Interdomain Routing Working Group
Internet-Draft
Intended status: Experimental
Expires: May 7, 2020

Y. Liu

S. Zhang

Q. Li

S. Peng

November 4, 2019

Requirement for the transparency of RPKI
draft-qingyuan-transparencyrpki-00

Abstract

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 May 7, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 2
2. Transparency Requirements 3
3. IANA Considerations 5
4. Security Considerations 5
5. References 5
Authors' Addresses 6

1. Introduction

The certification authority (CA) or independent resource management agency in the RPKI may adversely affect the associated Internet Number Resource (INR) when performing authentication or actions for authentication, such as RFC 8211 [RFC8211]. In Resource Public Key Infrastructure (RPKI) [RFC6480], the operation is called "adverse operation" if its consequence may reduce the amount of Internet Number Resources (INRs) and contrary to the wishes of this INR's owner. There are several forms of adverse operations on objects in the RPKI repository, including Deletion, Suppression, Corruption, Modification, Revocation, and Injection. The adverse operation caused by CA's error or repository operation errors or attacks may be an attack on objects in the RPKI repository [RFC7132].

According to the RPKI specification, even if the INR owner believes that the operation is adverse, the operation will be performed according to the established regulations. For example, RPKI establishes a top-down authoritative architecture based on regional Internet registry (RIRs), which allocates IP address space to the lower level (the upper level allocates to the lower level and the lower level reallocates to the lower level). The security benefits from RPKI are implemented through this architecture. However, in the architecture, CA or resource management agency can unilaterally revoke any IP resources under its control, thus may result in an authority that abuses power.

Therefore, it will cause serious security issues, once it is maliciously operated by some authorities. Therefore, we propose to establish a mechanism to increase the transparency of RPKI to curb strong CA or resource management agency.

2. Transparency Requirements

2.1 the transparency requirements for CA or resource management agencies in RPKI

In the current RPKI architecture, any adverse actions taken by a malicious CA or resource management agency are difficult to detect by others. Errors or attacks against CAs or management agency can cause IP addresses to be deleted or invalidated, which may have a significant impact on routing. The main reason for this type of problem is determined by the current architecture of RPKI. The current RPKI architecture has a centralized unilateral authorization, that is, the CA or resource management agency is free to perform any operations (issued, revoked, modified and updated) without any authentication and interaction. At the same time, RPKI's layered architecture gives CAs or resource management agency the ability to unilaterally revoke (or remove) IP prefixes under their control. This has led to concerns about the formation of powerful authorities in RPKI, which have the power to unilaterally operate IP resources and may abuse power. At present, it is difficult to distinguish whether an adverse operation is caused by improper operation of a resource management agency or a legitimate business operation.

This draft proposes to reduce the technical risk by improving the operational transparency of RPKI. The current RPKI specification places power entirely in the hands of CAs or resource management agencies. In order to solve this problem, the draft proposes: to add a two-way authorization operation for all operations on objects in the RPKI repository, that is, the CA or the resource management authority needs to obtain the authorization of the INR owner for the Deletion, Suppression, Corruption, Modification, revocation, and Injection operations on the resources owned by the INR holder. This two-way authorization meets the wishes of both the CA or the resource management agency and the INR owner and the agreement between them, and it can restrain the excessive power of the CA or resource management organization, which can operate the INR object arbitrarily without the permission of the INR owner. It is recommended to modify the operation mode of RPKI so that the operations on the INR objects need to meet the wishes of both the operator and the INR owner.

2.2 Transparency requirement for Relying Party in RPKI

In RPKI, each RP chooses its own set of trust anchors (TAs), which are specified in section 3 of [RFC8630]. Each RP maintains a local cache of RPKI objects and is consistent with the repository. Section 5 of [RFC6481] describes how to maintain a local cache. The RP needs to verify whether the resource certificate conforms to the configuration file described in Section 4 of [RFC6487]. Section 7.1

of [RFC6487] describes the process of verifying certificate resources and syntax that each RP should follow, and Section 7.2 introduces the process of RP performing certificate path verification. In order to verify the ROA, the RP needs to perform all the checks specified in [RFC6488], as well as additional specific verification steps to the ROA. More details on ROA verification are in Section 4 of [RFC6482].

