Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 25, 2019

A. Azimov
E. Bogomazov
Qrator Labs
R. Bush
Internet Initiative Japan
K. Patel
Arrcus, Inc.
J. Snijders
NTT

October 22, 2018

Verification of AS_PATH Using the Resource Certificate Public Key Infrastructure and Autonomous System Provider Authorization
draft-azimov-sidrops-aspa-verification-01

Abstract

This document defines the semantics of an Autonomous System Provider Authorization object in the Resource Public Key Infrastructure to verify the AS_PATH attribute of routes advertised in the Border Gateway Protocol.

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.

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 April 25, 2019.

Table of Contents

1. Introduction

The Border Gateway Protocol (BGP) was designed with no mechanisms to validate BGP attributes. Two consequences are BGP Hijacks and BGP Route Leaks [RFC7908]. BGP extensions are able to partially solve these problems. For example, ROA-based Origin Validation [RFC6483] can be used to detect and filter accidental mis-originations, and [I-D.ymbk-idr-bgp-eotr-policy] can be used to detect accidental route leaks. While these upgrades to BGP are quite useful, they still rely on transitive BGP attributes, i.e. AS_PATH, that can be manipulated by attackers.

BGPSec [RFC8205] was designed to solve the problem of AS_PATH validation. Unfortunately, strict cryptographic validation brought unaffordable computational overhead for BGP routers. BGPSec also proved to be vulnerable to downgrade attacks that can nullify all the work of AS_PATH signing. As a result, to abuse the AS_PATH or any

other signed transit attribute, an attacker merely needs to downgrade to 'old' BGP-4.

An alternative approach was introduced with soBGP [I-D.white-sobgp-architecture]. Instead of strong cryptographic AS_PATH validation, it was suggested to create an AS_PATH security function based on a shared database of ASN adjacencies. While such an approach has reasonable computational cost, the two side adjacencies don't provide a way to automate anomaly detection without high adoption rate - an attacker can easily up a one-way adjacency. SO-BGP suggested sharing data about adjacencies using additional BGP messages, which is recursively complex thus significantly increasing adoption complexity. In addition, the general goal to verify all AS_PATHs was not achievable given the indirect adjacencies at internet exchange points.

Instead of the general goal of checking AS_PATH correctness, this document focuses on solving real-world operational problems - automatic detection of malicious hijacks and route leaks. To achieve this goal a new AS_PATH verification procedure is defined which is able to automatically detect invalid (malformed) AS_PATHs in announcements that are received from customers and peers. This procedure uses a shared signed database of customer-to-provider relationships that is built using a new RPKI object - Autonomous System Provider Authorization (ASPA). This technique provides benefits for the participants even in a state of early adoption.

2. Anomaly Propagation

Both route leaks and hijacks have similar effects on ISP operations - they redirect traffic, resulting in increased latency, packet loss, or possible MiTM attacks. But the level of risk depends significantly on the propagation of these BGP anomalies. For example, a hijack that is propagated only to customers may concentrate traffic in a particular ISP's customer cone; while if the anomaly is propagated through peers, upstreams, or reaches Tier-1 networks, thus distributing globally, traffic may be redirected at the level of entire countries and/or global providers.

The ability to constrain propagation of BGP anomalies to upstreams and peers, without requiring support from the source of the anomaly (which is critical if source has malicious intent), should significantly improve the security of inter-domain routing and solve the majority of problems.

3. Autonomous System Provider Authorization

As described in [RFC6480], the RPKI is based on a hierarchy of resource certificates that are aligned to the Internet Number Resource allocation structure. Resource certificates are X.509 certificates that conform to the PKIX profile [RFC5280], and to the extensions for IP addresses and AS identifiers [RFC3779]. A resource certificate is a binding by an issuer of IP address blocks and Autonomous System (AS) numbers to the subject of a certificate, identified by the unique association of the subject's private key with the public key contained in the resource certificate. The RPKI is structured so that each current resource certificate matches a current resource allocation or assignment.

