ROVER
BGP Route Origin Verification via DNS

Joseph Gersch
RIPE64 Plenary
April 2012
Introduction to Rover

- Basic Purpose: Protect against IP Hijacks
- Discussed at Quebec IETF and internet drafts introduced at Paris IETF
- Complementary technology to RPKI
  - Some similarities, some differences

2 Basic Components:

- **Publish**
  - route origin data placed in the reverse-DNS, authenticated via DNSSEC signatures

- **Verify**
  - SW tools and appliances to match unique ISP operational procedures
ROVER Design Model

Applications tailored to unique ISP Operations

ROVER Access Methods

DNS DNSSEC etc.
ROVER Design Model

Applications tailored to unique ISP Operations

ROVER Access Methods

DNS DNSSEC etc.

Foundations / Protocols
- pre-existing DNS infrastructure
- IN-ADDR.ARPA signed with DNSSEC
- redundancy/resiliency
- real-time updates
ROVER Design Model

Applications tailored to unique ISP Operations

Small set of methods:
- Data Naming Convention
- Data Publishing Format
- Data Authentication
- “Best Effort” retrieval

Foundations / Protocols
- pre-existing DNS infrastructure
- IN-ADDR.ARPA signed with DNSSEC
- redundancy/resiliency
- real-time updates
ROVER Design Model

Applications tailored to unique ISP Operations

ROVER Access Methods

Small set of methods:
- Data Naming Convention
- Data Publishing Format
- Data Authentication
- “Best Effort” retrieval

ISP Applications:
- verify routing DB
- build prefix filters
- interface to RTR
- real-time notification/block
- (exponential retry)

Foundations / Protocols
- pre-existing DNS infrastructure
- IN-ADDR.ARPA signed with DNSSEC
- redundancy/resiliency
- real-time updates

DNS DNSSEC etc.
Reverse DNS publishing method

- General-Purpose Naming convention designed to specify CIDR address blocks. Example:
  - 129.82.128.0/18  -->  0.1.m.82.129.in-addr.arpa

- 2 New DNS records
  - **RLOCK**: Route lock (opt in)
  - **SRO**: “Secure Route Origin”
  - more as the concept evolves

- 2 Internet Drafts
  - draft-gersch-dnsop-revdns-cidr
  - draft-gersch-grow-revdns-bgp
Example:
publish origins for one /16 and four /18’s

<table>
<thead>
<tr>
<th>129.82</th>
<th>/16</th>
<th>/17</th>
<th>/18</th>
<th>/19</th>
<th>/20/</th>
<th>/21</th>
<th>/22</th>
<th>/23</th>
<th>/24</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>129.82/16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>AS 12145</td>
<td>129.82.0/16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>40</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>48</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>64</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>72</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>80</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>88</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>96</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>104</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>112</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>120</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>136</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>144</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>152</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>160</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>168</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>176</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>184</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>200</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>208</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>216</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>224</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>232</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>240</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>248</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Zone file: (uses CIDR reverse-DNS naming convention)

$ORIGIN 82.129.in-addr.arpa
$TTL 3600

@ IN RLOCK ; secure entire zone
m IN SRO 12145 ;129.82.0.0/16
0.0.m IN SRO 12145 ;129.82.0.0/18
1.0.m IN SRO 12145 ;129.82.64.0/18
0.1.m IN SRO 12145 ;129.82.128.0/18
1.1.m IN SRO 12145 ;129.82.192.0/18

; can now directly add /24 SROs
; or can let the lower octet do it

; existing delegations
0 IN NS rush.colostate.edu
1 IN NS rush.colostate.edu
;....
255 IN NS rush.colostate.edu

RLOCK = Route LOCK
SRO = Secure Route Origin
Automated provisioning tools have been written
The reverse DNS records can be used to:

- create route filters on a periodic basis for loading into a router
- perform real-time verifications
  - check a BGP announcement against the published authorized data in the reverse-DNS:
    - valid, invalid, unknown
  - Notify operator
  - interface to router and make adjustments
- other tools and building blocks
Avoid a Cyclic Dependency

- Can a low-level protocol like BGP depend on a higher-level protocol?
  - no, not if there is a hard dependency
  - yes, if the dependency has a “fail-safe”

- Rover uses “best effort” data retrieval with worldwide data distribution, redundancy and local caching. Applications can use query retries with exponential back-off.

- If the data is unreachable, the default is that routing works just as it works today.
Status

- ROVER Testbed available at “rover.secure64.com”
  - uses a shadow-zone for in-addr.arpa
  - suggests route origins based on BGPMON data retrieved from world-wide collectors
  - creates DNS zone files

- Several early adopter telecomm and ISPs are in the process of publishing route origins in their reverse DNS and signing with DNSSEC.

- RIPE and ARIN already DNSSEC sign the reverse DNS
Testbed Screenshot

- Show suggested route announcements

Step 3: Authorize route origins.

**suggested actions:**
- Accept All Advisories
- Accept Selected Advisory
- Toggle Advisory Peer/Transit

**select a subnet:**
- Create Route Authorization
- Create Zone Delegation

**select a zone record:**
- Delete Route Authorization

**When finished:**
- View/Save Zone File
- Return to Previous Page

Note: Peering/transit relations are calculated by an inference engine and are only 80% correct. You may have to make manual changes using the “toggle” button.
Thank You!

- I will be at the **DNS Working Group** if you have questions on the DNS CIDR naming convention or DNS record types.

- I will be presenting at the **IPv6 Working Group** to show how the naming convention works for IPv6 and how it can be used for other applications besides routing (e.g. GeoLocation).

- See me if you would like a demo or want to know more.