Caution!

- Make sure that your router IOS is bug free for RPKI; otherwise....
Check your prefix

Cisco (hosted by the RIPE NCC)

Public Cisco router: rpki-rtr.ripe.net

Telnet username: ripe / No password

Juniper (hosted by Kaia Global Networks)

Public Juniper routers: 193.34.50.25, 193.34.50.26

Telnet username: rpki / Password: testbed

source: http://www.ripe.net/lir-services/resource-management/certification/tools-and-resources
Configuration - Reference Link

Cisco


Juniper

RPKI Demo