Detecting and Preventing Route Hijacks

MENOG 13 - Kuwait, September 2013

Marco Hogewoning
External Relations Officer - Technical Advisor

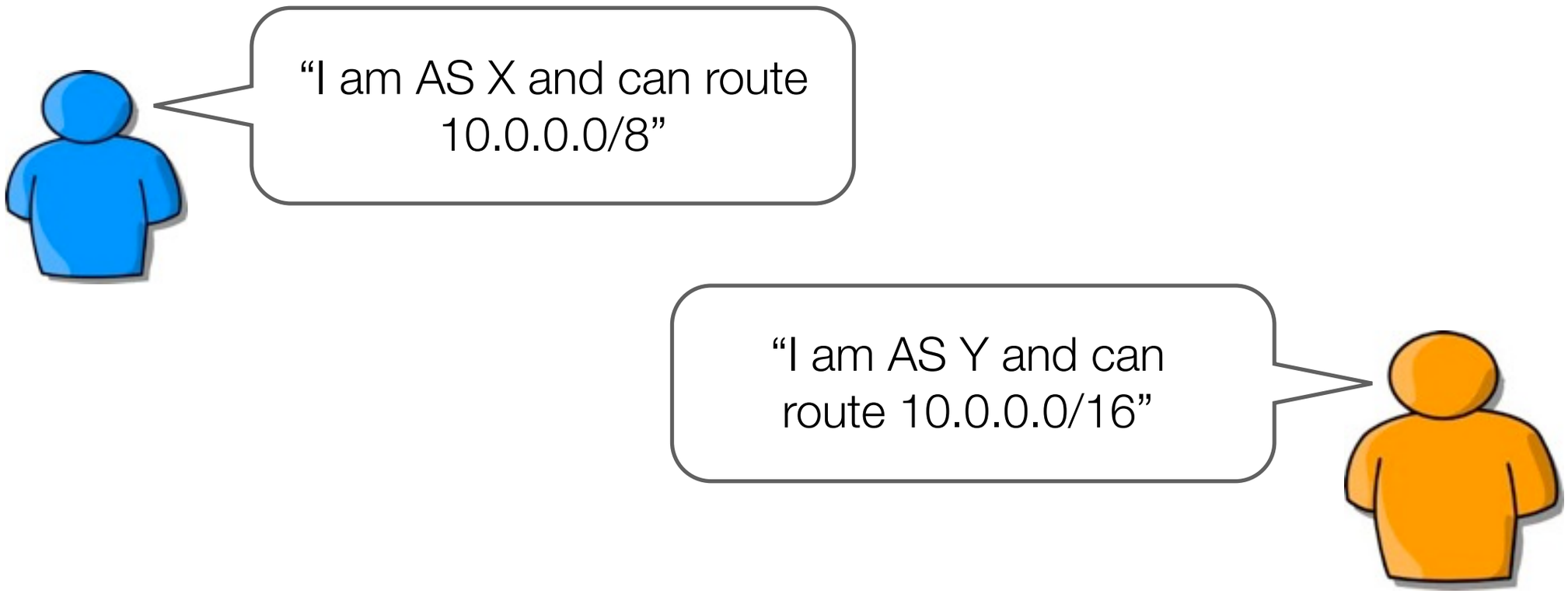
RIPE NCC

“Never attribute to malice that which is adequately explained by stupidity.”

-- Robert J. Hanlon

What Is a Route Hijack?

- Somebody else sending BGP messages that contain (part of) your IP address ranges



Detecting a Hijack?

- Monitor your routing table
  - Resource intensive and complicated to setup
- Configure it to break
  - Accept the route, don't allow traffic to flow! [*]
  - Customers (and monitoring) will notice
- Use a third party alerting service
  - Can they reach you?

[*] Don't Allow Packets to "Escape"

- Is there any reason why a packet destined for one of your IP addresses to leave your ASN?
- If the answer is "no"
  - Setup ACLs to drop those packets
  - Prevents people from redirecting packets (MITM)

```
interface uplink 0
ip access group 1 out
!
access-list 1 deny ip any 10.0.0.0 0.255.255.255
access-list 1 permit ip any any
```

