Towards A Longitudinal Study of Adoption of RPKI-Based Route Filtering

Ethan Katz-Bassett (University of Southern California)

with:
Andreas Reuter and Matthias Wahlisch (Freie Universität Berlin),
Brandon Schlinker (USC), Italo Cunha (UFMG Brazil), Randy Bush (IIJ),
Thomas C. Schmidt (HAW Hamburg), Doug Montgomery (NIST)
Background

Prefix hijack prevention using Resource Public Key Infrastructure requires three steps:

- **Route Origin Authorization (ROA)**
  - Attests which AS is authorized to announce IP prefix

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

- **Local Policy**
  - Decide handling of invalid BGP routes: drop? prefer valid?
Problem Statement & Challenge
Prefix hijack prevention using Resource Public Key Infrastructure requires three steps:

- **Route Origin Authorization (ROA)**: Attests which AS is authorized to announce IP prefix.
- **Route Origin Validation**: Router operation to verify BGP Updates based on ROA data.
- **Local Policy**: Decide handling of invalid BGP routes: drop? prefer valid?

**Goal**: Measure the adoption of RPKI-based filter policies.
Prefix hijack prevention using Resource Public Key Infrastructure requires three steps:

**Goal:** Measure the adoption of RPKI-based filter policies.

**Challenge:** Private data must be inferred from measurements.
Uncontrolled experiments are unsuitable

Natural (uncontrolled) experiments can lead to incorrect inference: Suppose an AS is announcing a valid prefix and an invalid one. Can we compare the 2 paths to infer route origin validation? NO! Not definitively, as multiple explanations are plausible:

**Observation:**
- Same paths
- Different paths
- No path to invalid

**Possible ROV inference:**
- No ROV
- ROV on 😊 path
- ROV on 😛 path

**Alternate explanation:**
- ROV policy to prefer valid, but none exist
- TE by Origin
- Limited visibility: Peer route not exported to monitor
We need controlled experiments
Hand-crafted ROAs and active BGP Updates from PEERING testbed.

+ Ground truth knowledge of:
  • Our neighbors/relationships
  • Our policies/announcements

+ Manipulate ROAs and Updates to:
  • Reproduce observations, independent of external events
  • Perform detailed analysis of subtle filter policies
  • Use an iterative approach, with results informing later interpretations
We need controlled experiments

Hand-crafted ROAs and active BGP Updates from PEERING testbed.

+ Ground truth knowledge of:
  • Our neighbors/relationships
  • Our policies/announcements

+ Manipulate ROAs and Updates to:
  • Reproduce observations, independent of external events
  • Perform detailed analysis of subtle filter policies
  • Use an iterative approach, with results informing later interpretations

Simplified example to expose that GBLX performs ROV
We need controlled experiments

Hand-crafted ROAs and active BGP Updates from PEERING testbed.

+ Ground truth knowledge of:
  • Our neighbors/relationships
  • Our policies/announcements

+ Manipulate ROAs and Updates to:
  • Reproduce observations, independent of external events
  • Perform detailed analysis of subtle filter policies
  • Use an iterative approach, with results informing later interpretations

Simplified example to expose that GBLX performs ROV
We need controlled experiments

Hand-crafted ROAs and active BGP Updates from PEERING testbed.

+ Ground truth knowledge of:
  - Our neighbors/relationships
  - Our policies/announcements

+ Manipulate ROAs and Updates to:
  - Reproduce observations, independent of external events
  - Perform detailed analysis of subtle filter policies
  - Use an iterative approach, with results informing later interpretations

Simplified example to expose that GBLX performs ROV
We need controlled experiments

Hand-crafted ROAs and active BGP Updates from PEERING testbed.

+ Ground truth knowledge of:
  • Our neighbors/relationships
  • Our policies/announcements

+ Manipulate ROAs and Updates to:
  • Reproduce observations, independent of external events
  • Perform detailed analysis of subtle filter policies
  • Use an iterative approach, with results informing later interpretations

Simplified example to expose that GBLX performs ROV
We need controlled experiments

Hand-crafted ROAs and active BGP Updates from PEERING testbed.

+ Ground truth knowledge of:
  - Our neighbors/relationships
  - Our policies/announcements

+ Manipulate ROAs and Updates to:
  - Reproduce observations, independent of external events
  - Perform detailed analysis of subtle filter policies
  - Use an iterative approach, with results informing later interpretations

Simplified example to expose that GBLX performs ROV
We need controlled experiments
Hand-crafted ROAs and active BGP Updates from PEERING testbed.