ASPAs are digitally signed objects that bind a selected AFI Provider AS number to a Customer AS number (in terms of BGP announcements not business), and are signed by the holder of the Customer AS. An ASPA attests that a Customer AS holder (CAS) has authorized a particular Provider AS (PAS) to propagate the Customer's IPv4/IPv6 announcements onward, e.g. to the Provider's upstream providers or peers. The ASPA record profile is described in [I-D.azimov-sidrops-aspa-profile].

4. Customer-Provider Verification Procedure

This section describes an abstract procedure that checks that pair of ASNs (AS1, AS2) is included in the set of signed ASPAs. The semantics of its usa are defined in next section. The procedure takes (AS1, AS2, ROUTE_AFI) as input parameters and returns three types of results: "valid", "invalid" and "unknown".

A relying party (RP) must have access to a local cache of the complete set of cryptographically valid ASPAs when performing customer-provider verification procedure.

1. Retrieve all cryptographically valid ASPAs in a selected AFI with a customer value of AS1. This selection forms the set of "candidate ASPAs."

2. If the set of candidate ASPAs is empty, then the procedure exits with an outcome of "unknown."

3. If there is at least one candidate ASPA where the provider field is AS2, then the procedure exits with an outcome of "valid."

4. Otherwise, the procedure exits with an outcome of "invalid."

Since an AS1 may have different set providers in different AFI, it should also have different set of corresponding ASPAs. In this case,

the output of this procedure with input (AS1, AS2, ROUTE_AFI) may have different output for different ROUTE_AFI values.

5. AS_PATH Verification

The AS_PATH attribute identifies the autonomous systems through which an UPDATE message has passed. AS_PATH may contain two types of components: ordered AS_SEQes and unordered AS_SETs, as defined in [RFC4271].

The value of each AS_SEQ component can be described as set of pairs {(AS(I), prepend(I)), (AS(I-1), prepend(I-1))...}. In this case, the sequence {AS(I), AS(I-1),...} represents different ASNs, that packet should pass towards the destination. When a route is received from a customer or a literal peer, each pair (AS(I-1), AS(I)) MUST belong to customer-provider or sibling relationship. If there are other types of relationships, it means that the route was leaked or the AS_PATH attribute was malformed. The goal of the above procedure is to check the correctness of this statement.

For 32-bit AS number compatible BGP speakers, if a route from ROUTE_AFI address family is received from a customer or peer, its AS_PATH MUST be verified as follows:

1. If the closest AS in the AS_PATH is not the receiver's neighbor ASN then procedure halts with the outcome "invalid";

2. If in one of AS_SEQ segments there is a pair (AS(I-1), AS(I)), and customer-provider verification procedure (Section 4) with parameters (AS(I-1), AS(I), ROUTE_AFI) returns "invalid" then the procedure also halts with the outcome "invalid";

3. If the AS_PATH has at least one AS_SET segment then procedure halts with the outcome "unverifiable";

4. Otherwise, the procedure halts with an outcome of "valid".

For BGP speakers that are not 32-bit AS compatible, the above procedure is slightly different. In point 2 if at least one AS(I-1), AS(I) is equal to AS_TRANS(23456), the corresponding pair must be passed without check using the customer-provider verification procedure.

If the output of the AS_PATH verification procedure is "invalid" the LOCAL_PREF SHOULD be set to 0 or the route MAY be dropped. If an "invalid" route has no alternative route(s) and it is propagated to other ASes despite the above, it MUST be marked with the GRACEFUL_SHUTDOWN community to avoid possible stable oscillations,

when an unchecked route received from a provider becomes preferred over an invalid route received from a customer. This also allows customers to detect malformed routes received from upstream providers.

If the output of the AS_PATH verification procedure is 'unverifiable' it means that AS_PATH can't be fully verified. Such routes should be treated with caution and SHOULD be processed the same way as "invalid" routes. This policy goes with full correspondence to [I-D.kumari-deprecate-as-set-confed-set].

The above AS_PATH verification procedure is able to check routes received from customers and peers. The ASPA mechanism combined with BGP Roles [I-D.ietf-idr-bgp-open-policy] and ROA-based Origin Validation [RFC6483] provide a fully automated solution to detect and filter hijacks and route leaks, including malicious ones.

