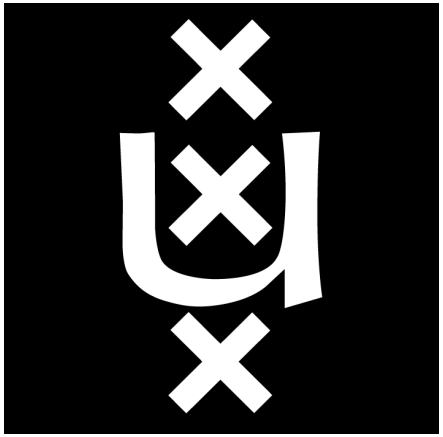
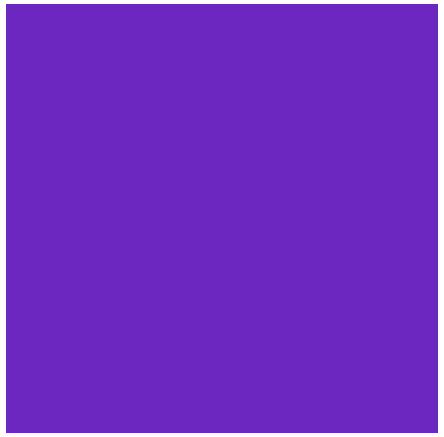
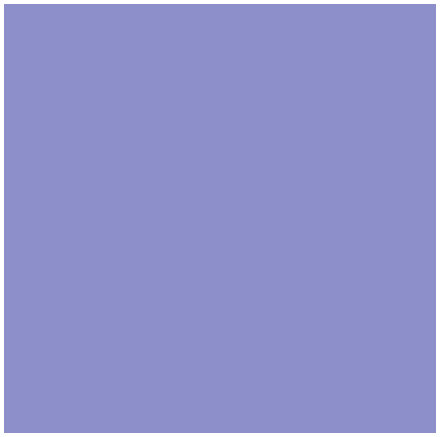
Authors:
Remy de Boer
<Remy.deBoer@os3.nl>
Javy de Koning
<Javy.deKoning@os3.nl>







BGP Origin Validation (RPKI)

What is RPKI?

- Designed to secure internet routing infrastructure
- Route origin validation
- Might be used for routing policies
- Certificates for proof of holdership

Why?

- BGP is currently a web of trust
- No validation or filtering can lead to outages
- Limit impact of misconfigurations
- Prevent Hijacking attempts

Research question

- *"How can we reliably determine which ASes are advertising invalid routes due to misconfigurations and how can we monitor this over the course of time?"*

Route Origin Authorization?

- Prefix
  - (145.96.0.0/15)
- Autonomous System Number
  - (1103)
- Maximum Length (optional)

Validation states

- Unknown
  - Announcement not covered by a ROA
- Invalid
  - Announcement covered by at least one ROA but no ROA matches
- Valid
  - Announcement covered AND matched by at least one ROA

Examples (1/3)

- Advertisement:
  - Prefix:
    - 195.169.0.0/16
  - AS number:
    - 1103
- ROA
  - Prefix:
    - 195.169.0.0/16
  - AS number:
    - 1103
  - Max length:
    - Not used (= 16)

