Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 8, 2022

C. Shen
CAICT
S. Zhang
NNIX
Z. Li
S. Zhuang
S. Chen
H. Wang
Huawei

March 7, 2022

ASPA Verification in the Presence of Regionalized AS-Relationships
draft-shen-sidrops-regionalized-as-relationships-00

Abstract

This document proposes a method for ASPA verification in the Presence of Regionalized AS-Relationships.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 8, 2022.

Copyright Notice

Table of Contents

1. Introduction

[RFC6811] defines a method for verifying the origin of BGP prefixes, which can resolve the most common source AS hijacking. Autonomous system provider authorisation (ASPA) [I-D.ietf-sidrops-aspa-verification] is a methodology to validate the entire AS path. ASPA verification procedures use a shared signed database of customer-to-provider relationships using a new RPKI object - Autonomous System Provider Authorization (ASPA). This method relies heavily on the accuracy of the shared signed database of customer-to-provider relationships.

Currently, two ASes may have different relationships at different interconnection points. For example:

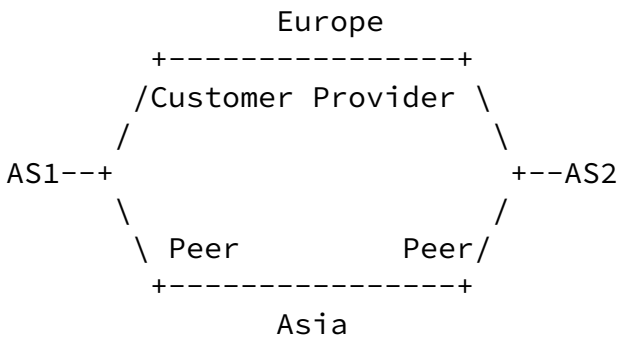

Figure 1: Hybrid Relationship Case 1

Case 1) AS1 is AS2's customer in Europe, but AS1 and AS2 establish P2P relationships in Asia;

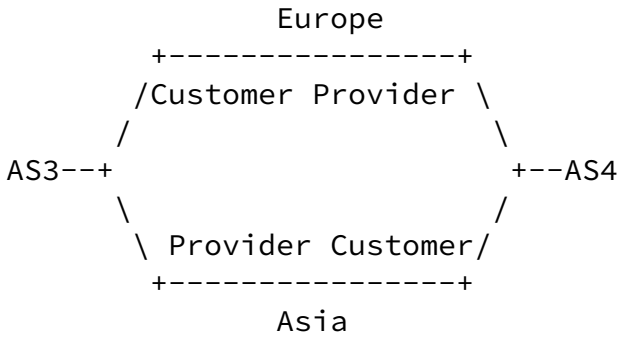

Figure 2: Hybrid Relationship Case 2

Case 2) AS3 is AS4's customer in Europe, on the contrary, AS4 is AS3's customer in Asia;

There are some other examples, not fully listed in this draft.

For case 1, AS1 signs one record ASPA(AS1, AFI, [AS2, ...]) per [I-D.ietf-sidrops-aspa-verification].

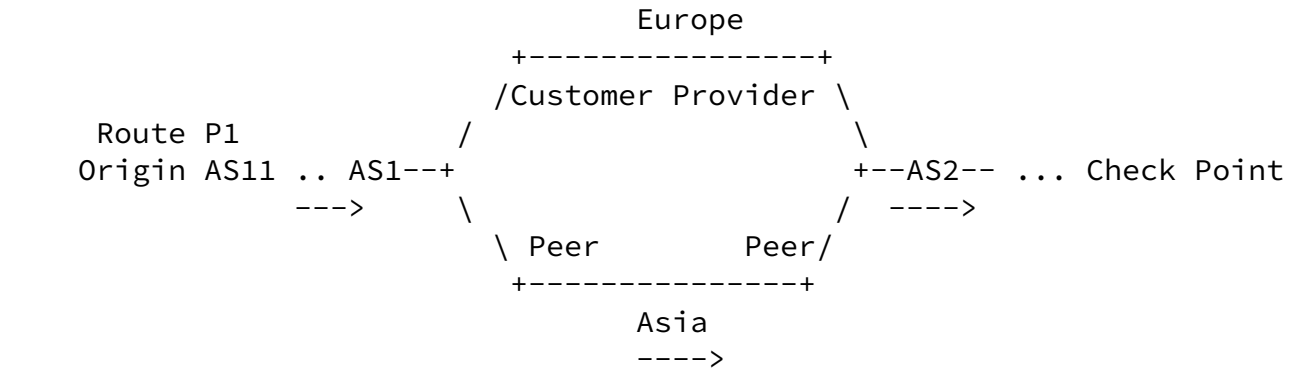

Figure 3: Problematic Use Case

As shown in Figure 3, the main processing steps per [I-D.ietf-sidrops-aspa-verification] are as follows:

1) Check Point receives the Route P1, AS-Path: AS2 (via Asia Link) AS1 ... AS11;

2) Check Point uses ASPA(AS1, AFI, [AS2, ...]) to validate AS-Pair (AS1 AS2) Per the AS_PATH verification procedure defined in [I-D.ietf-sidrops-aspa-verification], it will return the result "Valid".

