IRRedicator: Pruning IRR with RPKI-Valid BGP Insights

Minhyeok Kang†, Weitong Li§, Roland van Rijswijk-Deij§ ‡, Taekyoung "Ted" Kwon†, Taejoong Chung§
† Seoul National University, ‡ University of Twente, § Virginia Tech
Border Gateway Protocol (BGP)

• BGP is one of the most crucial components for sustaining global network connectivity

• However, BGP was not designed with security in mind (e.g., no route origin authentication)

THE POWER OF FALSE ADVERTISING —
How an Indonesian ISP took down the mighty Google for 30 minutes

Internet’s web of trust let a company you never heard of block your Gmail.

SEAN GALLAGHER • 11/6/2012, 11:07 AM

Google’s services went offline for many users for nearly a half-hour on the evening of November 5, thanks to an erroneous routing message broadcast by Moratel, an Indonesian telecommunications company. The outage might have lasted even longer if it hadn’t been spotted by a network engineer at CloudFlare who had a friend in a position to fix the problem.
Border Gateway Protocol (BGP)

- BGP is one of the most crucial components for sustaining global network connectivity
- However, BGP was not designed with security in mind (e.g., no route origin authentication)
Border Gateway Protocol (BGP)

• BGP is one of the most crucial components for sustaining global network connectivity

• However, BGP was not designed with security in mind (e.g., no route origin authentication)
Border Gateway Protocol (BGP)

• BGP is one of the most crucial components for sustaining global network connectivity

• However, BGP was not designed with security in mind (e.g., no route origin authentication)
Efforts to improve BGP security

• Internet Routing Registry (IRR) (1995)
  • widely used for sharing global routing information (> 68% of ASes)
  • lacks an authentication mechanism & has many outdated entries

• Resource Public Key Infrastructure (RPKI) (2008)
  • provides a cryptographically verifiable method of binding IP prefixes to their respective origin ASes
  • narrower coverage than IRR
    • has certificate dependencies in the hierarchy of RPKI
    • configuration issues in Route Origin Authorization (ROA) objects
Efforts to improve BGP security

- Internet Routing Registry (IRR) (1995)
  - widely used for sharing global routing information (> 68% of ASes)
  - lacks an authentication mechanism & has many outdated entries

- Resource Public Key Infrastructure (RPKI) (2008)
  - provides a cryptographically verifiable method of binding IP prefixes to their respective origin ASes
  - narrower coverage than IRR
    - has certificate dependencies in the hierarchy of RPKI
    - configuration issues in Route Origin Authorization (ROA) objects

Take the strengths of both IRR and RPKI in order to improve the BGP security
Datasets

<table>
<thead>
<tr>
<th>Auth. Objects</th>
<th>Measurement Period</th>
<th># of Objects</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROA</td>
<td>2011/01 – 2023/03</td>
<td>333 K</td>
</tr>
<tr>
<td>RADb</td>
<td>2016/08 – 2023/03</td>
<td>1.43 M</td>
</tr>
<tr>
<td>ALL-IRRrs</td>
<td>2019/12 – 2023/03</td>
<td>2.69 M</td>
</tr>
</tbody>
</table>

RADb + IRRs of Regional Internet Registries
The deployment status of IRR and RPKI

- **IRR**: 93% of BGP announcements are covered.
- **RPKI**: 40% of BGP announcements are covered.

Graph showing the percentage of BGP announcements covered by RPKI and IRR from 2011 to 2023.
The deployment status of IRR and RPKI

- **98%** of covered BGP announcements are valid
- **90%** of covered BGP announcements are valid
The deployment status of IRR and RPKI

a gap between the percentages of valid BGP announcements

Inconsistency?
Are they consistent with “each other”? 

- For IP prefixes registered in both IRR and RPKI, we examine whether they have the same origin AS as the one registered in RPKI.

<table>
<thead>
<tr>
<th>Date</th>
<th>RADb(#)</th>
<th>ALL-IRRs(#)</th>
<th>RADb(%)</th>
<th>ALL-IRRs(%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2020</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2021</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2022</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2023</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

More than 60,000 IP prefixes in IRR are inconsistent with RPKI.
Do inconsistent IP prefixes appear in BGP announcements?

• For BGP announcements verifiable through both RPKI and IRR, we track their frequency over time

More than 20,000 BGP announcements are covered by the inconsistent IP prefixes.
Do inconsistent IP prefixes appear in BGP announcements?

• For BGP announcements verifiable through both RPKI and IRR, we track their frequency over time

Do these inconsistent IRR objects have any specific characteristics?
Age of IRR objects

Age = latest date of our dataset - last modified date

10.8 years (consistent)

16.3 years (inconsistent)
Example: filtering with age

CDF

Age (years)

0 5 10 15 20 25 30

0 0.2 0.4 0.6 0.8 1

16.3

Remove

Const.

Inconst.

16 / 35
Example: filtering with age

1.6% of consistent IRR objects

10% of inconsistent IRR objects

16.3
How to deal with inconsistent IRR objects?

• Filtering IRR objects with their ages
  • setting a “good” threshold is challenging
    • conservatively → low coverage, aggressively → high mis-classification

• Utilizing RPKI to filter out inconsistent IRR objects
  • RPKI only covers 44% of IRR objects

• Leveraging patterns of BGP announcements datasets to identify inconsistent IRR objects
  • can be applied to all IRR objects!
BGP announcement pattern

- **Lifespan**: The difference in dates between the first and last observations, divided by a monitoring window size.

