An Operational Perspective on Routing Security

Geoff Huston
Chief Scientist, APNIC
On the Internet...
there are many ways to be bad!
there are many ways to be bad!

- Enlist a bot army and mount multi-gigabit DOS attacks
  - Extortion leverage and general mayhem
- Port Scan for known exploits
  - General annoyance
- Spew spam
  - Yes, there are still gullible folk out there!
- Mount a fake web site attack
  - And lure victims
- Mount a routing attack
  - And bring down an entire region / country / global network!
If I were bad (and greedy)...

I’d attack routing.

- Through **routing** I’d attack the **DNS**
- Through the DNS I’d lure traffic through an **interceptor web server**
- And be able to quietly collect users’ details

Welcome to today’s online fraud industry
I’d attack routing.

• Through routing I’d attack:
  – the route registry server system
  – the DNS root system
  – trust anchors for TLS and browser certificates
  – isolate critical public servers and resources
  – overwhelm the routing system with spurious information

And bring selected parts of the network to a complete chaotic halt!
How Pakistan knocked YouTube offline (and how to make it happen again)

Pakistan's telecommunications regulator has lifted the restrictions it imposed on video-sharing website YouTube.

The Pakistan Telecommunications Authority has told internet service providers (ISPs) to restore access to the site, according to a spokeswoman.

Google, the owner of YouTube, confirmed service had been restored in Pakistan.

The attempt to block the site, reportedly because of a "blasphemous" video clip, caused a near-global blackout of the site on Sunday.

A spokesman for YouTube told the BBC News website: "We are pleased to confirm that YouTube is again accessible in Pakistan."

It is reported that a trailer for a forthcoming film by Dutch filmmaker Rein Wenders, which portrays Islam in a negative light, was behind the restrictions.

A leading net professional told BBC News: "This was probably a simple mistake by an engineer at Pakistan Telecom. There's nothing to suggest this was malicious."

A Pakistan court bans YouTube.

The ban was lifted once PCCW had been told of the issue by YouTube engineers.

A statement from Google said that the problems lasted for "about two hours".

"Traffic to YouTube was routed according to erroneous internet protocols, and many users around the world could not access our site," it said.

"The fact YouTube is back in action makes me revise my thoughts on the clash between governments and freedom of speech," wrote Rory Cellan-Jones in his blog.
Some recent cases ...

208.65.153.0/24 originated by AS17557
   Advertisement of a more specific route by Pakistan Telecom that managed to take YouTube off the air in February 2008

61.0.0.0/8 originated by AS4678
   Advertisement of a more general route by a spammer in order to conceal their identity by using an anonymous source IP address, occurring intermittently 2004 – 2007

d000::/8 originated by AS28716
   Advertisement of a massive bogon more general route in IPV6 from 13 Nov 2009 until 15 Jan 2010 – and no one noticed for 2 months!
How many advertisements in today's BGP are "lies"?
### Possible Bogus Routes

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Origin AS</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>41.223.32.0/22</td>
<td>64932</td>
<td>GNL-AS-CN</td>
</tr>
<tr>
<td>41.223.198.0/24</td>
<td>64932</td>
<td>GNL-AS-CN</td>
</tr>
<tr>
<td>41.223.199.0/24</td>
<td>64932</td>
<td>GNL-AS-CN</td>
</tr>
<tr>
<td>46.9.0.0/16</td>
<td>64932</td>
<td>GNL-AS-CN</td>
</tr>
<tr>
<td>46.10.0.0/21</td>
<td>64932</td>
<td>GNL-AS-CN</td>
</tr>
<tr>
<td>46.12.0.0/21</td>
<td>64932</td>
<td>GNL-AS-CN</td>
</tr>
</tbody>
</table>

### Unallocated block

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Origin AS</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>41.223.200.0/24</td>
<td>64932</td>
<td>GNL-AS-CN</td>
</tr>
<tr>
<td>41.223.201.0/24</td>
<td>64932</td>
<td>GNL-AS-CN</td>
</tr>
<tr>
<td>41.223.202.0/24</td>
<td>64932</td>
<td>GNL-AS-CN</td>
</tr>
<tr>
<td>41.223.203.0/24</td>
<td>64932</td>
<td>GNL-AS-CN</td>
</tr>
<tr>
<td>41.223.204.0/24</td>
<td>64932</td>
<td>GNL-AS-CN</td>
</tr>
</tbody>
</table>

