ASPA-based BGP AS_PATH Verification and Route Leaks Solution

Kotikalapudi Sriram
US NIST


NANOG 89
October 2023
Outline of the Talk

• Brief refresh about BGP prefix hijacks, route leaks, and AS_PATH manipulations, RPKI-ROV, BGPsec
• Autonomous System Provider Authorization (ASPA)
• ASPA-based BGP AS_PATH verification & route leaks detection and mitigation
Border Gateway Protocol (BGP) Basics

→ BGP Update Flow

**Century Link**
AS 3356

**ISP AS A**

**XYZ Pizza Inc.**
AS 64500

**NIST**
AS 49

**P 3356 49**

**P 64500**

**P2C**

**C2P**

**P2C**

**P2C**

**P {A 3356 49}**

**LTE/5G Provider**

**Broadband Provider**

Prefixes:
- P 3356 49
- P 64500

Not shown but update for prefix Q also propagates to all other ASes.

Note: This is only an illustration.

P2C = Provider-to-customer
C2P = Customer-to-provider
p2p = peer-to-peer (lateral peers)
AS = autonomous system
AS = Autonomous System

Millions of BB/LTE/5G users
Border Gateway Protocol (BGP) Basics

BGP Update Flow

Data flow path 😊

Note: This is only an illustration.
Prefix Hijack

In general, ISPs prefer customer route announcements over those from other peers.

Note: This is only an illustration.
Route Origin Authorization (ROA) is signed by an ISP, Enterprise, or Customer. ROA authorizes an AS to originate one or more prefixes.

ROA (signed object)
Addresses: set of customer prefixes
maxLengths: associated with prefixes
Valid Origin: ASn

ROA is signed using the private key corresponding to an End-Entity certificate that is derived from the CA certificate.

Solution for Prefix Hijacking
Resource PKI (RPKI) and Route Origin Authorization (ROA)

- - - > IANA allocation
" Suballocation and RPKI certification

IANA

Route Origin Authorization (ROA) is signed by an ISP, Enterprise, or Customer. ROA authorizes an AS to originate one or more prefixes.

TA = Trust Anchor
CA = Certificate Authority
Each suballocation is represented in a certificate

X.509 Cert
Route Origin Validation (ROV)

ROV is performed at routers

- Routers match the prefix-origin pair in the route against the ROA data
- Determine route validity: Valid, Invalid, Unknown

RPKI Data Propagation

- RIR RPKI Repositories
- Other RPKI Repositories
- RPKI Validating Server
- RPKI Cache
- RPKI-Router protocol

RPKI operations in an AS

ROA Data

ROA Data
Forged-Origin Prefix Hijack

Attacker AS X conducts a prefix hijack with a forged-origin involving AS A

AS A has a ROA: \{P, AS A\}

Hijack succeeds 😞

P \{AS X, AS A\}

AS A

AS B

AS C

AS D

AS X

prefix P

ROA compliant
Route Origin Authorization (ROA) exists that authoritatively binds the prefix P to the origin AS1.

BGPsec Update:

- P, \{AS1, SKI1, AS2\}, \{SIG1-2\}
- P, \{AS1, SKI1, AS2, SKI2, AS3\}, \{SIG1-2, SIG2-3\}
- P, \{AS1, SKI1, AS2, SKI2, AS3, SKI3, AS4\}, \{SIG1-2, SIG2-3, SIG3-4\}
- P, \{AS1, SKI1, AS2, SKI2, AS3, SKI3, AS4, SKI4, AS5\}, \{SIG1-2, SIG2-3, SIG3-4, SIG4-5\}

* Next hop AS is signed over but not included in the forwarded BGPSEC update.

Note that if AS6 attempts to announce prefix P over a one-hop connection via AS1, it will not succeed because it never received a signed BGP announcement directly from AS1 – it can never fake being directly connected to AS1.

In general, ISPs prefer customer route announcements over those from other peers.