- **Uptime**: The number of days that BGP announcements have been observed, divided by a monitoring window size.

- **Relative uptime**: Uptime/lifespan.

**Monitoring window**: A time period from the start time to the latest date of our dataset.
• **Lifespan**
the difference in dates between the first and last observations, divided by a monitoring window size

• **Uptime**
the number of days that BGP announcements have been observed, divided by a monitoring window size

• **Relative uptime**
uptime/lifespan
**BGP announcement pattern**

- **Lifespan**
  the difference in dates between the first and last observations, divided by a monitoring window size

- **Uptime**
  the number of days that BGP announcements have been observed, divided by a monitoring window size

**Consistent IRR objects tend to be more recently used**
BGP announcement pattern

- **Lifespan**: the difference in dates between the first and last observations, divided by a monitoring window size.

- **Uptime**: the number of days that BGP announcements have been observed, divided by a monitoring window size.

- **Relative uptime**: uptime/lifespan

Consistent IRR objects tend to be more frequently announced in BGP than inconsistent ones.
**BGP announcement pattern**

- **Lifespan**
  the difference in dates between the first and last observations, divided by a monitoring window size

- **Uptime**
  the number of days that BGP announcements have been observed, divided by a monitoring window size

- **Relative uptime**
  uptime/lifespan

**Monitoring window**

a time period from the start time $t$ to the latest date of our dataset
**BGP announcement pattern**

- **Lifespan**
  - The difference in dates between the first and last observations, divided by a monitoring window size.

- **Uptime**
  - The number of days that BGP announcements have been observed, divided by a monitoring window size.

- **Relative uptime**
  - Uptime/lifespan

---

**Monitoring window**
- A time period from the start time $t$ to the latest date of our dataset.

---

**inconsistent IRR objects used to be actively announced**
BGP announcement pattern

- **Lifespan**: the difference in dates between the first and last observations, divided by a monitoring window size.

- **Uptime**: the number of days that BGP announcements have been observed, divided by a monitoring window size.

- **Relative uptime**: uptime/lifespan.

**Monitoring window**: a time period from the start time \( t \) to the latest date of our dataset.

Inconsistent ones become no longer announced in BGP.
Features

• Features
  • More than 300 features for each prefix-origin pair in IRR

• Metrics:
  • Lifespan, Uptime, Relative uptime
  • # of Ups/Downs, Active/Inactive Days

Model

Classification with rejection

LightGBM +

reject
Evaluation with two ground truth datasets

- RPKI
  - ROAs: IP prefix, origin AS
  - Origin AS is the owner of the IP prefix

- Transfer logs from RIRs
  - IP prefixes can be transferred between organizations
  - Transfer logs: IP prefix, source and recipient organizations
  - Recipient organization is the owner of the IP prefix

![Graph showing Precision, Recall, and F1 score for RPKI and Transfer Logs across different thresholds.](image)
Comparison with original IRR and RPKI-filtered IRR (IRRd4)
Comparison with original IRR and RPKI-filtered IRR (IRRD4)

The number of total IRR objects that remain after applying the respective filtering technique.

59% of IRR objects in original IRR dataset
Comparison with original IRR and RPKI-filtered IRR (IRRd4)

The percentage of IRR objects that are actively used in BGP among the respective total number of objects.

- **# of total**
- **% of active**
- **% of covered**
- **% of valid**

60% of IRR objects are used.
Comparison with original IRR and RPKI-filtered IRR (IRRd4)

While filtering out 59% of IRR objects, we still cover 88% of BGP announcements.
Comparison with original IRR and RPKI-filtered IRR (IRRd4)

the percentage of BGP announcements that are valid against the respective IRR dataset

94% of the covered BGP announcements are valid against IRR dataset filtered by our approach

94%
Comparison with original IRR and RPKI-filtered IRR (IRRd4)

*the percentage of valid BGP announcements slightly increases*
Discussion and future work

• Who would be responsible for applying our technique?
  • IRR vs. network operators

• Reducing false negatives
  • Grouping IRR objects by the prefixes and select the most up-to-date IRR object for each IP prefix

• Source code and dataset are publicly available
  • irredicator.netsecurelab.org
Conclusion

• Conduct a **longitudinal study of the inconsistencies** between IRR and RPKI
  • found that the number of inconsistent IRR objects increases

• Analyze the **characteristics of the inconsistent IRR objects**
  • captured distinct patterns between consistent and inconsistent IRR objects

• Propose an **ML-based IRR pruning technique**
  • successfully filtered out stale IRR objects (58.5% of the entire IRR)
  • [https://irredicator.netsecurelab.org/](https://irredicator.netsecurelab.org/)
Backup
Features

- 13 metrics
  - Uptime, Lifespan, Relative Uptime (=3)
  - # of Ups / Downs (=2)
  - min, max, avg, and std of Active/Inactive days (=8)

- Total 312 features
  - Window based features
    - 13 metrics * 20 monitoring windows = 260 features
  - Statistics for each metric
    - 13 metrics * 4 statistics = 52 features