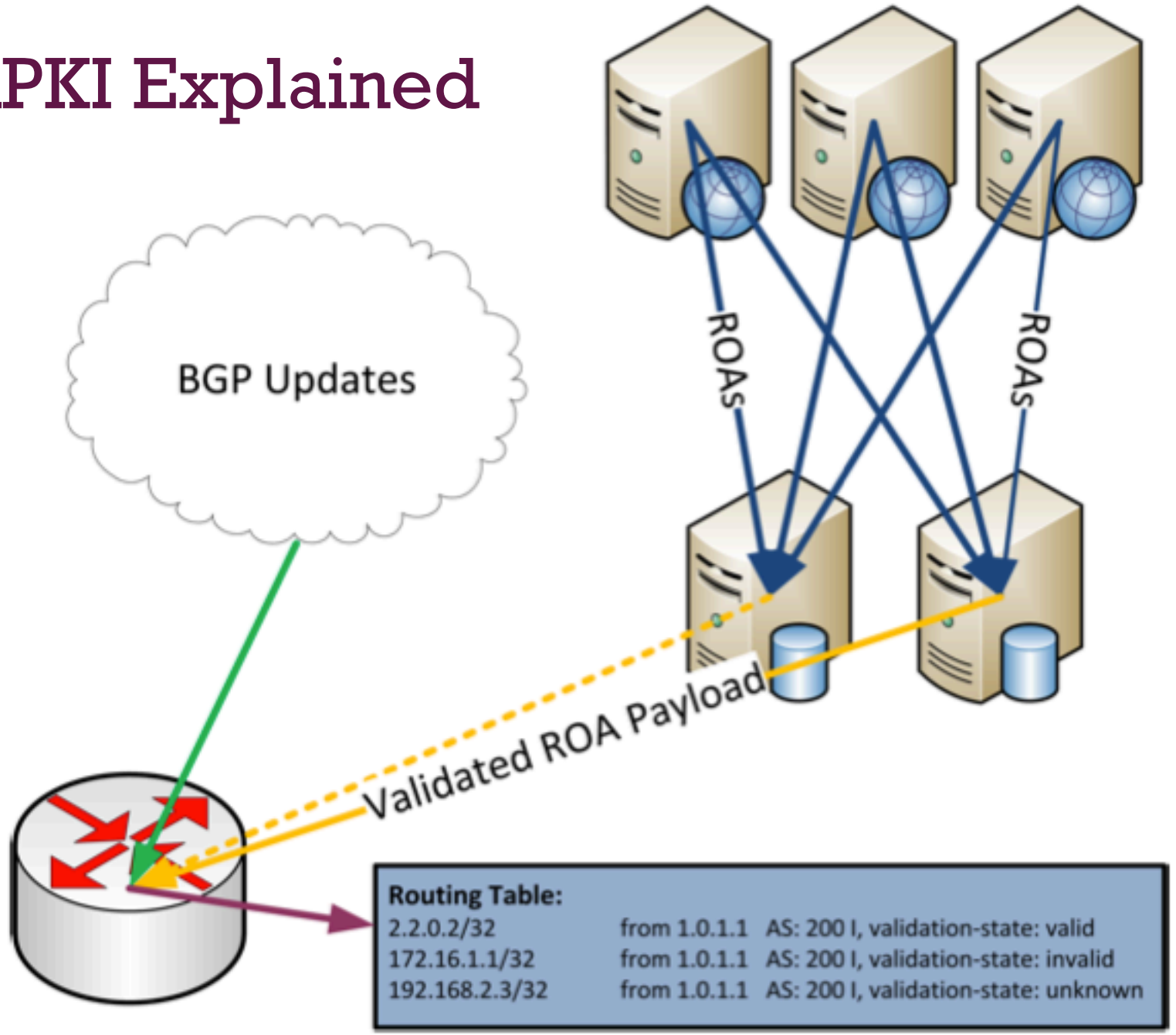
Examples (2/3)

- Advertisement:
  - Prefix:
    - 181.50.0.0/22
  - AS number:
    - 10620
- ROA
  - Prefix:
    - 181.50.0.0/13
  - AS number:
    - 14080
  - Max length:
    - 24

Examples (3/3)

- Advertisement:
  - Prefix:
    - 193.48.123.0/24
  - AS number:
    - 1724
- ROA
  - Prefix:
    - 193.48.0.0/14
  - AS number:
    - 2200
  - Max length:
    - 14

