RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Authorisation and validation in BGP - beyond origin

Tim Bruijnzeels | 10 April 2018 | RIPE NCC Educa

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 :)

ROA
10.0.0.0/20
From AS65001

Signed
10.0.0.0/20

10.0.0.0/20
To AS65002

signed AS65001

10.0.0.0/20
To AS65002

signed AS65001

To ASX

signed AS65002

BGPSec - AS65002 is trying to lie!

ROA
10.0.0.0/20
From AS65001

Signed
10.0.0.0/20

AS65001

AS65002

ASX

10.0.0.0/20
To AS65002

signed AS65001

Lift-off?

https://www.flickr.com/photos/fbthienvanhoc/6433042299

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?

https://www.flickr.com/photos/infowire/21523294814

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?

https://www.flickr.com/photos/infowire/21523294814

AS Cones - Simple AS Sets

TO	Customers
AS65002	None
AS65003	AS65001, AS65005, AS65006
ANY	None

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

I send updates
to AS65002
I don't send
customers

signed AS65001

AS cones - ok with simple policy

ROA
10.0.0.0/20
From AS65001

Signed
10.0.0.0/20

I send updates to AS65002
I don't send customers

signed AS65001

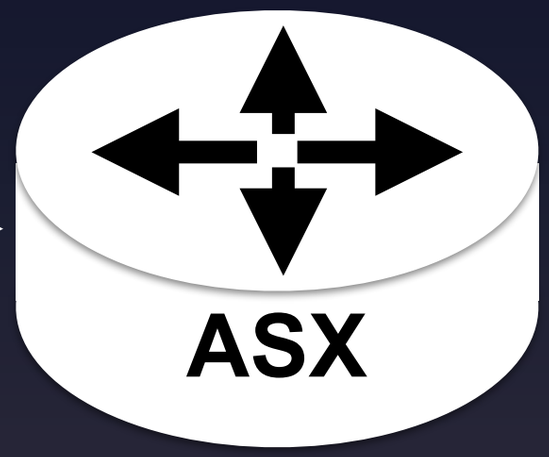
I send updates to ASX including AS65001

signed AS65002

AS cones - leak

ROA
10.0.0.0/20
From AS65001

Signed
10.0.0.0/20



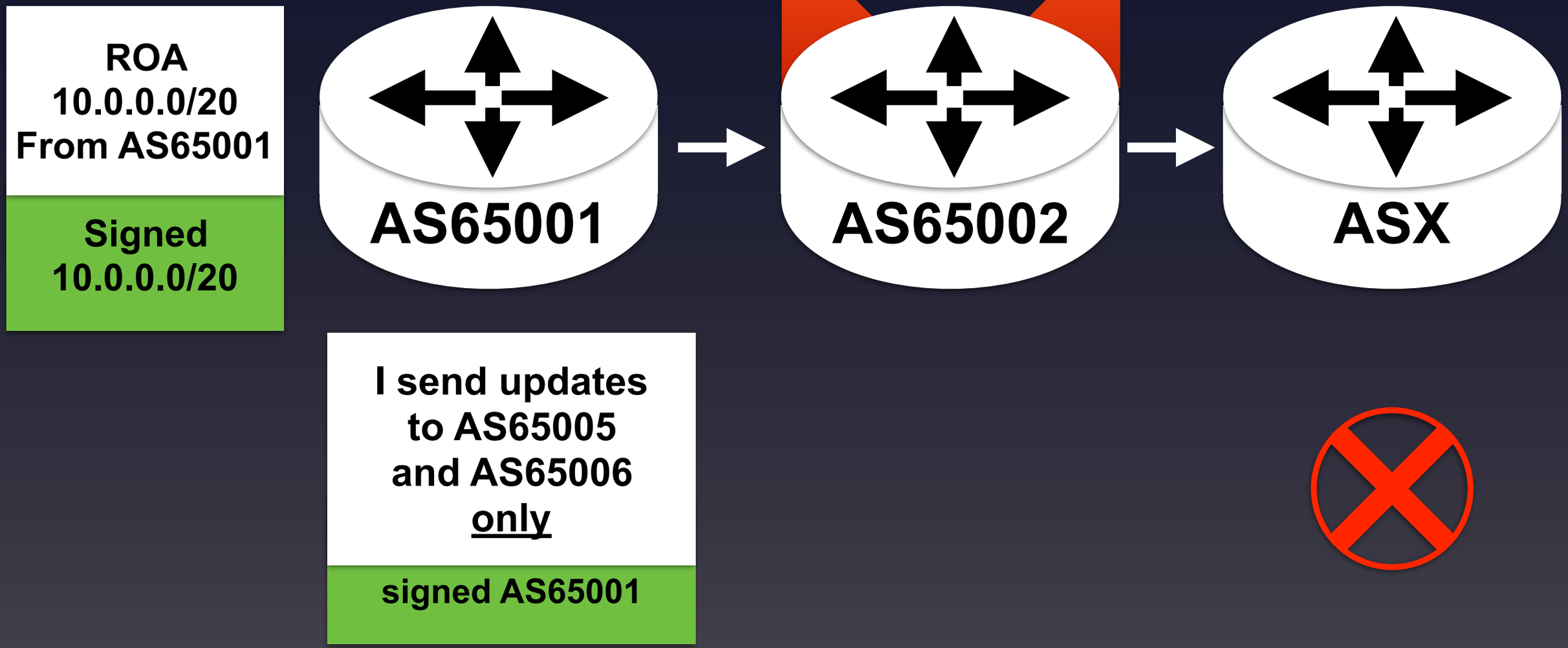
I send updates
to AS65002
I don't send
customers

signed AS65001

I send updates
to ASX
But not AS65001

signed AS65002

AS cones - undeclared upstream



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