Draft-ietf-sidr-bgpsec-protocol

Matt Lepinski
mlepinski@bbn.com

Draft-ietf-sidr-bgpsec-01

- Thank you to everyone who provided comments on the -00 draft

- Additional thanks to Wes George and Sandy Murphy who have ***already*** sent comments on the -01 draft!

pCount Field

- There was consensus at the Quebec meeting that BGPSEC should accommodate route servers that do not wish to increase the length of the AS-PATH.

- The -01 version adds a “pCount” field to address this route server issue and to permit adding multiple copies of an AS number without multiple signatures

Example (copies of AS number)

OLD (5 signatures)

AS-PATH : X Y Z Z Z

NEW (3 signatures)

pCount :	1	1	3
AS-PATH :	X	Y	Z

Note: AS Path Length is Sum of pCount

Note: This requires “expanding” the AS-PATH when we send an update
From a BGPSEC speaker to a non-BGPSEC speaker

pCount = 0 (Route Servers)

- A Route Server signs with its own AS
  - Maintains the security properties of BGPSEC
- A Route Server may set pCount to 0
  - This way a route server does not bias traffic away from itself by increasing the length of the AS-PATH
- Security Consideration
  - An entity that is not a route server could set pCount to 0 to bias traffic towards itself
  - If your peer is not a route server and sends you an update with pCount = 0, you should drop the update

Another pCount Example

OLD (6 signatures)

AS-PATH : W Y Z Z Z Z

Note: X is an “invisible” Route Server between W and Y

NEW (4 signatures)

pCount :	1	0	1	4
AS-PATH :	W	X	Y	Z

Question for the Working Group:

Is this a reasonable way to handle route servers?

Preventing Replay Attacks

- The primary goal of BGPSEC is to prevent your routes from being hijacked by malicious entities that have never legitimately been on the path for your prefix

- An additional goal of BGPSEC is to prevent someone that you used to do business with from replaying stale information to keep attracting your traffic

Preventing Replay Attacks

- Properties of replay attacks
  - Business relationships change on a slow time-scale
  - May be more difficult for humans to detect replay attacks than other types of route hijacking
- Current -01 draft has an expire-time mechanism to limit vulnerability to replay attacks
  - Goal of this mechanism is just to make sure that ancient business relationships do not come back to haunt you
  - Intent is that validity periods will be long, because business relationships don’ t change overnight

Preventing Replay Attacks

- There has been active discussion on the list on
  - Whether the benefits (replay protection) of the current expire-time mechanism are worth the cost
  - Concerns about the dangers of a misbehaving party who “beacons” too often
  - Possible alternative mechanisms
- We are not going to solve all this today
  - In order to have an informed debate about this mechanism, we probably need a better analysis of what is truly the cost of the current mechanism