Network Working Group
Internet-Draft
Intended status: Informational
Expires: September 22, 2016

G. Huston
G. Michaelson
APNIC
C. Martinez
LACNIC
T. Bruijnzeels
RIPE NCC
A. Newton
ARIN
A. Aina
AFRINIC

March 21, 2016

RPKI Validation Reconsidered
draft-ietf-sidr-rpki-validation-reconsidered-03

Abstract

This document proposes and alternative to the certificate validation procedure specified in RFC6487 that reduces aspects of operational fragility in the management of certificates in the RPKI.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document proposes and alternative to the certificate validation procedure specified in RFC6487 that reduces aspects of operational fragility in the management of certificates in the RPKI.

2. Certificate Validation in the RPKI

As currently defined in section 7.2 of [RFC6487], validation of PKIX certificates that conform to the RPKI profile relies on the use of a path validation process where each certificate in the validation path is required to meet the certificate validation criteria.

These criteria require in particular that the resources on each certificate in the validation path are "encompassed" by the resources on the issuing certificate. The first certificate in the path is required to be a trust anchor, and its resources are considered valid by definition.

For example, in the following sequence:

```
Certificate 1 (trust anchor):
 Issuer TA, Subject TA, Resources 192.0.2.0/24, AS64496-AS64500

Certificate 2:
 Issuer TA, Subject CA1, Resources 192.0.2.0/24, AS64496-AS64500

Certificate 3:
 Issuer CA1, Subject CA2, Resources 192.0.2.0/24, AS64496-AS64500

ROA 1:
 Embedded Certificate 4 (EE certificate):
 Issuer CA2, Subject R1, Resources 192.0.2.0/24

 Prefix 192.0.2.0/24, Max Length 24, ASN 64496
```

All certificates in this scenario are considered valid in that the resources on each certificate are encompassed by the issuing certificate. The roa "ROA1" is also considered valid here in this regard - the prefix is encompassed by the embedded EE certificate.

3. Operational Considerations

Resource allocations can change in the RPKI. And this can lead to situations where an "over-claiming" certificate is introduced.

Consider the following sequence:

```
Certificate 1 (trust anchor):
 Issuer TA, Subject TA, Resources 192.168.2.0/24, AS64496-AS64500

Certificate 2:
 Issuer TA, Subject CA1, Resources 192.168.2.0/24

Certificate 3:
 Issuer CA1, Subject CA2, Resources 192.168.2.0/24, AS64496-AS64500

ROA 1:
 Embedded Certificate 4 (EE certificate):
 Issuer CA2, Subject R1, Resources 192.168.2.0/24

 Prefix 192.168.2.0/24, Max Length 24, ASN 64496
```

Here Certificate 2 from the previous example was re-issued by TA to CA1 and certain AS resources were removed. However, CA1 failed to re-issue a new Certificate 3 to CA2. As a result Certificate 3 is now over-claiming and considered invalid, and by recursion ROA1 issued by CA2 is also invalid.

It should be noted that CA2 is not claiming any resources on ROA1 that it cannot receive on a new Certificate 3. If CA1 would only re-issue a Certificate 3 without the AS resources to CA2, then ROA1 would be considered valid without the need for any further action by CA2.

[RFC6492] describes the protocol for provisioning resource certificates. In this protocol new resource certificates are always issued by request of a child. If that protocol were strictly followed then CA1 would have known that its resource set was about to shrink, and it would have known that it issued some of those resources to its child CA2.

The protocol currently lacks normative wording on how CAs should deal with this situation, but one can imagine amending the protocol with normative instructions that would require CA1 to refuse to request a certificate with a shrunk resource set until all of its children would have requested new shrunk certificates where applicable. And that would forbid any parent CA to pro-actively re-issue a certificate with shrunk resource set before receiving a certificate re-issuance request from its child CA.

In practice such a model is unworkable for the CA higher in the path, because it has no control over if and when it can shrink a certificate for its children. Therefore higher level CAs will pro-actively re-issue shrunk resource certificates when resources are no longer validly held by a child.

The question here is whether the impact of such a re-issuance should be limited to just the resources that seem to be under dispute between TA and CA1, or all resources issued to CA2.

