Isolated and Distributed BGP Attacks, and RPKI – From the Perspective of RouteViews

Kevin Conte

March 15, 2020

Outline

- Background
- Problem and Motivation
- Methodology
- Conclusions

Background

Background

BGP (Border Gateway Protocol)

Background

BGP (Border Gateway Protocol)

- Protocol that allows Autonomous Systems to communicate.

Background

BGP (Border Gateway Protocol)

- Protocol that allows Autonomous Systems to communicate.
- Consists of advertisements between AS's

Background

BGP (Border Gateway Protocol)

- Protocol that allows Autonomous Systems to communicate.
- Consists of advertisements between AS's
- Peers advertise which prefixes they know how to get to, with the AS path to get there.

Background

BGP (Border Gateway Protocol)

- Protocol that allows Autonomous Systems to communicate.
- Consists of advertisements between AS's
- Peers advertise which prefixes they know how to get to, with the AS path to get there.
  - This AS path is not necessarily the shortest routing path, but it is the shortest AS path.

Background

BGP (Border Gateway Protocol)

- Protocol that allows Autonomous Systems to communicate.
- Consists of advertisements between AS's
- Peers advertise which prefixes they know how to get to, with the AS path to get there.
  - This AS path is not necessarily the shortest routing path, but it is the shortest AS path.
- Importantly, each advertisement includes an Origin AS.

Background

BGP (Border Gateway Protocol)

- Protocol that allows Autonomous Systems to communicate.
- Consists of advertisements between AS's
- Peers advertise which prefixes they know how to get to, with the AS path to get there.
  - This AS path is not necessarily the shortest routing path, but it is the shortest AS path.
- Importantly, each advertisement includes an Origin AS.
  - That is, which AS is advertising that it owns a particular prefix

BGP Announcements

- A BGP announcement consists of the following: Timestamp, Peer ASN, Peer IP, Prefix, AS_PATH, NEXT_HOP, Origin AS

BGP Announcements

- A BGP announcement consists of the following: Timestamp, Peer ASN, Peer IP, Prefix, AS_PATH, NEXT_HOP, Origin AS
- For the following example, assume the Timestamp is the same for both advertisements.

BGP Announcements

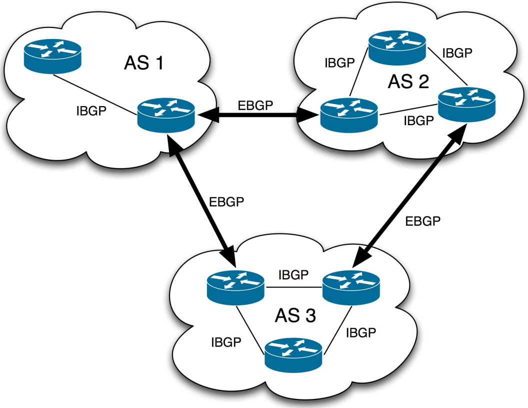
- A BGP announcement consists of the following: Timestamp, Peer ASN, Peer IP, Prefix, AS_PATH, NEXT_HOP, Origin AS
- For the following example, assume the Timestamp is the same for both advertisements.
- Also assume that the NEXT_HOP attribute is the same as the Peer IP

BGP Announcements

- A BGP announcement consists of the following: Timestamp, Peer ASN, Peer IP, Prefix, AS_PATH, NEXT_HOP, Origin AS
- For the following example, assume the Timestamp is the same for both advertisements.
- Also assume that the NEXT_HOP attribute is the same as the Peer IP
- Here, you can see that two different AS's are advertising that they own the same prefix. This is BAD.

```
Peer ASN, Peer IP, Prefix, AS_PATH, Origin AS
33437, 2001:4810::1, 2001::/32, 33437 ... 6939, 6939
3257, 2001:668:0:4::2, 2001::/32, 3257 ... 1101, 1101
```

