Measuring Adoption of RPKI Route Validation and Filtering

Andreas Reuter (andreas.reuter@fu-berlin.de)

Joint work with Randy Bush, Ethan Katz-Bassett, Italo Cunha, Thomas C. Schmidt, and Matthias Wählisch
Once upon a time ... someone incorrectly announced an IP prefix.

http://thlede.blogspot.com/2008/02/25/pakistan-blamed-for-
Once upon a time ... someone incorrectly announced an IP prefix.

For about 18 minutes on April 8, 2010, China Telecom advertised erroneous network traffic routes that instructed U.S. and other foreign Internet traffic to travel through Chinese servers.* Other serv-
Once upon a time ... someone incorrectly announced an IP prefix.

For about 18 minutes on April 8, 2010, China Telecom advertised erroneous network traffic routes that instructed U.S. and other foreign Internet traffic to travel through Chinese servers.* Other serv-

Russian-controlled telecom hijacks financial services’ Internet traffic

Visa, MasterCard, and Symantec among dozens affected by "suspicious" BGP mishap.
Enter RPKI

Prefix hijacking prevention using Resource Public Key Infrastructure
Enter RPKI

Prefix hijacking prevention using Resource Public Key Infrastructure

ROA Data

Authorization object: Which AS is allowed to announce an IP prefix
Prefix hijacking prevention using Resource Public Key Infrastructure

- **ROA Data**: Authorization object: Which AS is allowed to announce an IP prefix
- **Route Origin Validation**: Router operation to validate BGP Updates based on ROA data
- **Local Policy**: Decide handling of invalid BGP routes (drop?)
Enter RPKI

Prefix hijacking prevention using Resource Public Key Infrastructure

**ROA Data**
- Authorization object: Which AS is allowed to announce an IP prefix

**Route Origin Validation**
- Router operation to validate BGP Updates based on ROA data

**Local Policy**
- Decide handling of invalid BGP routes (drop?)

**ROA:** 10.20.0.0/16-24 AS100

- BGP: 10.20.0.0/16 AS100 ✅ Accept
- BGP: 10.20.0.0/16 AS666 ❌ Reject
Research Problem

Measure the adoption of RPKI-based filter policies.

Authorization object: Which AS is allowed to announce an IP prefix

Router operation to validate BGP Updates based on ROA data

Decide handling of invalid BGP routes (drop?)
Research Challenge

Authorization object: Which AS is allowed to announce an IP prefix

Router operation to validate BGP Updates based on ROA data

Decide handling of invalid BGP routes (drop?)

Measure the adoption of RPKI-based filter policies.

**Challenge:** Private policies must be inferred from measurements.
Two principle approaches

Uncontrolled experiments
Analysing existing BGP data and ROAs, trying to infer who is filtering.

Controlled experiments
Actively announcing BGP Updates and dynamically creating ROAs
Analyse resulting BGP data to infer who is filtering.

➔ Fast
➔ Easy

➔ Slow
➔ Needs experimental facilities
Uncontrolled Experiments: The Basic Idea

➔ Leverage divergence between AS paths of invalid and non-invalid routes to infer if an AS is filtering
Uncontrolled Experiments: The Basic Idea

➔ Leverage divergence between AS paths of invalid and non-invalid routes to infer if an AS is filtering

Vantage point (VP) peers with route collector (RC), sends full or partial feed of selected routes to it.

AS1 announces prefixes: \( P_1 \) (valid) and \( P_2 \) (invalid)

Vantage point selects routes with different AS path for the prefixes
Uncontrolled Experiments: The Basic Idea

- Leverage divergence between AS paths of invalid and non-invalid routes to infer if an AS is filtering

Vantage point (VP) peers with route collector (RC), sends full or partial feed of selected routes to it.

AS1 announces prefixes: $P_1$ (valid) and $P_2$ (invalid)

Filtering invalid routes?
Uncontrolled Experiments: Problems
Uncontrolled Experiments: Problems

→ Limited Control
Uncontrolled Experiments: Problems

➔ Limited Control

◆ Do not know origin AS policy. Traffic engineering might look like RPKI-based filtering.
Uncontrolled Experiments: Limited Control

Origin Policy

Vantage point chooses routes with different AS path

Origin announces prefixes: \( P_1 \) (valid) and \( P_2 \) (invalid)
Uncontrolled Experiments: Limited Control

Origin Policy

Is AS1 using RPKI-based filtering policy?