Note: This is only an illustration.
**Route Leak**

- **Anomalous data flow path**

---

**Century Link**
AS 3356

**ISP AS A**
route-leak propagated
P \{A 64500 3356 49\}

**XYZ Pizza Inc.**
AS 64500
prefix Q

**NIST**
AS 49
prefix P

**Broadband Provider**

**LTE/5G Provider**
Gravely unhappy
BB/5G/LTE users 😞

**Note:** This is only an illustration.

Data will not make it to NIST. XYZ can’t handle the traffic load and drops it.
Route Leaks Occur Frequently

Example AS Path Trajectories that are Route Leaks

- Route leak occurs if the Update is received on a down (P2C) or lateral (p2p) hop and then forwarded on an up (C2P) or lateral (p2p) hop.
Example AS Path Trajectories that are Not RouteLeaks

- Not a route leak: If once the BGP Update goes on a down (C2P) or lateral (p2p) hop, then all subsequent hops (if any) must be down (P2C).

P2C = Provider-to-customer
C2P = Customer-to-provider
p2p = peer-to-peer (lateral peers)
ASPA-based Solution for Mitigating BGP Route Leaks and AS_PATH Verification

IETF Drafts:

A helpful IETF presentation on ASPA algorithm accuracy:

Other IETF work related to route leak detection and mitigation:
ASPA: Autonomous System Provider Authorization

RPKI ASPA Object

Example:

• ASPA: \( AS_i, \{ AS_j, AS_k, AS_m \} \)
  transit providers

AS \( i \) signs an ASPA object in the RPKI to attest that AS \( j \), AS \( k \), and AS \( m \) are transit providers

• ASPAs are registered/stored in the RPKI repositories

For details of ASPA registration requirements, see Section 4 in
BGP Roles and ASPAs

- Provider
- Customer
- Lateral peer
- IXP Route Server (RS)
- RS-client
- Mutual transit

- RS to RS-client relationship is like a provider to customer relationship. The RS AS is included in the RS-client AS’s ASPA
- An AS having no providers registers an AS0 ASPA (i.e., ASPA containing only AS 0 as provider)
- Mutual transit ASes include each other in their ASPAs as provider

For details of ASPA registration requirements, see Section 4 in https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-verification
ASPA’s AS Path Anomaly Detection Capabilities

• Can detect and mitigate route leaks and improbable AS paths
• Can detect forged-origin prefix hijacks to some extent (slide 40)
• Can detect forged-path-segment prefix hijacks to some extent (slide 41)
• Limitations: ASPA method has limitations with regard to some forms of malicious AS path manipulations; mainly when a transit provider attacks its own customer with path manipulations (slide 43)
Route leaks involve one of four valley-free violations

AS(1) \rightarrow AS(2) \rightarrow AS(3)

- Consider routes originated or propagated by AS(1) and received at AS(3)
- All four forms of route leaks are detected at AS(3) if AS(1) has ASPA

* Assume AS(2) is not removing AS(1) from the AS path (that then gets into the realm of AS path manipulation)

ASPA: AS(1) \{AS(5)}
ASPA Hop Check Function

Definition:

\[
\text{hop}(\text{AS}(i), \text{AS}(j)) = \begin{cases} 
\text{P} & \text{if } \text{AS}(i) \text{ attests } \text{AS}(j) \text{ is a provider} \\
\text{nP} & \text{if } \text{AS}(i) \text{ attests } \text{AS}(j) \text{ is not a provider} \\
\text{nA} & \text{if } \text{AS}(i) \text{ does not have an ASPA}
\end{cases}
\]

\text{P}: \text{Provider} \\
\text{nP}: \text{not Provider} \\
\text{nA}: \text{no Attestation}

\text{AS}(i)-\text{AS}(j) \text{ peering:}
\text{u} = \text{Up (customer to provider (C2P))}
\text{d} = \text{Down (provider to customer (P2C))}
\text{l} = \text{Lateral (peer to peer (p2p))}
A note about AS Path representation style

• We collapse the AS prepends. So, the AS path is represented by unique ASes such as AS(1), AS(2), ..., AS(N).

• Thus AS(1) is the origin AS and AS(N) is the AS that is neighbor to the receiving/verifying AS.

