Internet Engineering Task Force M. Flechier
Internet-Draft M. Heusse
Intended status: Experimental A. Duda
Expires: 3 September 2026 Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG
2 March 2026

PAVA: BGP AS_PATH Validation by Querying ASes about Their Relationships
draft-flechier-sidrops-pava-01

Abstract

This document defines PAth VAlidation (PAVA), a scheme for validating the Border Gateway Protocol (BGP) AS_PATH field based on the AS relationships. Validation is performed by sending queries to the ASes along the path, each query containing information about the prefix and the relevant path segment. We implement querying the ASes in a path with a system relying on Domain Name System (DNS) and DNSSEC.

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 3 September 2026.

Copyright Notice

Table of Contents

1. Introduction

The Border Gateway Protocol [RFC4271] is not secure by design. However, the evolving context of the Internet brings the need to enhance its security, reflected in several schemes advanced along the years. Path Security (PATHSEC), conceptualized in [RFC7132] brings the need to secure the AS_PATH of BGP Update announcements to protect against vulnerabilities such as path hijacks and route leaks. Path hijacks are attacks that alter an AS_PATH, and route leaks as per [RFC7908] are incidents in which an announcement is propagated outside of its intended scope. Proposed solutions like BGPsec [RFC8205], OTC [RFC9234] and the use of a Large Community

[I-D.ietf-grow-route-leak-detection-mitigation] offer limited solutions to these issues. ASPA [I-D.ietf-sidrops-aspa-verification] is the best answer but has limited coverage in cases of complex relationships and needs up-to-date information in an often external repository constituted by the Resource Public Key Infrastructure (RPKI) [RFC6480].

PAth VAlidation (PAVA) aims to improve PATHSEC while supporting any kind of AS peering relationships as defined in [RFC9234] as well as any complex relationship configuration. Moreover, PAVA allows to keep the control of relationship information directly under the AS governance and responsibility. To this aim, PAVA carries out sequential queries targeting the ASes that appear in the AS_PATH and combines the answers to assess its validity. Each individual AS discloses only partial information about its immediate neighbors. In the validation step, PAVA verifies that all pairs of ASes in the AS_PATH are effectively neighbors and that the path is valley-free [Gao]. The valley-free rule guarantees protection against route leaks whereas the queried ASes guarantee protection against path forgeries.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Terminology and List of Acronyms

The following abbreviations are used.

C2P: Customer to Provider relationship

P2C: Provider to Customer relationship

P2P: Peer to Peer relationship

4. PAVA Operations

4.1. Principles

There are two parts in PAVA: the first one is the distribution of information related to AS relationships along a path and for a given destination prefix; the second one is the validation of the AS_PATH. The more information is available along a path, the more effective is the validation process, although partial deployment and adoption still offer partial verification.

Information distribution in PAVA relies on the deployment of DNS servers that share information pertaining to the local relationships of an AS with its neighbors. The information is relatively static and takes the form of a DNS zone file.

The verification of an AS_PATH comprises of cutting the AS_PATH in tiled segments of 3 ASes. The DNS server associated with the central AS in each triplet is in charge of providing an answer. The validating process compiles the received answers to determine the validity of the AS_PATH.

The verifying algorithm checks if the AS_PATH is valley-free [Gao] to prevent route leaks and path hijackings. The validator verifies that the list of answers is such that the relationships are first ascending with consistent C2P (up) and then descending with P2C (down), with possibly P2P between the asending and descending parts.

4.2. Validating AS Operations

4.2.1. DNS Queries

The AS_PATH is split into tiled segments of 3 unique ASN such that each AS in the AS_PATH is at the center of a triplet. The end segments are made of only 2 ASes (e.g. an AS_PATH of [4 3 2 1 1 1] corresponds to 4 segments [4 3], [4 3 2], [3 2 1] and [2 1]). The validator generates a DNS query for each triplet, to which adopting ASes SHOULD answer with a status among UP, DOWN, SUMMIT, or ERROR. The validating AS compiles the answers into a list of status for the verification step.

