Security Overlays on Core Internet Protocols – DNSSEC and RPKI

Mark Kosters
ARIN CTO
Why are DNSSEC and RPKI Important

- Two critical resources
  - DNS
  - Routing
- Hard to tell if compromised
  - From the user point of view
  - From the ISP/Enterprise
- Focus on government funding
Why DNSSEC? What is it?

• Standard DNS (forward or reverse) responses are not secure
  – Easy to spoof
  – Notable malicious attacks
• DNSSEC attaches signatures
  – Validates responses
  – Can not spoof
Reverse DNS at ARIN

• ARIN issues blocks without any working DNS
  – Registrant must establish delegations after registration
  – Then employ DNSSEC if desired

• Just as susceptible as forward DNS if you do not use DNSSEC
Reverse DNS at ARIN

• Authority to manage reverse zones follows allocations
  –“Shared Authority” model
  –Multiple sub-allocation recipient entities may have authority over a particular zone
Changes completed to make DNSSEC work at ARIN

• Permit by-delegation management
• Sign in-addr.arpa. and ip6.arpa. delegations that ARIN manages
• Create entry method for DS Records
  – ARIN Online
  – RESTful interface
  – Not available via templates
Changes completed to make DNSSEC work at ARIN

• Key holders create and submit Delegation Signer (DS) records after securing their zones locally
• DNSSEC users need to have signed a registration services agreement with ARIN to use these services
Reverse DNS in ARIN Online

First identify the network that you want to put Reverse DNS nameservers on...

<table>
<thead>
<tr>
<th>SELECT</th>
<th>DELEGATION</th>
<th>NAMESERVERS</th>
<th>DS RECORD KEY TAGS</th>
<th>AUTHORIZED ORGANIZATIONS</th>
</tr>
</thead>
</table>
| ✓      | 252.149.192.in-addr.arpa. | NS1.ARIN.NET
NS2.ARIN.NET
NS2.LACNIC.NET
SEC1.APNIC.NET
SEC1.AUTHDNS.RIPE.NET |                    | ARIN Operations               |

[MODIFY NAMESERVERS] [MODIFY DS RECORDS]
Reverse DNS in ARIN Online

...then enter the Reverse DNS nameservers...

Manage Reverse DNS

Using the text fields on the right, specify the hostnames (not the IP addresses) of the nameservers that should be authoritative for ALL the reverse DNS delegations listed on the left. Please note that any modifications will be applied to all listed delegations.

<table>
<thead>
<tr>
<th>SELECTED DELEGATIONS IN - NET-192-149-252-0-1</th>
<th>HOSTNAMES OF NAMESERVERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>252.149.192.in-addr.arpa.</td>
<td>Nameserver 1: NS1.ARIN.NET</td>
</tr>
<tr>
<td></td>
<td>Nameserver 2: NS2.ARIN.NET</td>
</tr>
<tr>
<td></td>
<td>Nameserver 3: NS2.LACNIC.NET</td>
</tr>
<tr>
<td></td>
<td>Nameserver 4: SEC1.APNIC.NET</td>
</tr>
<tr>
<td></td>
<td>Nameserver 5: SEC1.AUTHDNS.RIPE.NET</td>
</tr>
<tr>
<td></td>
<td>Nameserver 6:</td>
</tr>
<tr>
<td></td>
<td>Nameserver 13:</td>
</tr>
</tbody>
</table>

[Buttons: APPLY TO ALL, CANCEL]
DNSSEC in ARIN Online

...then apply DS record to apply to the delegation

<table>
<thead>
<tr>
<th>ZONE</th>
<th>CLASS</th>
<th>RR TYPE</th>
<th>KEY TAG</th>
<th>ALGORITHM</th>
<th>DIGEST TYPE</th>
<th>DIGEST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optional, ignored</td>
<td>Optional, &quot;IN&quot;</td>
<td>Must be &quot;DS&quot;</td>
<td>2 byte integer</td>
<td>1 byte integer</td>
<td>1 byte integer (5, 7 or 8)</td>
<td>The hex encoded digest</td>
</tr>
</tbody>
</table>

The DS records should be in the following format:

PASTE DS RECORD DATA BELOW

[Choose File] No file chosen  [UPLOAD FILE]

