Status Report
SIDR and Origination Validation

Geoff Huston

SIDR WG, IETF 71

March 2008

RPSEC Requirements

- From RPSEC the requirements are:
  - For Routing
    - Don’t increase convergence times
    - Allow for incremental deployment
    - Autonomous bootstrap
    - Local controls and local policies
    - Light touch on routers

RPSEC Requirements

- For infrastructure
  - Verification of data origination
  - Integrity of data
  - Resilience
  - Availability
  - No new imposed trust points

RPSEC on Origination

“Any BGP Security solution MUST support the ability of an address block holder to declare (in a secure fashion) the AS(es) that the holder authorizes to originate routes to its address block(s) or any portion thereof regardless of the relationship of the entities.

An associated delegation criteria is the requirement to allow for non-BGP stub networks. As a result, all secured BGP implementations MUST allow for the contemporaneous origination of a route for a prefix by more than one AS. “

draft-ietf-rpsec-bgpsecrec-09.txt

The SIDR Approach to Origination

Specification of a “Resource Public Key Infrastructure” (**RPKI**)

- Based on use of IP number resource extensions to PKIX Certificates (RFC 3779)
- A certificate hierarchy that conforms precisely to the IP address and AS allocation hierarchy
- Allows attestations or authorisations relating to IP addresses and AS numbers to be digitally signed by the certified resource holder
- Allows relying parties to validate such attestations within the context of the RPKI

The SIDR Approach to Origination

- Specification of a *protocol* between resource issuer and recipient to maintain an accurate certificate state at all times
  - relates allocation state to issued certificate state
- Specification of a *distributed publication repository structure*, allowing each CA and EE to publish signed products in local publication repositories
- Allow for Relying Parties to maintain a local cache of the current RPKI publication state in order to perform *local validation* operations

The SIDR Approach to Origination

Specification of two (so far!) signed objects in the RPKI framework to support origination validation:

- Specification of Route Origination Authorization (**ROA**) object to allow an address holder to authorize originating AS(s)
- Specification of a Bogon Origination Attestation (**BOA**) object to allow a resource holder to explicitly deny the validity of any origination using these resources

The SIDR Approach to Origination

- Approaches to **validated route update filter construction** may be considered
- Possible approaches:
  - Use of the RPKI BOA / ROA sets to generate filters for BGP speakers relating to origination acceptance

  or
  - Signed Internet Routing Registry objects to complement existing IRR-based filter construction tools with RPKI validation of IRR data

  or
  - Define additional RPKI objects in order to validate IRR objects to complement existing IRR-based tools

The SIDR Approach to Origination

- Approaches to Route object validation may be considered
  - A BGP Speaker *could* submit Route objects to a local RPKI validation engine that would attempt a match of the Route object to a valid published ROA or BOA in the RPKI
  - The validation outcome, coupled with local policy settings, *could* result in some form of local preference relative weighting that the relying BGP speakers could apply to the route object

Use of RPKI and BGP

- No required changes to BGP the protocol
  - For Example: Updates *could* contain a pointer to the associated ROA when looking at update validation, but this is neither required nor necessary
- Support piecemeal deployment models
  - For Example: Piecemeal use of ROAs and BOAs
  - Piecemeal use by BGP speakers
- Support local policy setting
  - ROA validation outcomes may set local BGP preferences
  - BOA validation outcomes may be used to apply local damping of an update
- No strict requirement to process online in real time
  - Alternative options to use near-line and near-time processing
  - May use a single processor per AS with a reverse iBGP feed of local preference settings according to local AS policy settings

Current SIDR Document Set

Resource PKI Documentation

- Architecture of the RPKI:
  draft-ietf-sidr-arch-03.txt
- Profile for RPKI Certificates:
  draft-ietf-sidr-res-certs-09.txt
- Profile for Route Origination Authorizations:
  draft-ietf-sidr-roa-format-02.txt
- Use of manifests o the RPKI publication repositories:
  draft-ietf-sidr-manifests-00.txt
- Certificate Policy for the RPKI:
  draft-ietf-sidr-cp-03.txt
- Template for Certification Practice Statement:
  draft-ietf-sidr-cps-irs-03.txt
  draft-ietf-sidr-cps-isp-02.txt