Workgroup: IDR and SIDR
Internet-Draft:
draft-sriram-sidrops-as-hijack-detection-05
Published: 9 January 2023
Intended Status: Standards Track
Expires: 13 July 2023
Authors: K. Sriram D. Montgomery
USA NIST USA NIST

AS Hijack Detection and Mitigation

Abstract

This document proposes a method for detection and mitigation of AS hijacking. In this mechanism, an AS operator registers a new object in the RPKI called 'ROAs Exist for All Prefixes (REAP)'. REAP is digitally signed using the AS holder's certificate. By registering a REAP object, the AS operator is declaring that they have Route Origin Authorization (ROA) coverage for all prefixes originated by their AS. A receiving AS will mark a route as Invalid if the prefix is not covered by any Validated ROA Payload (VRP) and the route origin AS has signed a REAP. Here Invalid means that the route is determined to be an AS hijack.

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 13 July 2023.

Copyright Notice

Table of Contents

1. Introduction

AS hijacking occurs when one AS accidentally or maliciously uses of another AS's AS number (ASN) as the origin ASN in a BGP announcement. The offending AS typically inserts its own ASN as the second ASN in the path after the hijacked origin ASN. The prefix in the announcement may sometimes belong to the hijacker. But AS hijacking is often done in conjunction with hijacking a third-party prefix. The hijacker would typically choose a third-party prefix that does not have Route Origin Authorization (ROA) [RFC6482] coverage. Then the route would receive NotFound rather than Invalid validation result when RPKI-based Origin Validation (RPKI-OV) [RFC6811] is performed. This benefits the hijacker because NotFound routes are commonly included in route selection by the receiver.

This document proposes a method for detection and mitigation of AS hijacking. In this mechanism, an AS operator registers a new object in the RPKI called 'ROAs Exist for All Prefixes (REAP)'. REAP is digitally signed using the AS holder's certificate. By registering a REAP object, the AS operator is declaring that they have Route Origin Authorization (ROA) coverage for all prefixes originated by their AS. A receiving AS will mark a route as Invalid if the prefix is not covered by any Validated ROA Payload (VRP) and the route origin AS has signed a REAP. Here Invalid means that the route is determined to be an AS hijack. It is assumed that a router that supports REAP is also RPKI [RFC6482] and RPKI-OV [RFC6811] capable.

To review some related work, the BGPsec protocol [RFC8205] effectively prevents AS hijack attacks but its adoption does not seem likely in the near future. The ASPA method [I-D.ietf-sidrops-aspa-verification] is designed principally for

detection of route leaks. In conjunction with checking peer ASN with BGP OPEN message (e.g., enforce-first-as [Cisco-IOS] or "peer_lookup_with_open" [Quagga]), ASPA also addresses AS hijacking in part. However, due to its vulnerability to cut and paste attacks in partial deployment, ASPA will often label such attacks as Unknown rather than Invalid. That gives leeway to an attacker to conduct AS hijacks in partial deployment. Even when an AS creates its ASPA object, if its transit provider does not, then the attacker can conduct the cut and paste attacks involving the AS. On the other hand, the proposed REAP method for detecting AS hijacks works much better even in partial deployment. If AS A creates its REAP object, then a REAP-enabled AS Z (anywhere in the Internet) can perform AS hijack detection for AS A independent of the adoption status of any other ASes. In other words, REAP can be deployed incrementally and the benefits accrue immediately for the REAP object creator and the ASes that have REAP-based AS hijack detection. Of course REAP and ASPA work in a complementary manner.

RPKI-OV is known to be vulnerable to forged-origin hijacks (see Section 4.3.1 in [NIST-800-189]), where a prefix and an origin AS that appear in a ROA are used together. However, in that case the attacker is likely competing with the legitimate Valid announcement for the prefix, and that makes the attack more conspicuous. Generally, the hijacker would seek to remain under the radar. So AS hijacks occur more commonly with a third-party prefix that does not have ROA coverage. The REAP method effectively detects and mitigates this form of attack.

2. AS Hijack Detection and Mitigation Method

This document specifies a new RPKI object called 'ROAs Exist for All Prefixes (REAP)'. As stated before, REAP is digitally signed using the AS holder's certificate. It contains only an AS number that belongs to the signer. By registering REAP, the AS operator is declaring that they have ROA coverage for all prefixes originated by their AS. REAP extends normal RPKI-OV processing to check if any NotFound route has an origin AS with a valid REAP object. If so, the NotFound result is changed to Invalid.

The algorithm to be followed in a receiving BGP router for validating a route is as follows:

1. Perform the RPKI-OV process [RFC6811] as normal.

2. If the result of RPKI-OV is NotFound and the origin AS has a valid (per X.509) REAP object, then replace NotFound with Invalid.

The operator SHOULD apply policy to reject routes with Invalid outcome in order to perform AS hijack mitigation along with prefix hijack mitigation.

3. IANA Considerations

IANA is requested to register the following RPKI Signed Object:

Name	OBJECT IDENTIFIER (OID) value	Reference
REAP	1.2.840.113549.1.9.16.1.TBD	[This document]

4. Security Considerations

The security considerations that apply to RPKI, ROAs, and RPKI-OV (see [RFC6480] [RFC6482] [RFC6811]) also apply to the procedure described in this document.

5. References

5.1. Normative References

[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>.

[RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", RFC 6482, DOI 10.17487/RFC6482, February 2012, <https://www.rfc-editor.org/info/rfc6482>.

[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>.

5.2. Informative References

[Cisco-IOS] "Cisco IOS IP Routing: BGP Command Reference (enforce-first-as)", Cisco IOS information webpage , , <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/command/irg-cr-book/bgp-a1.html#wp1026344430>.

[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 Resource Public Key Infrastructure (RPKI) Autonomous System Provider Authorization (ASPA) Objects", Work in

Progress, Internet-Draft, draft-ietf-sidrops-aspa-verification-11, 24 October 2022, <https://www.ietf.org/archive/id/draft-ietf-sidrops-aspa-verification-11.txt>.

[NIST-800-189] Sriram, K. and D. Montgomery, "Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation", NIST Special Publication NIST SP 800-189, , December 2019, <https://doi.org/10.6028/NIST.SP.800-189>.

[Quagga] "LCOV - code coverage report (peer_lookup_with_open)", Quagga information webpage , , <https://nowhere.ws/dump/quagga-srcdest-coverage/bgpd/bgpd.c.func.html>.

[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>.

Acknowledgements

The authors wish to thank Oliver Borchert and Kyehwan Lee for their review and comments.

Authors' Addresses

Kotikalapudi Sriram
USA National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899
United States of America

Email: ksriram@nist.gov

Doug Montgomery
USA National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899
United States of America

Email: dougm@nist.gov