Securing BGP:
The current state of RPKI

Geoff Huston
Chief Scientist, APNIC
Incidents

Google search results for "routing hijacks BGPmon" showing:

- Russian-controlled telecom hijacks financial services' Internet traffic...
- BGP routing attacks in 2014 - BGPmon
- Large hijack affects reachability of high traffic destinations | BGPmon
- Chinese ISP hijacks the Internet | BGPmon
- BGPstream and The Curious Case of AS12389 | BGPmon
- BGP instability, BGPmon.net, bogons, Hijack, IPv6, IRR, News and ...

About 2,410 results (0.37 seconds)
What happens when I announce your addresses in BGP?

All the traffic that used to go to you will now come to me

I can disrupt your service

I can inspect unencrypted traffic that was heading towards you

I can send out traffic as if it was you

I can emit spam, mount bot attacks, or misbehave

I can get a certificate in your name

I can inspect encrypted traffic heading to your servers

I can mount pernicious man-in-the-middle attacks
If I were evil

• I’d announce your routes
• Use an automated cert issuer to get a certificate issued for your domain name
• Attract all secure traffic intended for your service and pass it on (man-in-the-middle)
  • But I use _MY_ encryption to the end user, so I can see everything the end users does with your service, including their passwords
  • And its not clear that they will notice anything amiss
If I were evil

- I’d announce your routes
- Use an automated cert issuer to get a certificate issued for your domain name
- Attract all secure traffic intended for your service and pass it to the end user, so I can see what users does with your service, including their passwords
- And it’s not clear that they will notice anything amiss

This form of attack is challenging to prevent once the route hijack is installed. So a useful defence is to ensure that the routing system resists attempts to install route hijacks.
If I were evil

- I’d announce your routes
- Use an automated cert issuer to get a certificate issued for your domain name
- Attract all secure traffic intended for your service and pass it on (man-in-the-middle)
- But I use _MY_ encryption to the end user, so I can see everything the end users do with your service, including their passwords
- And it's not clear that they will notice anything

How can we counter route hijacks?

How can we tell what is a “genuine” route update and what’s a fake?
What do we do today?
What do we do today?

I ask you to route my net:
You look the net up on whois
If it all seems to match then accept the request and add it to the network filters for this customer
What do we do today?

I ask you to route my net:

You look the net up on whois

If it all seems to match then:

The awesome power of whois!

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 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 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 route to the network filters for this customer.

At least you are off the hook when the network police come knocking!!

Wanna break your contract and get kicked out of your customer?
What do we do today?

I ask you to route my net

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

Access filters may be automatically generated from route registry data
What do we do today?

I ask you to route my net

You ask for me to enter the details in

Access filters may be automatically gen
What do we do today?

I ask you to route my net

You ask for me to enter:

How current is this data?

Is it complete?

Can I trust it to use as an automatic filter generator for my routers?
What do we do today?

I ask you to route my net

You ask for me to enter this data?

A publicly accessible description of every import and export policy to every transit, peer, and customer, is difficult to maintain, and is not in the best business interests of many ISPs.
What’s the problem here?

• Whois lookups typically require manual processing.
  • This information is also somewhat informal so it often requires some level of interpretation and judgment
  • Whois lookups are an admission process, not a means to maintain route filters
• Letters of Authority are just a way to try and avoid liabilities – they are not a useful tool to manage routing
• Routing Registries come in all shapes and sizes!
  • Which is itself a problem – there is no single authoritative source
  • The expression of routing policies quickly becomes complex and error prone
  • Is this a case of attempting to harness too much information?
The RPKI Approach

• 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
Using Cryptography to tell “Good” from “Bad”

This looks a lot like an application of public/private key cryptography, with “authority to use” conveyed by a digital signature

• Using a private key to sign the authority, and the public key to validate the authority
• If the private key was held by the address holder then we have the notion of binding the control over an address to holding the private key
• We can use a conventional certificate infrastructure to support public key validation at the scale of the Internet
• But how can we inject trustable authority into this framework?
Trustable Credentials

How can we inject trustable authority into this framework?
Trustable Credentials

How can we inject trustable authority into this framework?

Bind the Registry and the key structure together:

• Use the existing address allocation hierarchy
  • IANA, RIRs, NIRs & LIRs, End holders

• Describe this address allocation structure using digital certificates

• The certificates do not introduce additional data – they are a representation of registry information in a particular digital format
Resource Certificates

• A resource certificate is a digital document that binds together an IP address block with the IP address holder’s public key, signed by the certification authority’s private key.

• The certificate set can be used to validate that the holder of a particular private key is held by the current legitimate holder of a particular number resource – or not!

• Community driven approach
  • Collaboration between the RIRs since 2006
  • Based on open IETF standards
    • Based on work undertaken in the Public Key Infrastructure (PKIX) and Secure Inter-Domain Routing (SIDR) Working Groups of the IETF
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
What Can we Sign?

• One approach is to look at the process of “permissions” that add an advertised address prefix to the routing system:
  • The address holder is “authorising” 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 sixes
  • An ‘originating address’

• This allows others to check the validity of a BGP route announcement:
  • 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
So ROAs can help

• An automated solution that checks the validity of a route announcement against a local repository of digital certificates:
  Which can be used to feed a BGP routing filter that can isolate certain instances of what looks like attempted route hijack
Are we using RPKI and ROAS

• Two questions:
  • What proportion of existing route advertisements have associated published ROAs?
  • What proportion of network operators will reject a route if the associated ROA set indicates an invalid route advertisement (possible route hijack)
Global: Validation Snapshot of Unique P/O pairs
725,917 Unique IPv4 Prefix-Origin Pairs

- **Invalid (605,632)**: 80.8%
- **Valid (54,505)**: 7.51%
- **Not-found (5,780)**: 0.80%
- **Not-found (91.70%)**

https://rpki-monitor.antd.nist.gov
ROA publication

Global: Validation History of Unique P/O pairs

Only IPv4 Prefixes

- Not found
- Valid
- Invalid

https://rpki-monitor.antd.nist.gov
Global: 25 Autonomous Systems with the most Address Space VALID by RPKI

NIST RPKI Monitor: 2017-08-14

https://rpki-monitor.antd.nist.gov
ROA Use

Measuring Adoption of RPKI Route Validation and Filtering

Andreas Reuter (andreas.reuter@fu-berlin.de)

Joint work with Randy Bush, Ethan Katz-Bassett, Italo Cunha, Thomas C. Schmidt, and Matthias Wählsch

https://ripe74.ripe.net/presentations/43-ovs-study-ripe74-plen-final.pdf
ROA Use

Results
We found at least 3 AS that deployed RPKI-based filtering!
None of them are large providers ...

| 2 AS filtered all invalid routes | 1 AS filtered selectively |

Conclusion

→ There are ASes that do RPKI-based filtering.
   Not many, not the big ones, but at least some (>3).

→ Uncontrolled experiments are unsuited to infer RPKI-based filtering policies

→ Controlled experiments are crucial to measuring adoption of RPKI-based filtering policies

Internet infrastructure requires proper monitoring.

https://ripe74.ripe.net/presentations/43-ovs-study-ripe74-plen-final.pdf
• If route hijacking is such a problem then why aren’t we all publishing ROAs and running ROA filters on our routers?

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

• Without everybody running BGPsec that it is not a very robust defence
  
  As long as a hijacker includes your ROA-described originating AS in the faked AS PATH the hijacker can still inject a false route

• If ROAs are challenging for operators, then BGPsec is far more so!
The Perfect can be the enemy of the Good

Maybe there are some “Good” things we can do right now instead of just waiting for BGPsec to work!
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
Thanks!