Use Forwarding Commitment to Describe Routing Intent

Yangfei Guo, Shenglin Jiang, Xiaoliang Wang, Ke Xu

APNIC 59 Routing Security SIG

Feb. 2025

Contents

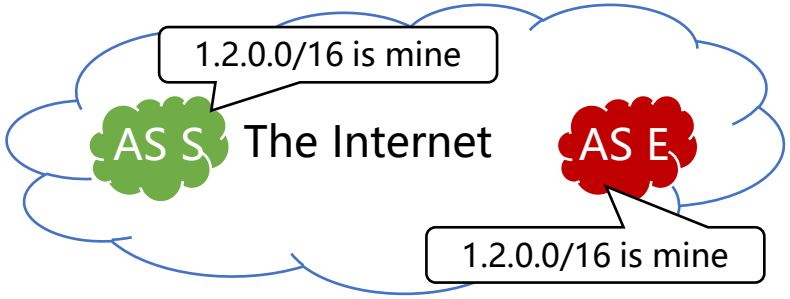
- Background
- Existing RPKI Signed Objects
- Forwarding Commitment (FC)

Contents

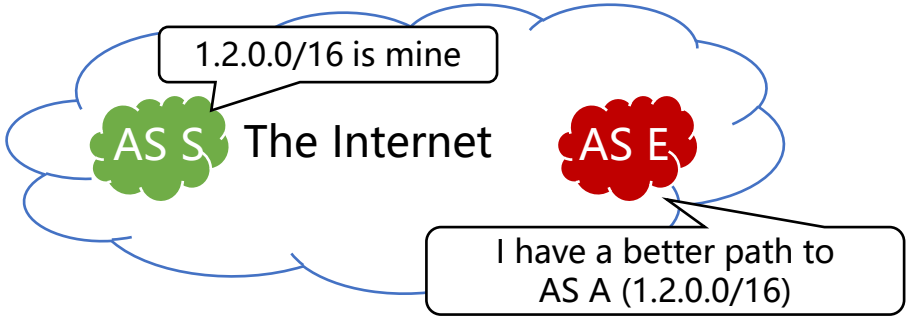
- Background
- Existing RPKI Signed Objects
- Forwarding Commitment (FC)

Background

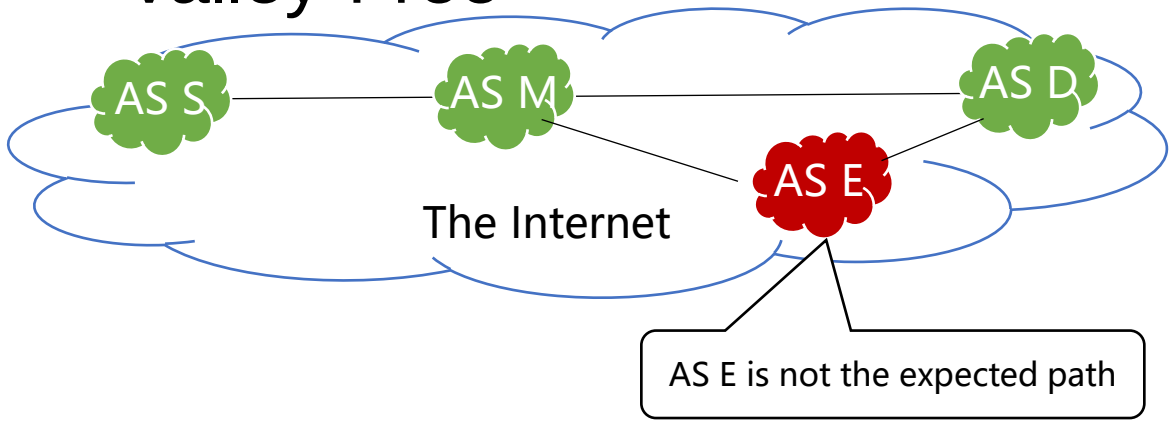
- Route Hijacks
  - Prefix Hijack



  - Path Hijack



- Route Leaks
  - Valley-Free



Routes from	To provider	To peer	To customer
From provider	Type 1	Type 3	Normal
From peer	Type 4	Type 2	Normal
From customer	Normal	Normal	Normal