Vantage point chooses routes with different AS path

Origin announces prefixes: \( P_1 \) (valid) and \( P_2 \) (invalid)
Uncontrolled Experiments: Limited Control

Origin Policy

Vantage point chooses routes with different AS path

Origin announces prefixes: $P_1$ (valid) and $P_2$ (invalid)
Uncontrolled Experiments: Limited Control

Origin Policy

Vantage point chooses routes with different AS path

Origin announces prefixes: $P_1$ (valid) and $P_2$ (invalid)

ROA:
Prefix: 10.20.0.0/22 - 22
ASN: Origin

10.20.0.0/22

10.20.0.0/24
Uncontrolled Experiments: Limited Control

Origin Policy

Path divergence at first hop is more likely to be the result of traffic engineering at origin.

Vantage point chooses routes with different AS path

Origin announces prefixes: $P_1$ (valid) and $P_2$ (invalid)
Path Divergence

Divergence between AS paths of routes with the same origin

Distr. of divergence points between pairs of distinct paths
monitor ('129.250.0.11', '2914'). Origins: 97

Fraction of path pairs

AS hop at which paths diverge
Path Divergence

Divergence between AS paths of routes with the same origin

Distr. of divergence points between pairs of distinct paths
monitor ('129.250.0.11', '2914'). Origins: 97

No significant difference between distributions indicates lack of widespread filtering

> Invalid routes (probably) have different AS paths for non-RPKI reasons
Uncontrolled Experiments: Problems

→ Limited Control

◆ Do not know origin AS policy. Traffic engineering might look like RPKI-based filtering.

◆ Cannot distinguish between filtering based on RPKI vs. filtering based on other attributes
Uncontrolled Experiments: Limited Control

Real World Example

Vantage point chooses routes with different AS path

Origin announces prefixes: $P_1$ (valid) and $P_2$ (invalid)
Uncontrolled Experiments: Limited Control

Real World Example

Is AS3356 using RPKI-based filtering policy?

Vantage point chooses routes with different AS path.

Origin announces prefixes: $P_1$ (valid) and $P_2$ (invalid).
Uncontrolled Experiments: Limited Control

Real World Example

Vantage point chooses routes with different AS path

Is AS3356 using RPKI-based filtering policy?  

No!

Vantage point is using route age as tie breaker.

Origin announces prefixes: P₁ (valid) and P₂ (invalid)
Uncontrolled Experiments: Problems

➔ Limited Control
  ◆ Do not know origin AS policy. Traffic engineering might look like RPKI-based filtering.
  ◆ Cannot distinguish between filtering based on RPKI vs. filtering based on other attributes
Uncontrolled Experiments: Problems

➔ Limited Control
  ◆ Do not know origin AS policy. Traffic engineering might look like RPKI-based filtering.
  ◆ Cannot distinguish between filtering based on RPKI vs. filtering based on other attributes

➔ Limited Visibility can lead to misclassification
Uncontrolled Experiments: Limited Visibility

- Analysing data from different sets of vantage points can yield different classifications
Uncontrolled Experiments: Limited Visibility

- Analysing data from different sets of vantage points can yield different classifications

Vantage point chooses routes with different AS path

AS1 announces prefixes: $P_1$ (valid) and $P_2$ (invalid)
Uncontrolled Experiments: Limited Visibility

- Analysing data from different sets of vantage points can yield different classifications

Vantage point chooses routes with different AS path

Is AS2 using RPKI-based filtering policy?

AS1 announces prefixes: $P_1$ (valid) and $P_2$ (invalid)
Uncontrolled Experiments: Limited Visibility

→ Analysing data from different sets of vantage points can yield different classifications

VP

VP2

Is AS2 using RPKI-based filtering policy? **Probably not!**

Another vantage point chooses routes with same AS path

Vantage point chooses routes with different AS path

AS1 announces prefixes: $P_1$ (valid) and $P_2$ (invalid)
Uncontrolled Experiments: Limited Visibility

Analysing data from different sets of vantage points can yield different classifications.