+ Ground truth knowledge of:
  • Our neighbors/relationships
  • Our policies/announcements

+ Manipulate ROAs and Updates to:
  • Reproduce observations, independent of external events
  • Perform detailed analysis of subtle filter policies
  • Use an iterative approach, with results informing later interpretations

Simplified example to expose that GBLX performs ROV
We need controlled experiments

Hand-crafted ROAs and active BGP Updates from PEERING testbed.

+ Ground truth knowledge of:
  • Our neighbors/relationships
  • Our policies/announcements

+ Manipulate ROAs and Updates to:
  • Reproduce observations, independent of external events
  • Perform detailed analysis of subtle filter policies
  • Use an iterative approach, with results informing later interpretations

Simplified example to expose that GBLX performs ROV
We need controlled experiments

Hand-crafted ROAs and active BGP Updates from PEERING testbed.

+ Ground truth knowledge of:
  • Our neighbors/relationships
  • Our policies/announcements

+ Manipulate ROAs and Updates to:
  • Reproduce observations, independent of external events
  • Perform detailed analysis of subtle filter policies
  • Use an iterative approach, with results informing later interpretations

Simplified example to expose that GBLX performs ROV
We need controlled experiments

Hand-crafted ROAs and active BGP Updates from PEERING testbed.

+ Ground truth knowledge of:
  • Our neighbors/relationships
  • Our policies/announcements

+ Manipulate ROAs and Updates to:
  • Reproduce observations, independent of external events
  • Perform detailed analysis of subtle filter policies
  • Use an iterative approach, with results informing later interpretations

Simplified example to expose that GBLX performs ROV
We need controlled experiments

Hand-crafted ROAs and active BGP Updates from PEERING testbed.

+ Ground truth knowledge of:
  • Our neighbors/relationships
  • Our policies/announcements

+ Manipulate ROAs and Updates to:
  • Reproduce observations, independent of external events
  • Perform detailed analysis of subtle filter policies
  • Use an iterative approach, with results informing later interpretations

Simplified example to expose that GBLX performs ROV
We need controlled experiments

Hand-crafted ROAs and active BGP Updates from PEERING testbed.

+ Ground truth knowledge of:
  • Our neighbors/relationships
  • Our policies/announcements

+ Manipulate ROAs and Updates to:
  • Reproduce observations, independent of external events
  • Perform detailed analysis of subtle filter policies
  • Use an iterative approach, with results informing later interpretations

Simplified example to expose that GBLX performs ROV
We need controlled experiments

Hand-crafted ROAs and active BGP Updates from PEERING testbed.

+ Ground truth knowledge of:
  • Our neighbors/relationships
  • Our policies/announcements

+ Manipulate ROAs and Updates to:
  • Reproduce observations, independent of external events
  • Perform detailed analysis of subtle filter policies
  • Use an iterative approach, with results informing later interpretations

Simplified example to expose that
GBLX performs ROV
We need controlled experiments

Hand-crafted ROAs and active BGP Updates from PEERING testbed.

+ Ground truth knowledge of:
  • Our neighbors/relationships
  • Our policies/announcements

+ Manipulate ROAs and Updates to:
  • Reproduce observations, independent of external events
  • Perform detailed analysis of subtle filter policies
  • Use an iterative approach, with results informing later interpretations

Simplified example to expose that GBLX performs ROV
We need controlled experiments

Hand-crafted ROAs and active BGP Updates from PEERING testbed.

+ Ground truth knowledge of:
  • Our neighbors/relationships
  • Our policies/announcements

+ Manipulate ROAs and Updates to:
  • Reproduce observations, independent of external events
  • Perform detailed analysis of subtle filter policies
  • Use an iterative approach, with results informing later interpretations

Simplified example to expose that GBLX performs ROV
We need controlled experiments

Hand-crafted ROAs and active BGP Updates from PEERING testbed.

+ Ground truth knowledge of:
  • Our neighbors/relationships
  • Our policies/announcements

+ Manipulate ROAs and Updates to:
  • Reproduce observations, independent of external events
  • Perform detailed analysis of subtle filter policies
  • Use an iterative approach, with results informing later interpretations

Simplified example to expose that GBLX performs ROV