Core Internet Protocols

• **Two critical resources that are unsecured**
  – Domain Name Servers
  – Routing

• **Hard to tell if compromised**
  – From the user point of view
  – From the ISP/Enterprise
DNS
How DNS Works

Question: www.arin.net A

Resolver

Caching forwarder (recursive)

root-server

www.arin.net A

www.arin.net A

Ask net server @ X.gtld-servers.net (+ glue)

gtld-server

Ask arin server @ ns1.arin.net (+ glue)

positor

www.arin.net A

Add to cache

www.arin.net A

192.168.5.10

arin-server

192.168.5.10
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 *should* 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>
<tbody>
<tr>
<td></td>
<td>252.149.192.in-addr.arpa.</td>
<td>NS1.ARIN.NET NS2.ARIN.NET NS2.LACNIC.NET SEC1.APNIC.NET SEC1.AUTHDNS.RIPE.NET</td>
<td></td>
<td>ARIN Operations</td>
</tr>
</tbody>
</table>

[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.

**SELECTED DELEGATIONS IN - NET-192-149-252-0-1**

252.149.192.in-addr.arpa.

**HOSTNAMES OF NAME SERVERS**

<table>
<thead>
<tr>
<th>Nameserver 1:</th>
<th>NS1.ARIN.NET</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nameserver 2:</td>
<td>NS2.ARIN.NET</td>
</tr>
<tr>
<td>Nameserver 3:</td>
<td>NS2.LACNIC.NET</td>
</tr>
<tr>
<td>Nameserver 4:</td>
<td>SEC1.APNIC.NET</td>
</tr>
<tr>
<td>Nameserver 5:</td>
<td>SEC1.AUTHDNS.RIPE.NET</td>
</tr>
<tr>
<td>Nameserver 6:</td>
<td></td>
</tr>
<tr>
<td>Nameserver 13:</td>
<td></td>
</tr>
</tbody>
</table>
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 (5, 7 or 8)</td>
<td>1 byte integer (1 or 2)</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

File contents must be plain text

[Parse DS Record]

