RIPE NCC IRR training

4 February 2011

Zurich, Switzerland

Jeroen Massar
jeroen@unfix.org

Generate from DB

- **You need to store the information already, thus why not automate it?**
- **Want to keep clicking on the site, making mistakes or just write a script once which mails the updates out every evening?**
- **Generate objects from your customer DB and generate your router config with rtconfig.**

- **Use SVN to store updates to router configs so that you can see when.**
- **Check out RANCID for this too.**
- **Create a PGP key for your robot so that it can automatically sign everything**

Monitor your address space

- **Watch BGP**
  - **BGPmon (http://bgpmon.net)**
  - **RIPE RIS (http://ris.ripe.net)**
  - **RIPE Labs Tools (http://labs.ripe.net)**
  - **Colorado BGPmon (http://bgpmon.netsec.colostate.edu/)**

  These might notify you of a hijack

- **Watch your local network:**
  - **Use NetFlow / sFlow**

BCP 38 (RFC 2827)

"Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing"

- **In short: Do not send packets to the network that you should not be originating**

- **Do source-route filtering as close to the source as possible**
  - **Watch out for "multi-homed" customers**

Techniques:

- **Simple firewall rule blocking out the prefix**
- **Unicast RPF**

  When there is no route towards that prefix it should not originate it
- **Various device specific techniques eg in DSLAMs / Cable concentrators which also look at MAC addresses**

Protect your BGP

- **Don't let anything else but the IX/peers talk to your BGP daemons**
- **BGP with TCP/MD5**
- **Generalized TTL Security Mechanism (GTSH)**
  - **Set TTL to 255 at sender and verify on receiver that the TTL is still 255**
  - **Packets then have to be from the same link and cannot have been routed**
- **Only accept packets from known MAC addresses**
- **Use arpwatch alike tools to make sure no new MACs are introduced on a switch, next to monitoring the switch that the cable was not unplugged**

- **Use RPSL**
  - **Put your route/route6 objects in the IRR**
  - **Generate prefix filters from it**

- **There are various secure routing proposals, unfortunately none in wide deployment**

- **Monitor your own prefix on the Internet so that you at least know that it is being used somewhere else by somebody else, of course inform folks of the hijack**
- **Using multiple prefixes can be useful because of that as they need to steel all your prefixes to be able to bring you down at ISPs that accept their advertisement**

Resource Public Key Infrastructure (RPKI)

- **Public Key Infrastructure to be able to verify BGP signatures**
- **X.509 based, RFC3779**
- **Signature Types**
  - **Route Origin Attestations (ROA)**
    - **"I am the signed origin"**
  - **Adjacency Attestations (AAO)**
    - **"We peer together"**
- **Offline verification**
- **Open Source:**

  https://subvert-rpki.hactrn.net/

IRT object

- http://www.ripe.net/db/support/security/irt/irt-h2.html **(google: RIPE IRT object)**

- **Put an IRT object on all your parent objects, that way abuse reports will find your way much easier**
  - **and thus you can resolve those problems**
  - **customers will be happier**
  - **other ISPs will be happy that you are resolving issues and help you out with other issues**

Communities

- **Go to RIPE meetings**
- **Come to SwiNOG (http://www.swinog.ch)**

- **Be secure and active part of:**
  - **iNOC-DBA (http://www.pch.net/inoc-dba/)**
  - **CERT (http://www.cert.org)**
  - **FIRST (http://www.first.org)**
  - **NSP-SEC (http://www.nspsec.org)**
    - **They physically meet at RIPE meetings**
  - **OPS-Trust (http://www.ops-trust.net)**
  - **PeeringDB (http://www.peeringdb.com)**

No More IPv4 (almost ;)

- **Last /8's allocated to the RIRs**
- **When they are out, IPv4 is out.**
- **No more new customers unless you start doing NAT for your customers and other icky stuff…. (got a Playstation/xbox and want to play games, that won't work with multiple layers of NAT….)**

- **Thus:** **Get IPv6 years AGO!**

and otherwise, really really hurry….

Questions?

Jeroen Massar

JRM1-RIPE

http://unfix.org/~jeroen/

jeroen@unfix.org