VP1 announces prefixes: $P_1$ (valid) and $P_2$ (invalid).

Another vantage point chooses routes with the same AS path.

Is AS2 using RPKI-based filtering policy? **Probably not!**

We don’t have a complete view of AS-level Internet. Inference without considering missing data can lead to misclassification!
Uncontrolled Experiments: Problems

➔ Limited Control

◆ Do not know origin AS policy. Traffic engineering might look like RPKI-based filtering.

◆ Cannot distinguish between filtering based on RPKI vs. filtering based on other attributes

➔ Limited Visibility can lead to misclassification
Uncontrolled Experiments: Problems

➔ Limited Control
  ◆ Do not know origin AS policy. Traffic engineering might look like RPKI-based filtering.
  ◆ Cannot distinguish between filtering based on RPKI vs. filtering based on other attributes

➔ Limited Visibility can lead to misclassification

➔ Not possible to reproduce
Uncontrolled Experiments: Problems

➔ Limited Control

◆ Do not know origin AS policy. Traffic engineering might look like RPKI-based filtering.

◆ Cannot distinguish between filtering based on RPKI vs. filtering based on other attributes

➔ Limited Visibility can lead to misclassification

➔ Not possible to reproduce

Inferring if a specific AS is using RPKI-based filtering on the basis of uncontrolled experiments is prone to misclassification!
Controlled Experiments
Controlled Experiments

Hand-crafted ROAs *and* BGP Updates
Controlled Experiments: Advantages

Hand-crafted ROAs and BGP Updates

→ Limited Control

◆ We know the routing policy of origin AS
Controlled Experiments: Advantages

Hand-crafted ROAs and BGP Updates

➔ Limited Control

◆ We know the routing policy of origin AS
◆ Can distinguish between RPKI-based filtering vs. filtering based on other attributes by changing ROAs/Updates
Controlled Experiments: Advantages

Hand-crafted ROAs and BGP Updates

➔ Limited Control
  ◆ We know the routing policy of origin AS
  ◆ Can distinguish between RPKI-based filtering vs. filtering based on other attributes by changing ROAs/Updates

➔ Limited Visibility is less of an issue, we only care about our prefixes
Controlled Experiments: Advantages

Hand-crafted ROAs \textit{and} BGP Updates

\begin{itemize}
  \item Limited Control
    \begin{itemize}
      \item We know the routing policy of origin AS
      \item Can distinguish between RPKI-based filtering vs. filtering based on other attributes by changing ROAs/Updates
    \end{itemize}
  \item Limited Visibility is less of an issue, we only care about our prefixes
  \item Can repeat experiments and target specific AS.
\end{itemize}
Controlled Experiments: Our Setup

**BGP**

Announce prefixes $P_A$ (Anchor) and $P_E$ (Experiment)

- Same RIR DB route object
- Same length
- Minimal bit difference
- Announced at the same time
- Announced from same origin AS
- Announced to same peers

**RPKI**

Issue ROAs for both prefixes

Periodically change ROA for experiment prefix

➔ Flips announcement from VALID to INVALID to VALID once a day

(Yes, we operate a grandchild RPKI CA ;)
Controlled Experiments: Observations

Situation: Origin and vantage point peer directly

Vantage point chooses routes with same AS path

Origin announces prefixes: \( P_A \) (valid) and \( P_E \) (valid)
Controlled Experiments: Observations

Situation: Origin and vantage point peer directly

Vantage point chooses routes with same AS path

Origin announces prefixes: $P_A$ (valid) and $P_E$ (valid)
Controlled Experiments: Observations

Situation: Origin and vantage point peer directly

**Observation 1**: VP has no route for $P_E$ now that it’s announcement is invalid

**Conclusion**: VP is using RPKI-based filtering.
Controlled Experiments: Observations

Situation: Origin and vantage point peer directly

**Observation 2**: VP has route via AS X for $P_E$ now that it’s announcement is invalid

Vantage point chooses routes with different AS path

Origin announces prefixes: $P_A$ (valid) and $P_E$ (invalid)

