



Meet the Falcons

Ciprian Marginean

ciprian.marginean@ams-ix.net

Aris Lambrianidis

aris.lambrianidis@ams-ix.net

What are the Falcons?

- A new pair of route servers
- Based on BIRD (Cisco does not scale easily nor support all features)
- Available only in Amsterdam (for now)





Why go to the trouble?

- Prefix hijack (or misconfiguration) mitigation
“no mechanism has been specified within BGP to validate the authority of an AS to announce NLRI information (prefixes)” (RFC4272 3.2)

How do we do it?

- RPKI validation (RFC6480)
- BGP community tagging based on RPKI status (*valid, invalid, unknown*)
- IRRdb object filtering or tagging

What's new to the Falcons?

Feature	Legacy	Falcon
BGP community based routing policies		<input checked="" type="checkbox"/>
IRRdb based routing policies	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Inbound Routing Policies	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
RPKI prefix validation and filtering		<input checked="" type="checkbox"/>
IRRdb prefix validation and filtering		<input checked="" type="checkbox"/>
AS Path prepending		<input checked="" type="checkbox"/>

Is it difficult to configure?

Peering with AMS-IX



Disable AMS-IX peering

Peering with Legacy route-servers



Disable Legacy peering

Peering with Falcon route-servers



Enable Falcon peering

One more click...

✕

Enable Falcon peering

Mode *

- ✓ Filtering based on IRRdb data
- Filtering based only on RPKI data
- Filtering based on both IRRdb and RPKI data
- No prefix filtering, just tagging

Close

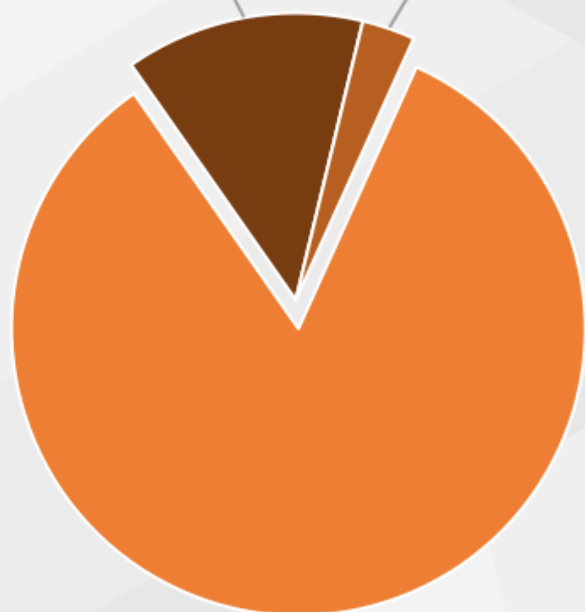
The IPv4 stats

Active peers: 71

Valid: 583 - 13%

Invalid: 129 - 3%

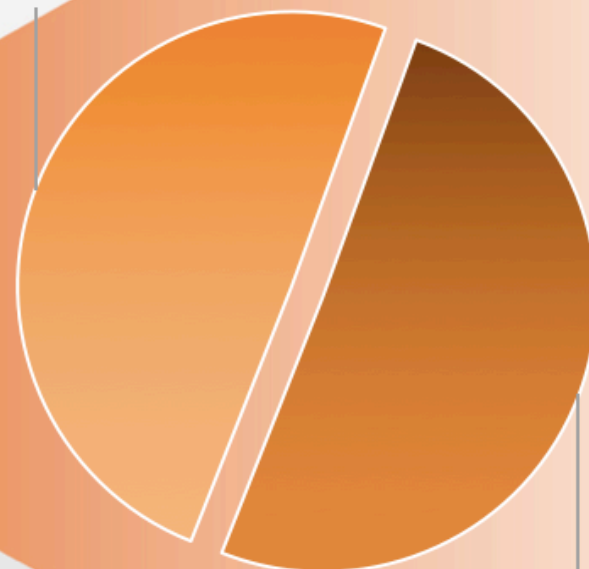
ROA



Unknown: 3610 - 84%

Invalid: 2142 - 50%

IRRdb



Valid: 2180 - 50%

The IPv6 stats

Active peers: 48

Valid: 88 - 25%

Invalid: 3 - 1%

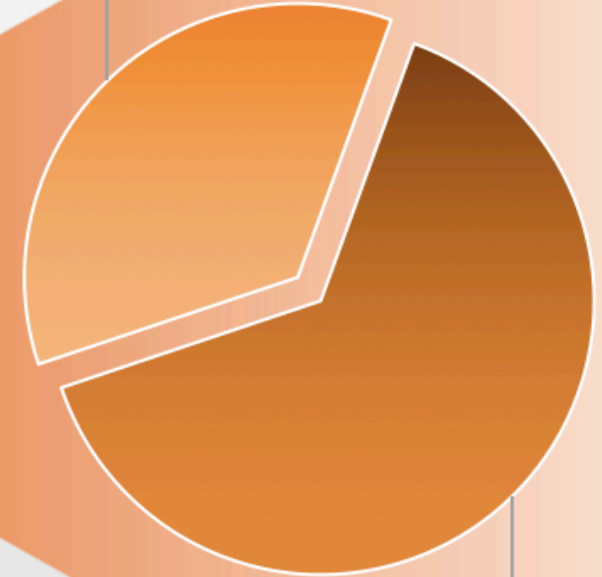
ROA



Unknown: 262 - 74%

Invalid: 126 - 36%

IRRdb



Valid: 227 - 64%

Why that many RPKI invalids?

- **More specifics without ROA** 55%
- **Assignment to downstream** 35%
- **Company acquisitions / mergers** 5%
- **IGP leakage** 5%
- **Hijack** 0%

Why that many RPKI invalids?