BGP



Source: noction.com

RPKI Overview

RPKI Overview

- Resource Public Key Infrastructure

RPKI Overview

- Resource Public Key Infrastructure
- Introduced in 2011 to add security to BGP

RPKI Overview

- Resource Public Key Infrastructure
- Introduced in 2011 to add security to BGP
- Developed by the IETF (Internet Engineering Task Force)

RPKI Overview

- Resource Public Key Infrastructure
- Introduced in 2011 to add security to BGP
- Developed by the IETF (Internet Engineering Task Force)
- Consists of Route Origin Authorizations (ROAs)
    - ASN, Prefix, Max Length, Not Before, Not After

RPKI Overview

- Resource Public Key Infrastructure
- Introduced in 2011 to add security to BGP
- Developed by the IETF (Internet Engineering Task Force)
- Consists of Route Origin Authorizations (ROAs)
  - ASN, Prefix, Max Length, Not Before, Not After
- Such objects, when validated, are called Validated ROA Payloads (VRPs).

RPKI Overview

- Resource Public Key Infrastructure
- Introduced in 2011 to add security to BGP
- Developed by the IETF (Internet Engineering Task Force)
- Consists of Route Origin Authorizations (ROAs)
  - ASN, Prefix, Max Length, Not Before, Not After
- Such objects, when validated, are called Validated ROA Payloads (VRPs).
- Example:

```
ASN,     Prefix,           Max Length, Not Before, Not After
AS12345, 128.223.0.0/16, 16,           2011-01-21, 2014-02-28
```

RPKI, cont.

- Also consists of TALs, or Trust Anchor Locations

RPKI, cont.

- Also consists of TALs, or Trust Anchor Locations
- RPKI is all based on trust

RPKI, cont.

- Also consists of TALs, or Trust Anchor Locations
- RPKI is all based on trust
- Those validating route prefixes against ROAs are trusting the TALs to provide correct information.

RPKI, cont.

- Also consists of TALs, or Trust Anchor Locations
- RPKI is all based on trust
- Those validating route prefixes against ROAs are trusting the TALs to provide correct information.
- Thus, there are only a handful of TALs:

RPKI, cont.

- Also consists of TALs, or Trust Anchor Locations
- RPKI is all based on trust
- Those validating route prefixes against ROAs are trusting the TALs to provide correct information.
- Thus, there are only a handful of TALs:
  - IANA (Interent Assigned Numbers Authority).
    - The "root" of the Internet

RPKI, cont.

- Also consists of TALs, or Trust Anchor Locations
- RPKI is all based on trust
- Those validating route prefixes against ROAs are trusting the TALs to provide correct information.
- Thus, there are only a handful of TALs:
  - IANA (Interent Assigned Numbers Authority).
    - The "root" of the Internet
  - ARIN (American Registry for Internet Numbers)

RPKI, cont.

- Also consists of TALs, or Trust Anchor Locations
- RPKI is all based on trust
- Those validating route prefixes against ROAs are trusting the TALs to provide correct information.
- Thus, there are only a handful of TALs:
  - IANA (Interent Assigned Numbers Authority).
    - The "root" of the Internet
  - ARIN (American Registry for Internet Numbers)
  - APNIC (Asia-Pacific Network Information Centre)

RPKI, cont.

- Also consists of TALs, or Trust Anchor Locations
- RPKI is all based on trust
- Those validating route prefixes against ROAs are trusting the TALs to provide correct information.
- Thus, there are only a handful of TALs:
  - IANA (Interent Assigned Numbers Authority).
    - The "root" of the Internet
  - ARIN (American Registry for Internet Numbers)
  - APNIC (Asia-Pacific Network Information Centre)
  - AFRINIC (African Network Information Centre)

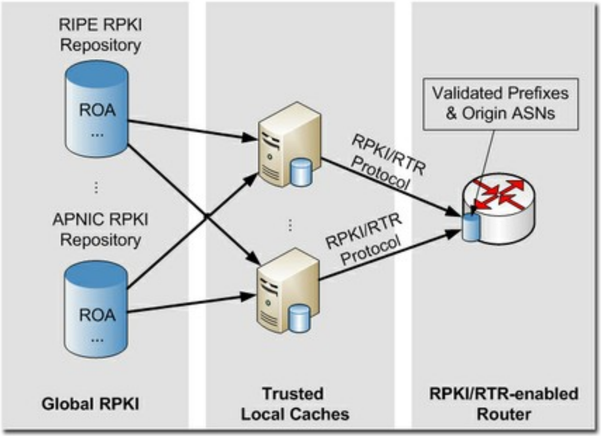
RPKI, cont.