File contents must be plain text

[APPLY TO ALL] [CANCEL]
Reverse DNS: Querying ARIN’s Whois

Query for the zone directly:

```
Whois> whois -h whois.arin.net 252.149.192.in-addr.arpa

Name: 252.149.192.in-addr.arpa.
Updated: 2014-08-20
NameServer: SEC1.APNIC.NET
NameServer: NS1.ARIN.NET
NameServer: NS2.LACNIC.NET
NameServer: SEC1.AUTHDNS.RIPE.NET
NameServer: NS2.ARIN.NET
KeyTag: 18508
Algorithm: 5
DigestType: 1
Digest: 84A741F15E878A088F3884EBE1F0E56EA8599295
KeyTag: 18508
Algorithm: 5
DigestType: 2
Digest: A9B8659C7795166863DE6FEC47808B58ED0CC6ADB0AA5E25B8F46FE87D3D7CBA
Ref: https://whois.arin.net/rest/rdns/252.149.192.in-addr.arpa.
```
DNSSEC in Zone Files

; File written on Mon Feb 24 17:00:53 2014
; dnssec_signzone version 9.3.6-P1-RedHat-9.3.6-20.P1.el5_8.6

0.74.in-addr.arpa.
86400 IN NS NS3.COVAD.COM.
86400 IN NS NS4.COVAD.COM.
10800 NSEC 1.74.in-addr.arpa. NS RRSIG NSEC
10800 RRSIG NSEC 5 4 10800 20140306210053 (20140224210053 57974 74.in-addr.arpa.
oNk3GVaCWj2j8+EAroPncqnZeQjm8h4w51nSD2VUi7YtR9FvYLF/j4KO+8qYz3TAixb9c05c8EVIhtY1grXEdOnm3OJyapora0DpbHt8FdwYvwp9Tq4oVbxVyuSNXriZ2Mq55IMgDR3nAT
BLP5UClxUWkgvS/6poF+W/1H4QY=)
1.74.in-addr.arpa.
86400 IN NS NS3.COVAD.COM.
86400 IN NS NS4.COVAD.COM.
10800 NSEC 10.74.in-addr.arpa. NS RRSIG NSEC
10800 RRSIG NSEC 5 4 10800 20140306210053 (20140224210053 57974 74.in-addr.arpa.
DKYGzSDtIypDVcer5e+XuwoDW4auKy6G/OCV
VTcfQGk+3iyy2CEK0ZuMZXFaaDvXnaxey9R1
mjams519Ghxpi2qOnnk0w6iB6mR5cNkYlkL0h
lu+IC4Buhr6DqM4HbJWCZcMXKEtWE0a6dMf+tH
sa+50V7ezX5LCuDVQvP6p0LftAE=)
### DNSSEC in Zone Files

<table>
<thead>
<tr>
<th>Record Type</th>
<th>Time-to-Live (sec)</th>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>NS</td>
<td>86400</td>
<td>0.121.74.in-addr.arpa</td>
<td>NS</td>
<td>DNS1.ACTUSA.NET.</td>
</tr>
<tr>
<td>NS</td>
<td>86400</td>
<td>0.121.74.in-addr.arpa</td>
<td>NS</td>
<td>DNS2.ACTUSA.NET.</td>
</tr>
<tr>
<td>NS</td>
<td>86400</td>
<td>0.121.74.in-addr.arpa</td>
<td>NS</td>
<td>DNS3.ACTUSA.NET.</td>
</tr>
<tr>
<td>DS</td>
<td>86400</td>
<td>0.121.74.in-addr.arpa</td>
<td>DS</td>
<td>AEEDA98EE493DFF5F33208ECB0FA4186BD 8056</td>
</tr>
<tr>
<td>DS</td>
<td>86400</td>
<td>0.121.74.in-addr.arpa</td>
<td>DS</td>
<td>66E6D421894AFE2AF0B350BD8F4C54D2EBA5 DA72A615FE64BE8EF600C6534CEF</td>
</tr>
<tr>
<td>RRSIG</td>
<td>86400</td>
<td>0.121.74.in-addr.arpa</td>
<td>RRSIG</td>
<td>DS 5 5 86400 20140306210053 ( 20140224210053 57974 74.in-addr.arpa. n+aPxBHuf+sbzQN4LmHzl0i0C/hkaSV03q1y 6J0KjqNPzYqtxLgZjU+IL9qhtIOocgNQib9l gFRmZ9inf2bER435GMsa/nnjpVVWW/MBRKxf Pcc72w2iOAMu2G0prtVT08ENxtu/pBfnsOZK nhCY8U0BOYLOLE5Whtk3X0uX9+U= )</td>
</tr>
<tr>
<td>NSEC</td>
<td>10800</td>
<td>1.121.74.in-addr.arpa</td>
<td>NSEC</td>
<td>NS DS RRSIG</td>
</tr>
<tr>
<td>RRSIG</td>
<td>10800</td>
<td>1.121.74.in-addr.arpa</td>
<td>RRSIG</td>
<td>NSEC 5 5 10800 20140306210053 ( 20140224210053 57974 74.in-addr.arpa. YvRowkdVDfv+PW42ySNUwW8S8jRyV6EKKRxen+8f42dS8jC8yV6EKKRxe)</td>
</tr>
</tbody>
</table>
# DNSSEC