- **More specifics without ROA** 55%
- **Assignment to downstream** 35%
- **Company acquisitions / mergers** 5%
- **IGP leakage** 5%
- **Hijack** 0%

Why that many RPKI invalids?

- More specifics without ROA 55%
- **Assignment to downstream** 35%
- Company acquisitions / mergers 5%
- IGP leakage 5%
- Hijack 0%

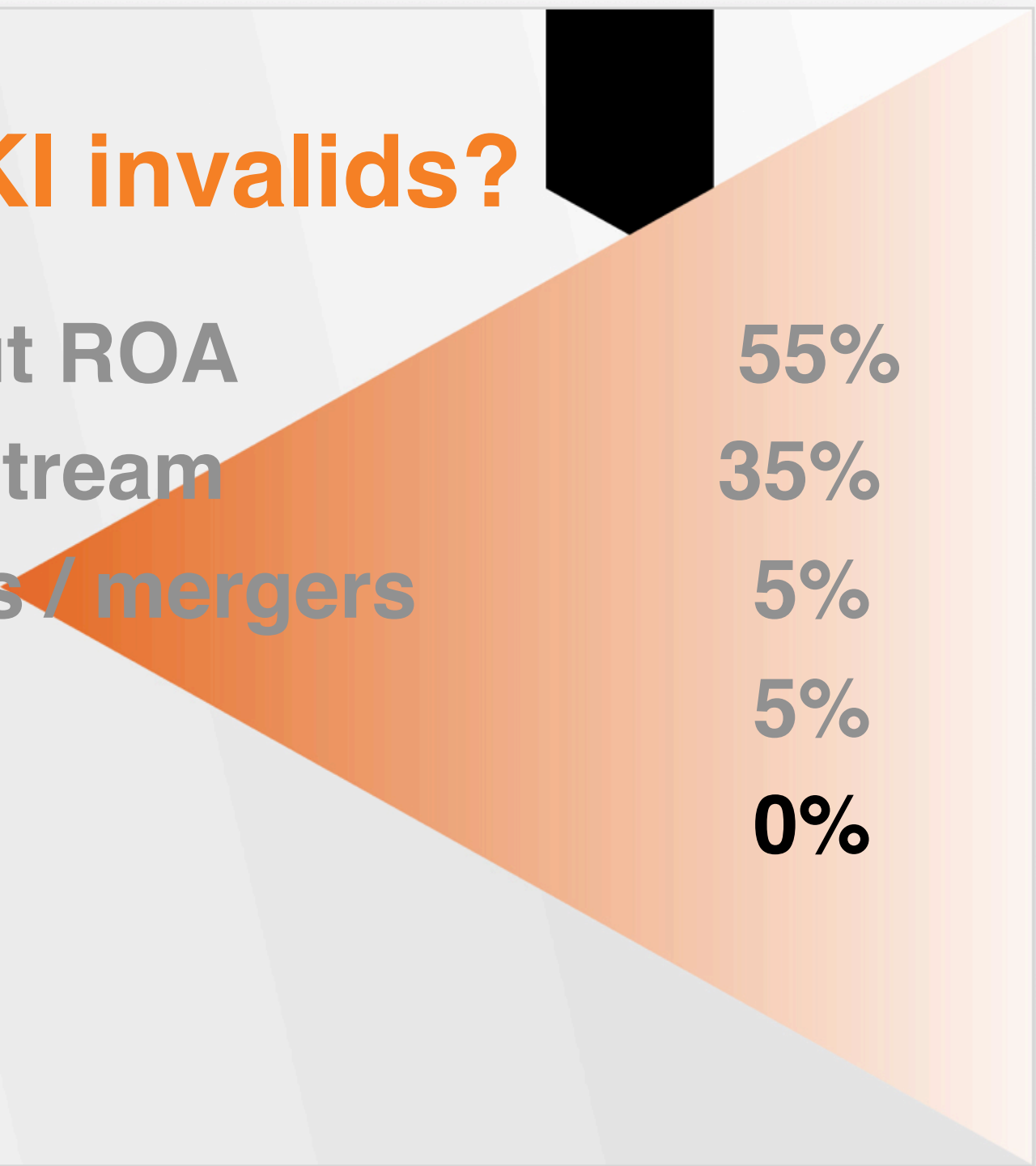
Why that many RPKI invalids?

- More specifics without ROA 55%
- Assignment to downstream 35%
- **Company acquisitions / mergers 5%**
- IGP leakage 5%
- Hijack 0%

Why that many RPKI invalids?

- More specifics without ROA 55%
 - Assignment to downstream 35%
 - Company acquisitions / mergers 5%
 - **IGP leakage** 5%
 - Hijack 0%
-

Why that many RPKI invalids?

- More specifics without ROA 55%
 - Assignment to downstream 35%
 - Company acquisitions / mergers 5%
 - IGP leakage 5%
 - **Hijack** 0%
- 

Key take aways?

- **Lower the barrier for customers needing more tools to make security focused decisions**
- The routing policy is still controlled by the customer
- The Falcons are running in production in parallel with existing ones

Key take aways?

- Lower the barrier for customers needing more tools to make security focused decisions
- **The routing policy is still controlled by the customer**
- The Falcons are running in production in parallel with existing ones

Key take aways?

- Lower the barrier for customers needing more tools to make security focused decisions
- The routing policy is still controlled by the customer
- **The Falcons are running in production in parallel with existing ones**



Will there be anything else, sir?

- Highly flexible, per peer BGP attribute manipulation using communities:
 - set MED
 - set ORIGIN
 - set prepend AS
- BGP ADD-PATH
- ~~More configuration options: (IRRDB or Web portal) + communities~~
- DDoS attack mitigation – L2 filtering



Any questions?

This is still WiP, any feedback is welcome!

`noc@ams-ix.net`