ROVER
BGP Route Origin Verification via DNS

Joseph Gersch
RIPE64 Plenary
April 2012

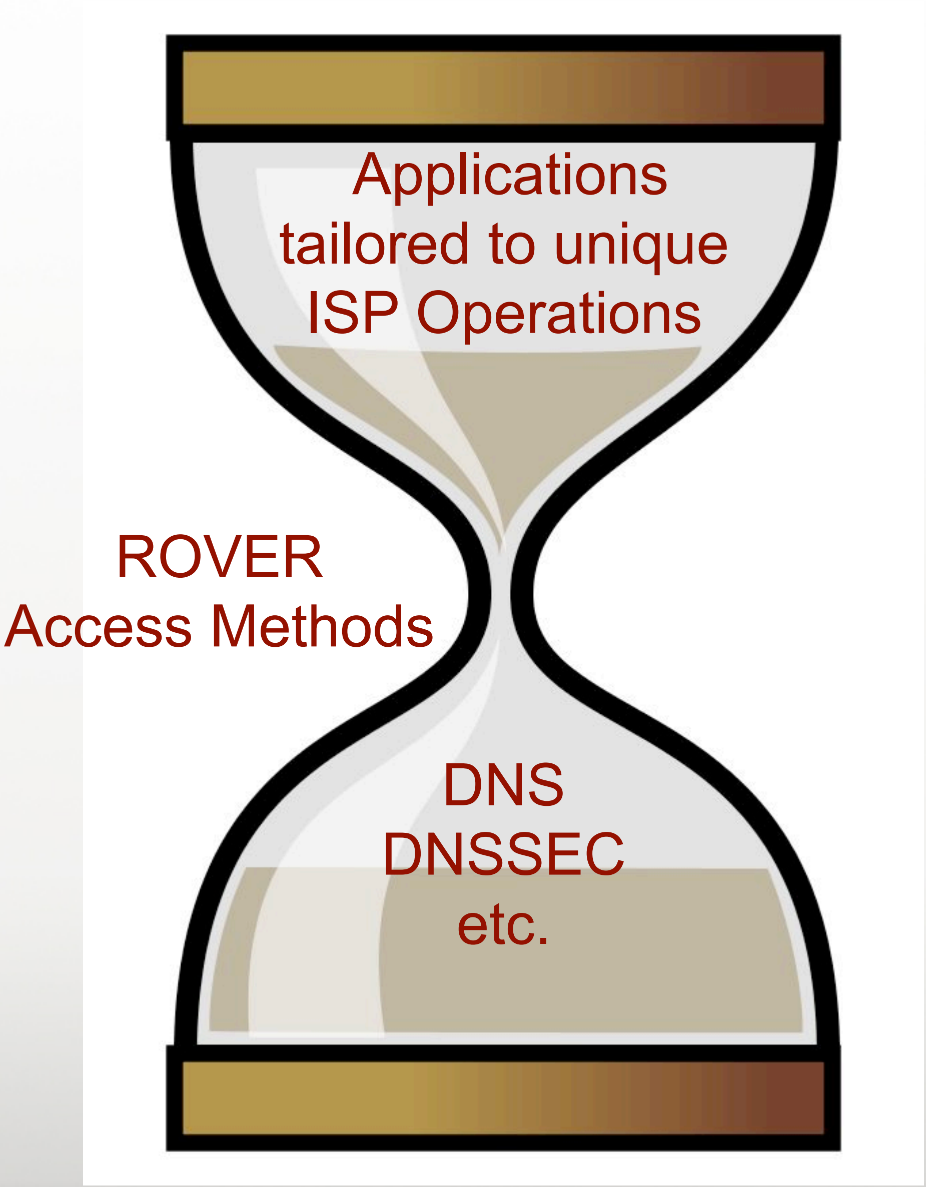
SECURE64

