Some Thoughts on Integrity in Routing

Geoff Huston
Chief Scientist, APNIC
What we want...

- We want the routing system to advertise the **correct** reachability information for "**legitimately connected** prefixes at all times
- That means that we want to **avoid**:
  - promulgating reachability for bogus address prefixes
  - promulgating incorrect paths for reachable prefixes
  - blocking paths for legitimately connected prefixes
What do we do today?

I ask you to route my address prefix

You look for these addresses on whois*

If it all seems to match then accept the request and add it to the network filters for this customer

* As usual, its not as simple as that, as there are a number of whois servers, and you probably have to negotiate across a number of them to get what you are after, or to be assured that the entry is not in any of the registry data collections
What do we do today?

I ask you to route my address prefix

You look for these addresses on whois

If it all seems to match, then request:

The awesome power of whois!

* As usual, it's not as simple as that, as there are a number of whois servers, and you probably have to negotiate across a number of them to get what you are after, or to be assured that the entry is not in any of the registry data collections.
What do we do today?

I ask you to route my address prefix.

You look for these addresses on whois servers.

If it all seems to match then accept the request and add it to the network filters for this customer.

This is a manual process that relies on ascii pattern matching, it is error prone, does not scale, and provides no ongoing assurance.
What do we do today?

I ask you to route my net

You ask for me to provide a “Letter of Authority”

   Which is an effort to absolve you of all liability that may arise from announcing this route

You then add the to the network filters for this customer
What do we do today?

I ask you to route my net.

You ask for me to provide a "Letter of Authority".

Which is an effort to absolve you of all liability that may arise from announcing this route.

You then add the traffic to customer
What do we do today?

I ask you to route my net.

You ask for me to provide a "Letter of Authority".

Which is an effort to absolve you of all liability that may arise from announcing this route.

You then add the to the network filters for this customer.

This is little more than blame shifting.

This is no good at detecting incorrect routing requests.

But at least you are off the hook when the network police come knocking!!
What do we do today?

I ask you to route my net

You ask for me to enter the details in a route registry

Your routers’ access filters may be automatically generated from the route registry data that I entered
What do we do today?

I ask you to route my net

You ask for me to enter the details in

Your routers’ access filters may be at
the route registry data that I entered
What do we do today?

I ask you to route my net.

You ask me to enter the details in a route registry.

Your routers' access filters may be automatically generated from the route registry data that I entered.

- How current is this data?
- Is it complete?
- Can it be tampered with?
- Who entered this data? With what authority?
- Can I trust it to use the stored information as an automatic filter generator for my network?
What do we do today?

I ask you to route my net.

You ask for me to enter the details in a route registry.

Your routers' access filters may be automatically generated from the route registry data that I entered.

How current is this data? Is it complete? Can it be tampered with? Can I trust it to use the stored information as an automatic filter generator for my network?

A publicly accessible description of every import and export policy to every transit, peer, and customer, has proved to be extremely difficult to maintain.

Today, we have many routing registries, not one, and the quality of the data in those registries is close to impossible to ascertain.
What’s the problem here?

• None of these approaches are very satisfactory as a complete solution to this problem

• Let’s take a step back and see if we can use digital signature technology to assist here.

• If we can, then we can construct automated systems that will recognise validly signed attestations about addresses and their use
Registry Role

• The registry plays the role of a neutral third party ‘trust point’ that can provide an impartial record of which entity is the current holder of an IP address

• Which is fine for humans, but of limited use to automated systems

• How can we automate the validation function that allows an entity to validate whether or not a party is the current holder of an IP address?
Crypto to the rescue!

• Public / Private keys can be really useful here
  – I sign <something> using my private key and send it to you
  – Using my public key you can be assured that:
    • I signed this (and no one else)
    • I cannot deny that I signed it
    • What I signed has not been altered on the way between me and you
  – The assurance can be automated, and does not necessarily rely on a manual process of matching ascii text
The RPKI

• If I have the association between a public key and a number block registered by the RIR, then
  – Instead of performing a human match between the registry entry and the party you can get the party to sign an attestation using their local private key
  – If the attestation can be validated by the public key published by the RIR then you have automated the validation function and don’t need eyeballs to read web pages to validate the ‘rights’ of use of IP addresses
The RPKI Certificate Service

- Enhancement to the RIR Registry
  - Offers verifiable proof of the number holdings described in the RIR registry

- Resource Certification is an opt-in service
  - Number Holders choose to request a certificate
    - Derived from registration data
**BGPSEC: BGP + RPKI Origination**

- One approach is to look at the process of “permissions” that add an advertised address prefix to the routing system:
  - The address holder is authorizing a network to originate a route advertisement into the routing system

- The **ROA** is a digitally signed version of this authority. It contains:
  - An address prefix (and range of ‘allowed’ prefix sizes)
  - An originating ASN

- This allows others to check the validity of a BGP route origination:
  If there is a valid ROA, and the origin AS matches the AS in the ROA, and the prefix length is within the bounds of the ROA, then the announcement has been entered into the routing system with the appropriate permissions
BGPSEC: BGP + RPKI Propagation

- In BGP AS Path manipulation is also a problem
- How can a BGPSEC speaker know that the AS Path in a BGP Update is genuine?
- Answering this question in BGPSEC gets very messy very quickly!

In my opinion: It’s highly unlikely that we will see widespread uptake of BGPSEC anytime soon, if ever, largely due to the overheads associated with AS path signing.
Errrr – why isn’t this being adopted by ISPs?

• Cryptography and Certificate management are operationally challenging:
  which is often seen as one more thing to go wrong!

• Validation of signed data is convoluted – maybe it should’ve been simpler

• Its not just ROAs – you need AS Path protection as well
  – As long as a hijacker includes your ROA-described originating AS in the faked AS PATH then the hijacker can still inject a false route
  – If ROAs are challenging for operators, then BGPsec is far more so!
The Perfect is the Enemy of the Good

Maybe there are some “Good” things we can do right now instead of just waiting for BGPsec to be sorted out!
More Ideas?

• Waiting for everyone to adopt a complex and challenging technology solution is probably not going to happen anytime soon

• Are that other things we can do that leverage the RPKI in ways that improve upon existing measures?
  – Use ROAs to digitally sign a LOA?
  – Digitally sign whois entries?
  – Digitally sign Routing Policy descriptions in IRRs

  – Signed data could help a user to determine if the information is current and genuine
  – This would not directly impact routing infrastructure, but instead would improve the operators’ route admission process to automatically identify routing requests that do not match signed registry / routing database information
What should we do?

• We could keep on thinking about how to make a routing infrastructure that is impervious to attempts to coerce it into false states
  – But it seems that we are not sure how to do this, and not sure who would pay the cost of trying to do this!

AND/OR

• Perhaps we should undertake some focussed work on open BGP monitoring and alarm services that allow us to detect and identify routing issues as they arise, and assist network operators to respond quickly and effectively
Thanks!