Authorisation and validation in BGP - beyond origin
Origin Validation

• Origin Validation is useful
  - Provisioning
  - Fat fingers
  - Disallow hijack by more specific announcements

• But not enough
  - Origin ASN can be faked
  - Route leaks (violation of policy) still possible
BGPsec - nobody lied :)
BGPSec - AS65002 is trying to lie!

ROA 10.0.0.0/20
From AS65001
Signed 10.0.0.0/20

AS65001

10.0.0.0/20
To AS65002
signed AS65001

AS65002

ASX
Lift-off?
So what’s the issue?

- Fundamental view of security as a data problem

- Takes too much computing
  - Only available in Bird and Quagga, not hardware routers
  - 45 minutes to load table (theoretically)

- Everyone needs to participate
  - Or else a downgrade attack would allow lies
  - No incremental deployment
So, what’s next?
Respect roles and issues

• Providers
  - Willing, protect reputation and don’t want to be liable for issues

• IXPs
  - Increasingly offering security as a service, but remain neutral

• Transit providers
  - Filtering means loss of revenue
  - Net neutrality

• Stubs
  - Some want to block bad traffic (hacks/spam) even if no alternative
Why do security?

• For the good of the internet, isn’t good enough

• There need to be clear benefits for participants

• Open questions:
  - Will resource holders demand that their addresses are not hijacked?
  - Will stub networks demand that bad traffic is blocked earlier?
  - Will regulators step in?
Other restrictions

- Must allow for incremental uptake
- Must not require new hardware
- Authorisations be easy to maintain and debug
- Validation must be easy to maintain and debug
- Must be fast to propagate
- Must be so easy, that there is no excuse.
So, what’s next?
### AS Cones - Simple AS Sets

<table>
<thead>
<tr>
<th>TO</th>
<th>Customers</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS65002</td>
<td>None</td>
</tr>
<tr>
<td>AS65003</td>
<td>AS65001, AS65005, AS65006</td>
</tr>
<tr>
<td>ANY</td>
<td>None</td>
</tr>
</tbody>
</table>

**Signed AS65001**

- Similar to: export to ASX announce AS-SET-X
- Authoritative signatures!
- Much easier to find (parsing RPSL near impossible)
- Work is being done to prepare a draft in the IETF
AS cones - partial

ROA
10.0.0.0/20
From AS65001
Signed
10.0.0.0/20

AS65001

I send updates
to AS65002
I don’t send customers

signed AS65001

AS65002

ASX
AS cones - ok with simple policy

ROA
10.0.0.0/20
From AS65001
Signed
10.0.0.0/20

AS65001
I send updates to AS65002
I don’t send customers
signed AS65001

AS65002
I send updates to ASX including AS65001
signed AS65002

ASX
AS cones - leak

ROA
10.0.0.0/20
From AS65001
Signed
10.0.0.0/20

AS65001

AS65002

ASX

I send updates to AS65002
I don’t send customers
signed AS65001

I send updates to ASX
But not AS65001
signed AS65002
AS cones - undeclared upstream

- **AS65001**
  - ROA: 10.0.0.0/20
  - Signed: 10.0.0.0/20
- **AS65002**
- **ASX**

I send updates to AS65005 and AS65006 only

signed AS65001

Tim Bruijnzeels | 10 April 2018 | RIPE NCC Educa
Summary

- Builds on existing practice of AS-SETs
- Can be extended to declare exclusive upstreams
- Simplified RPSL sub-set
  - Only what is really useful
  - Compatible: can be expressed as RPSL
- Leverage RPKI for signature by ASN
- Easy to find policy for ASN
- Validation in validator, no crypto on routers
Questions

tim@ripe.net