- RFC 7908 - Problem Definition and Classification of BGP Route Leaks

Contents

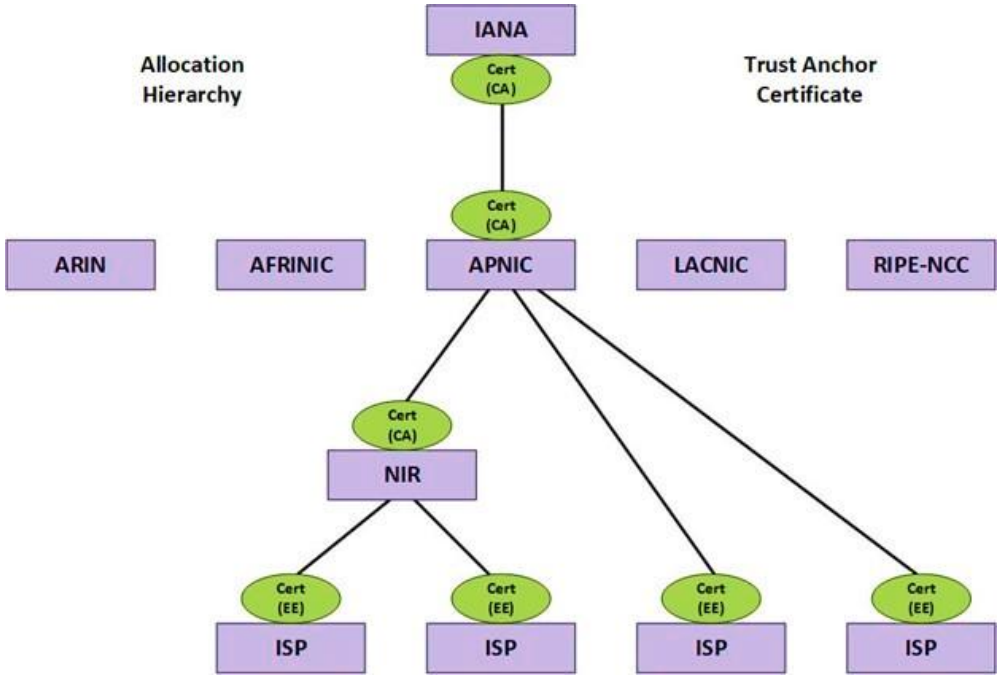
- Background
- Existing RPKI Signed Objects
- Forwarding Commitment (FC)

Existing RPKI Signed Objects

- Currently, RPKI has several signed objects for inter-domain routing security, including,
  - ROA
  - SPL
  - ASPA
  - ASRA

ROA (Route Origin Authorizations)

- ROA: a prefix or IP address holder authorizes an AS to originate route objects.
- The allocation of Internet Number Resources (IP prefixes and AS numbers) follows the hierarchy.




```
RouteOriginAttestation ::= SEQUENCE {
  version [0]   INTEGER DEFAULT 0,
  asID          ASID,
  ipAddrBlocks  SEQUENCE (SIZE(1..2)) OF ROAIPAddressFamily }
```

It perfectly adapts RPKI architecture.

- MANRS - What is route origin validation?
- RFC 9582 - A Profile for Route Origin Authorizations (ROAs)

SPL (Signed Prefix List)

- SPL: the complete list of prefixes which an AS may originate in the BGP.
- Substitute of `route-set` in IRR [RFC2622]
- Mitigation
  - Prefix hijacks
  - AS forgery:
    - Offending AS inserts victim AS as origin
  - Forged-origin prefix hijacks
    - Offending AS inserts valid <prefix, origin AS> as origin
- It says it can mitigate Type 5
  - No max-length field, no more-specific Prefix

```
RpkiSignedPrefixList ::= SEQUENCE {
  version [0]     INTEGER (0..MAX) DEFAULT 0,
  asID            INTEGER (1..4294967295),
  prefixBlocks    SEQUENCE (SIZE(0..2)) OF AddressFamilyAddressPrefixes }
```

It is routing intent description.