<table>
<thead>
<tr>
<th><strong>Apr 2016</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Orgs with DNSSEC</td>
<td>134</td>
</tr>
<tr>
<td>Total Number of Delegations</td>
<td>593,946</td>
</tr>
<tr>
<td>DNSSEC Secured Zones</td>
<td>619</td>
</tr>
<tr>
<td>Percentage Secured</td>
<td>0.1 %</td>
</tr>
</tbody>
</table>
DNSSEC Validating Resolvers

- www.internetsociety.org/deploy360/dnssec/
- www.isc.org/downloads/bind/dnssec/
Reverse DNS Management and DNSSEC in ARIN Online

- Available on ARIN’s website
  http://www.arin.net/knowledge/dnssec/
What is RPKI?

- **Resource Public Key Infrastructure**
- Attaches digital certificates to network resources
  - AS Numbers
  - IP Addresses
- Allows ISPs to associate the two
  - Route Origin Authorizations (ROAs)
  - Can follow the address allocation chain to the top
What does RPKI accomplish?

• Allows routers or other processes to validate route origins
• Simplifies validation authority information
  – Trust Anchor Locator
• Distributes trusted information
  – Through repositories
Hierarchy of Resource Certificates

ICANN
0.0.0.0/0
 0::/0

ARIN
128.0.0.0/8
192.0.0.0/8

LACNIC

AFRINIC

RIPE
NCC

APNIC

Regional ISP
128.177.0.0/16

Other Small ISP
192.78.12.0/24

Some Small ISP
128.177.46.0/20
Route Origin Attestations

- ICANN
  - 0.0.0.0/0
  - 0::/0

- ARIN
  - 128.0.0.0/8
  - 192.0.0.0/8

- Regional ISP
  - 128.177.0.0/16

- Some Small ISP
  - 128.177.46.0/20
    - AS53659

- Other Small ISP
  - 192.78.12.0/24
    - AS2000

- LACNIC

- AFRINIC

- RIPE

- NCC

- APNIC
Current Practices
What does RPKI Create?

• It creates a repository
  – RFC 3779 (RPKI) Certificates
  – ROAs
  – CRLs
  – Manifest records
A Repository Directory containing an RFC3779 Certificate, two ROAs, a CRL, and a manifest
Relationships

- **Parent Cert**
  - Parent Manifest
  - CRL
    - Serial numbers of all revoked certs
  - Manifest
    - EE Certificate
      - URI/hash of CRL
      - URI hash of all ROAs
      - URI of all child certs
  - ROA
    - EE certificate
    - ASN
    - List of IP prefixes & max lengths

- **Certificate**
  - List of IP & ASN Resources
  - AIA, URI of the parent cert
  - SIA, URI of the manifest

- **Child Cert**

- **Parent Key**

- **Certificate Key**

- **Signs**
- **Points to (has URI for)**
Repository Use

• Pull down these files using a manifest-validating mechanism
• Validate the ROAs contained in the repository
• Communicate with the router marking routes “valid”, “invalid”, “unknown”
• Up to ISP to use local policy on how to route
Possible Data Flow for Operations

- RPKI Web interface -> Repository
- Repository aggregator -> Validator
- Validated entries -> Route Checking
- Route checking results -> local routing decisions (based on local policy)
How you can use ARIN’s RPKI System?