• In the diagrams, for simplicity, we only show indices of ASes, i.e., AS positions. Do not mistake them for AS numbers.

```
AS(1) -> AS(2) -> AS(3) -> AS(4)  N = 4
```

Simplified representation

```
1 -> 2 -> 3 -> 4
```

These numbers are AS position indices, not AS numbers.
Example when Upstream AS Path is **Valid**

Verifying AS receives the BGP route from a Customer or Lateral Peer;
• The received AS path \{AS(3) AS(2) AS(1)\} is **Valid** (not route leak)

ASPA hop check:
- **P**: Provider
- **nP**: not Provider
- **nA**: no Attestation

ASPs:
- AS(1), \{AS(2)\}
- AS(2), \{AS(3)\}
Example when Upstream AS Path is Invalid

- **ASPA hop check:**
  - **P:** Provider
  - **nP:** not Provider
  - **nA:** no Attestation

AS path \{AS(4) AS(3) AS(2) AS(1)\} received at the Verifying AS is **Invalid** based on ASPAs

- **AS(3) has AS 0 ASPA**

- **AS(4) is the leaker and may / may not have an ASPA... the Verifying AS has local knowledge that AS(4) is its customer**

**Diagram:**
- **Up-ramp:** 1, 2, 3
- **Verifying AS**
- **AS(3) has AS 0 ASPA**
- **Up (C2P)**
- **Upstream path**
- **Route leak**
- **AS(4) has AS 0 ASPA**
Algorithm for Upstream AS Path Verification

- If the hop() function for each hop in the AS path is $P$, the AS path is **Valid** (not route leak) and return.

- Else, if the hop() function for any hop in the AS path is $nP$, the AS path is **Invalid** (route leak) and return.

- Else, the AS path validity is **Unknown** (may or may not be a route leak) and return.
ASPA Verification of Downstream AS Path: Invalid Outcome

Any two hops in opposite directions are $nP$ per ASPA ($j > i$) (facing each other)

ASPA hop check:
P: Provider
nP: not Provider
nA: no Attestation

Receiver/Verifying AS

ASPA Verification of Downstream AS Path: Invalid Outcome

Any two hops in opposite directions are $nP$ per ASPA ($j > i$) (facing each other)
ASPA Verification of Downstream AS Path: Valid Outcome

The only permissible path trajectories for **Valid** outcome are an inverted V or inverted V with a one hop p2p at the apex

AS(1), \{AS(2)\}  
AS(2), \{AS(3)\}  
AS(5), \{AS(4)\}  
AS(6), \{AS(5)\}  
AS(7), \{AS(6)\}
AsPA Verification of Downstream AS Path: Unknown Outcome

In partial deployment, an Unknown outcome occurs when the available AsPA’s do not produce an Invalid (slide 25) or Valid (slide 26) outcome for the AS_PATH.
ASPA Verification of Downstream AS Path: Formal Algorithm Development
ASPA Verification of Downstream AS Path

(K, L) representation of downstream AS path

ASPA of AS(3) does not include AS(4) or it does not exist

ASPA of AS(6) does not include AS(5) or it does not exist

K = 3

L = 6

nP or nA

nP or nA

Verifying AS receives the BGP route from a Provider

nP: not Provider
nA: no Attestation

P: Provider

ASPA Verification of Downstream AS Path

AS(1), {AS(2)}
AS(2), {AS(3)}
AS(7), {AS(6)}
AS(8), {AS(7)}
AS(9), {AS(8)}

nP or nA

nP or nA

Verifying AS

Up-ramp: 1, 2, 3
Down-ramp: 6, 7, 8, 9

Up

Down

Downstream path

Verifying AS receives the BGP route from a Provider
Valid downstream AS path when $L - K < 1$

- The AS path is Valid with/without the $nP$ or $nA$ hop in the middle
- AS path is trivially Valid if the AS path length is 1 or 2 (no ASPA needed)

ASPA hop check:
- $P$: Provider
- $nP$: not Provider
- $nA$: no Attestation

AS-AS peering:
- $u = Up$
- $d = Down$
- $l = Lateral$

ASPA of AS(3) does not exist or it does not include AS(4)
ASPA of AS(4) does not exist or it does not include AS(3)

ASPAs:
- AS(1), {AS(2)}
- AS(2), {AS(3)}
- AS(5), {AS(4)}
- AS(6), {AS(5)}
- AS(7), {AS(6)}

$K = 3$

$nP (d, l)$ or $nA (u, d, l)$

$L = 4$

$N = 7$

Verifying AS
For $L-K \geq 2$, only Invalid or Unknown are possible.