Index	ROA-ROV-state	SPL-ROV-state	Route Selection
1	Valid	Valid	Eligible
2	Valid	NotFound	Eligible
3	Valid	Invalid	Ineligible
4	NotFound	Valid	Eligible
5	NotFound	NotFound	Eligible
6	NotFound	Invalid	Ineligible
7	Invalid	Valid	Ineligible
8	Invalid	NotFound	Ineligible
9	Invalid	Invalid	Ineligible

BGP Security Threats Addressed by SPL-ROV

1. AS Forgery While Hijacking an ROA-ROV-NotFound Prefix
2. AS Forgery Together with a Conflicting ROA
3. AS Accidentally Strips AS_PATH and Mis-Originates Prefixes
4. Attack Surface Reduction
5. AS can declare itself "Not Originating Prefixes in the Internet

- draft-ietf-sidrops-spl-verification-00 - Signed Prefix List (SPL) Based Route Origin Verification and Operational Considerations
- draft-ietf-sidrops-rpki-prefixlist-04 - A profile for Signed Prefix Lists for Use in the Resource Public Key Infrastructure (RPKI)

ASPA (Autonomous System Provider Authorization)

- ASPA: stores and verifies cryptographically protected AS-level relationship information.

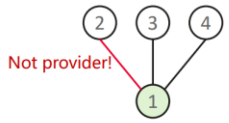
```
ASProviderAttestation ::= SEQUENCE {
  version [0]   INTEGER DEFAULT 0,
  customerASID  ASID,
  providers     ProviderASSet }
```

- The ASPA mechanism can be very roughly summarized into the following key points:
  - ASPA stores customer-to-provider information in RPKI
    - One customer AS associated with a set of provider ASes
  - ASPA is useful for verifying BGP AS_PATH attribute content
    - AS_PATH that violates the "valley-free" routing principle can be detected with ASPA objects information

- draft-ietf-sidrops-aspa-verification-20 - BGP AS_PATH Verification Based on Autonomous System Provider Authorization (ASPA) Objects
- draft-ietf-sidrops-aspa-profile-19 - A Profile for Autonomous System Provider Authorization

ASPA
(Autonomous System Provider Authorization)

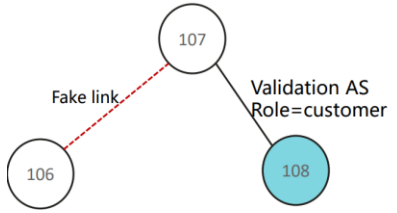
Case 1: Cannot cross-check the correctness of registration



- AS1 registers: AS2, AS3, and AS4 are my providers
- But, AS2 is not its provider
- The incorrectness cannot be detected by the ASPA data registered by AS2

Case 2: Cannot detect hijack introduced by provider

- Route received by AS108: {Origin ASN=106, AS path = [107, 106]}



ASPA records:

	AS106	AS107
ASPA	provider-set = {105}	provider-set = {0}

- **ASPA result: valid**
- Analysis: In the current ASPA design, any downstream path with length no longer than 2 will be considered valid