---

**Note:** The above prefixes are examples of potential boggy routes, and the unallocated block prefixes represent unused IP addresses. The origins and specific details can vary widely, so it's important to cross-reference with authoritative sources for accurate information.
getting the point yet?
still more!
wake me up when we're done
almost done…
**Possible Bogus Routes and AS Announcements**

**Possible Bogus Routes**

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Origin AS</th>
<th>AS Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:07f0::35</td>
<td>AS17832</td>
<td>SDXGIX-AS-KR Korea Internet Security Agency</td>
</tr>
<tr>
<td>2001:07f0::32</td>
<td>AS23634</td>
<td>E-DNS-IP WIDE Project</td>
</tr>
<tr>
<td>2402:ac0c::32</td>
<td>AS57575</td>
<td>AARNET-AS-AU Australian Academic and Research Network (AARNet)</td>
</tr>
<tr>
<td>2404:0078:0001::348</td>
<td>AS17893</td>
<td>PALAU-AS-AP Palau National Communications Corp.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unallocated block</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:7f0:0:4:: - 2001:7f0:0:fff::ffff:ffff:ffff:ffff</td>
</tr>
<tr>
<td>2402:ec0b:0: - 2402:ec0b:fff:ffff:ffff:ffff:ffff:ffff</td>
</tr>
<tr>
<td>2404:00: - 2404:00:fff:ffff:ffff:ffff:ffff:ffff</td>
</tr>
</tbody>
</table>

Report: Allocated and Unallocated IPv6 address blocks

No Bogus ASs

Report: Allocated and Reserved AS blocks
What's the base problem here?

No one seems to want to care enough about the integrity of the network to address routing integrity!
Today's Routing Environment is Insecure

- Routing is built on sloppy mutual trust models
- Routing auditing is a low value activity that noone performs with any level of thoroughness
- We have grown used to lousy solutions and institutionalized lying in the routing system
Routing is a shared problem

It’s a “tragedy of the commons” situation:

– Nobody can single-handedly apply rigorous tests on the routing system
– And the lowest common denominator approach that everyone can apply is to apply no integrity tests at all
But we need better routing security – don't we?

• But what does this “need” mean beyond various mantras, noble intentions and vague generalities about public safety and benefit?
  – Who wants to pay for decent security?
  – What’s the business drivers for effective security?
  – How do you avoid diversions into security pantomimes and functionless veneers?

Can you make effective security a preferred alternative?
Risk Management

• Adding operational security measures is not about being able to create and maintain absolute security. Its about a pragmatic approach to risk mitigation, using a trade-off between cost, complexity, flexibility and outcomes.

• Its about making an informed and reasoned judgment to spend a certain amount of resources in order to achieve an acceptable risk outcome.
Threat Model

Understanding routing threats:

– What might happen?
– What are the likely consequences?
– What’s my liability here?
– How can the consequences be mitigated?
– What’s the set of cost tradeoffs?
– Does the threat and its consequences justify the cost of implementing a specific security response?
Threats

• Corrupting the routers’ forwarding tables can result in:
  – Misdirecting traffic (subversion, denial of service, third party inspection, passing off)
  – Dropping traffic (denial of service, compound attacks)
  – Adding false addresses into the routing system (support compound attacks)
  – Isolating or removing the router from the network

• The beauty of a routing attack is that you don’t need to corrupt the victim’s system – indeed you are relying on the victim’s system running correctly!
Collective vs Unilateral Response

- **Unilateral** action has its limits in effectiveness
- **Collective** action is challenging
  - How much duplication of effort is entailed?
  - Is the threat a shared assessment?
  - Can we pool our resources and work together on a common threat model?
  - What tools do we need?
  - Are there beneficial externalities that are also generated?
  - What’s the framework for collective action?