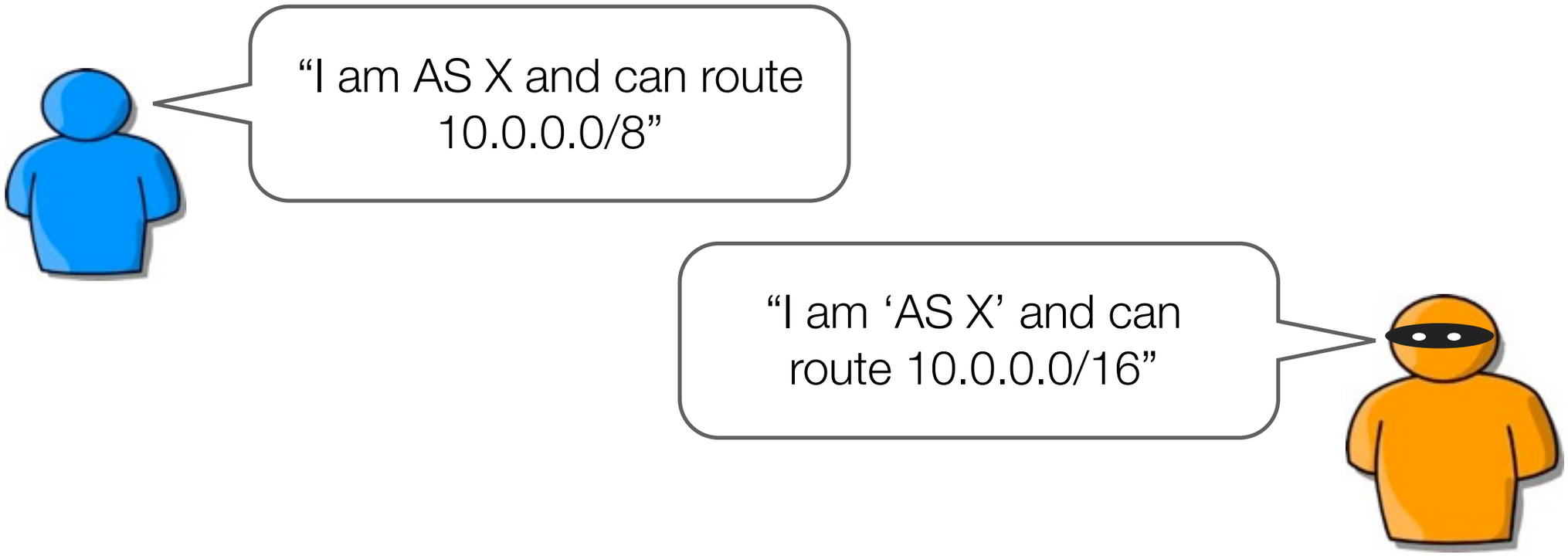
RPKI and RIPE NCC Validator

- Designed to detect and automatically take action against hijacks coming into your network

- RIPE NCC Validator gets a copy of the current RIS database (Route Information Service)
- A standalone validator can flag and alert you about your space being announced by somebody else.

The Malicious Version

- Somebody else sending BGP messages that contain (part of) your IP address ranges
- With your ASN in the path
  - You will never see those updates!



Using Inbound BGP Filters

- RPKI right now provides limited protection against a spoofed AS origin
  - You can only detect and block more specifics
- Somebody has to provide the attacker with an uplink and allow him to announce the route
- It makes sense to filter your customers announcements (and your own)
  - Most ‘attacks’ are simply mistakes


Please Don't
Litter
Help Keep Your
Community Clean

Common BGP Filtering Practice

- Filter all incoming customer announcements
  - Only allow ASNs and prefixes that are really assigned or allocated to them
- Filter all your outgoing BGP announcements
  - You can also make that typo

- If every network applies this logic, you can trust the core of the network to be clean and secure

RIPE Database As a Source

- RIPE Database doubles as routing registry
  - Use it to verify customer announcements
  - Create prefix filters based on ASN origin
- Especially useful when provisioning single- or dual-homed customers operating a stub
- Single whois query gives all prefixes registered for a specific AS number

```
$ whois -h whois.ripe.net -- '-a -r -i or -T route AS3333'\
| grep route | awk '{print $2};'
```

Side note: Anti-spoofing (BCP38)

- Is there any reason why a customer should send you a packet with a source IP address that is not assigned or allocated to him?

- Setup filters to drop those packets
  - Common functionality in access concentrators
  - Please also apply to (virtual) servers, datacenter and leased line connections

Unicast Reverse Path Forwarding (uRPF)

- Only accept a packet on an interface when the route to reach the source address is via that interface
  - Known as ‘strict’ mode
- ‘Loose’ mode will forward when there is a route, regardless of interface
  - Useful for asymmetric traffic flows
  - Useless when the device has a default route

(Postmortem) Analysis of Incidents

- RIPE NCC collects an extensive set of BGP updates using the RIS collector network
- We offer direct access to 3 months of data
  - Use looking glass and visual tools to locate the source
  - Use the RIPE Database to get contact details
  - Figure out what went wrong

- All in 1 Interface: RIPE Stat
  - http://stat.ripe.net

Questions?