**Conclusion**: VP uses RPKI-based filtering *selectively*. 
Controlled Experiments: Observations

Situation: Origin and vantage point do not peer directly, other AS on path

- Vantage point chooses routes with same AS path
- Origin announces prefixes: $P_A$ (valid) and $P_E$ (valid)
Controlled Experiments: Observations

Situation: Origin and vantage point do not peer directly, other AS on path

Vantage point chooses routes with same AS path

Origin announces prefixes: $P_A$ (valid) and $P_E$ (valid)
Controlled Experiments: Observations

Situation: Origin and vantage point do not peer directly, other AS on path

**Observation 1**: VP has no route for $P_E$ now that it’s announcement is invalid

Conclusion: VP or AS X (or both) are using RPKI-based filtering.
Controlled Experiments: Observations

Situation: Origin and vantage point do not peer directly, other AS on path

**Observation 2**: VP has different route for $P_E$ now that it’s announcement is invalid.

Conclusion: VP or AS X (or both) are using RPKI-based filtering.
Controlled Experiments: Observations

Situation: Origin and vantage point do not peer directly, other AS on path

Observation 2: VP has different route for $P_E$ now that it’s announcement is invalid

Resolve ambiguity by:

$\rightarrow$ Establishing direct peering with VP
Controlled Experiments: Observations

Situation: Origin and vantage point do not peer directly, other AS on path

Observation 2: VP has different route for $P_E$ now that it’s announcement is invalid

Resolve ambiguity by:

- Establishing direct peering with VP
- Checking if AS X has a vantage point
Results
Results

We found at least 3 AS that deployed RPKI-based filtering!

None of them are large providers ...

2 AS filtered all invalid routes

1 AS filtered selectively

Another measurement study found other results.
Results

We found at least 3 AS that deployed RPKI-based filtering!

None of them are large providers.

Confirmed by repeated experiments and talking to operators.

Another measurement study found other results.
Conclusion

➔ There are ASes that do RPKI-based filtering. Not many, not the big ones, but at least some (>3).

➔ Uncontrolled experiments are unsuited to infer RPKI-based filtering policies

➔ Controlled experiments are crucial to measuring adoption of RPKI-based filtering policies

Internet infrastructure requires proper monitoring.
Next Steps

→ We will extend our measurement methodology.

→ We will establish a live monitoring system with public access.

BGP monitoring is based on collaboration!

→ Please, establish direct peering with PEERING testbed.
  ◆ https://peering.usc.edu/peering/

→ Please, peer with public route collectors.
Next Steps

Have you enabled RPKI-based OV on a router today?
Backup
Path Diversity

Path Diversity Distribution of a single vantage point

For ~50% of origins, there is exactly one distinct AS path.

When invalid routes are included, path diversity of some origins increases.

➔ Invalid routes tend to have different AS paths than non-invalid routes.
Vantage Point Visibility Matters
Prefixes and their Origins

Some VP have a near ‘global’ view.

Some VPs see barely anything.

![Graph showing distribution of prefixes and origins among vantage points.](image)

- **Y-axis (left graph):** 
  - # of prefixes
  - Scale: $10^0$ to $10^6$

- **Y-axis (right graph):** 
  - # of origins
  - Scale: $10^0$ to $10^5$

- **X-axis:** 
  - Vantage points ranked by number of prefixes seen

- **Legend:**
  - Some VP have near ‘global’ view.
  - Some VPs see barely anything.
Vantage Point Visibility Matters

Prefixes of invalid routes and their reasons for invalidity

Some VPs have very few invalid prefixes
Some none at all

Reason for invalidity

Vantage points ranked by number of prefixes seen

bad as
bad as&len.
bad len.
Vantage Point Visibility Matters

Per-Origin Prefix Visibility

→ Virtually all VPs have some origin AS they only ‘see’ incompletely. Oops!
Invalid Announcements: Path Diversity

Path diversities of origins with at least 1 non-invalid and 1 invalid prefix as seen from vantage points

All paths

Non-invalid paths

Distinct paths to origin