Improving the Security and Robustness of Internet Routing

Georgos Siganos: siganos@gmail.com
Michalis Faloutsos: michalis@cs.ucr.edu
Origin AS Validation
Path Validation
S-BGP, SoBGP
RPSEC
Deployment Problems
What can we do today?

- IRR + RIR
- MyAS (RIPE)
- Our Approach
even for RIPE!!!

- Announced but **NOT** registered for RIPE prefixes 7866.
- **24%** can not be Verified for RIPE.
- MyAS uses different data than RIR&IRR

Wait!!!
Data & Methodology
Validation Results
ISP Reaction
Data & Methodology

- RIR-IRR
- How we do the validation
▼ ARIN
▼ RIPE
▼ APNIC
▼ JPNIC, TWNIC, KRNIC, CCAIR
▼ LACNIC
▼ BRNIC
▼ (AFRNIC)
For the first two cases we check both the last asn and the second to last.
Can AS3333 be the origin of 193.0.0.0/21?

**Origin Validation (RIPE, APNIC)**

- **aut-num**: AS3333
- **as-name**: RIPE-NCC-AS
- **descr**: RIPE Network Coord. Centre
- **remarks**: +-------------------------+
  | AMS-IX Nikhef             |
  +-------------------------+
- **admin-c**: AMR68-RIPE
- **admin-c**: RDK-RIPE
- **tech-c**: OPS4-RIPE
- **mnt-by**: RIPE-NCC-MNT
- **source**: RIPE

- **inetnum**: 193.0.0.0 - 193.0.7.255
- **netname**: RIPE-NCC
- **descr**: RIPE Network Coord. Centre
- **descr**: Amsterdam, Netherlands
- **remarks**: Used for RIPE NCC infr.
- **country**: NL
- **admin-c**: AMR68-RIPE
- **admin-c**: RDK-RIPE
- **tech-c**: OPS4-RIPE
- **status**: ASSIGNED PI
- **mnt-by**: RIPE-NCC-MNT
- **mnt-lower**: RIPE-NCC-MNT
- **source**: RIPE

- **route**: 193.0.0.0/21
- **descr**: RIPE-NCC
- **origin**: AS3333
- **mnt-by**: RIPE-NCC-MNT
- **changed**: ripe-dbm@ripe.net 19980225
- **changed**: joao@ripe.net 19980720
- **changed**: joao@ripe.net 20000908
- **source**: RIPE
Can AS10745 be the origin of 192.149.252.0/24?

<table>
<thead>
<tr>
<th>NetHandle:</th>
<th>NET-192-149-252-0-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>OrgID:</td>
<td>ARIN</td>
</tr>
<tr>
<td>Parent:</td>
<td>NET-192-0-0-0-0</td>
</tr>
<tr>
<td>NetName:</td>
<td>ARIN-NET</td>
</tr>
<tr>
<td>NetRange:</td>
<td>192.149.252.0 - 192.149.252.255</td>
</tr>
<tr>
<td>NetType:</td>
<td>assignment</td>
</tr>
<tr>
<td>RegDate:</td>
<td>1997-11-05</td>
</tr>
<tr>
<td>Updated:</td>
<td>2004-05-03</td>
</tr>
<tr>
<td>NameServer:</td>
<td>NS1.ARIN.NET</td>
</tr>
<tr>
<td>NameServer:</td>
<td>NS2.ARIN.NET</td>
</tr>
<tr>
<td>TechHandle:</td>
<td>ARIN-HOSTMASTER</td>
</tr>
<tr>
<td>Source:</td>
<td>ARIN</td>
</tr>
</tbody>
</table>

| route:           | 192.149.252.0/24    |
| descr:           | ARIN                |
| notify:          | rtreg@arin.net     |
| mnt-by:          | MNT-ARIN            |
| changed:         | lwang@arin.net 19990225 |
| source:          | ARIN                |

Origin Validations (ARIN)
Can AS7195 be the origin of 200.24.75/24?

aut-num: 7195
owner: Telecorp Colombia S.A.
city: Bogota
country: CO
owner-c: FEH2

inetnum: 200.24.75/24
status: reassigned
owner: El portal de Internet S.A.
city: Bogota
country: CO
owner-c: FEH2
tech-c: FEH2
inetrev: 200.24.75/24
nserver: NS.GLOBALONE.NET.CO
nserver: NS2.GIP.NET
nserver: NS3.GIP.NET
inetnum-up: 200.24.64/19
Evaluation of Approach

- Dec. 28 2004 - Jan. 09 2005
- Origin AS Validation
- Reactive Approach
## Origin AS Flags

### Aggregate Numbers

<table>
<thead>
<tr>
<th>Unique (Prefix,Origin AS)</th>
<th>RRC03</th>
<th>RV2</th>
<th>RRC06</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Flags</td>
<td>164,152</td>
<td>177,507</td>
<td>158,498</td>
</tr>
<tr>
<td>Percentage of Flags</td>
<td>3.5%</td>
<td>3.4%</td>
<td>3.8%</td>
</tr>
</tbody>
</table>

### Table

<table>
<thead>
<tr>
<th>Unique (Prefix,Origin AS)</th>
<th>RRC03</th>
<th>RV2</th>
<th>RRC06</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Flags</td>
<td>6,008</td>
<td>6,109</td>
<td>6,039</td>
</tr>
<tr>
<td>Percentage of Flags</td>
<td>3.5%</td>
<td>3.4%</td>
<td>3.8%</td>
</tr>
</tbody>
</table>
IP Prefixes per RIR
As seen by RRC03
Flags per RIR
As seen by RRC03
Percentage of flags per RIR

As seen by RRC03
Validation Details

AS seen by RRC03

Strong validation
Weak validation
Heuristics

ARIN
RIPE
APNIC
LACNIC
ERX-RIR
LEGACY

0  7.000  14.000  21.000  28.000  35.000
Origin AS Flags

Grouped by the country of registration of the AS
Evolution of Origin AS
Events & Flags
Grouped by the origin AS
Unique (prefix,origin) tuples (Flags) per hour grouped by the origin AS

CDF of unique (prefix,origin) tuples (Flags)

0 1 2 3

0.6 0.7 0.8 0.9 1.0

RIPE
APNIC
LACNIC
ARIN
ERX
RIR
LEGACY

Unique (prefix,origin) tuples (Flags) per hour grouped by the origin AS

Flags per RIR
The profile of a routing leak

- AS9121 Event
- How fast ISPs reacted?
Flags by AS9121
As seen by RV2
AS9121 Event One

AS seen by RV2
ISP reaction time
Event One
Bad Entries in the routing table of RV2

UTC Time December 24, 2004 (Event Two)

AS9121 Event Two
AS seen by RV2
Conclusions

- We can validate ~97% of the prefixes
- A reactive approach would generate 0-3 flags per hour.
- Can we resolve routing errors within minutes?