Route Hijacking and the role of RPKI in Securing Internet Routing Infrastructure

Fakrul Alam
Senior Training Officer
APNIC
fakrul@apnic.net
### BGP 101

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>AS_PATH</th>
<th>Age</th>
<th>Attrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>2406:6400::/32</td>
<td>2001:df2:ee00::1</td>
<td>65531 65533 65535</td>
<td>05:30:49</td>
<td>[{Origin: i}]</td>
</tr>
<tr>
<td>2406:6400::/32</td>
<td>2001:df2:ee11::1</td>
<td>65530 65420</td>
<td>05:30:49</td>
<td>[{Origin: i}]</td>
</tr>
</tbody>
</table>

![Network Diagram]

- **2406:6400::/32**
- **2001:db8:ab::1**
- **2001:db8::/32**
Current Practice

• 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

Receive Request  LOA Check  Create Associate Prefix / AS Filter
Filter Where?

- Secure BGP Templates
  - https://www.team-cymru.org/ReadingRoom/Templates/secure-bgp-template.html
RPKI
Resource Public Key Infrastructure

IP Address & AS Number

Digital Certificate
BGP 101 + RPKI

Network  | Next Hop      | AS_PATH | Age  | Attrs
---------|---------------|---------|------|--------
V* > 2406:6400::/32 | 2001:df2:ee00::1 | 65531 65533 65535 | 05:30:49 | [{Origin: i}]
I > 2406:6400::/32 | 2001:df2:ee11::1 | 65530 65420 | 05:30:49 | [{Origin: i}]

2406:6400::/32

2001:db8:ab::1

64512

65530 65532 65534

65420

2001:db8::/32

65531 65533 65535
PKI In Other Application

• HTTPS
  – Web Address as RESOURCE
  – Hierarchical Trust Model
  – CA as the root of the TRUST
  – Browser does the VERIFICATION

• DNSSEC
  – Zone as RESOURCE
  – Hierarchical Trust Model
  – . as the root of the TRUST
  – DNS Resolver does the VERIFICATION
What About RPKI?
The Eco System
RPKI Trust Anchor

Resource Allocation Hierarchy

Trust Anchor Certificate

Issued Certificates match allocation actions

Cert / CUST-A
2001:DB8::/48
Public Key

Cert / CUST-B
2001:DB8:1::/48
Public Key

Cert / USER
2001:DB8:1::/56
Public Key

Cert / CUST-C
2001:DB8:2::/48
Public Key

Cert / APNIC
2001:DB8::/32
Public Key

ISP
ISP
ISP
ISP
ISP
ISP

APNIC
AFRINIC
RIPE NCC
LACNIC
NIR
RPKI Implementation

1. Publish ROA

2. RPKI Cache Validator

3. Router Configuration

• As an Announcer/LIR
  - You choose if you want certification
  - You choose if you want to create ROAs
  - You choose AS, max length

• As a Relying Party
  - You can choose if you use the validator
  - You can override the lists of valid ROAs in the cache, adding or removing valid ROAs locally
  - You can choose to make any routing decisions based on the results of the BGP Verification (valid/invalid/unknown)
Activate RPKI engine

1. Click on "Certification".
2. Select "I want to operate in the MyAPNIC RPKI portal." or "I want to host my own certification authority and run an RPKI engine myself.
3. Click on "I accept, Create my Certification Authority."
Create ROA

ROA Configuration

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

- Create ROA for smaller block.
How Do We Verify?

```
fakrul@console ~> whois -h whois.bgpmon.net " --roa 45192 202.125.97.0/24"
O - Valid

ROA Details

Origin ASN: AS45192
Not valid Before: 2016-06-22 00:00:00
Not valid After: 2020-07-22 00:00:00
Trust Anchor: rpki.apnic.net
Prefixes: 202.125.97.0/24
```

```
fakrul@jobbgp:~$ show bgp global rib 202.125.96.0/24
Network: 202.125.96.0/24
  Next Hop: 202.12.29.113
  AS_PATH: 4608 24115 4826 131107
  Age: 00:06:26

ASN  Prefix  Validity
131107 202.125.96.0/24 VALID
```

```
BGP Preview

| AS Number | 131107 |
| AS Name   | APNICTRAINING-DC ASN for APNICTRAINING LAB DC, AU |
| IP Address| 2001:df2:ee00:ee00::50 |
| BGP Prefix| 2001:df2:ee00::/48 |
| Validation Result | Valid |
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```