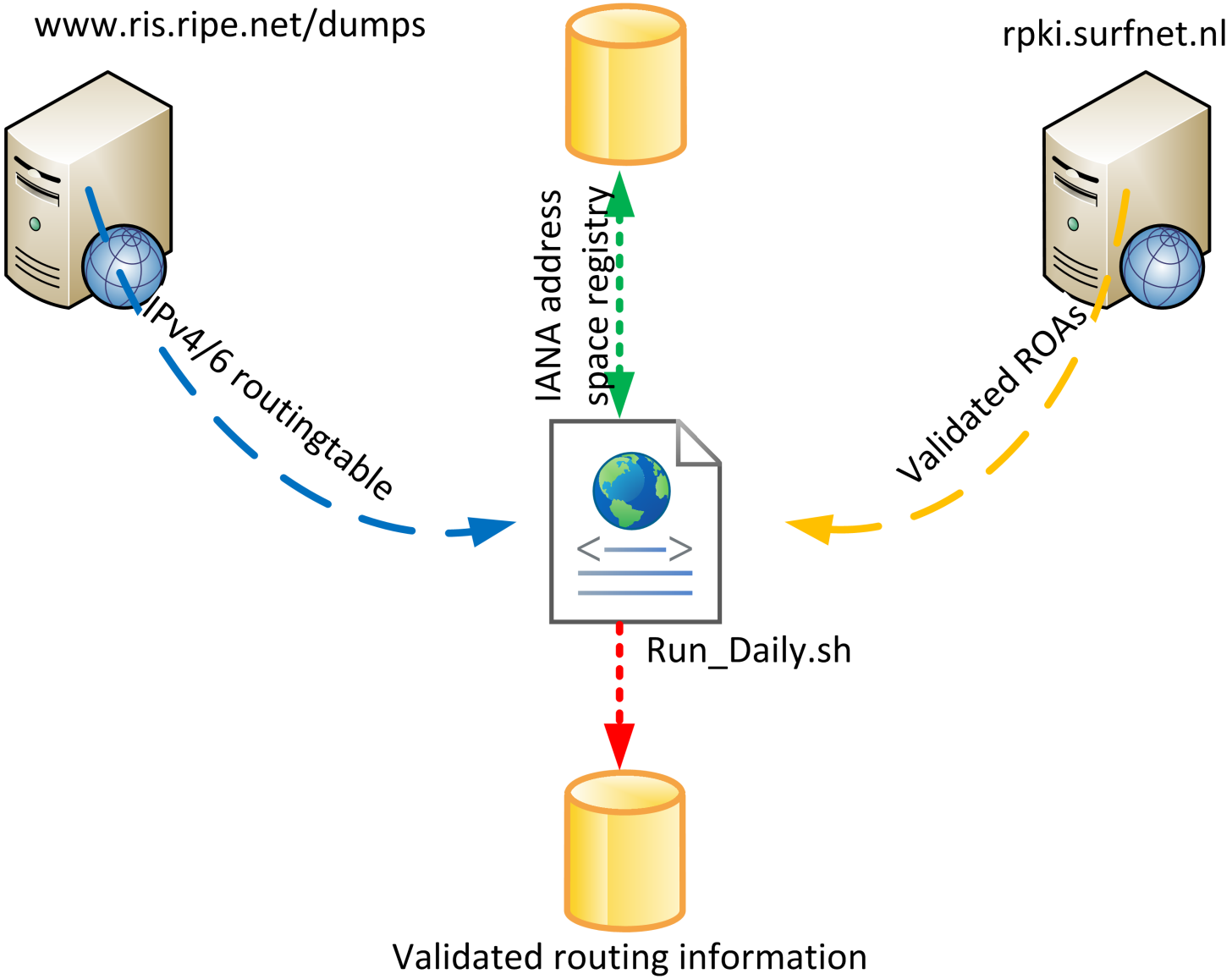
RPKI Explained



Tools used

- Python/PHP/MySQL/Google Chart
- Twitter bootstrap
- RIPE RPKI Validator
- RIPE Global routing table (RIS)
- IANA address space registry