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



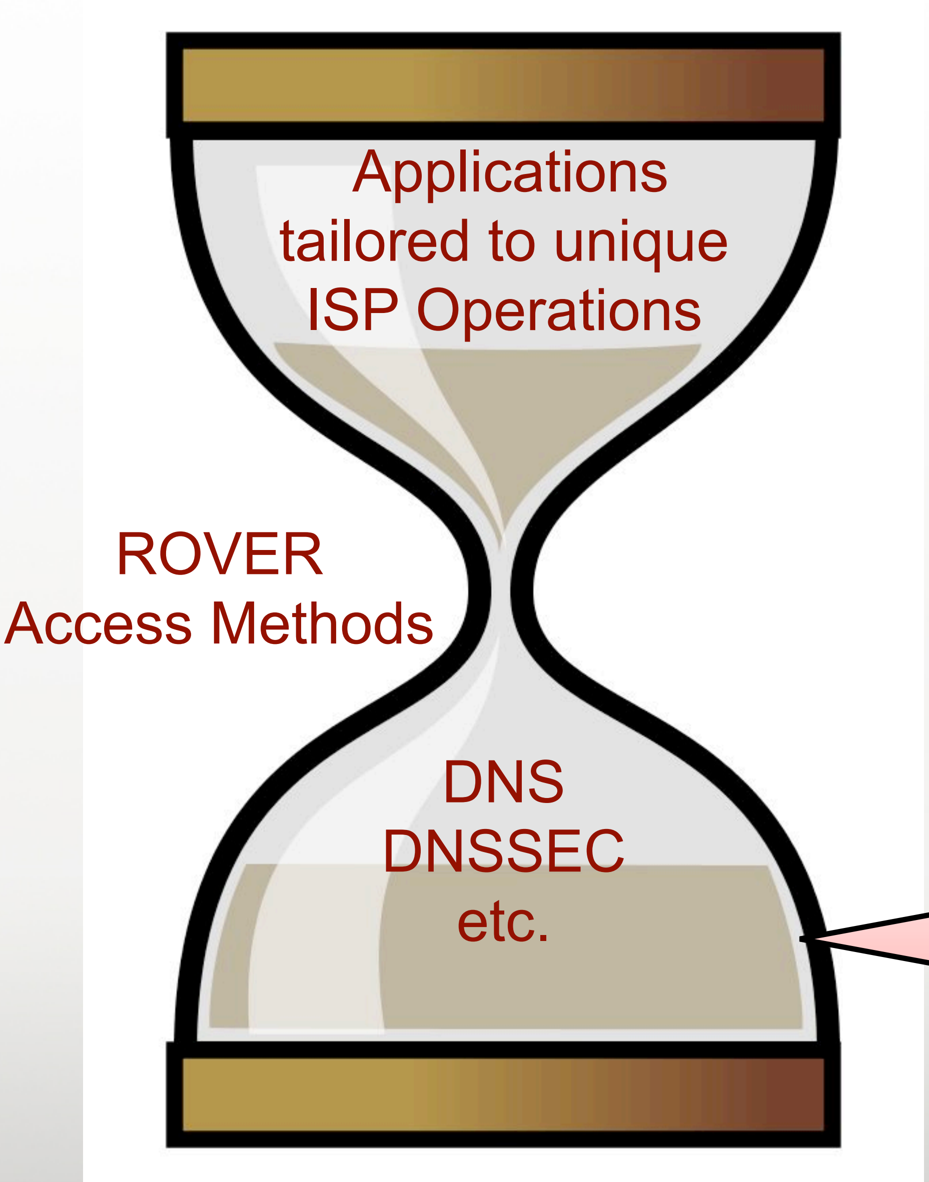
Applications tailored to unique ISP Operations

ROVER Access Methods

DNS
DNSSEC
etc.