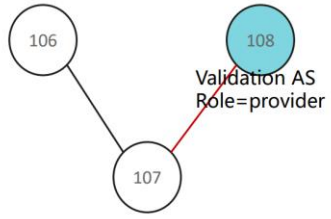
```
root@ip-s8:~/gengnan/bgp/openbgpd-portable # bgpctl s rib
flags: * = Valid, > = Selected, I = via IBGP, A = Announced,
       S = Stale, E = Error
origin validation state: N = not-found, V = valid, ! = invalid
aspa validation state: ? = unknown, V = valid, ! = invalid
origin: i = IGP, e = EGP, ? = Incomplete

flags  vs destination          gateway          lpref   med aspath origin
*>     V-V 192.106.0.0/24      10.107.10.154     100     0 107 106 i
*>     V-V 192.107.0.0/24      10.107.10.155     100     0 107 i
AI*>   V-? 192.108.0.0/24      0.0.0.0           100     0 i
```

- **Expected result: invalid-hijack**

Case 3: Cannot detect leakage with partial registration

- Route received by AS108: {Origin ASN=106, AS path = [107, 106]}



ASPA records:

	AS106	AS107
ASPA	No data	provider-set = {108}

- **ASPA result: unknown**
- Analysis: When do upstream check, hop-check(106, 107) returns No Attestation because AS106 has no record

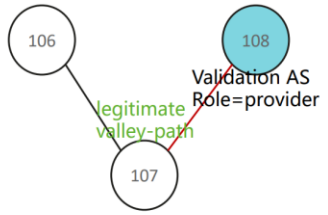
```
root@ip-s8:~/gengnan/bgp/openbgpd-portable # bgpctl s rib
flags: * = Valid, > = Selected, I = via IBGP, A = Announced,
       S = Stale, E = Error
origin validation state: N = not-found, V = valid, ! = invalid
aspa validation state: ? = unknown, V = valid, ! = invalid
origin: i = IGP, e = EGP, ? = Incomplete

flags  vs destination          gateway          lpref   med aspath origin
*>     V-? 192.106.0.0/24      10.107.10.154     100     0 107 106 i
*>     V-V 192.107.0.0/24      10.107.10.155     100     0 107 i
AI*>   V-? 192.108.0.0/24      0.0.0.0           100     0 i
```

- **Expected result: invalid**

Case 4: Cannot cope with complex scenarios

- Route received by AS108: {Origin ASN=106, AS path = [107, 106]}



ASPA records:

	AS106	AS107
ASPA	provider-set = {105}	——

- **ASPA result: invalid**
- Analysis: In the current ASPA design, legitimate valley-paths hybrid/partial transit relationships cannot be coped with

```
root@ip-s8:~/gengnan/bgp/openbgpd-portable # bgpctl s rib
flags: * = Valid, > = Selected, I = via IBGP, A = Announced,
       S = Stale, E = Error
origin validation state: N = not-found, V = valid, ! = invalid
aspa validation state: ? = unknown, V = valid, ! = invalid
origin: i = IGP, e = EGP, ? = Incomplete

flags  vs destination          gateway          lpref   med aspath origin
*>     V-! 192.106.0.0/24      10.107.10.154     100     0 107 106 i
*>     V-V 192.107.0.0/24      10.107.10.155     100     0 107 i
AI*>   V-? 192.108.0.0/24      0.0.0.0           100     0 i
```

- **Expected result: valid**

- APNIC56 Routing Security SIG - Autonomous System Relationship Authorization

ASRA
(Autonomous System Relationship Authorization)

- ASRA: AS can optionally register more detailed AS relationships, and ASPA can be enhanced.

```
ASRelationshipAttestation ::= SEQUENCE {
  version [0]   INTEGER DEFAULT 0,
  SignerASID  ASID,
  ASRAsubcategory  subcategory,
  Relationships     RelationshipASSet }
```

  - > Usage 1: Cross-check the correctness of registration
  - > Usage 2: Identify fake links
  - > Usage 3: Improve deployment benefits under partial registration
  - > Usage 4: Cope with complex scenarios

- APNIC56 Routing Security SIG - Autonomous System Relationship Authorization

ASRA
(Autonomous System Relationship Authorization)

- ASRA: AS can optionally register more detailed AS relationships, and ASPA can be enhanced.
- It says its limitation: Can detect route leakage and fake link hijacking, but cannot prevent and identify AS path tampering (BGPsec for path protection)

Segal's Law:
A man with one watch always knows what time it is.
A man with two watches is never sure.
How about when ASRA is in conflict with ASPA?

