draft-ietf-sidr-bgpsec-reqs-01 diffs from -00 (Jul)

sidr / IETF Taipei

2011.11.15

Randy Bush <randy@psg.com>

Detect Modifications

A BGPsec design must allow the receiver of an announcement to detect if an AS has added or deleted any AS number other than its own in the path attribute. This includes modification to the number of AS prepends.

Transparent RSs

A BGPsec design MUST support 'transparent' route servers, meaning that the AS of the route server is not counted in downstream BGP AS-path-length tie-breaking decisions.

Route Leaks

What are 'Route Leaks'?

Not Mis-Originations

Hijack - no permission from resource holder

Squatting - had permission from the resource holder once upon a time

Rent - permission from the resource holder for some time period (customer is leaving)

Transfer - Resource moves from one party to the other

Note that these are all 'caught' by BGPsec Reqs

Not Protocol Violations

AS-Path – modification of AS-Path

NLRI – modification of NLRI

Note that these are all 'caught' by BGPsec Reqs

Policy Violations?

- Are they 'Policy Violations'?
- What Policy?
  - Peer 'leaking' from one peer to another?
  - Customer offering transit between upstreams?
  - Peer offering transit to peer?
- These are 'violations' of business policy

Protocol Not Intent

- We can not know business relationships, is A a peer of B, a customer, or something more complex?
- So we can not know if A **should have** announced P to B, we can only know if she **did** announce the prefix to B
- Business policy on the Internet changes every 36ms
- We already have a protocol to distribute policy or its effects, it is called BGP
- BGPsec validates that the protocol has not been violated, and is not about intent or business policy

http://puck.nether.net/bgp/leakinfo.cgi

- Jared Mauch's useful service to "find either persistent or Transient routing leaks that exist."
- Relies on built-in 'knowledge' of which ASs are Tier-1s and
- Detects customers leaking between Tier-1s
- Raises significant false positives because of this assumed knowledge
- No one would think of betting their routing on it

IRR and Other Policy Publication

- Voluntary and relying on someone expressing their policy properly
- Under-populated
- Can not change as often as policy, extra step in provisioning cycle
- Expresses high level intent but not fine grained, e.g. per prefix per path
- If it matches actual BGP policy, then it would work, but by essentially being the same data in two places, a well-known recipe for errors

Business Intent is a Human Concept

- We do not have the Do What I Mean button
- We have a means to say what we mean, BGP
- BGP shows the effects of what we mean, not the actual intent
- Any external publication of what we mean
  - is not acceptable at any sufficiently detailed level
  - would change every 36ms

Bar Time

So let's meet in the bar and see if we can actually define 'route leaks' in a useful way.

I.e. they can be formally described

They can be formally detected with known error bounds