SIDR Approach

- SBGP and SoBGP represented different tradeoffs between processing load and levels of assurance
  - A new WG (RPSEC) was formed to list set of functional requirements that a secured routing framework should address
  - Working reached an agreement on using signed credentials to validate the function of route origination
  - WG also stalled on the topic of path validation
  - WG could not get to considering adherence to policy constraints

- In 2005, SIDR was created
  - IDR was pretty busy
  - Had lots of BGP extensions in form of WG documents
  - BGP Changes were time consuming and complicated
  - WG Mandate for multiple implementations slowed the publication process
  - New WG would be an easier approach as the design and prototypes for early RPKI and origin validation were done

SIDR Approach

- RPKI, ROV, and BGPSec work had something in common
  - Separate Data outside BGP that can be used to validate (inband data of) BGP
  - As opposed to, e.g. SO-BGP with in-band data, remember telco SS5 and Blue Boxes?
  - Quick to deploy and get deployment experience
  - Allowed this work to be developed in SIDR (outside IDR)

Solutions

- RPKI, ROV
  - Separate Resource Public Key Infrastructure (RPKI)
    - Managed by (IANA and) RIRs by acting as a Trust Anchors (TAs) and Certificate Authorities (CA)
  - Used for verification of Origin AS authorization of a given prefix
  - Backward compatible
  - Incremental Deployment trivial
  - Quick to deploy and get deployment experience

Solutions

- BGPSec
  - Performs Path validation by using cryptographic signatures
    - Stronger: Path Validation as well as Origin Validation
  - Replaces standard AS_PATH with BGPsec_Path attribute
  - Relies on RPKI to manage Keys and validate signatures
  - Reasonably secure solution that is computationally expensive and results in creation of larger update messages

Solutions

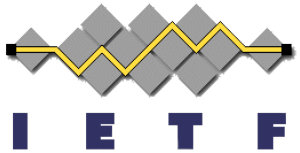
- ASPA
  - Validates the authenticity of the AS_Path information
  - Differs from BGPSec which provides cryptographic proof of the path integrity
    - Instead checks path integrity based on the AS relationships by leveraging RPKI infrastructure
  - Computationally less expensive than BGPSec when performing path validation

Alternatives

- IRR
  - Set of distributed public databases (maintained by RIRs) where network operators register their:
    - Routing policies
    - IP address ownership
  - Policy is stored in the Routing Policy Specification Language (RPSL)
    - Operators can query (whois) and access the data
  - Used to generate automatic filters for the routers to ensure only valid routing data is accepted
  - Helps in preventing route hijacking

Alternatives

- Peerlock
  - Operates on a list of Tier-1 ASNs
  - Filtering policy that rejects any routes with those Tier-1 ASNs coming from a customer session
  - Manual mechanism that requires updates to the List periodically (out-of-band co-ordination)
- ARIN's Origin AS
  - Opional ARIN directory that allowed IP address owners to list Authorised ASNs
  - Allowed ISPs to validate Letter of Authority (LOA)
  - Implemented as a Filtering Policy



Thank you