```
Network: 202.125.96.0/24
Prefixes: 202.125.96.0/24
```
RPKI in Action

- **{bgp4}** Routers validate updates from other BGP peers
- **{rtr}** Caches feeds routers using RTR protocol with ROA information
- **{rsync}** Caches retrieves and cryptographically validates certificates & ROAs from repositories
RPKI Implementation Issues
**RPKI Data Violation: Invalid ASN**

- Invalid origin AS is visible

```bash
fakrul@gbgp:-/go$ go bgp global rib 213.192.242.0/23
<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>AS_PATH</th>
<th>Age</th>
<th>Attrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>213.192.242.0/23</td>
<td>202.12.29.113</td>
<td>4608 1221 4637 1273 12541 01:22:01</td>
<td>[{Origin: i} {Med: 0} {LocalPref: 100}]</td>
<td></td>
</tr>
</tbody>
</table>
```

- From private ASN!

```bash
fakrul@gbgp:-/go$ whois -h whois.bgpmon.net "--roa 12541 213.192.242.0/23" 2 - Not Valid: Invalid Origin ASN, expected 8903

fakrul@gbgp:-/go$ go bgp global rib 103.10.77.0/24
<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>AS_PATH</th>
<th>Age</th>
<th>Attrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>103.10.77.0/24</td>
<td>202.12.29.113</td>
<td>4608 1221 4637 174 9490 58587 45951 65530 01:20:25</td>
<td>[{Origin: i} {Med: 0} {LocalPref: 100}]</td>
<td></td>
</tr>
</tbody>
</table>
```

```bash
fakrul@gbgp:-/go$ whois -h whois.bgpmon.net "--roa 65530 103.10.77.0/24" 2 - Not Valid: Invalid Origin ASN, expected 45951
```
RPKI Data Violation: Fixed Length Mismatch

- Most of the cases involve an invalid prefix (fixed length mismatch)
  - Further allocation to the customer

```json
{
  "validated_route": {
    "route": {
      "origin_asn": "AS58456",
      "prefix": "202.70.91.0/24"
    },
    "validity": {
      "state": "Invalid",
      "reason": "as",
      "description": "At least one VRR Covers the Route Prefix",
      "VRRs": {
        "matched": false,
        "unmatched_as": [
          "asn": "AS23752",
          "prefix": "202.70.64.0/19",
          "max_length": 19
        ]
      },
      "unmatched_length": false
    }
  }
}
```
Fiji

Total ASNs delegated by RIR: 8, Visible IPv4 routes: 50, Visible IPv6 routes: 5

http://rpki.apnictraining.net/output/fj.html
Moving Forward

• RPKI adoption is growing
  – You are encouraged to create ROA. Experiment, test, play and develop
  – You can implement in you infrastructure and do origin validation

• Something to consider
  – Upgrade at least ASBRs to RPKI capable code
  – In most cases, operators create ROAs for min length and advertise longest prefix
  – Some ROAs are invalid due to further allocation to customers

• https://www.apnic.net/ROA
Data Collection

• GoBGP
  – https://github.com/osrg/gobgp

• RPKI Dashboard
  – https://github.com/remydb/RPKI-Dashboard

• RIPE RPKI Statistics
  – https://lirportal.ripe.net/certification/content/static/statistics/world-roas.html

• RIPE Cache Validator API
  – http://rpki-validator.apnictraining.net:8080/export
Thank You