6. Disavowal of Provider Authorizaion

An ASPA is a positive attestation that an AS holder has authorized its provider to redistribute received routes to the provider's providers and peers. This does not preclude the provider AS from redistribution to its other customers. By creating an ASPA where the provider AS is 0, the customer indicates that no provider should further announce its routes. Specifically, AS 0 is reserved to identify provider-free networks, Internet exchange meshes, etc.

An ASPA with a provider AS of 0 is a statement by the customer AS that the its routes should not be received by any relying party AS from any of its customers or peers.

By convention, an ASPA with a provider AS of 0 should be the only ASPA issued by a given AS holder; although this is not a strict requirement. A provider 0 ASPA may coexist with ASPAs that have different provider AS values; though in such cases, the presence or absence of the provider AS 0 ASPA does not alter the AS_PATH verification procedure.

7. Siblings (Complex Relations)

There are peering relationships which can not be described as strictly simple peer-peer or customer-provider; e.g. when both parties are intentionally sending prefixes received from each other to their peers and/or upstreams.

In this case, two symmetric ASPAs records {(AS1, AS2), (AS2, AS1)} must be created by AS1 and AS2 respectively.

8. Security Considerations

ASPA issuers should be aware of the verification implication in issuing an ASPA - an ASPA implicitly invalidates all routes passed to upstream providers other than the provider ASs listed in the collection of ASPAs. It is the Customer AS's duty to maintain a correct set of ASPAs.

While the ASPA provides a check of an AS_PATH for routes received from customers and peers, it doesn't provide full support for routes that are received from upstream providers. So, this mechanism guarantees detection of both malicious and accidental route leaks and provides partial support for detection of malicious hijacks: upstream transit ISPs will still be able to send hijacked prefixes with malformed AS_PATHs to their customers.

9. Acknowledgments

The authors wish to thank authors of [RFC6483] since its text was used as an example while writing this document.

10. References

10.1. 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>.

[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>.

10.2. Informative References

[I-D.azimov-sidrops-aspa-profile] Azimov, A., Uskov, E., Bush, R., Patel, K., Snijders, J., and R. Housley, "A Profile for Autonomous System Provider Authorization", draft-azimov-sidrops-aspa-profile-00 (work in progress), June 2018.

[I-D.ietf-idr-bgp-open-policy] Azimov, A., Bogomazov, E., Bush, R., Patel, K., and K. Sriram, "Route Leak Prevention using Roles in Update and Open messages", draft-ietf-idr-bgp-open-policy-02 (work in progress), January 2018.

[I-D.kumari-deprecate-as-set-confed-set]
Kumari, W. and K. Sriram, "Deprecation of AS_SET and AS_CONFED_SET in BGP", draft-kumari-deprecate-as-set-confed-set-12 (work in progress), July 2018.

[I-D.white-sobgp-architecture]
White, R., "Architecture and Deployment Considerations for Secure Origin BGP (soBGP)", draft-white-sobgp-architecture-02 (work in progress), June 2006.

[I-D.ymbk-idr-bgp-eotr-policy]
Azimov, A., Bogomazov, E., Bush, R., and K. Patel, "Route Leak Detection and Filtering using Roles in Update and Open messages", draft-ymbk-idr-bgp-eotr-policy-02 (work in progress), March 2018.

[RFC3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", RFC 3779, DOI 10.17487/RFC3779, June 2004, <https://www.rfc-editor.org/info/rfc3779>.

[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>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[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>.

[RFC6483] Huston, G. and G. Michaelson, "Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs)", RFC 6483, DOI 10.17487/RFC6483, February 2012, <https://www.rfc-editor.org/info/rfc6483>.

[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>.

Authors' Addresses

Alexander Azimov
Qrator Labs

Email: aa@qrator.net

Eugene Bogomazov
Qrator Labs

Email: eb@qrator.net

Randy Bush
Internet Initiative Japan

Email: randy@psg.com

Keyur Patel
Arrcus, Inc.

Email: keyur@arrcus.com

Job Snijders
NTT Communications
Theodorus Majofskistraat 100
Amsterdam 1065 SZ
The Netherlands

Email: job@ntt.net