Proposing validation state “Unverified”

IETF 103 Bangkok
draft-borchert-sidrops-rpki-state-unverified-00
draft-borchert-sidrops-bgpsec-state-unverified-00

O. Borchert, D. Montgomery
National Institute of Standards and Technology
Proposal

• We propose adding the state “Unverified” to prefix origin validation and BGPsec path validation.

• This allows a well defined distinction between validated updates from non-validated updates.

• This will require updates to
  • RFC 6811, RFC 8097
    • draft-borchert-sidrops-rpki-state-unverified-00
  • and RFC 8205
    • draft-borchert-bgpsec-state-unverified-00
Reasoning

- If operators start creating policies for “NotFound” it becomes vital to distinguish between “NotFound” and not verified route prefixes.

- There are situations where validation is not performed (yet/ever).
  - No connection to validation cache yet / data not yet synchronized with validation cache
  - Operator chooses not to validate specific routes
  - “Lazy Evaluation” – asynchronous evaluation to prevent hold ups
  - Others...

- An unverified route is not the same as a verified route and vice versa
  - The lack of the state “Unverified” waters down the meaning of all other states.
    - RFC 6811 urges to use NotFound for unverified updates.
    - RFC 8205 does not mention what to do with unverified routes.
  - “Unverified” allows to signal within iBGP if an update was in fact validated or not.
    - The absence of the community string value does not make this clear.

- Each validation state of RFC 6811: “Valid”, “Invalid”, “Not-Found” and RFC 8205 “Valid”, “Not-Valid” is the result of well defined algorithms.
  - Not being validated must be a well defined state as well.
Real World Usage we found:

• Juniper
  • Provides the state “unverified”

• NIST BGP-SRx
  • Provides the state “undefined”

• Others?
Update to RFC 6811

Add the state:

- Unverified: Specifies the state of a route prefix on which no evaluation has been performed.

Paragraph 2. Prefix-to-AS Mapping Database

Update the statement:

“If validation is not performed on a Route, the implementation SHOULD initialize the validation state of such a route to "NotFound".”

with:

“If no evaluation of a route prefix is performed in any form, the implementation MUST initialize the validation state of such a route to "Unverified".”

draft-borchert-sidrops-rpki-state-unverified
Update to RFC 8097

Paragraph 2. Origin Validation State Extended Community

Extend the Table

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Lookup result = &quot;valid&quot;</td>
</tr>
<tr>
<td>1</td>
<td>Lookup result = &quot;not found&quot;</td>
</tr>
<tr>
<td>2</td>
<td>Lookup result = &quot;invalid&quot;</td>
</tr>
</tbody>
</table>

with:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Lookup result = &quot;valid&quot;</td>
</tr>
<tr>
<td>1</td>
<td>Lookup result = &quot;not found&quot;</td>
</tr>
<tr>
<td>2</td>
<td>Lookup result = &quot;invalid&quot;</td>
</tr>
<tr>
<td>3</td>
<td>Lookup result = &quot;unverified&quot;</td>
</tr>
</tbody>
</table>

draft-borchert-sidrops-rpki-state-unverified
5.1 Overview of BGPsec Validation

…

“The validation procedure results in one of two states: 'Valid' and 'Not Valid’”

…

“BGPsec validation need only be performed at the eBGP edge.”

…

The following sentence should be added saying:

“BGPsec routes MUST be initialized using the BGPsec validation state "Unverified" until proper evaluation of the BGPsec route has been performed.”