- APNIC56 Routing Security SIG - Autonomous System Relationship Authorization

Contents

- Background
- Existing RPKI Signed Objects
- Forwarding Commitment (FC)

BGP Model

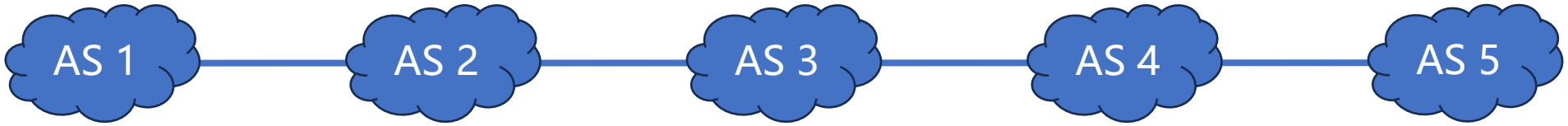
- Basic BGP route propagation pattern:
  - Receive routes from Previous hop and accept them.
  - Update routes to Next hop according to local routing policy.



- Only three hops are involved:
  - Previous, can be null (i.e., the originator).
  - Local
  - Next, can be null.

Goals

- Detect route propagation that violates local routing intent
- Prevent route leaks.
  - Verify the validity of BGP AS_PATH according to FCs



FC Signed object

- We only trust our routing policy. [IRR-autnum]
- Forwarding Commitment
  - Version: 0
  - ASid: local AS number, issuer’s AS number
  - PreviousASes: upstream ASes
    - If it is None, it means local AS is originator.
  - NextASes: downstream ASes.
  - ASes: origination ASes, references to ROA/SPL.
    - Default is None for any.

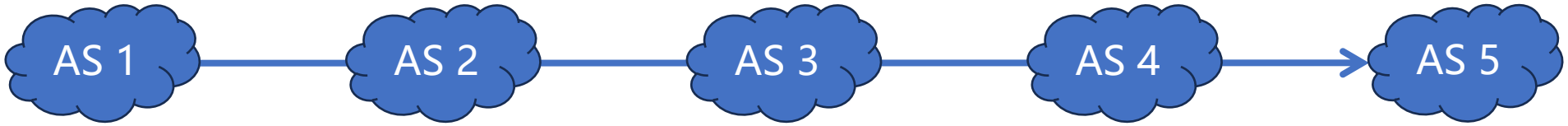
FC
Version
ASid
PreviousASes
NextASes
ASes

Verification Results

- Verification Results:
  - **Totally valid**: each AS in AS_PATH has FC and each FC's *ASes* field is specified.
  - **Valid**: each AS in AS_PATH has FC but some FCs' *ASes* field are NONE/ANY.
  - **Unknown**: none of AS in AS_PATH has FC.
  - **Invalid**: some AS in AS_PATH has FC.

Verification Results: Totally Valid

- **Totally valid**: each AS in AS_PATH has FC and each FC's *ASes*_field is specified.