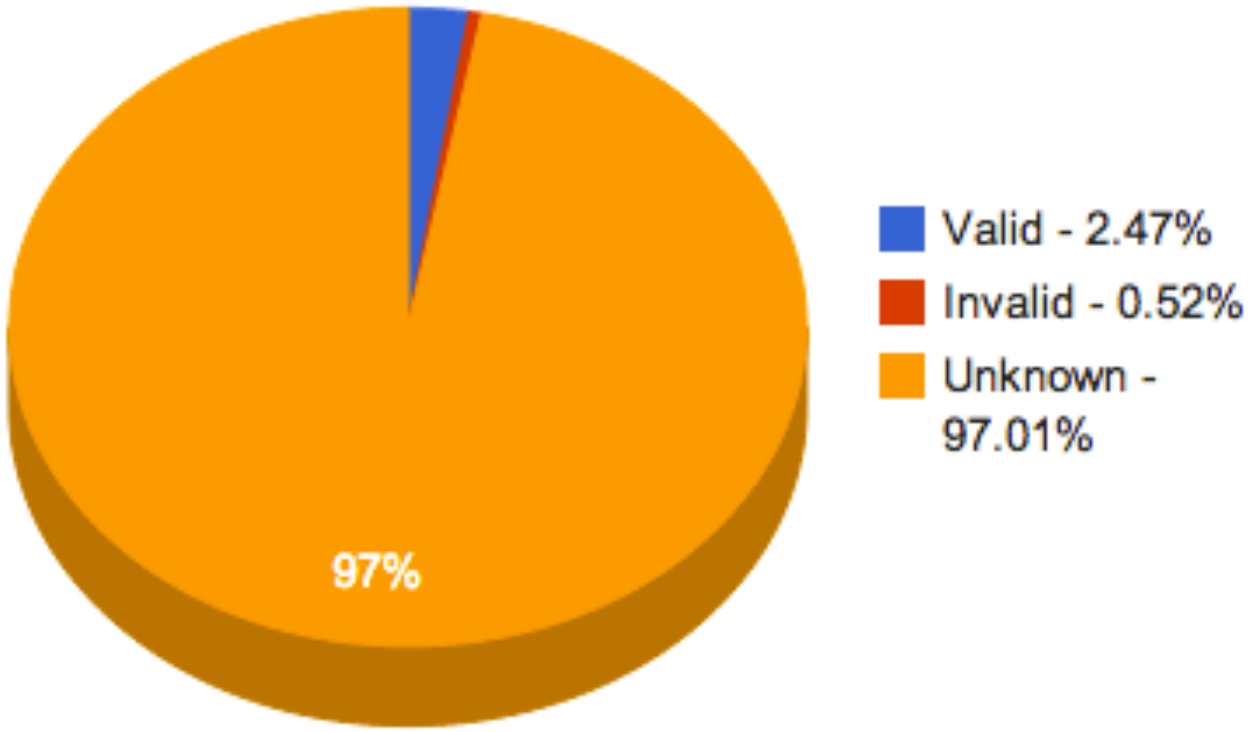
Data sources



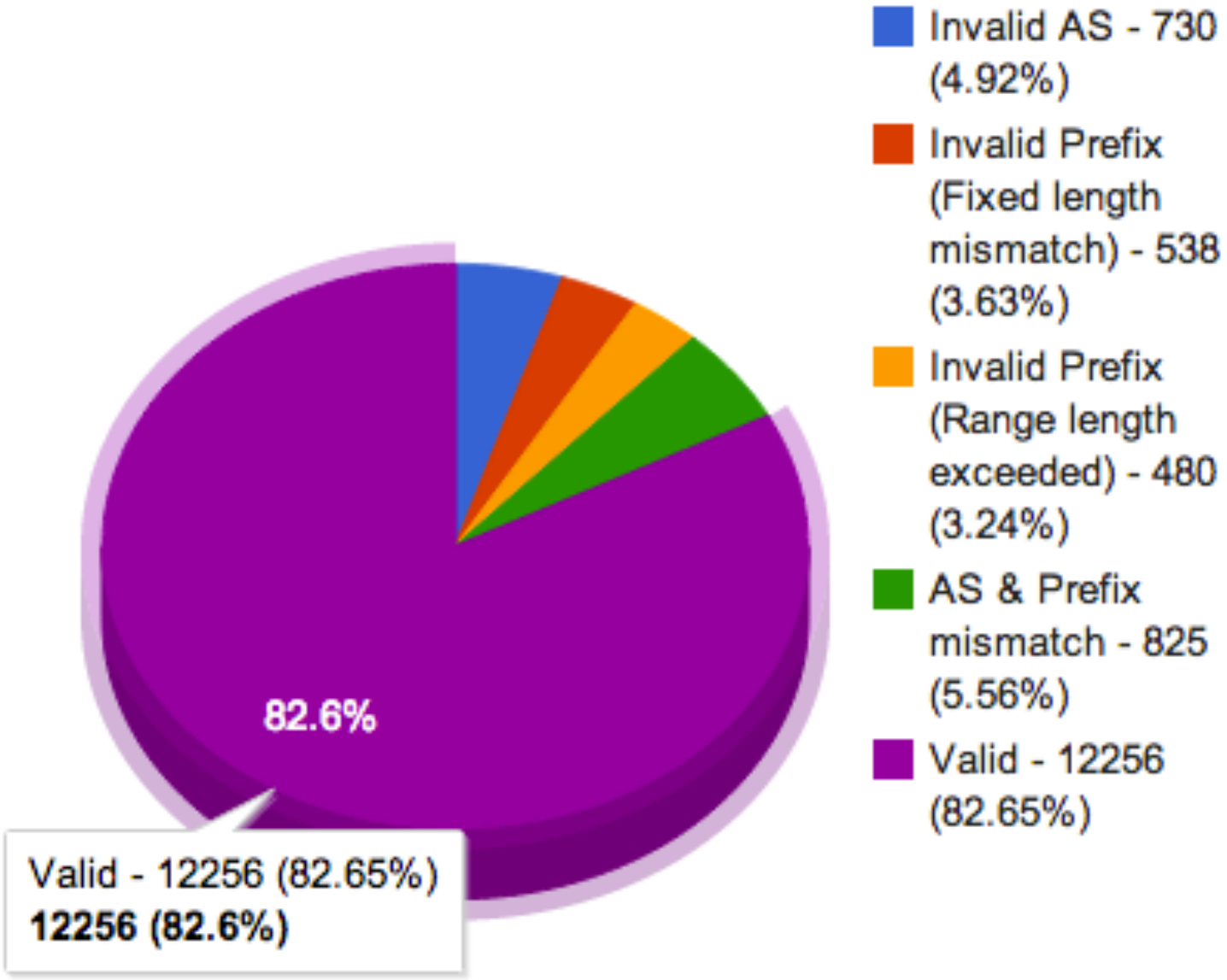
+ Measurements and Results

Global RPKI statistics

- 495838 prefixes in routing table (July 1st).
- Validation state for 14829 prefixes (2.99%).