Illustration for $L-K = 2$

ASPA hop check:  
- **P**: Provider  
- **nP**: not Provider  
- **nA**: no Attestation

AS–AS peering:  
- **u** = Up  
- **d** = Down  
- **l** = Lateral

Verification Result

- **Invalid**
- **Unknown**

Arrows indicate direction of ASPA hop check.
Theorems that help design the algorithm

**Theorem 1**: The downstream AS path is **Valid** if and only if \( L-K \leq 1 \). If \( L-K \geq 2 \), then the AS path can be **Unknown** or **Invalid**, but never **Valid**.

**Theorem 2**: For \( L-K \geq 2 \), the validity of the whole AS path is the same as that of the partial path \( AS(K), AS(K+1), ..., AS(L-1), AS(L) \). The partial path can only be either **Invalid** or **Unknown**. It is **Invalid** if there exist \( u \) and \( v \) (\( u \) and \( v \) in the range from \( K+1 \) to \( L-1 \)) such that \( u \leq v \) and \( \text{hop}(AS(u-1), AS(u)) = nP \) and \( \text{hop}(AS(v+1), AS(v)) = nP \). Otherwise, the partial path is **Unknown**.

Function \( \text{hop()} \) is defined on slide 20.

Proofs exist; see next two slides; also see reference [1] below.

Proof: For $L-K \geq 2$, only Invalid or Unknown are possible

Illustration for $L-K = 3$

ASPA hop check:
- P: Provider
- nP: not Provider
- nA: no Attestation

AS-AS peering:
- u = Up
- d = Down
- l = Lateral

Verification Result:
- Invalid

Arrows indicate direction of ASPA hop check
Proof: For $L-K \geq 2$, only Invalid or Unknown are possible

Illustration for $L-K = 3$

ASPA hop check:
P: Provider
nP: not Provider
nA: no Attestation

AS-AS peering:
u = Up
d = Down
l = Lateral

→ Arrows indicate
direction of
ASPA hop check

<table>
<thead>
<tr>
<th>Hop 3-4</th>
<th>Hop 4-5</th>
<th>Hop 5-6</th>
<th>AS path</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\rightarrow$ nP {d, l}</td>
<td>Any: P, nP, or nA</td>
<td>$\leftarrow$ nP {d, l}</td>
<td>Invalid</td>
</tr>
<tr>
<td>$\rightarrow$ nP {d, l}</td>
<td>$\leftarrow$ nP {d, l}</td>
<td>$\leftarrow$ nA {u, d, l}</td>
<td>Invalid</td>
</tr>
<tr>
<td>$\rightarrow$ nP {d, l}</td>
<td>$\leftarrow$ nA {u, d, l}</td>
<td>$\leftarrow$ nA {u, d, l}</td>
<td>Unknown</td>
</tr>
<tr>
<td>$\rightarrow$ nP {d, l}</td>
<td>$\leftarrow$ P {u}</td>
<td>$\leftarrow$ nA {u, d, l}</td>
<td>Unknown</td>
</tr>
<tr>
<td>$\rightarrow$ nA {u, d, l}</td>
<td>$\rightarrow$ nP {d, l}</td>
<td>$\leftarrow$ nP {d, l}</td>
<td>Invalid</td>
</tr>
<tr>
<td>$\rightarrow$ nA {u, d, l}</td>
<td>$\rightarrow$ nP {d, l}</td>
<td>$\leftarrow$ nA {u, d, l}</td>
<td>Unknown</td>
</tr>
<tr>
<td>$\rightarrow$ nA {u, d, l}</td>
<td>$\rightarrow$ nA {u, d, l}</td>
<td>$\leftarrow$ nP {d, l}</td>
<td>Unknown</td>
</tr>
<tr>
<td>$\rightarrow$ nA {u, d, l}</td>
<td>$\rightarrow$ nA {u, d, l}</td>
<td>$\leftarrow$ nA {u, d, l}</td>
<td>Unknown</td>
</tr>
<tr>
<td>$\rightarrow$ nA {u, d, l}</td>
<td>$\rightarrow$ P {u}</td>
<td>$\leftarrow$ nP {d, l}</td>
<td>Unknown</td>
</tr>
<tr>
<td>$\rightarrow$ nA {u, d, l}</td>
<td>$\rightarrow$ P {u}</td>
<td>$\leftarrow$ nA {u, d, l}</td>
<td>Unknown</td>
</tr>
</tbody>
</table>
Algorithm for Downstream AS Path Verification