Actually here should return the result "Invalid", not the result "Valid", because the AS-Relationship between AS1 and AS2 in Asia is P2P, not C2P.

This problem arises because of the existence of regionalized AS-Relationships. This document proposes a method for ASPA verification in the Presence of Regionalized AS-Relationships.

2. Definitions and Acronyms

- ASPA: Autonomous system provider authorisation
- C2P: Customer to Provider
- OV: Origin Validation
- P2C: Provider to Customer
- P2P: Peer to Peer
- RP: Relying Party
- RPKI: Resource Public Key Infrastructure

3. Regionalized AS-Relationships

This section discusses how to obtain regionalized AS-Relationships on routers.

Option 1: Add a Region ID field to ASPA Object

Each organization holds an AS number reports its C2P business relationship information to the RIR where it is located. The key information reported: the customer's AS number, the customer's provider AS number list (one or more), the region identifier, the region identifier is newly added by the present draft, and identifies the customer's business relationship with the one or more of its Providers in the same region is C2P. Each RIR maintains C2P business relationship information like maintaining ROA related information, when the region identifier is empty, it indicates that the business relationship between the Customer and the one or more of its Providers in all regions is C2P.

RP (Relying Party) obtains all the C2P business relationship information from each RIR, and generates the ASPA Validation Database entries.

RFC8210[RFC8210] RPKI-Router Protocol extension supports the ability to carry region identifier when delivering the ASPA Validation Database to routers, and delivers the enhanced ASPA Validation Database from RP to routers.

Option 2: Local Management of the enhanced C2P business relationships

Locally, by analyzing the global Internet routing table and various Internet public data, a regionalized C2P business relational database is sorted out.

Option 3: TBD

By processing as above, AS1 signs one record ASPA(AS1, AFI, [AS2, ...], Europe).

4. Operations

Once we get the Regionalized AS-Relationships, the main processing steps in section 1 (Figure 3) will be changed as follows:

1) Check Point receives the Route P1, AS-Path: AS2 (via Asia Link) AS1 ... AS11;

2) Check Point uses ASPA(AS1, AFI, [AS2, ...], Europe) to validate AS-Pair (AS1 AS2) Per the AS_PATH verification procedure [I-D.ietf-sidrops-aspa-verification], because the ASPA record contains region identifier information, further confirm which region the [AS1 AS2] connection is in (we can use various tools such as TraceRoute etc. This needs to be described in detail in next revision.), if we get the region identifier information of the latter is different from the ASPA records (In current case, what we get is Asia, not Europe), then the ASPA verification will return the result "Invalid".

From the above processing results, we can see that the solution proposed in this draft has worked and solved the problem described in the second section.

5. IANA Considerations

No IANA actions are required for this document.

6. Security Considerations

This document does not change the security properties of RPKI and ASPA.

7. Contributors

The following people made significant contributions to this document:

TBD

8. Acknowledgements

TBD.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC6811] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", RFC 6811, DOI 10.17487/RFC6811, January 2013, <https://www.rfc-editor.org/info/rfc6811>.

[RFC7908] Sriram, K., Montgomery, D., McPherson, D., Osterweil, E., and B. Dickson, "Problem Definition and Classification of BGP Route Leaks", RFC 7908, DOI 10.17487/RFC7908, June 2016, <https://www.rfc-editor.org/info/rfc7908>.

[RFC8210] Bush, R. and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol, Version 1", RFC 8210, DOI 10.17487/RFC8210, September 2017,

<https://www.rfc-editor.org/info/rfc8210>.

9.2. Informative References

[I-D.ietf-sidrops-aspa-verification]
Azimov, A., Bogomazov, E., Bush, R., Patel, K., and J. Snijders, "Verification of AS_PATH Using the Resource Certificate Public Key Infrastructure and Autonomous System Provider Authorization", draft-ietf-sidrops-aspa-verification-08 (work in progress), August 2021.

Authors' Addresses

Chen Shen
CAICT
No.52, Hua Yuan Bei Road
Beijing 100191
China

Email: shenchen@caict.ac.cn

Shicong Zhang
NNIX
No. 198, Qidi Road, Xiaoshan District
Hangzhou 311200
China

Email: zsc@nnix.cn

Zhenbin Li
Huawei
156 Beiqing Road
Beijing 100095
China

Email: lizhenbin@huawei.com

Shunwan Zhuang

Huawei
156 Beiqing Road
Beijing 100095
China

Email: zhuangshunwan@huawei.com

Shuanglong Chen
Huawei
156 Beiqing Road
Beijing 100095
China

Email: chenshuanglong@huawei.com

Haibo Wang
Huawei
156 Beiqing Road
Beijing 100095
China

Email: rainsword.wang@huawei.com