When will you stop asking all these bloody annoying stupid questions and just tell me what to do!
Things YOU can do
Use a Robust Network Design

Isolate your network at the edge:
  – Route all traffic at the edge
  – NO sharing LANs
  – NO shared IGPs
  – NO infrastructure tunnels

Isolate your customers from each other:
  – NO shared access LANs

Isolate routing roles within the network:
  – Exterior-facing interface routers
  – Internal core routers
Protect your Routers

• Protecting routing infrastructure
  – ssh access to the routers
  – maintain filter lists
  – user account management
  – access log maintenance
  – snmp read / write access control lists
  – protect configurations
  – monitor configuration changes

• Protecting configuration control of routers is an essential part of network security
Protect your BGP

Basic BGP configuration tasks:
- No redistribution from iBGP into the IGP
- Use session passwords and MD5 checksums to protect all BGP sessions
- For iBGP use the local loopback address as the nexthop (next-hop-self)
- Use filter lists to protect TCP port 179
- Use maximum prefix limiting (hold mode rather than session kill mode preferred)
- Use maximum as path limiting
- Use a silent recovery from mal-formed Updates
- Use eBGP multi-hop with care (and consider using TTL hack)
- Align route reflectors with topology to avoid iBGP traffic floods

Operating BGP:
- Use soft clear to prevent complete route withdrawals
- Use BGP session state and BGP update monitors and generate alarms on session instability and update floods
Protect your BGP

• Check your router config with a current best practice configuration template
  – Rob Thomas’ template at: http://www.team-cymru.org/ReadingRoom/Templates/secure-bgp-template.html is a good starting point
Managing Routes

Take care of what you learn, because your peers and upstreams will trust you to have performed the appropriate checks before you advertise these routes.

Always authenticate customer routing requests

Check validity of the address – route registries are your friend!
• Own space – validate request against local route object registry
• Other space – validate request against RIR route object database registered POC
  — This is often harder than it originally looks!

This does not prevent the deliberate lie, but it can catch the accidental typo.
Even so...
After all this effort, it's not all that good is it?
Alternatively, can we tweak BGP so that it can detect the difference between good and evil, and only advertise “good” routes?
A (random) BGP Update

2010/01/26 00:03:35 rcvd UPDATE w/ attr:
   nexthop 203.119.76.3, origin i, path 4608 1221 4637 3561
   3356 4657 4773
   124.197.64.0/19
Routing Security

• The basic routing payload security questions that need to be answered are:
  – **Who** injected this address prefix into the network?
  – Did they have the necessary **credentials** to inject this address prefix? Is this a valid address prefix?
  – Is the forwarding path to reach this address prefix **trustable**?

• And can these questions be answered by any BGP speaker quickly and cheaply?
BGP Update Validation

2010/01/26 00:03:35 rcvd UPDATE w/ attr:
  nexthop 203.119.76.3, origin i, path 4608 1221 4637 3561
  3356 4657 4773
  124.197.64.0/19

- is 124.197.64.0/19 a “valid” prefix?
BGP Update Validation

2010/01/26 00:03:35 rcvd UPDATE w/ attr:

nexthop 203.119.76.3, origin i, path 4608 1221 4637 3561
3356 4657 4773
124.197.64.0/19

- is 124.197.64.0/19 a “valid” prefix?
- is AS4773 a “valid” ASN?
BGP Update Validation

2010/01/26 00:03:35 rcvd UPDATE w/ attr:

- nexthop 203.119.76.3, origin i, path 4608 1221 4637 3561 3356 4657 4773
- 124.197.64.0/19

- is 124.197.64.0/19 a “valid” prefix?
- is AS4773 a “valid” ASN?
- is 4773 an “authorized AS to advertise a route to this prefix?”
BGP Update Validation

2010/01/26 00:03:35 rcvd UPDATE w/ attr:

next hop 203.119.76.3, origin i, path 4608 1221 4637 3561 3356 4657 4773
124.197.64.0/19