- Also consists of TALs, or Trust Anchor Locations
- RPKI is all based on trust
- Those validating route prefixes against ROAs are trusting the TALs to provide correct information.
- Thus, there are only a handful of TALs:
  - IANA (Interent Assigned Numbers Authority).
    - The "root" of the Internet
  - ARIN (American Registry for Internet Numbers)
  - APNIC (Asia-Pacific Network Information Centre)
  - AFRINIC (African Network Information Centre)
  - RIPE NCC (Réseaux IP Européens Network Coordination Centre)

RPKI, cont.

- Also consists of TALs, or Trust Anchor Locations
- RPKI is all based on trust
- Those validating route prefixes against ROAs are trusting the TALs to provide correct information.
- Thus, there are only a handful of TALs:
  - IANA (Interent Assigned Numbers Authority).
    - The "root" of the Internet
  - ARIN (American Registry for Internet Numbers)
  - APNIC (Asia-Pacific Network Information Centre)
  - AFRINIC (African Network Information Centre)
  - RIPE NCC (Réseaux IP Européens Network Coordination Centre)
  - LACNIC (Latin America and Caribbean Network Information Centre)

RPKI



Source: labs.ripe.net

RIRs

Source: ripe.net

Problem and Motivation

- Taejoong Chung, et. al, RPKI is Coming of Age: A Longitudinal Study of RPKI Deployment and Invalid Route Origins, 2019

Problem and Motivation

- Taejoong Chung, et. al, RPKI is Coming of Age: A Longitudinal Study of RPKI Deployment and Invalid Route Origins, 2019
- This paper shows a negative correlation between the increase in deployment of RPKI and the decrease in the number of invalid route origins.

Number of Invalid Origins

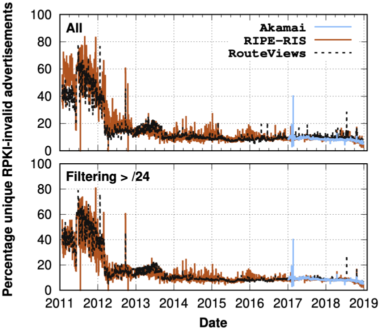


Figure 4: The percentage of invalid BGP announcements from Akamai, RIPE-RIS, and RouteViews datasets: for the first two years of its deployment, about 20.76% of the RPKI-covered BGP announcements are invalid.

Source: Chung, et. al

RPKI Deployment across the RIR's

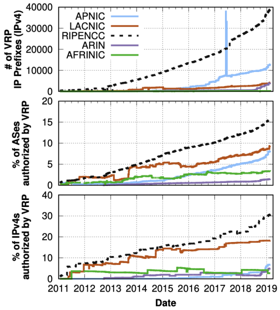


Figure 2: The growth of RPKI in terms of the # of VRP IP prefixes, the % of ASes where some of their IPv4 addresses are covered by VRPs to all ASes managed by the RIR, the % of IPv4 addresses covered by VRPs to all assigned IPv4 addresses for the RIR.

