draft-ietf-sidr-origin-ops-13 diffs from -10 (July)

sidr / IETF Taipei

2011.11.15

Randy Bush <randy@psg.com>

Timing of Cache

Timing of inter-cache synchronization is outside the scope of this document, but depends on things such as how often routers feed from the caches, how often the operator feels the global RPKI changes significantly, etc.

As inter-cache synchronization within an operator does not impact global RPKI resources, an operator MAY choose to synchronize quite frequently.

'Close'

As RPKI-based origin validation relies on the availability of RPKI data, operators SHOULD locate caches close to routers that require these data and services. ~~A router can peer with one or more nearby caches.~~ 'Close' is, of course, complex. One should consider trust boundaries, routing bootstrap reachability, latency, etc.

Multi-Origin

If a prefix is legitimately announced by more than one AS, ROAs for all of the ASs SHOULD be issued so that all are considered Valid.

…

Operators owning prefix P should issue ROAs for all ASs which may announce P.

Which Attribute

Some providers may choose to ~~use the large~~ set Local-Preference ~~hammer. Others might choose~~ based on the RPKI validation result. Other providers may not want the RPKI validation result to ~~let AS-Path rule and set their internal metric, which comes~~ be more important than AS-path length -- these providers would need to map RPKI validation result to some BGP attribute that is evaluated in BGP's path selection process after AS-Path is evaluated. Routers implementing RPKI-based origin validation MUST provide such options to operators.

Overloading Local-Pref

Local-Preference may be used to carry both the validity state of a prefix along with it's traffic engineering characteristic(s). It is likely that an operator already using Local-Preference will have to change policy so they can encode these two separate characteristics in the same BGP decision process. attribute without negatively impact or opening privilege escalation attacks.

Accepting Invalid

Announcements with Invalid origins ~~MAY~~ SHOULD NOT be used, but ~~SHOULD~~ MAY be ~~less preferred~~ used to meet special operational needs. In such circumstances, the announcement SHOULD have a lower preference than ~~those with~~ that given to Valid or NotFound.

No State Signaling

Validity state signaling SHOULD NOT be accepted from a neighbor AS. The validity state of a received announcement has only local scope due to issues such as scope of trust, RPKI synchrony, and [I-D.ietf-sidr-ltamgmt].

Cache Timing

It is hoped that testing and deployment will produce advice on relying party cache loading and timing.