• Hosted
• Hosted using ARIN’s RESTful service
• Delegated using Up/Down Protocol
Hosted RPKI

• Pros
  – Easier to use
  – ARIN managed

• Cons
  – No current support for downstream customers to manage their own space (yet)
  – Tedious through the IU if you have a large network
  – We hold your private key
Hosted RPKI with RESTful Interface

• Pros
  – Easier to use
  – ARIN managed
  – Programmatic interface for large networks

• Cons
  – No current support for downstream customers to manage their own space (yet)
  – We hold your private key
Delegated RPKI with Up/Down

• Pros
  – You safeguard your own private key
  – Follows the IETF up/down protocol

• Cons
  – Hard to setup
  – Need to operate your own RPKI environment
Hosted RPKI in ARIN Online

To participate in Hosted RPKI, you will need to do the following:

1. Generate a ROA Request Generation Key Pair.
2. Select Hosted.
3. Read and agree to the RPKI Terms of Service.
4. Enter your ROA Request Generation Public Key into the field provided.
5. Click Submit.

Hosted
Hosted RPKI in ARIN Online

Organization Hosted RPKI Terms of Service

AGREEMENT

☐ I agree to the ARIN Hosted RPKI Terms of Service

You must accept the Hosted RPKI Terms of Service in order to proceed. Access a printable .pdf version of the Hosted RPKI Terms of Service.

Enter your initials

Continue

TERMS OF SERVICE

AMERICAN REGISTRY FOR INTERNET NUMBERS, LTD.
RPKI TERMS OF SERVICE AGREEMENT

YOU MUST READ AND ACCEPT THIS RPKI TERMS OF SERVICE AGREEMENT (THIS "AGREEMENT") BEFORE ACCESSING OR USING ANY RPKI SERVICES (AS DEFINED BELOW). IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT ACCESS OR USE ANY RPKI SERVICES.
Hosted RPKI in ARIN Online

Enter your ROA Request Generation Public Key below.

ROA Request Generation Public Key:
Learn more about the ROA Request Generation Key Pair. Or, just how to create one and extract the public key.

-----BEGIN PUBLIC KEY-----
MIIBljANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvBhoSmbRQhbSpTIM2Pqn
hWcHL/6SHORJGctuoMUS6tvamlqgdTZJw+8POFku+wIOLgUJOEw763rQVTsAq8WZ
vs6px2FNr6CJftKaR3fg/T083vHYiMTYJnJbVPKJjdSQSylyUWleR2hYh/4LEOyK
MPr3zAuDS2QOi6778OY/kpTEsCrwzp+dM4KtLGOQbyrkfSVIHgux5pCMzsQP/8nP
son5vOlkWtkuFNmg8pXgLfEdBR6MC0Y7eKaTeYM6EEJ7rhUCY69SUq+SFmuwYFs
7YNrzRAErF9THpEWqOaOxaSu/4nwLVJ2oexksT6k4hsEWPadxJ0P3E0FHSb/YlfOS
fwIDAQAB
-----END PUBLIC KEY-----
Hosted RPKI in ARIN Online

Hosted Certificates

Information
Each resource certificate entry displays the number of Route Origin Authorizations (ROAs), IP addresses or ranges, and Autonomous System Numbers (ASNs) covered by that certificate, and the date of the certificate's last update. For a listing of data elements for a given resource certificate, select Details.

For more information about resource certificates, visit ARIN's RPKI section.

ARIN

Updated: 03-20-2013

ROAs: 0  Nets: 20  ASNs: 10
Hosted RPKI in ARIN Online

Create a Route Origin Authorization (ROA) Request for SAMPLE-ORG

There are two ways to create and submit a ROA Request to ARIN:

**Browser Signed ROA Request** Complete the required fields below and digitally sign the ROA Request using the private key that corresponds with the public key you registered with ARIN.

**Signed ROA Request.** You must construct a precisely formatted text block containing your ROA Request information, and sign it using the private key that corresponds with the public key you registered with ARIN.

[Form fields]

ROA Name: 
Origin AS: 
Start Date: 03-20-2013
End Date: 03-20-2023
Prefix: 
Max Length: 
Private Key: Choose File No file chosen

This key will not be uploaded to ARIN.
Hosted RPKI in ARIN Online

Create a Route Origin Authorization (ROA) Request for SAMPLE-ORG

There are two ways to create and submit a ROA Request to ARIN:

**Browser Signed ROA Request** Complete the required fields below and digitally sign the ROA Request using the private key that corresponds with the public key you registered with ARIN.