ROVER Design Model

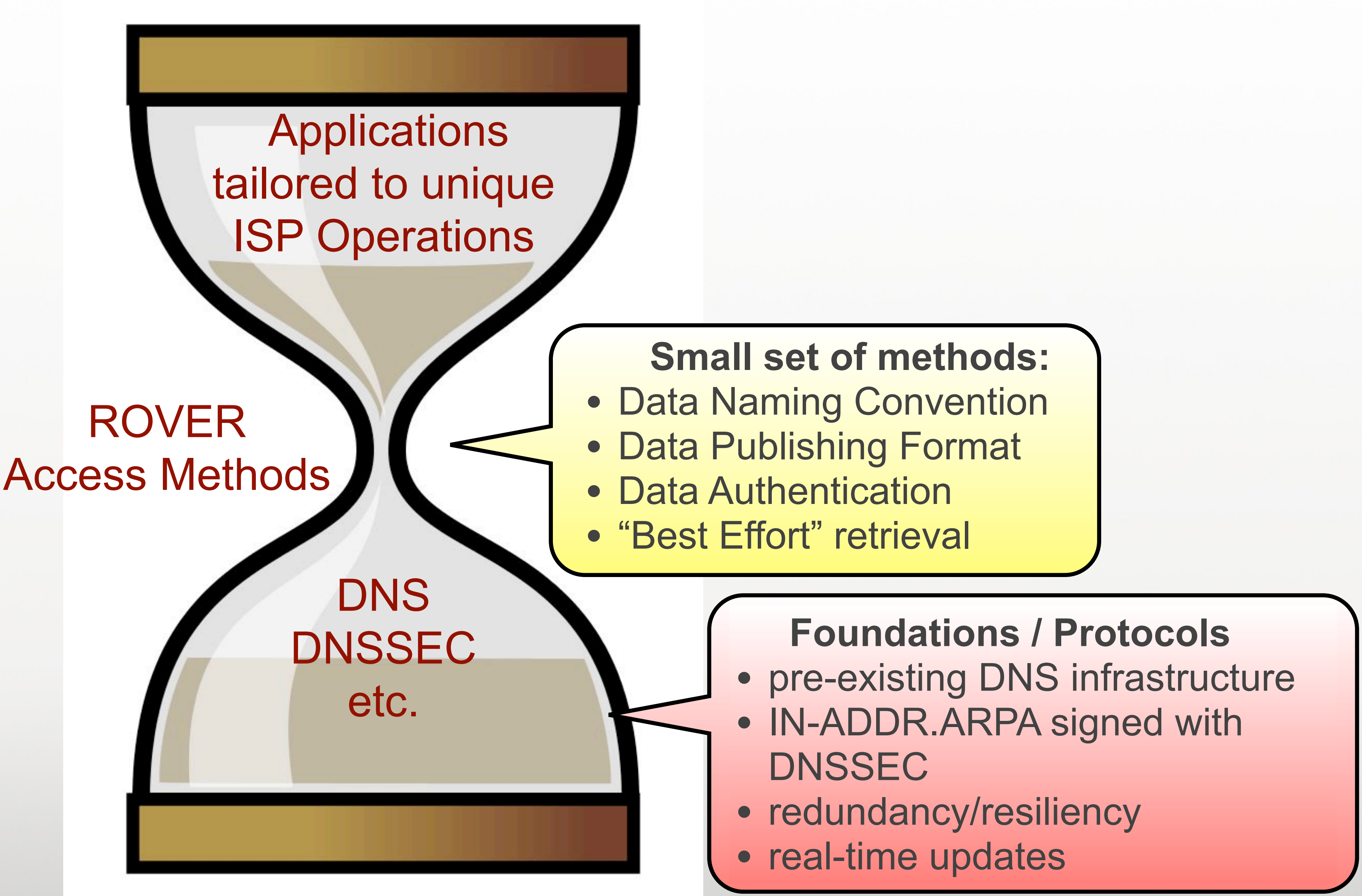
SECURE64



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

DNS
DNSSEC
etc.

