Network Working Group
Internet-Draft
Updates: 6487 (if approved)
Intended status: Standards Track
Expires: April 11, 2016

G. Huston
G. Michaelson
APNIC

October 9, 2015

Update to RPKI Validation
draft-huston-sidr-validity-00.txt

Abstract

This document updates the RPKI certificate validation procedure as specified in Section 7.2 of RFC6487.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

This document updates the RPKI certificate validation procedure as specified in Section 7.2 of [RFC6487], by replacing the section 7.2 of [RFC6487] with the specification contained here.

2. The RPKI Certification Path Validation

Validation of signed resource data using a target resource certificate, and a specific set of number resources, consists of verifying that the digital signature of the signed resource data is valid, using the public key of the target resource certificate, and also validating the resource certificate in the context of the RPKI, using the path validation process. This path validation process verifies, among other things, that a prospective certification path (a sequence of n certificates) satisfies the following conditions:

1. for all 'x' in {1, ..., n-1}, the Subject of certificate 'x' is the Issuer of certificate ('x' + 1);

2. certificate '1' is issued by a trust anchor;

3. certificate 'n' is the certificate to be validated; and

4. for all 'x' in {1, ..., n}, certificate 'x' is valid for the specific set of resources.

RPKI validation for a specific set of resources entails verifying that all of the following conditions hold, in addition to the Certification Path Validation criteria specified in Section 6 of [RFC5280]:

1. The certificate can be verified using the Issuer's public key and the signature algorithm

2. The current time lies within the certificate's Validity From and To values.

3. The certificate contains all fields that MUST be present, as specified by [RFC6487], and contains values for selected fields that are defined as allowable values by this specification.

4. No field, or field value, that the [RFC6487] specification defines as MUST NOT be present is used in the certificate.

5. The Issuer has not revoked the certificate. A revoked certificate is identified by the certificate's serial number being listed on the Issuer's current CRL, as identified by the CRLDP of the certificate, the CRL is itself valid, and the public key used to verify the signature on the CRL is the same public key used to verify the certificate itself.

6. The resource extension data contained in this certificate "encompasses" the entirety of the resources in the specific resource set ("encompass" in this context is defined in Section 7.1 of [RFC6487]).

7. The Certification Path originates with a certificate issued by a trust anchor, and there exists a signing chain across the Certification Path where the Subject of Certificate 'x' in the Certification Path matches the Issuer in Certificate 'x + 1' in the Certification Path, and the public key in Certificate 'x' can verify the signature value in Certificate 'x+1'.

A certificate validation algorithm MAY perform these tests in any chosen order.

There exists the possibility of encountering certificate paths that are arbitrarily long, or attempting to generate paths with loops as means of creating a potential denial-of-service (DOS) attack on an Relying Party (RP). An RP executing this procedure MAY apply further heuristics to guide the certification path validation process to a halt in order to avoid some of the issues associated with attempts to validate such malformed certification path structures. Implementations of resource certificate validation MAY halt with a validation failure if the certification path length exceeds a locally defined configuration parameter.

3. Security Considerations

This update is intended to improve the robustness of the RPKI framework by altering the procedure of the original validation path that included an "encompassing" condition applied pairwise to the certificates used in the validation path.

The intent of this update is to ensure that all certificates on a validation path encompass the resources that are included in the validation query, but to remove the "encompassing" constraint on the resources used in pairwise comparison. This change to the validation procedure reduces the criticality of strict orchestration of the sequence of certificate issuance and revocation in those circumstances, and can thereby improve the robustness of the RPKI as a consequence, without altering the underlying semnatics of the association of a public key value across a collection of number resources.

4. IANA Considerations

No updates to the registries are suggested by this document.

5. Acknowledgements

Thanks

6. Normative References

[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, <http://www.rfc-editor.org/info/rfc5280>.

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

Authors' Addresses

Geoff Huston
Asia Pacific Network Information Centre
6 Cordelia St
South Brisbane, QLD 4101
Australia

Phone: +61 7 3858 3100
Email: gih@apnic.net

George Michaelson
Asia Pacific Network Information Centre
6 Cordelia St
South Brisbane, QLD 4101
Australia

Phone: +61 7 3858 3100
Email: ggm@apnic.net