Measurement Data on AS_SET and AGGREGATOR: Implications for {Prefix, Origin} Validation Algorithms

Presentation at the IETF SIDR WG Meeting, July 2010

Presenter: K. Sriram

(Contributors: NIST BGP Security Team)

July 2010

Contact: ksriram@nist.gov  dougm@nist.gov
Terminology Clarification

In the slides that follow:

**First AS after AS_SET** =
First AS to the immediate left of the AS_SET

(When present, AS_SET occurs in the rightmost position with respect to the position of octets in the protocol message)

**Origin AS**: When there is no AS_SET present, the Origin AS is the right most AS in the AS_SEQUENCE.
Enumeration Tree and Stats - 1

BGP Update Data
Routeviews OREGON - Feb. 2009

- BGP Update 1,783,668
  - AS_SET
    - 1323 (0.07%)
      - Aggregator 1322
        - Matches the First AS after AS_SET 1303
          - Private ASN* 19
        - Does’t Match the First AS after AS_SET 19
          - Not Private ASN 0
      - No Aggregator
        - 1
  - No AS_SET
    - 1,782,345 (99.93%)
      - Aggregator
        - 158,224
          - Matches the Origin AS 143,058
            - Private ASN* 13,485
          - Doesn’t Match the Origin AS 151,666
            - Not Private ASN 1,681
        - No Aggregator
          - 1,624,121

*Aggregator is a Private ASN

Private ASN range = [64512 – 65535]
Enumeration Tree and Stats - 2

BGP RIB Entry

11,387693

AS_SET
1749 (0.02%)

- Aggregator
  1749
  Matches the First AS after AS_SET 1689
  Private ASN*
  52

- No Aggregator
  0
  Does’t Match the First AS after AS_SET 60
  Not Private ASN
  8 (0.00007%)

No AS_SET
11,385944 (99.98%)

- Aggregator
  865620
  Matches the Origin AS 830030
  Private ASN*
  32330

- No Aggregator
  10,520324
  Doesn’t Match the Origin AS 35590
  Not Private ASN
  3260

*Aggregator is a Private ASN

Private ASN range = [64512 – 65535]
Enumeration Tree and Stats - 3

BGP Update Data
Routeviews OREGON - Feb. 2009

- BGP Update 1,783,668
  - AS_SET 1323 (0.07%)
    - Aggregator 1322
      - Matches the First AS after AS_SET 1303
        - Private ASN* 19
    - No Aggregator 1
      - Doesn’t Match the First AS after AS_SET 19
        - Not Private ASN 0
  - No AS_SET 1,782,345 (99.93%)
    - Aggregator 158,224
      - Matches the Origin AS 143,058
        - Private ASN* 13,485
    - No Aggregator 1,624,121
      - Doesn’t Match the Origin AS 15,166
        - Not Private ASN 16,811

*Aggregator is a Private ASN
Private ASN range = [64512 – 65535]
Enumeration Tree and Stats - 4

BGP RIB Data
Routeviews, OREGON - Aug. 26, 2009, 4:00pm

BGP RIB Entry 11,387693

- AS_SET 1749 (0.02%)
  - Aggregator 1749
    - Matches the First AS after AS_SET 1689
      - Private ASN* 52
    - Doesn’t Match the First AS after AS_SET 60
      - Not Private ASN 8 (0.00007%)
  - No Aggregator 0

- No AS_SET 11,385944 (99.99%)
  - Aggregator 865620
    - Matches the Origin AS 830030
      - Private ASN* 32330
    - Doesn’t Match the Origin AS 35590
      - Not Private ASN 3260
  - No Aggregator 10,520324

*Aggregator is a Private ASN
Private ASN range = [64512 – 65535]
Implications for the Algorithms

- It has been proposed to treat the AGGREGATOR as the Origin AS whenever an AS_SET is present (in {prefix, origin} validation algorithms).

- This can potentially lead to a new type of hijack attack possibility:
  - Attacker artificially places an AS_SET in his announcement
  - Sets the AGGREGATOR attribute value to the legitimate ASN
  - Places attacker’s own ASN in the first AS position after (i.e., immediate left of) the AS_SET

- Data (slides 2, 3) shows that AGGREGATOR attribute is almost always present and matches with the ASN in the first AS position after the AS_SET.

- The few cases when the two don't match are predominantly cases where the AGGREGATOR attribute is a private ASN (64512 – 65535). There should no ROAs anyway with private ASNs (in the context of global eBGP).

- Recommendation (based on the above observations):
  - It is better (more secure) to always take the first AS after the AS_SET as the Origin (disregard the AGGREGATOR)
  - This also keeps the algorithm simpler.