[APPLY TO ALL] [CANCEL]
Reverse DNS: Querying ARIN’s Whois Query for the zone directly:

```
Whois> whois -h whois.arin.net 136.136.192.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+EAR0PncqnZeQjm8h4w51nS
 D2VUi7Ytr9FvYLF/j4KO+8qYZ3TAixb9c05c
 8EVIhtY1grXEd0m30zJPZyaoa0DpbHt8FdwY
 vwpU9Tq40VbXVyuSNXr1Z2Mq55I1MgDR3nAT
 BLP5UC1xWeKgrV/6pof+W1H4QY= )

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+XuwoDW4auKv6G/OCV
 VTcfQGk+3iyy2CEK0ZuMXFAadVxnaey9R1
 mjams519Ghxp2q0nnk0w6iB6mR5cNkYlkL0h
 lU+IC4BuH6DqM4HbJcZcMXKEtWE0a6dMf+tHsa+50V7ezX5LCuDVQVp6p0LftAE= )
**DNSSEC in Zone Files**

<table>
<thead>
<tr>
<th>Domain</th>
<th>TTL</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.121.74.in-addr.arpa.</td>
<td>86400</td>
<td>NS</td>
<td>DNS1.ACTUSA.NET.</td>
</tr>
<tr>
<td></td>
<td>86400</td>
<td>NS</td>
<td>DNS2.ACTUSA.NET.</td>
</tr>
<tr>
<td></td>
<td>86400</td>
<td>NS</td>
<td>DNS3.ACTUSA.NET.</td>
</tr>
<tr>
<td></td>
<td>86400</td>
<td>DS</td>
<td>46693 5 1 (</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>AEEDA98EE493DFF5F33208ECB0FA4186BD8056 )</td>
</tr>
<tr>
<td></td>
<td>86400</td>
<td>DS</td>
<td>46693 5 2 (</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>66E6D421894AFE2AF0B350BD8F4C54D2EBA5DA72A615FE64BE8EF600C6534CEF )</td>
</tr>
<tr>
<td></td>
<td>86400</td>
<td>RRSIG</td>
<td>DS 5 5 86400 20140306210053 (</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>20140224210053 57974 74.in-addr.arpa.n+aPxBHuf+sbzQN4LmHzl0i0C/hkaSVO3q1y</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6J0KjqNPzYqtLgZjU+IL9qht00cgNQib9lfgFRmZ9inf2bER435GMsa/nnjpVWVW/MBRKxf</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Pcc72w2i0AMu2G0prtVTO8ENxtu/pBfnsOZKnhCY8U0BOYLE5Whtk3X0uX9+U= )</td>
</tr>
<tr>
<td>10800</td>
<td>NSEC</td>
<td>1.121.74.in-addr.arpa. NS DS RRSIG</td>
<td></td>
</tr>
<tr>
<td>10800</td>
<td>RRSIG</td>
<td>NSEC 5 5 10800 20140306210053 (</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>20140224210053 57974 74.in-addr.arpa.YvRowkdVDfv+PW42ySNUwW8S8jRyV6EKKRx</td>
</tr>
</tbody>
</table>
DNSSEC Validating Resolvers

- [www.internetsociety.org/deploy360/dnssec/](http://www.internetsociety.org/deploy360/dnssec/)
### DNSSEC Statistics

<table>
<thead>
<tr>
<th></th>
<th>Sept 7, 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Orgs with DNSSEC</td>
<td>137</td>
</tr>
<tr>
<td>Total Number of Delegations</td>
<td>602,230</td>
</tr>
<tr>
<td>DNSSEC Secured Zones</td>
<td>628</td>
</tr>
<tr>
<td>Percentage Secured</td>
<td>0.1 %</td>
</tr>
</tbody>
</table>
Reverse DNS Management and DNSSEC in ARIN Online

• Available on ARIN’s website

http://www.arin.net/knowledge/dnssec/
Routing
Routing Architecture

- The Internet uses a *two level* routing hierarchy:
  - **Interior** Routing Protocols, used by each network to determine how to reach all destinations that line within the network
  - **Interior** Routing protocols maintain the current topology of the network
Routing Architecture

- The Internet uses a *two level* routing hierarchy:
  - **Exterior** Routing Protocol, used to link each component network together into a single whole
  - **Exterior** protocols assume that each network is fully interconnected internally
Exterior Routing: BGP

- BGP is a large set of bilateral (1:1) routing sessions
  - A tells B all the destinations (prefixes) that A is capable of reaching
  - B tells A all the destinations that B is capable of reaching
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

LACNIC

AFRINIC

RIPE

NCC

APNIC

Regional ISP
128.177.0.0/16

Some Small ISP
128.177.46.0/20

Other Small ISP
192.78.12.0/24

128.177.0.0/16
AS17025

128.177.46.0/20
AS53659

192.78.12.0/24
AS2000
Current Practices

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

128.177.0.0/16
128.177.46.0/20
AS53659

192.78.12.0/24
AS2000

192.0.0.0/8
What does RPKI Create?

• It creates a repository
  – RFC 3779 (RPKI) Certificates
  – ROAs
  – CRLs
  – Manifest records
Repository View

./ba/03a5be-ddf6-4340-a1f9-1ad3f2c39ee6/1:
  total 40
-rw-r--r-- 1 143  143  1543 Jun 26  2009 ICcaIRKhGHJ-TgUZv8GRKqkidR4.roa