- is 124.197.64.0/19 a “valid” prefix?
- is AS4773 a “valid” ASN?
- Is 4773 an “authorized AS to advertise a route to this prefix?
- Is the AS Path valid?
  - Is AS 4657 a valid AS, and did AS 4773 advertise this route to AS 4657?
  - Is AS 3356 a valid AS, and did AS 4657 advertise this route to AS 3356?
  - etc
A Foundation for Routing Security

• The use of authenticatable attestations to allow automated validation of:
  – the authenticity of the route object being advertised
  – authenticity of the origin AS
  – the binding of the origin AS to the route object

• Such attestations used to provide a cost effective method of validating routing requests
  – as compared to the today’s state of the art based on techniques of vague trust and random whois data mining
A Foundation for Routing Security

Adoption of some basic security functions into the Internet’s routing domain:

• Injection of reliable trustable data
  A Resource PKI as the base of validation of network data

• Explicit verifiable mechanisms for integrity of data distribution
  Adoption of some form of certified authorization mechanism to support validation of credentials associated with address and routing information
A Starting Point

• How can you certify who what which address?
  – follow the allocation trail
  – Certification of the “Right-of-Use” of IP Addresses and AS numbers as a linked attribute of the Internet’s number resource allocation and distribution framework

For example:

APNIC (the “Issuer”) certifies that:
  the certificate “Subject”
    whose public key is contained in the certificate
    is the current holder of a set of IP address and AS resources
      that are listed in the certificate extension

APNIC does NOT certify the identity of the subject, nor their good (or evil) intentions!
Resource Certificates

Resource Allocation Hierarchy

AFRINIC  RIPE NCC  ARIN  APNIC  LACNIC

NIR1  NIR2

ISP  ISP  ISP  ISP  ISP  ISP  ISP  ISP
Resource Certificates

Resource Allocation Hierarchy

AFRINIC  RIPE NCC  ARIN  APNIC  LACNIC

Issued Certificates match allocation actions

ISP  ISP  ISP  ISP  ISP  ISP  ISP  ISP
Resource Certificates

Resource Allocation Hierarchy

Issuer: APNIC
Subject: NIR2
Resources: 192.2.0.0/16
Key Info: <nir2-key-pub>
Signed: <apnic-key-priv>

Issued Certificates

AFRINIC  RIPE NCC  ARIN  APNIC  LACNIC

ISP  ISP  ISP  ISP4  ISP  ISP  ISP  ISP
Resource Certificates

Resource Allocation
Hierarchy

Issuer: APNIC
Subject: NIR2
Resources: 192.2.0.0/16
Key Info: <nir2-key-pub>
Signed: <apnic-key-priv>

Issuer: NIR2
Subject: ISP4
Resources: 192.2.200.0/24
Key Info: <isp4-key-pub>
Signed: <nir2-key-priv>
Resource Certificates

Resource Allocation Hierarchy

Issuer: APNIC
Subject: NIR2
Resources: 192.2.0.0/16
Key Info: <nir2-key>
Signed: <apnic-key-priv>

Issuer: NIR2
Subject: ISP4
Resources: 192.2.200.0/22
Key Info: <isp4-key>
Signed: <nir2-key-priv>

Issuer: ISP4
Subject: ISP4-EE
Resources: 192.2.200.0/24
Key Info: <isp4-ee-key>
Signed: <isp4-key-priv>

Issued Certificates

AFRINIC | RIPE NCC | ARIN | APNIC | LACNIC
What could you do with Resource Certificates?

• You could sign “routing authorities” with your private key, providing an authority for an AS to originate a route for the named prefix. Any Relying Party could validate this authority in the RPKI.

• You could use the private key to sign routing information in an Internet Route Registry.

• You could attach a digital signature to a protocol element in a routing protocol.