The DNS query is of the following form:

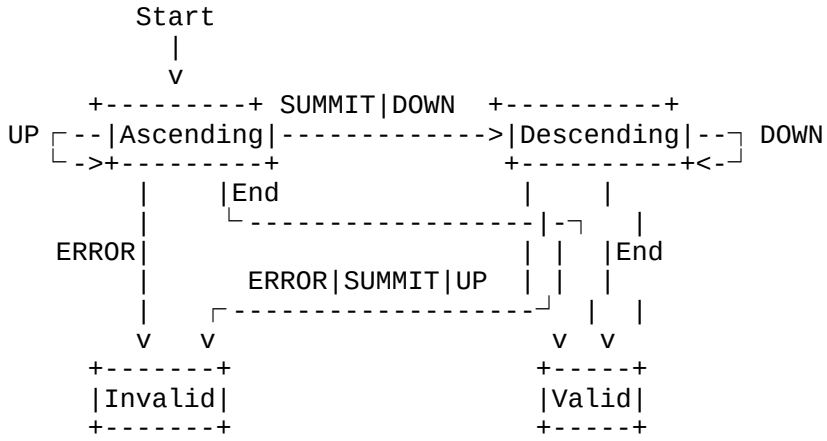
[Prefix].[AS3].[AS1].[AS2].bgp.arpa,

where the Prefix corresponds to the prefix of the NLRI field from the BGP Update being verified, and AS1, AS2, and AS3 correspond to the ASes in the segment [3 2 1] at stakes. All fields are encoded in plaintext.

Queries resulting in a DNS error or without any answer after a reasonable time, are attributed the UNKNOWN status.

4.2.2. Path Verification

The finite state machine below processes the list of gathered status in the order of announcement propagation, that is in reverse from the AS_PATH order. The finite state machine decides on the outcome of the verification, either valid or invalid, in the sense of route eligibility as defined in [RFC4271].



4.3. DNS Operations

4.3.1. Segment Status

A segment of three ASes alongside a prefix forms a PAVA tuple ([3 2 1], prefix). The return status for a tuple depends on the BGP topology relationships (the relationships follow common definitions as used in [RFC9234]). This status SHOULD be adapted in cases of complex relationships. The use of a prefix provides flexibility and fine-tuning in defininig a status.

The status MUST be one of UP, DOWN, SUMMIT, ERROR. The status is defined as such, following the pairwise relationships in the segment (AS3-AS2, AS2-AS1):

* SUMMIT: (C2P, P2P), (C2P, P2P)

* UP: (C2P, C2P)

* DOWN: (P2P, P2C), (P2C, P2C)

* ERROR: any other case

4.3.2. Zone File Creation

PAVA uses the TXT Resource Record (RR) to store its status. An AS implementing PAVA SHOULD create a master file corresponding to its zone listing any possible segment it knows to be part of, with the answer as a status corresponding to said segment. The use of wildcards MAY be useful to limit the size of the generated master file.

5. Complementarity of PAVA with Other Proposals

5.1. BGPsec

BGPsec, defined in [RFC8205], allows cryptographic verification of BGP paths by means of recursive signatures of the path. BGPSec prevents attacks that alter the AS path but does not cope with route leaks, and adds burden to the routers with cryptographic operations. Furthermore, it does not tolerate partial deployment.

5.2. OTC

Only-To-Customer is a BGP attribute shared with BGP Open messages defined in [RFC9234]. OTC prevents route leaks in BGP sessions and is a great way to mitigate them. It however does not offer any additional PATHSEC mechanism, which means that ASes need to trust BGP Update messages. It does not prevent path forgeries.

5.3. ASPA

Current work on AS_PATH Verification based on Autonomous System Provider Authorization (ASPA) [I-D.ietf-sidrops-aspa-verification] brings similar security guarantees as PAVA. ASPA protects against simple path forgeries and route leaks and relies on the RPKI which is already widely used for Route Origin Authorization (ROA). However, ASPA handles complex relationships through the blanket of labelling any as a Provider to Provider relationship. In contrast, PAVA addresses those relationships through per-destination prefix verifications, which allows fine-tuning and flexibility. The two approaches are also be complementary, providing different information that can be used to achieve further verification.

