Network Working Group
Internet-Draft
Intended status: Informational
Expires: November 5, 2020

J. Snijders
NTT

May 4, 2020

A Default Validation Policy for the use of RPKI Manifests in the global Internet Routing System.

draft-spaghetti-sidrops-rpki-manifest-validation-01

Abstract

Manifests are a critical cornerstone to the global Resource Public Key Infrastructure (RPKI).

RFC 6486 describes a validation decision tree which introduced the notion of 'local policy', creating space for ambiguity. This ambiguity has led to various RPKI implementations producing different output when presented with the same input, but also leads to severe operational security implications.

This document updates RFC 6486 and introduces the notion of a default policy for Manifest validation to encourage harmony between implementations.

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 will expire on November 5, 2020.

Table of Contents

1. Introduction

Manifests [RFC8416] are a critical cornerstone to the global Resource Public Key Infrastructure RPKI [RFC6480].

RFC 6486 describes a validation decision tree which introduced the notion of 'local policy', creating space for ambiguity. This ambiguity has led to various RPKI implementations producing different output when presented with the same input, but also operational security implications.

This document updates RFC 6486 and introduces the notion of a global policy for Manifest validation to encourage harmony between implementations.

2. Suggested Reading

It is assumed that the reader understands BGP, [RFC4271], the RPKI [RFC6480], Route Origin Authorizations (ROAs) [RFC6482], RPKI-based Prefix Validation, [RFC6811], and Origin Validation Clarifications [RFC8481].

3. The Problem

It seems there is a mental trap in the RPKI system: contrary to intuition, implementers should focus on validation policies which minimize the number of Validated ROA Payloads (VRPs) at a RPKI cache. If RPKI cache implementers mistreat untrusted network data and 'salvage whatever is possible', a number of critical issues are introduced which compromise our ability to deploy RPKI ROV incrementally. Only a single path through the RFC 6486 decision tree is suitable for use in the global Internet system, as such that path is the Default Policy.

If a dangerous condition is detected, not only MUST the manifest at the publication point be distrusted, but all VRPs encompassed by the IPAddrBlocks for which authority was delegated towards the Certificate Authority (CA) at the distrusted pulication point be removed from the RP's output. If the result is no VRPs at all (for example because the RPKI subsystem is detected to be compromised at the root), that is a preferred state for the Internet routing system. The alternative is that a compromised RPKI system will permanently disrupt the global Internet routing system.

4. Examples of Problematic Behavior

4.1. AS0 and Delegation

Suppose that an address space holder of 2001:DB8::/32 delegates prefixes to multihomed end users. Operationally, it is not sensible that the 2001:DB8::/32 be advertised or accepted, so the address space holder creates exactly one ROA for 2001:DB8::/32 with asID set to 0. Finally, the address space holder creates ROAs for the /48 (prefix, ASN) pairs, as delegated.

At this point, the manifest includes a mininum of two ROAs, but only one is being received by the RPKI cache (specifically, the 2001:DB8::/32 AS0 ROA, not the other more-specific ROAs). The result of this is that the longer-prefix advertisement of (example

delegation) by AS(example ASN) is invalid if the 2001:DB8::/32 ROA AS0 transformed into a VRP by the RPKI cache.

RPKI caches would damage the network if the above scenario would happen.

5. Update to RFC 6486

This section replaces section 6 of [RFC6486] in its entirety.

The goal of an Relying Party (RP) is to determine which signed objects to use for validating assertions about INRs and their use (e.g., which VRPs to use in the construction of route filters). The global Internet routing system is expected to benefit from uniform application of a similar validation policy, as such in the following sections we describe a sequence of tests that the RP MUST perform to determine the manifest state of the given publication point according to the default policy. We then discuss the risks associated with using signed objects in the publication point, given the manifest state; we also provide suitable warning text that SHOULD be placed in a user-accessible log file. Note that if a certificate is deemed unfit for use due to default policy, then any signed object that is validated using this certificate also SHOULD be deemed unfit for use (regardless of the status of the manifest at its own publication point).