Source: Chung, et. al

What I Wanted To Do

- Distinguish between BGP Hijacks and BGP Misconfigurations

Why I Can't Do That

- AIMS-KISMET 2020 – University of California, San Diego

Why I Can't Do That

- AIMS-KISMET 2020 – University of California, San Diego
  - I had the opportunity to meet with several researchers about this topic

Why I Can't Do That

- AIMS-KISMET 2020 – University of California, San Diego
  - I had the opportunity to meet with several researchers about this topic
  - Most notably, Teejay Chung, the primary author of the aforementioned paper

Why I Can't Do That

- AIMS-KISMET 2020 – University of California, San Diego
  - I had the opportunity to meet with several researchers about this topic
  - Most notably, Teejay Chung, the primary author of the aforementioned paper
  - Researchers have been attempting to do this years

Why I Can't Do That

- AIMS-KISMET 2020 – University of California, San Diego
  - I had the opportunity to meet with several researchers about this topic
  - Most notably, Teejay Chung, the primary author of the aforementioned paper
  - Researchers have been attempting to do this years
  - Best tool we have is CAIDA's BGPstream

Example of Impossibility

```
Peer AS, Peer IP, Prefix, AS PATH, Origin AS
123, 128.223.56.195, 193.56.78.0/24, 123 ... 456, 456
124, 193.57.223.16, 193.56.78.0/24, 124 ... 557, 557
```

Example of Impossibility

```
Peer AS, Peer IP, Prefix, AS PATH, Origin AS
123, 128.223.56.195, 193.56.78.0/24, 123 ... 456, 456
124, 193.57.223.16, 193.56.78.0/24, 124 ... 557, 557
125, 190.34.56.23, 193.56.78.0/24, 125 .. 12345, 12345
```

What I'm Doing

What I'm Doing

- Analyzing the trend of both isolated and distributed BGP attacks

What I'm Doing

- Analyzing the trend of both isolated and distributed BGP attacks
- Correlating that trend to the deployment status of RPKI

What I'm Doing

- Analyzing the trend of both isolated and distributed BGP attacks
- Correlating that trend to the deployment status of RPKI
  - As of August 2019, RPKI now contains more than 100,000 VRPs.

What I'm Doing

- Analyzing the trend of both isolated and distributed BGP attacks
- Correlating that trend to the deployment status of RPKI
    - As of August 2019, RPKI now contains more than 100,000 VRPs.
    - This is promising for future success of RPKI

Datasets

Datasets

- RouteViews
  - Courtesy of the University of Oregon
  - http://archive.routeviews.org

Datasets

- RouteViews
  - Courtesy of the University of Oregon
  - http://archive.routeviews.org
- Historical ROA data
  - Courtesy of RIPE
  - https://ftp.ripe.net/rpki

Tools Used

Tools Used

- For parsing BGP data:
  - bgpreader (https://bgpstream.caida.org/docs/tools/bgpreader)

Tools Used

- For parsing BGP data:
  - bgpreader (https://bgpstream.caida.org/docs/tools/bgpreader)
- For parsing Historical ROAs:
  - Ziggy (https://github.com/NLnetLabs/ziggy)
  - Routinator (https://github.com/NLnetLabs/routinator)

Tools Used

- For parsing BGP data:
  - bgpreader (https://bgpstream.caida.org/docs/tools/bgpreader)
- For parsing Historical ROAs:
  - Ziggy (https://github.com/NLnetLabs/ziggy)
  - Routinator (https://github.com/NLnetLabs/routinator)
- Also, a mixture of Python 3.8+ and POSIX-compliant shell scripts
  - Code to be uploaded to github soon...

Methodology

- Define an isolated attack as two discrete AS's advertising ownership of the same prefix

Methodology

- Define an isolated attack as two discrete AS's advertising ownership of the same prefix
- Define a distributed attack as greater than two discrete AS's advertising ownership of the same prefix

Methodology

- Define an isolated attack as two discrete AS's advertising ownership of the same prefix
- Define a distributed attack as greater than two discrete AS's advertising ownership of the same prefix
- Samples taken every two days from 21 January 2011 $\rightarrow$ 29 February 2020

Methodology

- Define an isolated attack as two discrete AS's advertising ownership of the same prefix
- Define a distributed attack as greater than two discrete AS's advertising ownership of the same prefix
- Samples taken every two days from 21 January 2011 $\rightarrow$ 29 February 2020
- Compare the trend of isolated and distributed attacks against the deployment status of RPKI