Crisp Description

1. If the AS path length $1 \leq N \leq 2$, then the path is trivially Valid and the procedure halts.
2. Else, now $N > 3$. Formulate the AS path (unique ASes) using the $(K, L)$ representation (slide 29).
   
   If $L-K \leq 1$, then the AS path is Valid and the procedure halts.

   (Note: For $L-K \geq 2$, to determine whether the AS path is Invalid or Unknown, we only need to focus on the portion of the path from AS($K$) to AS($L$).)

3. Else, now $L-K \geq 2$.
   
   Consider the partial path represented by AS($K$), AS($K+1$), ..., AS($L-1$), AS($L$).
   If there exist $u$ and $v$ in the range from $K+1$ to $L-1$ such that $u \leq v$ and
   
   $\text{hop}(\text{AS}(u-1), \text{A}(u)) = nP$, and
   
   $\text{hop}(\text{AS}(v+1), \text{A}(v)) = nP$,  
   
   then the AS path is Invalid and the procedure halts.

4. Else, the AS path is Unknown and the procedure halts.

The detailed algorithm is in the IETF draft (ietf-sidrops-aspa-verification)
Prevention of Route Leaks at Local AS

- RFC 9234: Only to Customer (OTC) Attribute
- Add the OTC Attribute on eBGP ingress (if not already present) when a route is received from a Provider, IXP Route Server, or Lateral Peer
- If the OTC Attribute is present, do not propagate the route to a Provider, IXP Route Server, or Lateral Peer at eBGP egress
- If the OTC Attribute is not present, the route may be propagated to any type of peer at eBGP egress
ASPA Path Verification: Highlighting Some Key Properties

• These properties are early adoption incentives
• For the key properties descriptions (next 5 slides), assume that malicious AS path manipulations are not involved, especially removal of certain ASes from the AS path.
• An example of ASPA’s limitation with regard to malicious AS path manipulation is on slide 43
Only two ASes A and B are doing ASPA
• AS A propagates a route to a customer or lateral peer
• AS B receives the route from a customer or lateral peer
• If the AS_PATH involves a route leak, it is always detected and mitigated at AS B
Corollary of Property 1

• In effect, if most major ISPs are ASPA compliant, the propagation of route leaks in the Internet will be severely limited.
The forged-origin prefix hijack attack involving AS A is detected and mitigated at AS B

Conducts forged-origin prefix hijack involving AS A as the origin

- Only two ASes A and B are doing ASPA and ROA/ROV
- AS B receives the forged route sent by AS X (attacker) in the upstream direction (from a customer or lateral peer)
ASPA Path Verification: Property 3

- AS B receives the forged route sent by AS X (attacker) in the upstream direction (from a customer or lateral peer)

The prefix hijack with forged-path-segment involving {AS B, AS A} is detected and mitigated at AS D

Conducts a prefix hijack with forged-path-segment involving {AS B, AS A}
ASPA Path Verification: Property 4

- All routes within the ASPA island are fully protected from route leaks
Shortcoming: AS_PATH maliciously shortened by a provider – undetectable

- Consider AS path verification at AS 5
- All ASes are doing ASPA
- AS 4 (provider) wants AS 5 (customer) to prefer its path
- AS 4 shortens the AS_PATH
- AS 5 chooses the manipulated shorter route via AS 4
- Since other ASes are good, if AS4 does not drop AS5’s (customer’s) data traffic, then the traffic still reaches the destination via a feasible and route-leak free path.

- BGPsec can provide full AS_PATH protection
- But it lacks route leak protection
- Use ASPA and BGPsec in a complementary way
Thank you

Questions?

Email: ksriram@nist.gov