5.1. Tests for Determining Manifest State

For a given publication point, the RP MUST perform the following tests to determine the manifest state of the publication point:

1. For each CA using this publication point, select the CA's current manifest (the "current" manifest is the manifest issued by this CA having the highest manifestNumber among all valid manifests, and where manifest validity is defined in Section 4.4 [RFC6486]. If the publication point does not contain a valid manifest, see Section 6. Lacking a valid manifest, the following tests cannot be performed.

2. To verify completeness, an RP MUST check that every file at each publication point appears in one and only one current manifest, and that every file listed in a current manifest is published at the same publication point as the manifest.

3. If files exist at the publication point that do not appear on any manifest, those can be ignored.

4. If files are listed in a manifest that do not appear at the publication point, see Section 6.

5. Check that the current time (translated to UTC) is between thisUpdate and nextUpdate. If the current time does not lie within this interval, then see Section 6, but still continue with the following tests.

6. Verify that the listed hash value of every file listed in each manifest matches the value obtained by hashing the file at the publication point. If the computed hash value of a file listed on the manifest does not match the hash value contained in the manifest, then see Section 6.

7. An RP MUST check that the contents of each current manifest conforms to the manifest's scope constraints, as specified in Section 2.

8. If a current manifest contains entries for objects that are not within the scope of the manifest, then the out-of-scope entries SHOULD be disregarded in the context of this manifest. If there is no other current manifest that describes these objects within that other manifest's scope, then see Section 6.

For each signed object, if all of the following conditions hold:

the manifest for its publication and the associated publication point pass all of the above checks;

the signed object is valid; and

the manifests for every certificate on the certification path used to validate the signed object and the associated publication points pass all of the above checks;

then the RP can conclude that no attack against the repository system has compromised the given signed object, and the signed object MUST be treated as valid (relative to manifest checking).

6. What to do when the CA's Publication Point is Distrusted

Once the RP has concluded the data at the publication point is distrusted, the RP MUST remove all VRPs encompassed by the IPAddrBlocks for which "right-of-use" authority was delegated to the CA at the distrusted publication from its output, regardless of the Trust Anchors.

7. TODO

- o Mention RIR transfer cases

- o The case for a most conservative approach: a 'fail-closed' policy on the RPKI plane results in an collective ability to deploy ROV on the shared EBGP plane: as the default remains 'fail open' (aka 'pre RPKI world'), operators in turn can deploy 'invalid == reject' policies on their EBGP sessions incrementally. A brilliant strategy, however it strongly depends erring to the side of caution (distrust?) in the validation process.

- o A publication point should not be 'repaired' by an RP using locally cached files if the RP's pulling process resulted in a distrusted publication point. The CA publication point is a remote entity which must assume the RP has no prior knowledge of the publication point. Locally cached files only exist to reduce network load.

8. Security Considerations

... where to start

9. IANA Considerations

None

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>.

[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>.

[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>.

[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>.

[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>.

[RFC8416] Ma, D., Mandelberg, D., and T. Bruijnzeels, "Simplified Local Internet Number Resource Management with the RPKI (SLURM)", RFC 8416, DOI 10.17487/RFC8416, August 2018, <https://www.rfc-editor.org/info/rfc8416>.

[RFC8481] Bush, R., "Clarifications to BGP Origin Validation Based on Resource Public Key Infrastructure (RPKI)", RFC 8481, DOI 10.17487/RFC8481, September 2018, <https://www.rfc-editor.org/info/rfc8481>.

10.2. Informative 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>.

Appendix A. Acknowledgements

The authors wish to thank Rob Austein, Geoff Huston, Stephen Kent, Matt Lepinski, Martin Hoffman, Randy Bush, Theo de Raadt, William McCall for their insights and contributions which helped create this document.

Author's Address

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

Email: job@ntt.net