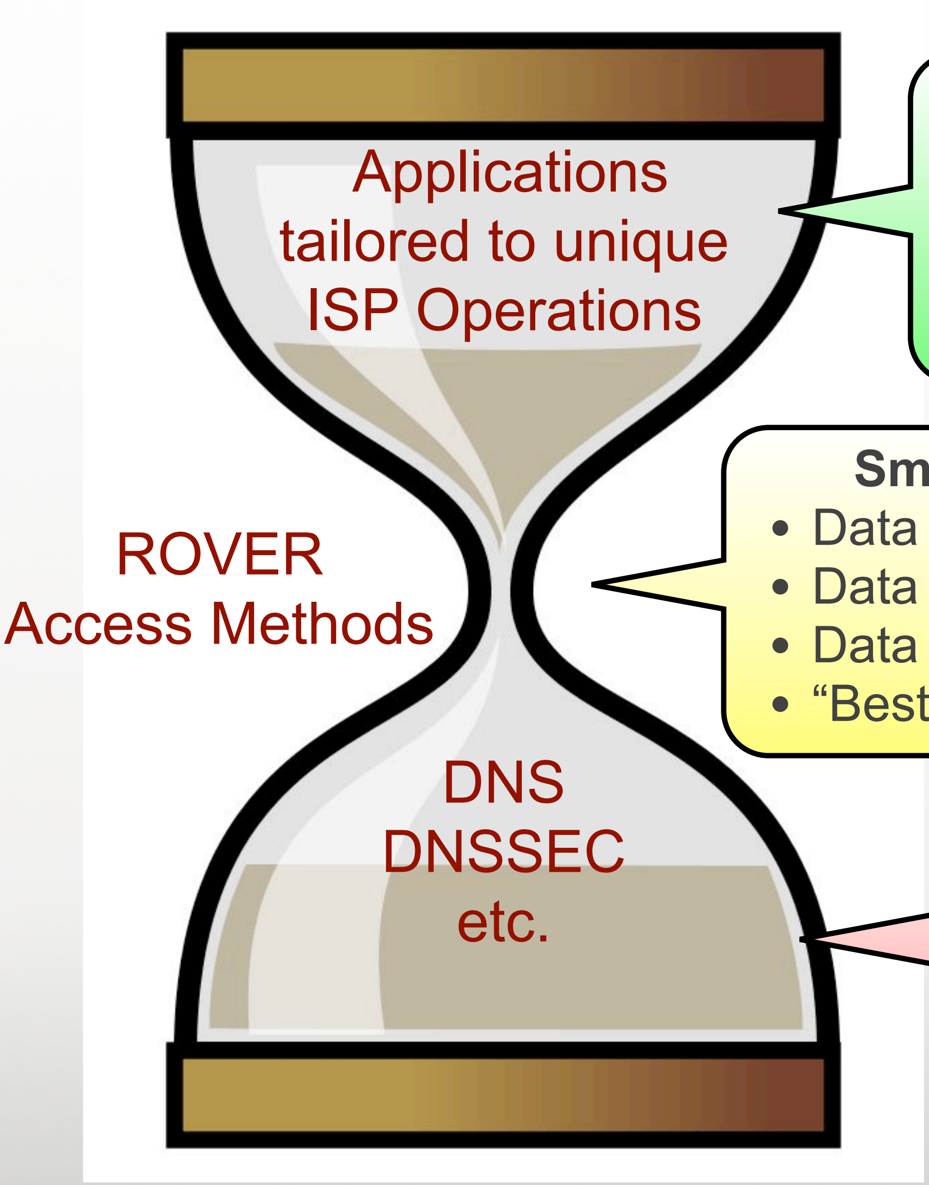
Small set of methods:

- 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

DNS
DNSSEC
etc.

ISP Applications:

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

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

Reverse DNS publishing method

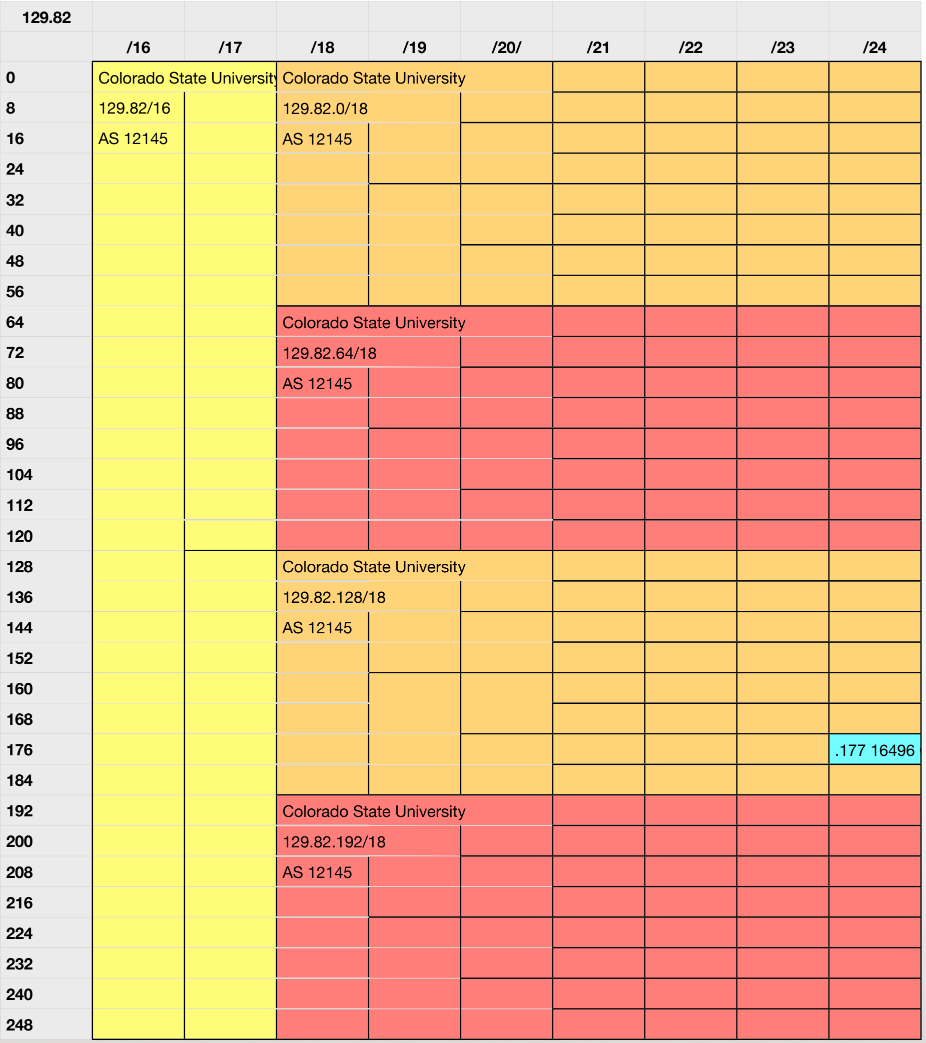
- General-Purpose Naming convention designed to specify CIDR address blocks. Example:
  - 129.82.128.0/18 --> 0.1.m.82.129.in-addr.arpa

- 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



129.82									
	/16	/17	/18	/19	/20/	/21	/22	/23	/24
0	Colorado State Universit		Colorado State University						
8	129.82/16		129.82.0/18						
16	AS 12145		AS 12145						
24									
32									
40									
48									
56									
64			Colorado State University						
72			129.82.64/18						
80			AS 12145						
88									
96									
104									
112									
120									
128			Colorado State University						
136			129.82.128/18						
144			AS 12145						
152									
160									
168									
176									.177 16496
184									
192			Colorado State University						
200			129.82.192/18						
208			AS 12145						
216									
224									
232									
240									
248									