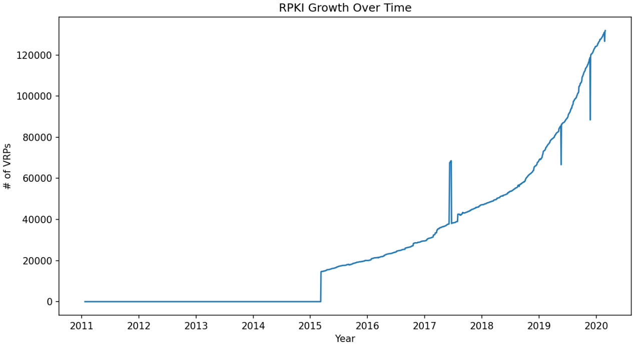
Methodology

- Define an isolated attack as two discrete AS's advertising ownership of the same prefix
- Define a distributed attack as greater than two discrete AS's advertising ownership of the same prefix
- Samples taken every two days from 21 January 2011 $\rightarrow$ 29 February 2020
- Compare the trend of isolated and distributed attacks against the deployment status of RPKI
- Step One is to look at deployment trend of RPKI

Methodology

- Define an isolated attack as two discrete AS's advertising ownership of the same prefix
- Define a distributed attack as greater than two discrete AS's advertising ownership of the same prefix
- Samples taken every two days from 21 January 2011 $\rightarrow$ 29 February 2020
- Compare the trend of isolated and distributed attacks against the deployment status of RPKI
- Step One is to look at deployment trend of RPKI
- Then, look at BGP Attack trends

RPKI Deployment



Source: Self

A Note about the Spike

- This is caused by APNIC migrating to a new route management system.

A Note about the Spike

- This is caused by APNIC migrating to a new route management system.
- As a result, there was a bunch of incorrectly validated ROAs

A Note about the Spike

- This is caused by APNIC migrating to a new route management system.
- As a result, there was a bunch of incorrectly validated ROAs
- Clearly, it was fixed quickly

Distributed Attack Example

- Take the previouse BGP announcement example
- Timestamp is: 2011-01-01 12:00 +00:00
- Total of 7 AS's advertising ownership of the same prefix
- Good indicator that this is a distributed attack

```
Peer ASN, Peer IP, Prefix, AS_PATH, Origin AS
33437, 2001:4810::1, 2001::/32, 33437 ... 6939, 6939
3257, 2001:668:0:4::2, 2001::/32, 3257 ... 1101, 1101
7018, 2001:1890:111d::1, 2001::/32, 7018 ... 29259, 29259
...
```

A note about the Results

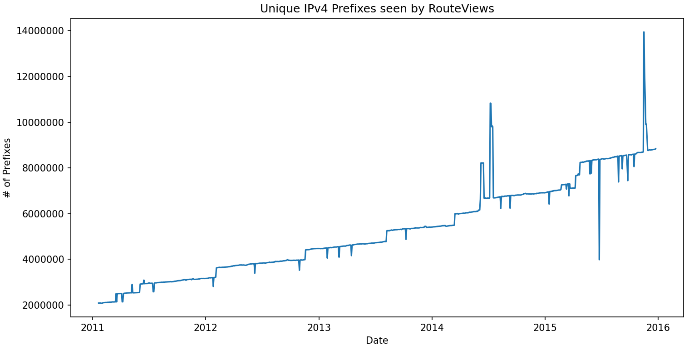
- All results presented are *preliminary*
- Full results will be available in the report.