FC 1
AS 1
NIL
AS 2
AS 1

FC 2
AS 2
AS 1
AS 3
AS 1

FC 3
AS 3
AS 2
AS 4
AS 1

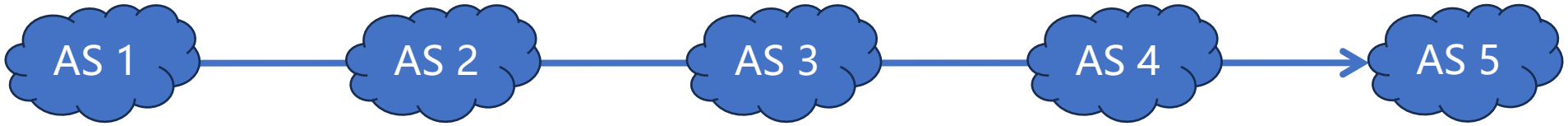
FC 4
AS 4
AS 3
AS 5
AS 1

FC 5
AS 5
AS 4
NIL
AS 1

ROA 1
AS 1
10.0.0.0/20
Max-length: 24

Verification Results: Valid

- **Valid**: each AS in AS_PATH has FC but some FCs' *ASes* field are NONE/ANY; or the originator doesn't issue ROA/SPL.



FC 1
AS 1
NIL
AS 2
AS 1

FC 2
AS 2
AS 1
AS 3
-

FC 3
AS 3
AS 2
AS 4
AS 1

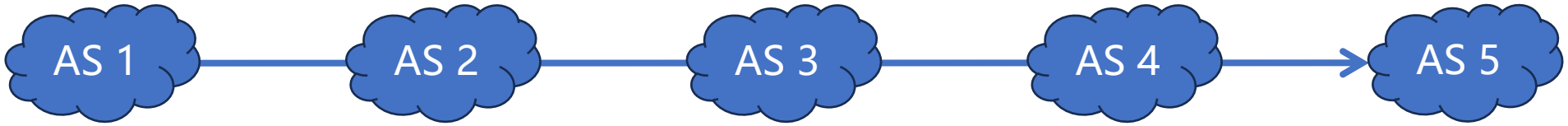
FC 4
AS 4
AS 3
AS 5
-

FC 5
AS 5
AS 4
NIL
AS 1

ROA 1
AS 1
10.0.0.0/20
Max-length: 24

Verification Results: Unknown

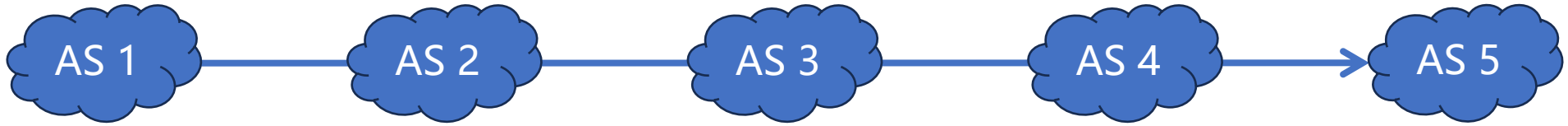
- **Unknown**: none of AS in AS_PATH has FC.



ROA 1
AS 1
10.0.0.0/20
Max-length: 24

Verification Results: Invalid

- **Invalid**: some AS in AS_PATH has FC.



FC 1
AS 1
NIL
AS 2
AS 1

ROA 1
AS 1
10.0.0.0/20
Max-length: 24

FC 3
AS 3
AS 2
AS 4
AS 1

FC 4
AS 4
AS 3
AS 5
AS 1

FC 5
AS 5
AS 4
NIL
AS 1

Differences

- BGPsec
  - On-path AS path forgery detection and prevention
- ROA/SPL
  - Prefix Origin Validation
- ASPA/ASRA
  - Business relationship

Conclusion

- Forwarding Commitment (FC) aims at detecting route propagation that violates local routing intent and preventing route leaks.
- It can
  - Protect the business relationship
  - Be incrementally deployable, benefiting early adopters
  - Provide fine management for TE
- Limitations
  - Totally Valid is a new concept that is not widely accepted.

Thank you!

guoyangfei@zgclab.edu.cn

APNIC 59 Routing Security SIG

Feb. 2025

Analysis: total number of FCs

- $Total\ FC\ objects\ = AVG_P * N_S * AVG_D \approx 4\ * 65000\ * 3.28 = 852800$
  - AVG_P: average AS Path Length
  - N_S: number of Stub ASes
  - AVG_D: average degree

- BGP in 2022 – the routing table | APNIC Blog