The Usage of Maxlength

Alexander Azimov, Yandex
mitradir@yandex-team.ru
Default Behavior: ROV

Default behavior – something that works in most cases.
The recommended default behavior for ROV – reject invalids.
When Route Becomes Invalid?

If the set of candidate ROAs is not empty **AND** none of candidate ROAs:
- Has asID value that matches the origin AS;
- Has maxlen length higher or equal then the prefix length.
When Route Becomes Invalid?

If the set of candidate ROAs is not empty **AND** none of candidate ROAs:

• Has asID value that matches the origin AS;
• Has maxlen higher or equal then the prefix length.

Does it really work out of the box in most cases?
Hosted CA

RIPE – suggests maxlength equal to the current prefix length;
APNIC – suggests maxlength equal to the current prefix length;
ARIN – TBD;
AFNIC – suggests maxlength equal to the current prefix length;
LACNIC – hosted ROAs are not available;
Maxlength & Invalids: Reject by Default?

- **Ingress filtering**
  - works by default for leafs;
  - doesn't work by default for transit ISPs (blackhole, etc.);

- **Egress filtering**
  - works by default for Tier1;
  - doesn't work by default for everybody else (blackhole, etc.);
Security Perspective: ROA + ASPA

<table>
<thead>
<tr>
<th>Mistake</th>
<th>BGP Hijacks</th>
<th>BGP Route Leaks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROA</td>
<td></td>
<td>ASPA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Malicious</th>
<th>BGP Hijacks</th>
<th>BGP Route Leaks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROA + ASPA</td>
<td></td>
<td>ROA + ASPA</td>
</tr>
</tbody>
</table>

In perfect world maxlenlength is not needed to fight malicious activity.
Security Perspective: Partial Adoption

• What if you specified maxlength=23 (or smaller);
• What if your upstream provider is rejecting invalids;
• What if somebody announces /24, even with invalid ASN;
• And invalid route is propagated, and thus preferred;
• What you will do? (accept postmortem)
Maxlength: Is It working by default?

• Ingress filtering  
  • works by default for leafs;  
  • doesn't work by default for transit (blackhole, etc.);

• Egress filtering  
  • works by default for Tier1;  
  • doesn't work by default for everybody else (blackhole, etc.);

• Security risks at the state of partial adoption;
Invalids & Maxlength

Global: Detailed Validation Results for 'Invalid'
7,563 Unique IPv4 Prefix/Origin Pairs

- invalid:AS (3,470)
- invalid:ML (3,249)
- invalid:AS-ML (392)
- invalid:AS-SET (52)

- invalid:AS-SET 0.88%
- invalid:AS-ML 11.64%
- invalid:ML 42.40%
- invalid:AS 45.28%
Question to WG

Some networks are setting maxlength to /32, /128;
Other networks are already crafting RPKI-cache to increase maxlength;
Significant number of networks are using defaults from RIRs portals.

Ignore? Accuse? Lead?