5.4. ASRA

Efforts for AS_PATH Verification based on Autonomous System Relationship Authorization (ASRA) in [I-D.sriram-sidrops-asra-verification] aims at obviating some vulnerabilities of ASPA by publishing every relationship an AS has instead of just its providers. ASRA helps further detecting complex path forgeries like PAVA but like ASPA, it does not focus on handling complex relationships, but can provide additional information to work with PAVA.

6. IANA Considerations

This document uses a second-level new special domain bgp.arpa

7. Security Considerations

PAVA is subject to the following security issues and concerns. PAVA also aims to follow security requirements provided in [RFC7353].

* Relying on the DNS infrastructure means being exposed to security issues from DNS and DNSSEC, be it protocol vulnerabilities or attacks like distributed denial of service (DDoS).

* The DNS system used to provide information may also disclose routing interests from some ASes. This is limited through the use of status that recover several cases, but in-depth analysis of a massive number of queries could reveal more information than intended.

* Partial deployment means partial information and as such, verification can not be completely thorough unless every AS in the path has adopted PAVA. As such, partial deployment only provides partial security.

* The system relies on the information provided by the ASes. Incorrect information can result in incorrect verification of the AS_PATH.

8. References

8.1. 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>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <https://www.rfc-editor.org/info/rfc6480>.

[RFC7132] Kent, S. and A. Chi, "Threat Model for BGP Path Security", RFC 7132, DOI 10.17487/RFC7132, February 2014, <https://www.rfc-editor.org/info/rfc7132>.

[RFC7353] Bellovin, S., Bush, R., and D. Ward, "Security Requirements for BGP Path Validation", RFC 7353, DOI 10.17487/RFC7353, August 2014, <https://www.rfc-editor.org/info/rfc7353>.

[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>.

[RFC8205] Lepinski, M., Ed. and K. Sriram, Ed., "BGPsec Protocol Specification", RFC 8205, DOI 10.17487/RFC8205, September 2017, <https://www.rfc-editor.org/info/rfc8205>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC9234] Azimov, A., Bogomazov, E., Bush, R., Patel, K., and K. Sriram, "Route Leak Prevention and Detection Using Roles in UPDATE and OPEN Messages", RFC 9234, DOI 10.17487/RFC9234, May 2022, <https://www.rfc-editor.org/info/rfc9234>.

[I-D.ietf-sidrops-aspa-verification] Azimov, A., Bogomazov, E., Bush, R., Patel, K., Snijders, J., and K. Sriram, "BGP AS_PATH Verification Based on Autonomous System Provider Authorization (ASPA) Objects", Work in Progress, Internet-Draft, draft-ietf-sidrops-aspa-verification-24, 19 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-verification-24>.

[I-D.sriram-sidrops-asra-verification]
Sriram, K., Geng, N., and A. Herzberg, "Autonomous System Relationship Authorization (ASRA) as an Extension to ASPA for Enhanced AS Path Verification", Work in Progress, Internet-Draft, draft-sriram-sidrops-asra-verification-03, 3 November 2025, <https://datatracker.ietf.org/doc/html/draft-sriram-sidrops-asra-verification-03>.

[I-D.ietf-grow-route-leak-detection-mitigation]
Sriram, K. and A. Azimov, "Methods for Detection and Mitigation of BGP Route Leaks", Work in Progress, Internet-Draft, draft-ietf-grow-route-leak-detection-mitigation-12, 25 February 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-grow-route-leak-detection-mitigation-12>.

8.2. Informative References

[Gao] Gao, L. and J. Rexford, "Stable Internet routing without global coordination", 2001.

Acknowledgements

Thanks to all of the contributors.

Contributors

Sebastien Viardot
Grenoble INP
Email: sebastien.viardot@grenoble-inp.fr

Jun Zhang
Huawei
Email: junzhang1@huawei.com

Houda Labiod
Huawei
Email: houda.labiod@huawei.com

Authors' Addresses

Maxence Flechier
Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG
38000 Grenoble
France
Email: maxence.flechier@univ-grenoble-alpes.fr

Martin Heusse
Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG
Email: martin.heusse@univ-grenoble-alpes.fr

Andrzej Duda
Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG
Email: andrzej.duda@univ-grenoble-alpes.fr