RPKI and Internet Routing Security
~ The regional ISP operator view ~

APNIC 29/APRICOT 2010

NEC BIGLOBE, Ltd. (AS2518)
Seiichi Kawamura
Agenda

• Routing practices of the regional ISP today

• How this may change with RPKI and what may improve
Question: Routing Infrastructure today

- What data sources do we trust, to keep “my routing table” a sensible one so I can route my customers packets to their rightful destination and not have angry calls at me?
- Is the data we rely on good enough?
- What actions do we take with those data?
- Are those methods/actions good enough to keep my customers happy?
My view

• What data sources do we trust for routing?
  - Various IRRs
    • RADB, ALTDB, NTTCOM, JPIRR......
  - Registry Databases
  - Projects
    • REX, Team Cymru, Route Views, etc
  - e-mail
  - web or ftp sites
    • Sites provided by IANA, registries, etc.
  - Social gatherings?
My view

• Is the data we rely on good enough?
  - On a regional scale, maybe.
    • JPIRR, an IRR run by JPNIC is very clean.
    • Current methods, plus the effort to keep data sources clear and accurate may work in small countries.
  - Maybe not enough on a global scale.
    • Not all routed ASes are on IRRs.
    • e-mails are full of typo’s. IPv6 make things worse.
      (draft-ietf-6man-text-addr-representation)
    • Many mistakes on IRRs. Resolving problems can be hard on global scale.
My view

• What actions do we take with those data?
  - Mostly a static filter generation. (prefix, as-path, BGP community, etc)
  - We tend to keep filters on the safe side.

• Are these methods/actions good enough to keep my customers happy?
  - The time has come to go one step further.

The possibility that data source may show incorrect data, is holding us from implementing a strong prevention against misuse.
But the internet has worked fine for me... why would I need to do something different?
Why RPKI?

- Continuous routing incidents, with big impacts
  - YouTube Hijacking, etc.
  - Attacks may come from anywhere.
- The hopes for a safe and secure “internet as an infrastructure”.
- Resources depleting.
  - IPv4 address transfers.
    - Allows for divide and transfer.
  - Smaller route advertising, more bogus routes (not necessarily bogons).

Reliability of resources and routes are in need.
What is RPKI?

RPKI: Resource Public Key Infrastructure

- X.509 certificate style
- Number resources (prefix, as-numers)

SSL certs validate domains ↔ RPKI certs validate IP and ASN

A simple way of understanding this.

A framework to use X.509 Certificates on AS numbers and IP address resources, to make Internet routing secure by means of a trustable data source.
Certificate types and functions at a glance

Certificate types

1. Resource Certificate (CA or EE):
   - IPv4/IPv6 prefixes
   - AS numbers

Functions using the Certificates

1. Route Origin Authorization (ROA)
   - Ties between a prefix and an AS number that routes it. Signed by a Cert.

There’s more, see IETF SIDR-WG work for more.
Address Allocation and Routing today

- **Allocation**: 203.136.0.0/16
  - **JPNIC/APNIC**
- **Assignment**: 203.136.1.0/24
  - **BIGLOBE**
- **Peering**
  - **JPIRR, RADB, ALTDB, etc**
  - **whois query**
- **Hand written updates to IRR objects**
- **Check and generate filters**
- **Mis-configuration Easily happens**
- **Assignments**
  - **ISP A**
  - **ISP C**
  - **Cust A**

Statically generated filters
Key aspects of the RPKI architecture

• RIRs will give you a Certificate showing you the rightful owner.
  - Cannot transfer resource without proper transactions.

• The rightful prefix owner only, can associate an AS number with the prefix.
  - No one else can do this. Requires a valid cert.

• Check against received routes.
  - Router can query the RPKI data to see if the origin and AS number do actually match with a signed object.

Disclaimer: This hasn’t happened yet. The following slides are my imagination of what may happen.
Imagination: So what’s it going to be like?

A DB of RPKI objects (Certs, ROAs, etc)

Allocations come with Certs

JPNIC/APNIC

203.136.0.0/16

IRR register

Repository

Dynamically check origin against received routes

Origin Validation

Peering

BIGLOBE

Static filtering data (Path filtering)

IRR register

IRR (JPIRR, RADB)

Path Validation

ISP A

ISP B

ISP C

ISP A

ISP B

ISP C

!! not part of RPKI !!
Imagination: What will change for ISPs?

- Address management teams will have to deal with certificates.
  - If you have customers, then you may have to issue certs.
  - Key management may become part of job.
- Routing team will have to create new objects (ROAs), manage them, and possibly create them for customers as well.
- Routers may have to be configured to accept data collected from the repositories to validate routes against ROAs.
- PIs will need Certificates and ROAs also.
Imagination: Players involved

- **Routing operators**
  - If you use IRR as part of your job, you have something new to play with.
  - IRR will stick around for a while, but we should stop the “e-mail” culture and rely more on these tools.

- **Address management team**
  - Get used to PKI, or find someone who’s good with it.

- **Customer support**
  - If you have BGP customers, you may need to have a user interface to cover for RPKI.

- **NOC**
  - The top level engineers should be aware of RPKI.
What should ISPs do?

• Don’t panic
  • NIRs have not even started.
  • Just having a certificate will not do much just yet.

• Where is all the talk happening?
  • IETF (sidr-WG)
  • RIRs

• What should I do now?
  • Do the best that you can do
    • Use IRRs properly, don’t hijack people’s route, be aware of hijacked routes, be aware of reachability of your prefixes, use tools, etc
  • Get interested in RPKI. Try it out.