To reduce the risk of RPKI, the RP should be able to detect when the RPKI error caused the BGP route to be incorrectly classified as "invalid". The RP can check if it has received all the objects in the manifest, and if the manifest is valid. If the manifest is invalid, the RP should issue an alert for missing information (as indicated in Section 6.5 of [RFC6486]), and the RP decides to respond to this alert at its discretion.

The event that the misconfigured or attacked CA or resource management agency incorrectly adds or destroys the ROA is not transparent. If the resource management agency ensures that its manifest is consistent with the objects in the repository, the RP will not issue an alert. The current RPKI specification does not focus on alerts, but it is important. Although the alerts themselves don't solve the problem, they do indicate that there is a problem and can trigger a mitigation mechanism.

There is another important threat to transparency: mirror world attack. In a mirror world attack, the resource management agency in an adversarial RPKI provides a view of the RPKI for some RPs while a different view for other RPs. The current RPKI has no mechanism to prevent such attack. The current RPKI system relies entirely on RPs to acquire, update, and verify all signature objects. Therefore, a RP is very likely to obtain the wrong ROAs due to the wrong operation or misbehavior of the issuer, so it cannot distinguish whether this is an error or a normal operation. Therefore, the current architecture of RPKI determines that it is difficult to defend against malicious operations by CA or resource management agency and more complex collusion attacks.

In the current RPKI system, the RP node is considered to be secure and reliable. If the RP is malicious, its connected BGP router can be a victim, causing serious routing security problems and corresponding blocking IP addresses. A malicious RP provides an incorrect manifest of valid ROAs, which causes the router to make an error in the validity of the route origination, and indirectly causes some legitimate IP address traffic to be blocked or redirected. For the above problems, under the current architecture and mechanism of RPKI, it is difficult to distinguish whether the operation on various resource certificate objects is due to the misconfiguration (or the malicious behavior) of the resource management agency, or the normal

contract between the issuer and the recipient of the resource certificate.

At the same time, the current RPKI system makes the load of RPs very heavy. The RPs need to perform the acquisition, verification and synchronization of all resource certificates and ROAs, and also need to interact with the BGP routers connected to them. The reliability, security, and performance of RPs are the bottleneck of the entire RPKI system.

3. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

4. Security Considerations

5. 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>.

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, DOI 10.17487/RFC2629, June 1999, <https://www.rfc-editor.org/info/rfc2629>.

[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>.

[RFC6481] Huston, G., Loomans, R., and G. Michaelson, "A Profile for Resource Certificate Repository Structure", RFC 6481, DOI 10.17487/RFC6481, February 2012, <https://www.rfc-editor.org/info/rfc6481>.

[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>.

[RFC6486] Austein, R., Huston, G., Kent, S., and M. Lepinski, "Manifests for the Resource Public Key Infrastructure (RPKI)", RFC 6486, DOI 10.17487/RFC6486, February 2012, <https://www.rfc-editor.org/info/rfc6486>.

[RFC6487] Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", RFC 6487, DOI 10.17487/RFC6487, February 2012, <https://www.rfc-editor.org/info/rfc6487>.

[RFC6488] Lepinski, M., Chi, A., and S. Kent, "Signed Object Template for the Resource Public Key Infrastructure (RPKI)", RFC 6488, DOI 10.17487/RFC6488, February 2012, <https://www.rfc-editor.org/info/rfc6488>.

[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>.

[RFC8211] Kent, S. and D. Ma, "Adverse Actions by a Certification Authority (CA) or Repository Manager in the Resource Public Key Infrastructure (RPKI)", RFC 8211, DOI 10.17487/RFC8211, September 2017, <https://www.rfc-editor.org/info/rfc8211>.

[RFC8360] Huston, G., Michaelson, G., Martinez, C., Bruijnzeels, T., Newton, A., and D. Shaw, "Resource Public Key Infrastructure (RPKI) Validation Reconsidered", RFC 8360, DOI 10.17487/RFC8360, April 2018, <https://www.rfc-editor.org/info/rfc8360>.

Authors' Addresses

Yaping Liu

Shuo Zhang

Qingyuan Li
No. 230, West Waihuan Street. Higher Education Mega Center
Guangzhou, Guangdong 510006
China

Email: liqingyuan94@live.cn

Sufang