• You could issue signed derivative certificates for any sub-allocations of resources.
Signed Objects

Resource Allocation Hierarchy

AFRINIC  RIPE NCC  ARIN  APNIC  LACNIC

Issued Certificates

Route Origination Authority
“ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24”

Attachment: <isp4-ee-cert>

Signed, ISP4 <isp4-ee-key-priv>
Signed Object Validation

Resource Allocation Hierarchy

AFRINIC  RIPE NCC  ARIN

APNIC  LACNIC

ISP  ISP  ISP  ISP  ISP

Issued Certificates

Route Origination Authority
“ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24”

Attachment: <isp4-ee-cert>

Signed, ISP4 <isp4-ee-key-priv>

1. Did the matching private key sign this text?
Resource Allocation Hierarchy

AFRINIC RIPE NCC ARIN

APNIC NIR2

LACNIC

Issued Certificates

Route Origination Authority
“ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24”

Attachment: <isp4-ee-cert>

Signed, ISP4 <isp4-ee-key-priv>

2. Is this certificate valid?
Signed Object Validation

Resource Allocation Hierarchy

AFRINIC  RIPE NCC  ARIN

ARPANIC  LACNIC

LIR1  NIR2

ISP  ISP  ISP  ISP  ISP

Issued Certificates

Trust Anchor

3. Is there a valid certificate path from a Trust Anchor to this certificate?

Route Origination Authority
“ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24”

Attachment: <isp4-ee-cert>

Signed,
ISP4 <isp4-ee-key-priv>
Signed Object Validation

Resource Allocation Hierarchy

Validation Outcomes
1. ISP4 authorized this Authority document
2. 192.2.200.0/24 is a valid address, derived from an APNIC allocation
3. ISP4 holds a current right-of-use of 192.2.200.0/24
4. A route object, where AS65000 originates an advertisement for the address prefix 192.2.200.0/24, has the explicit authority of ISP4, who is the current holder of this address prefix

Route Origination Authority
“ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24”

Attachment: <isp4-ee-cert>

Signed,
ISP4 <isp4-ee-key-priv>
A (partial) architecture for securing BGP origination

- Distributed RPKI Publication Repositories (Certificates and Routing Authorities)
- Synchronization
- Local RPKI processor
- BGP Filter (Origin AS + prefix mask)
- BGP Speaker
What about AS Path Validation?
It's complicated!
Progress

• Specifications submitted to the SIDR WG of the IETF:
  – Specification of a profile for Resource certificates
  – Specification of the distributed publication repository framework
  – Specification of the architecture of the RPKI
  – Specification of profiles for Route Origination Authorization objects (ROAs)
  – Specification of the Issuer / Subject resource certificate provisioning protocol
Progress

• Implementation Progress
  • Four independent implementation efforts for various aspects of the RPKI are underway at present
    – Tools for Resource Certificate management
      • Requests, Issuance, Revocation, Validation
    – Issuer / Subject certificate provisioning protocol
    – Functional RPKI Engine instance for an RIR integrated into MyAPNIC’s production environment
    – Relying Party local cache management
    – RPKI validation tools
Intentions

• Create underlying framework for introducing route validation measures in BGP
• Assist ISP business process accuracy with Peering and Customer Configuration tool support
• Improve the integrity of published data through the signing and verification capability in Whois, IRR and similar
Concerns

• Will this work for securing BGP?
  – The major issue here is that of partial use and deployment
  – Any security mechanism has to cope with partial deployment
    • Which means that the basic conventional approach of “what is not certified and proved as good must be bad” will not work until everyone adopts this approach
    • This is a problem is the task of validation of origination
  – In BGP we need to think about both origination and the AS Path of a route object
    • And AS path validation is going to be very challenging indeed in an environment of piecemeal use of secure credentials
  – A partially secured environment may be more operationally expensive, but no more secure than what we have today
Concerns

• Is a trust hierarchy the best approach to use?
  – The concern here is concentration of vulnerability
    • If validation of routing information is dependant on the availability and validity of a single root trust anchor then what happens when this single digital artifact is attacked?
  – But can you successfully incorporate robust diversity into a supposedly secure trust framework?
    • This is challenging!
Concerns

• Is this the only way to achieve generally useful outcomes?
  – Is this form of augmentation to BGP to enforce “protocol payload correctness” over-engineered, and does it rely on impractical models of universal adoption?
  – Can routing anomaly detectors adequately detect the most prevalent forms of typos and deliberate lies in routing with a far lower overhead, and allow for unilateral detection of routing anomalies?
Security only works in practice if:

we can make secure mechanisms cheaper, easier, more robust, and more effective than existing practices
Thank You

Questions?