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

ROVER Verification

SECURE64

- 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

SECURE64

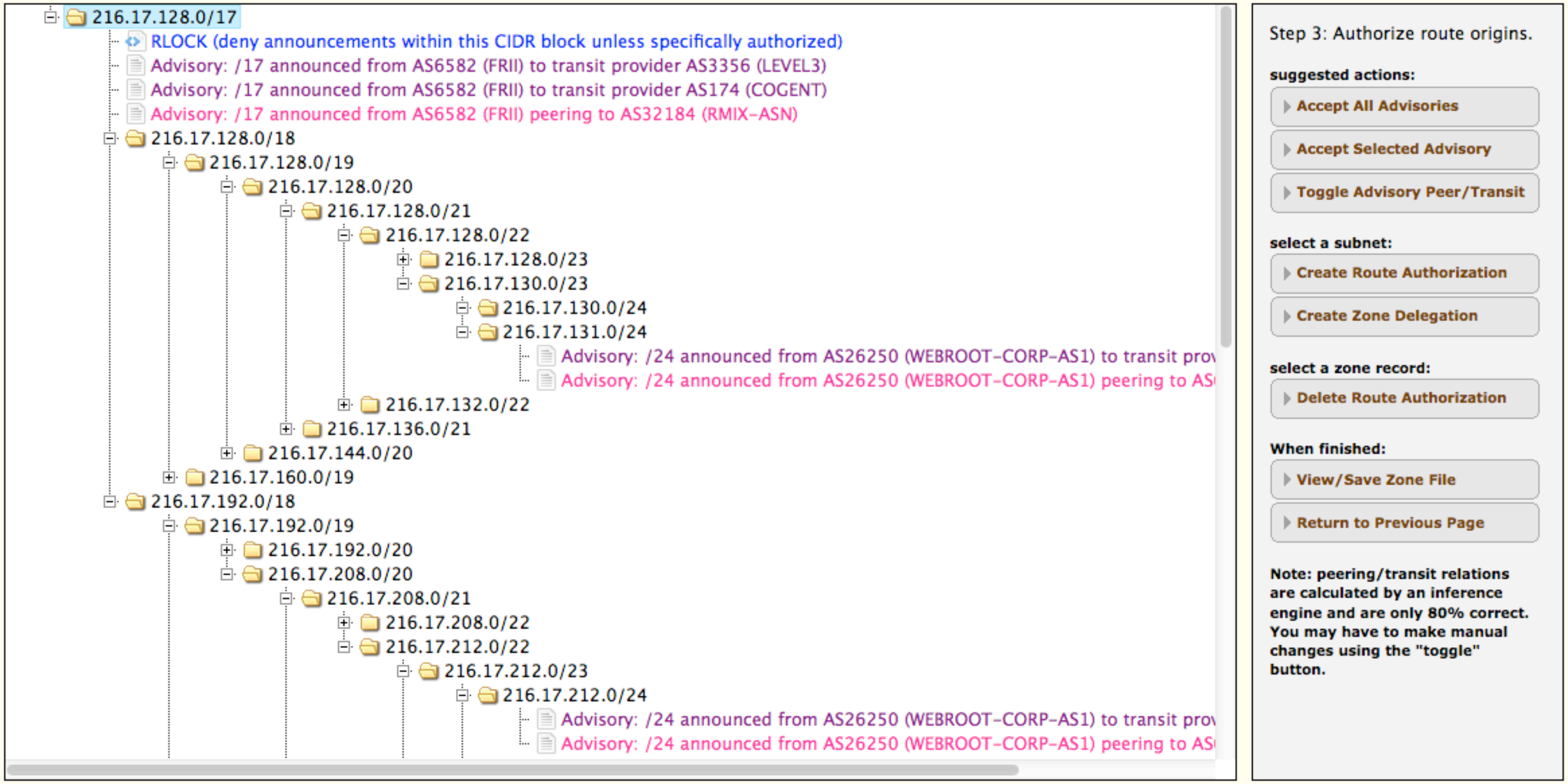
- Can a low–level protocol like BGP depend on a higher–level protocol?
  - no, not if there is a hard dependency
  - yes, if the dependency has a “fail–safe”
- Rover uses “best effort” data retrieval with world–wide data distribution, redundancy and local caching. Applications can use query retries with 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



```
216.17.128.0/17
    RLOCK (deny announcements within this CIDR block unless specifically authorized)
    Advisory: /17 announced from AS6582 (FRII) to transit provider AS3356 (LEVEL3)
    Advisory: /17 announced from AS6582 (FRII) to transit provider AS174 (COGENT)
    Advisory: /17 announced from AS6582 (FRII) peering to AS32184 (RMIX-ASN)
    216.17.128.0/18
        216.17.128.0/19
            216.17.128.0/20
                216.17.128.0/21
                    216.17.128.0/22
                        216.17.128.0/23
                        216.17.130.0/23
                            216.17.130.0/24
                            216.17.131.0/24
                                Advisory: /24 announced from AS26250 (WEBROOT-CORP-AS1) to transit prov
                                Advisory: /24 announced from AS26250 (WEBROOT-CORP-AS1) peering to AS
                    216.17.132.0/22
                216.17.136.0/21
            216.17.144.0/20
        216.17.160.0/19
    216.17.192.0/18
        216.17.192.0/19
            216.17.192.0/20
            216.17.208.0/20
                216.17.208.0/21
                    216.17.208.0/22
                    216.17.212.0/22
                        216.17.212.0/23
                            216.17.212.0/24
                                Advisory: /24 announced from AS26250 (WEBROOT-CORP-AS1) to transit prov
                                Advisory: /24 announced from AS26250 (WEBROOT-CORP-AS1) peering to AS
```

Step 3: Authorize route origins.

suggested actions:

select a subnet:

select a zone record:

When finished:

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!

SECURE64

- 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