-rw-r--r-- 1 143  143  1403 Jun 26  2009 cKxLCU9umS-qD4DOOkAK0M2US0.cer
-rw-r--r-- 1 143  143   485 Jun 26  2009 dSmerM6uJGLWMMQT12esy4xyUAA.crl
-rw-r--r-- 1 143  143  1882 Jun 26  2009 dSmerM6uJGLWMMQT12esy4xyUAA.mnf
-rw-r--r-- 1 143  143  1542 Jun 26  2009 nB0gDFtWffKk4VWgln-12pdFtE8.roa

A Repository Directory containing an RFC3779 Certificate, two ROAs, a CRL, and a manifest
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
  – create ROAs through ARIN Online
  – create ROAs using ARIN’s RESTful service

• Delegated using Up/Down Protocol
Hosted RPKI - ARIN Online

• **Pros**
  – Easy to pick up and use
  – ARIN managed

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

• **Pros**
  – Programmatic interface for large networks
  – ARIN managed

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

- **Pros**
  - You safeguard your own private key
  - Follows the IETF up/down protocol

- **Cons**
  - Extremely 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 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

**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-----
MIIBljANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvBhoSmbRQhbSpTIM2PqnhWcHL/6SHORJGctuoMUS6tVamlqgdTZJw+8POFku+WIOLgUJOEw763rQVTsAq8WZvs6px2FNr6CJftKAr3f9/T083vHYiMtYJnJbVPKJjdSOSlyUWleR2hYh/4LEOyKMPr3zAuDS2QOi6778OY/kpTEsCzwzp+dM4KtLGOQbyrkfSVIhgu5pCMzsQP/8nPson5vOlkWtkuFNg8pXgLfeBR6MC0Y7eKaTeYM6EEJ7rhUCY69SUq+SFMuwYFs57YNzRAErF9THpEWqOaOxaSu/4nwLVJ2oxksT6k4hsEWPdxJ0P3E0FHSb/YffOSfWIDAQAB
-----END PUBLIC KEY-----

Submit
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

Create Roa  View Resources  View Roas  View Details
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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROA Name</td>
<td></td>
</tr>
<tr>
<td>Origin AS</td>
<td></td>
</tr>
<tr>
<td>Start Date</td>
<td>03-20-2013</td>
</tr>
<tr>
<td>End Date</td>
<td>03-20-2023</td>
</tr>
<tr>
<td>Prefix</td>
<td></td>
</tr>
<tr>
<td>Max Length</td>
<td>*</td>
</tr>
<tr>
<td>Private Key</td>
<td>Choose File: No file chosen</td>
</tr>
</tbody>
</table>
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

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

SUBMIT SIGNED ROUTE ORIGIN AUTHORIZATION

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: Hjnse52POzaVFupNDBGqYXZVyImr78wSd4A1XEMUpj4vVmpJWWHnKoZRupDvB2OBtwcJJEyx4KUWPgHUIt8VhdCYroyuZGRxJkJdTTeq8c0FT2QQjduD+GmwUWLvtnSD26VZdYUrXM6WniTVwL96UV6sKbJGTx40GqD5tJq6612QpC6K+Y+JEISgauVyy2htnAPI5r17ZGY42Fb9c1CEoE8GmT/FWY+CX6UmKsxJ8LQ0NGR2XUeGKZyc2k5gKiSCog976VnlIt88/z5jOmlGkYQoQvk6uy+yYUKreC+GyNqPYPaVGAq61jYIDXMhDTSjWdGRiV2dNQ8zMmoDOgm9A==

BACK  Submit Signed ROA Request
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:

1. Generate an RFC 6492 *Up/Down Identity.xml*.
2. Select Up/Down.
3. Read and agree to the RPKI Terms of Service.
4. Submit your *Up/Down Identity.xml*.
5. Click Submit.
Delegated with Up/Down
Delegated with Up/Down

<table>
<thead>
<tr>
<th>Resource Class</th>
<th>Certifiable Net(s)</th>
<th>Certifiable Net(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>APNIC</td>
<td>NET-153-23-0-0-1</td>
<td>NET-209-239-96-0-2</td>
</tr>
<tr>
<td>RIPE</td>
<td>NET-141-193-0-0-1</td>
<td>NET-216-205-64-0-1</td>
</tr>
<tr>
<td></td>
<td>NET-216-205-144-0-1</td>
<td></td>
</tr>
</tbody>
</table>

**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:** MADSTAFFER 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 Certificate Authority
• Have a highly available repository
• Create a CPS
# RPKI Statistics

<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>47</td>
<td>68</td>
<td>108</td>
<td>153</td>
<td>187</td>
<td>220</td>
<td>250</td>
<td>263</td>
</tr>
<tr>
<td>ROAs</td>
<td>60</td>
<td>106</td>
<td>162</td>
<td>239</td>
<td>308</td>
<td>338</td>
<td>370</td>
<td>410</td>
</tr>
<tr>
<td>Covered Resources</td>
<td>82</td>
<td>147</td>
<td>258</td>
<td>332</td>
<td>430</td>
<td>482</td>
<td>528</td>
<td>582</td>
</tr>
<tr>
<td>Up/Down Delegated</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>
Q&A