Results

Internet Protocol	Prefixes	Isolated	Distrubted
IPv4	13144978	273429	6335
IPv6	581418	6927	365

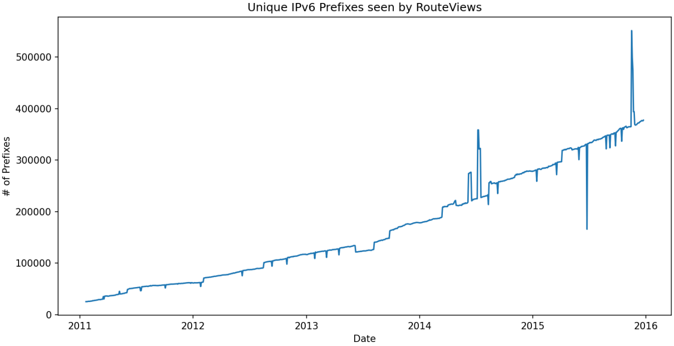
Table: Summary

IPv4 Unique Prefixes



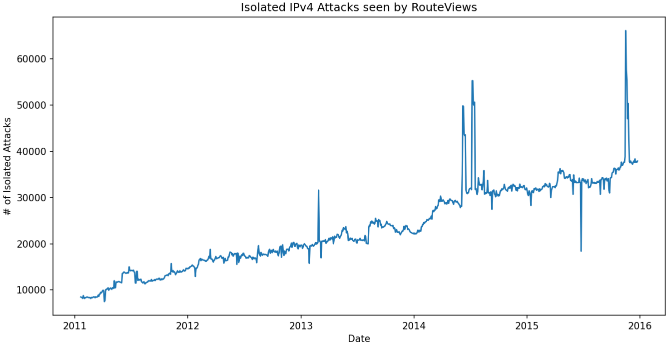
Source: Self

IPv6 Unique Prefixes



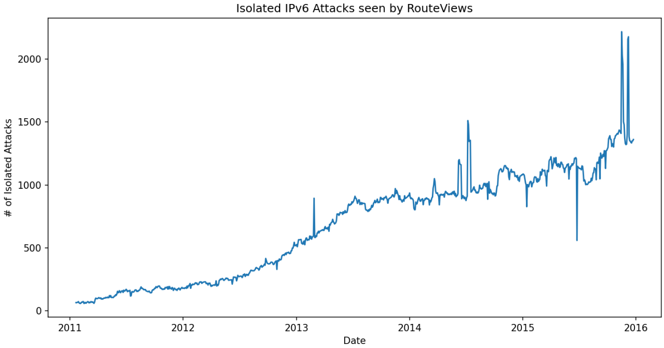
Source: Self

IPv4 Isolated Attacks



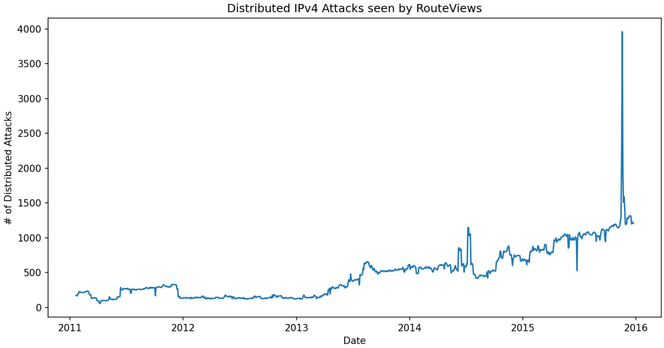
Source: Self

IPv6 Isolated Attacks



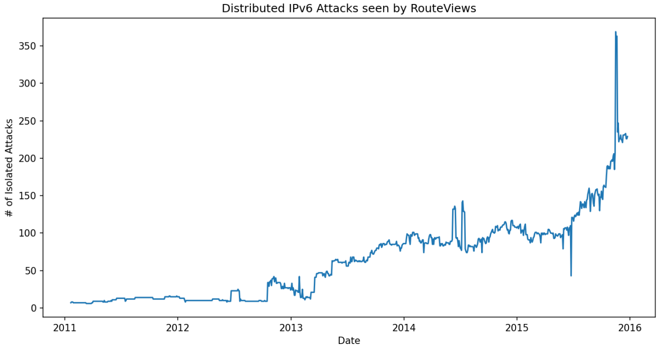
Source: Self

IPv4 Distributed Attacks



Source: Self

IPv6 Distributed Attacks



Source: Self

Questions?