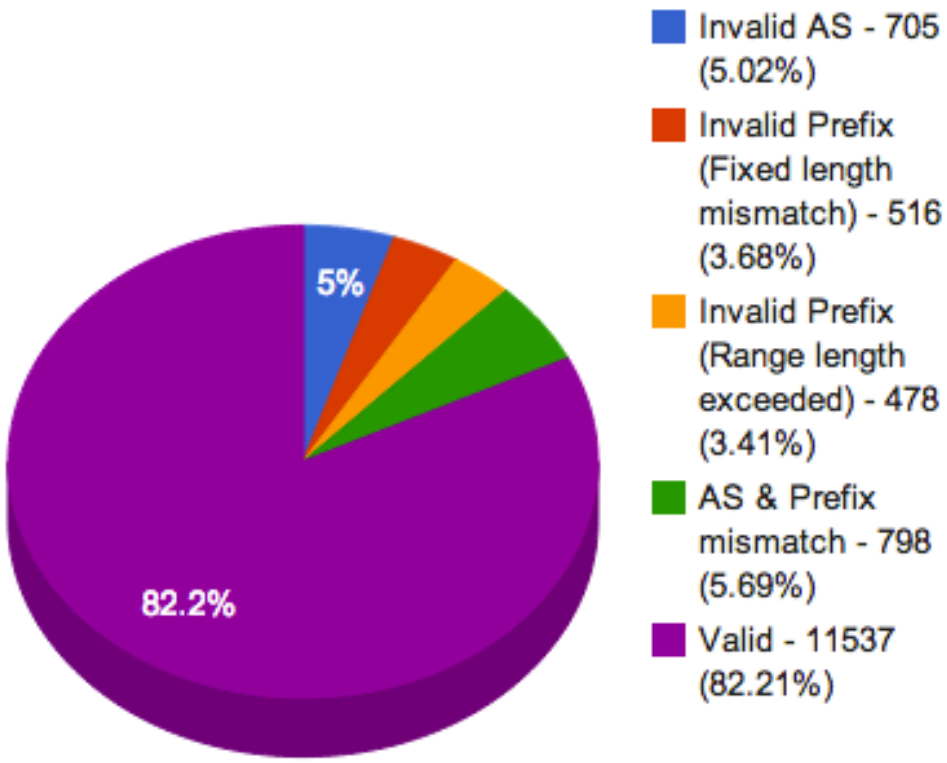


Distribution of invalids

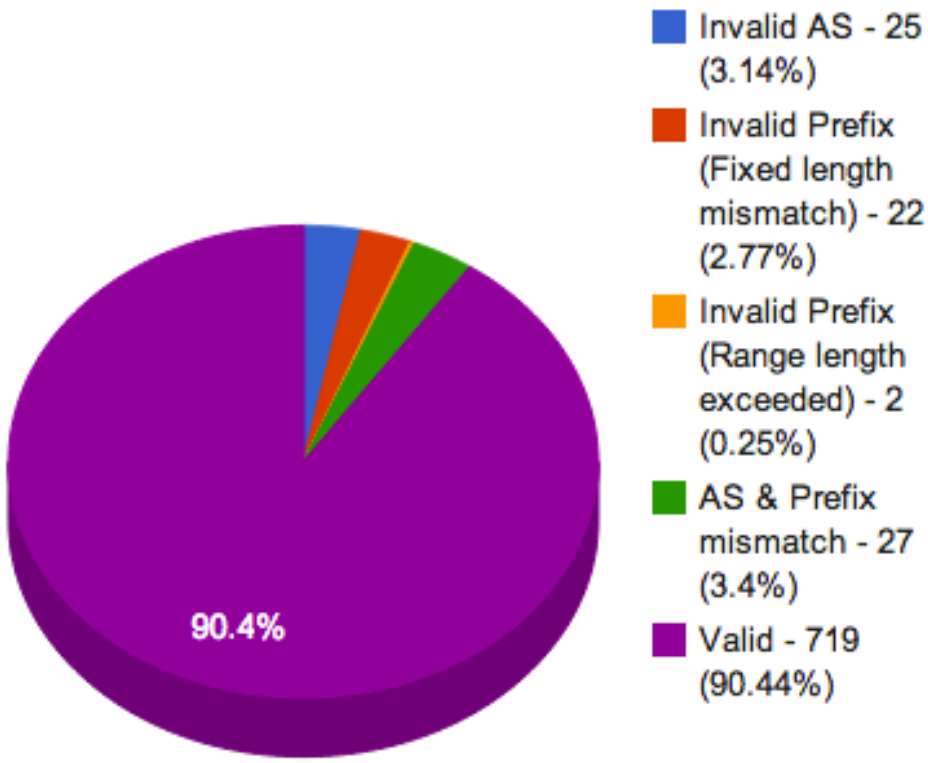


IPv4 vs IPv6

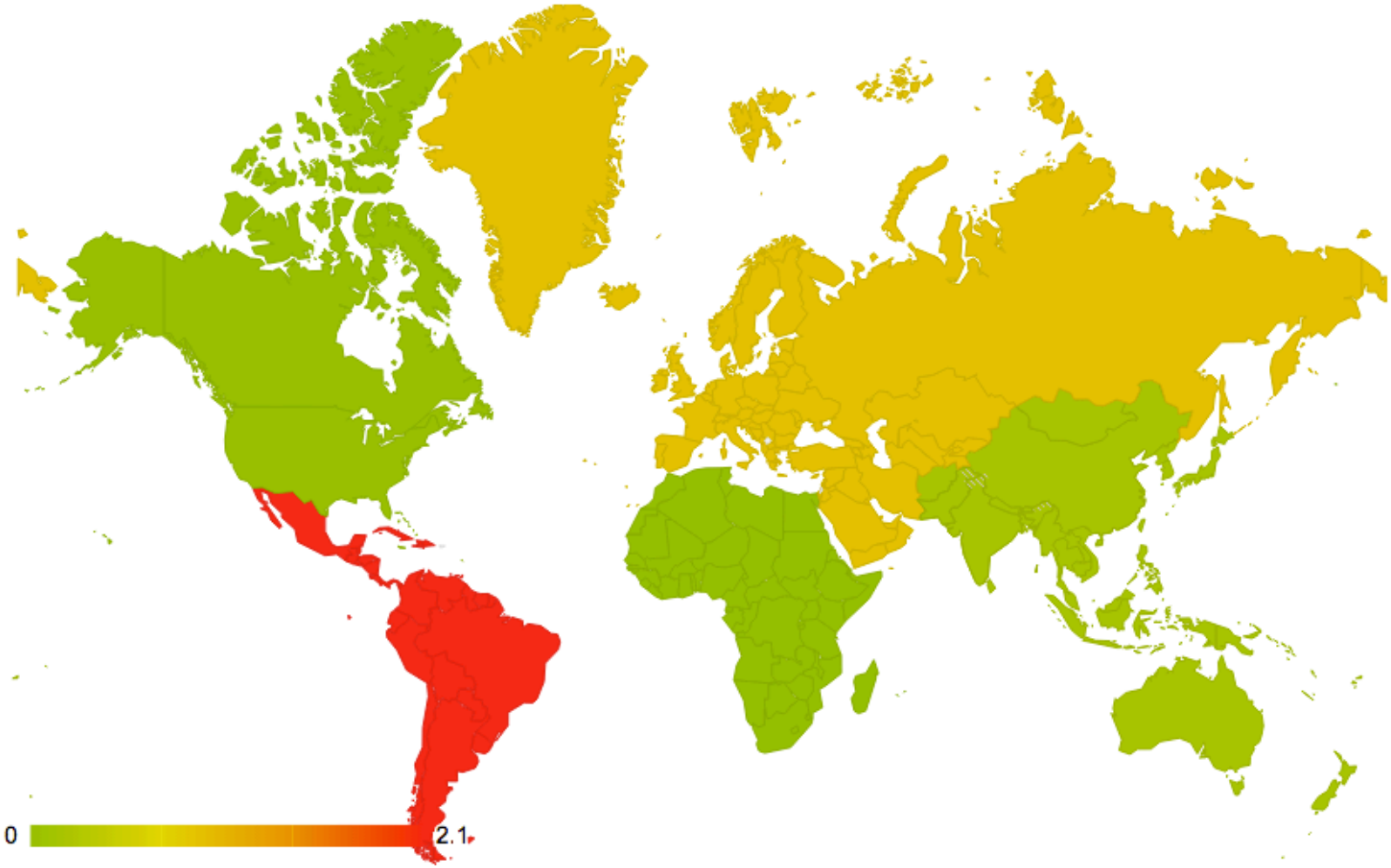
Distribution of RPKI prefixes for IPv4



Distribution of RPKI prefixes for IPv6



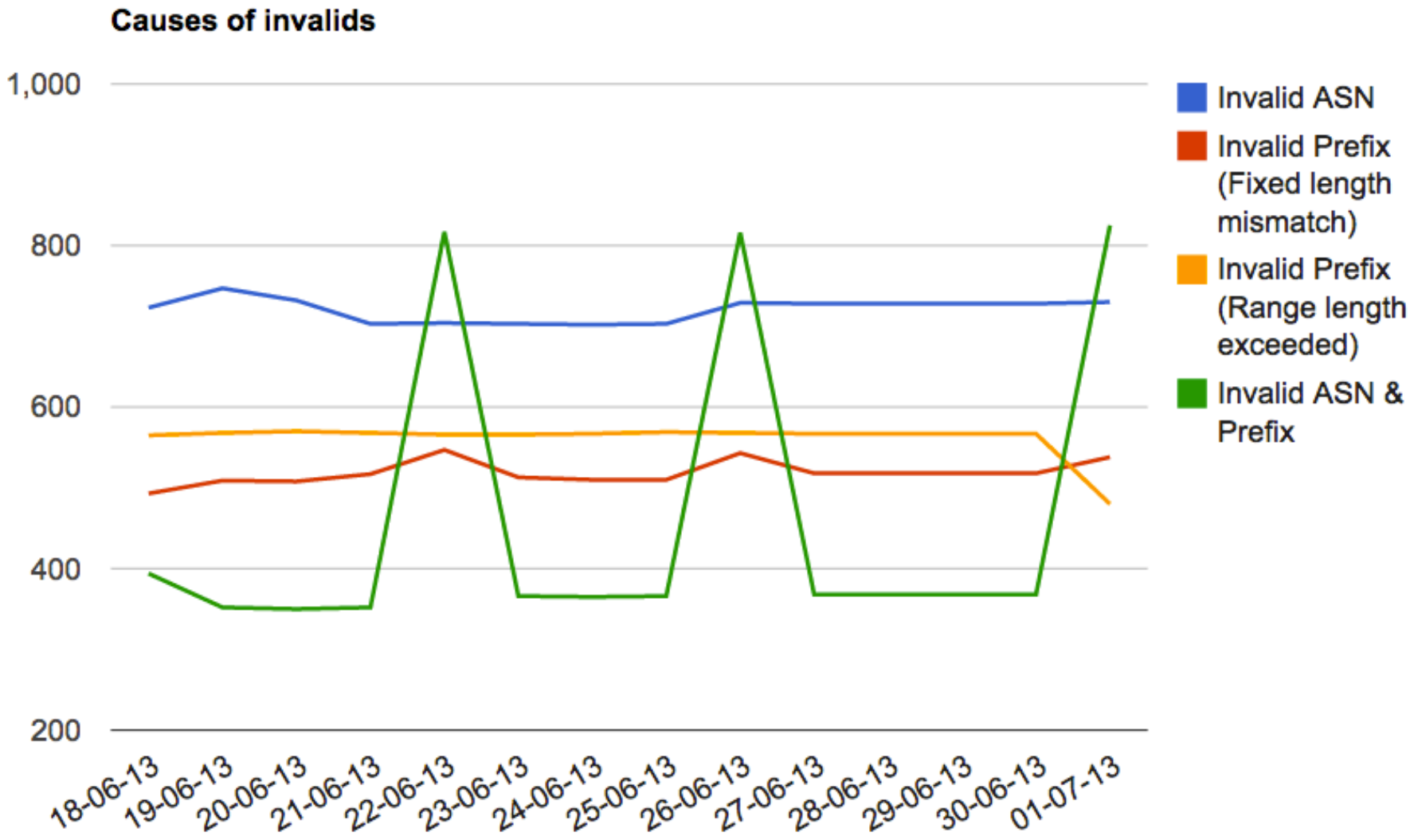
Origin of invalids



RIR Statistics

RIR	Total	Valid	Invalid	Unknown	RPKI Adoption Rate
AFRINIC	10839 (100%)	12 (0.11%)	0 (0%)	10827 (99.89%)	0.11%
APNIC	116379 (100%)	84 (0.07%)	212 (0.18%)	116083 (99.75%)	0.25%
ARIN	182009 (100%)	199 (0.11%)	30 (0.02%)	181780 (99.87%)	0.13%
LACNIC	56294 (100%)	5561 (9.88%)	1184 (2.1%)	49549 (88.02%)	11.98%
RIPE	128726 (100%)	6400 (4.97%)	1147 (0.89%)	121179 (94.14%)	5.86%

Monitoring over time



Weird stuff

01-07-2013	
ASN	count
2065	92
1942	82
1724	66
35104	64
2457	62
1937	39
1945	33
1723	32
197890	17
8649	16

30-06-2013	
ASN	count
35104	64
8649	16
197890	16
2199	13
2471	12
27947	12
24954	9
27817	9
197860	8
9180	7


Demo!!

Conclusion

- Dashboard for operators and RIRs
- Distribution of invalids
- Insight in:
  - Configuration mistakes
  - Adoption rate RPKI
  - Detailed prefix information
- Daily stats monitoring

Future work

- Performance improvements
- Even more statistics
  - Data already available
- Extensible framework

Q&A

- https://github.com/remydb/RPKI-Dashboard