**Signed ROA Request** You must construct a precisely formatted text block containing your ROA Request information, and sign it using the private key that corresponds with the public key you registered with ARIN.

**Browser Signed**

- **ROA Name:** Test-ROA
- **Origin AS:** 23456
- **Start Date:** 03-20-2013
- **End Date:** 03-20-2023
- **Prefix:** 70.182.32.0/24
- **Max Length:** 24

**Signed**

- **Private Key:** Key Loaded

* denotes optional field

This key will not be uploaded to ARIN.
This information will not be saved until you click the **Submit** button below. Note that the signature is used by ARIN to ensure that the ROA Request was signed with your private key. Please verify that the information below is correct. Click **Submit** to send the request, or click **Back** to make changes.

**ROA Name:** Test-ROA  
**Origin AS:** 23456  
**Validity Period:** 03-20-2013 to 03-20-2023  
**Resources:** 70.182.32.0/24 max length 24  
**Signature:**  
Hjnse52POzaVFupNDGqYXZVyImr78wSd4A1XEMUpj4vVmpJWWHnKoZRupDvB20BtwcJJEyx4KUWPgHUu8VhdCYroyuZGRxJkDlTeq8c0FT2QQdjuD+GmwULvtnSD26VZdYUrXM6WniTVwL96UV6sKbJGTx40GqD52tdJq6612QpC6K+Y+JEISgauVyy2htnAPI5r1ZqY42Fb9c1CEoE8GmT/FWY+CX6UmlKsxJ8LQ0NGR2XUeGKZyc2k5gKiSCog976Vnit88/z5jOm1GkYQoQvk6uy+yYUKreC+GyNqPYYPAvGAq61jYIDXMhDTSjWdGRiV2dNQ8zMmoDQgm9A==
Your ROA request is automatically processed and the ROA is placed in ARIN’s repository, accompanied by its certificate and a manifest. Users of the repository can now validate the ROA using RPKI validators.
Delegated with Up/Down

Up/Down RPKI

To participate in Up/Down Delegated RPKI you will need to do the following:

2. Select Up/Down.
3. Read and agree to the RPKI Terms of Service.
4. Submit your UpDown Identity.xml.
5. Click Submit.
Delegated with Up/Down
Delegated with Up/Down

ACTIVITY AND CORRESPONDENCE LOG

Date: 08-30-2013 09:54:59
Message: Ticket Status: Closed
Ticket Resolution: Processed

Date: 08-30-2013 09:54:58
By: ARIN Web
Subject: [ARIN-20130830-X1] - UpDown Identity Exchange Successful
Attachments: ARIN.SPRN.parent-response.xml
Message: The UpDown parent response for organization SPRN is attached.
Some of your resources are drawn from legacy space that is managed by another RIR.

Date: 08-30-2013 09:54:36
Message: Ticket Status: Approved

Date: 08-30-2013 09:54:36
By: MAIDSTAFFER RSDER
Subject: [ARIN-20130830-X1] - UpDown Identity Exchange - APPROVED
Delegated with Up/Down

- You have to do all the ROA creation
- Need to setup a CA
- Have a highly available repository
- Create a CPS
Updates within RPKI outside of ARIN

• The four other RIRs are in production with Hosted CA services as well
• ARIN, RIPE, and APNIC have delegated working for the public
• Major routing vendor support
• Public domain routing code support – Quagga and BIRD
ARIN Status

- Hosted CA deployed 15 Sept 2012
- Web Delegated CA deployed 16 Feb 2013 (deprecated from lack of use)
- Delegated using “Up/Down” protocol deployed 7 Sept 2013
- RESTful interface deployed 1 Feb 2014
## RPKI Usage

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Certified Orgs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>47</td>
<td>68</td>
<td>108</td>
<td>153</td>
<td>187</td>
<td>220</td>
<td>250</td>
<td></td>
</tr>
<tr>
<td>ROAs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>19</td>
<td>60</td>
<td>106</td>
<td>162</td>
<td>239</td>
<td>308</td>
<td>338</td>
<td>370</td>
</tr>
<tr>
<td>Covered Resources</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>30</td>
<td>82</td>
<td>147</td>
<td>258</td>
<td>332</td>
<td>430</td>
<td>482</td>
<td>528</td>
</tr>
<tr>
<td>Up/Down Delegated</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
Why is RPKI important?

- Provides more credibility to identify resource holders
- Leads to better routing security
Q&A