4. An Amended RPKI Certification Validation Process

4.1. Changes to existing standards

The following is a amended specification of certificate validation as described in section 7.2 item number 6 of certificate validation in [RFC6487] that describes the validation of resources in the RPKI path:

> The Relying Party MUST keep a set of verified resources for the certificate independent of the RFC3779 extension itself, that is built up using the following approach:
>
> > For any of the resource extensions that use the "inherit" element as described in sections 2.2.3.5 and 3.2.3.3 of [RFC3779], the corresponding resources of this type should be

taken from the parent certificate, where this issuer is the subject.

For any other resources the intersection of the quoted resources on this certificate and the parent certificate is kept. If any resources were found on this certificate that were not present on the parent certificate a warning SHOULD be issued to help operators rectify this situation.

If the the set of verified resources obtained this way is empty, then the certificate MUST be considered invalid.

Note that if this approach would be used in the example we cite in section 3 of this document, Certificate 3 would have a verified resource set that contains only "192.0.2.0/24", and a warning would be issued with regards to resources "AS64496-AS64500". ROA1 would be considered valid because the quoted prefix was also part of the verified resource set of the embedded Certificate 4.

4.2. An example

Consider the following example under the amended approach:

```
Certificate 1 (trust anchor):
 Issuer TA, Subject TA, Resources 192.168.2.0/24, AS64496-AS64500

  Verified resources: 192.168.2.0/24, AS64496-AS64500
  Warnings: none

Certificate 2:
 Issuer TA, Subject CA1, Resources 192.168.2.0/24

  Verified resources: 192.168.2.0/24
  Warnings: none

Certificate 3:
 Issuer CA1, Subject CA2, Resources 192.168.2.0/24, AS64496-AS64500

  Verified resources: 192.168.2.0/24
  Warnings: overclaim for AS64496-AS64500

ROA 1:
 Embedded Certificate 4 (EE certificate):
 Issuer CA2, Subject R1, Resources 192.168.2.0/24

  Verified resources: 192.168.2.0/24
  Warnings: none

  Prefix 192.168.2.0/24, Max Length 24, ASN 64496

  ROA1 is considered valid because the prefix matches the verified
  resources on the embedded EE certificate.

ROA 2:
 Embedded Certificate 5 (EE certificate):
 Issuer CA2, Subject R2, Resources 192.168.3.0/24

  Verified resources: none
  Warnings: overclaim for 192.168.3.0/24

  Prefix 192.168.3.0/24, Max Length 24, ASN 64496

  ROA2 is considered invalid because the prefix does not
  match the verified resources on the embedded EE certificate.
  The amended approach cannot lead to ROAs showing up as valid
  for resources that are not verified on the full path from the
  Trust Anchor down to the ROA.
```

5. Security Considerations

The problem described in section 3 of this document has not occurred to date. So one could consider this a low probability problem today. However the potential impact on routing security would be high if the inconsistency occurred near the apex of the RPKI hierarchy and would invalidate the entirety of the sub-tree located below the point of this inconsistency.

The proposed process does not change the probability of this problem, but it limits the impact to just the resources that are under dispute. As far as the authors can see there are no real new problems introduced by this approach.

It should be noted that although this is a problem with a low probability today this is largely due to the fact that most current RPKI systems use their own Trust Anchor and do not support any large number of delegated CAs. If this changes and the issuance and publication of a certificate, by the parent, and its use, by a child, are handled by different organisations more commonly, then the probability of this problem will increase.

6. IANA Considerations

No updates to the registries are suggested by this document.

7. Acknowledgements

TBA.

8. Normative References

[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, <http://www.rfc-editor.org/info/rfc3779>.

[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>.

[RFC6492] Huston, G., Loomans, R., Ellacott, B., and R. Austein, "A Protocol for Provisioning Resource Certificates", RFC 6492, DOI 10.17487/RFC6492, February 2012, <http://www.rfc-editor.org/info/rfc6492>.

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

Carlos M. Martinez
Latin American and Caribbean IP Address Regional Registry
Rambla Mexico 6125
Montevideo 11400
Uruguay

Phone: +598 2604 2222
Email: carlos@lacnic.net

Tim Bruijnzeels
RIPE Network Coordination Centre
Singel 258
Amsterdam 1016 AB
The Netherlands

Email: tim@ripe.net

Andrew Lee Newton
American Registry for Internet Numbers
3635 Concorde Parkway
Chantilly, VA 20151
USA

Email: andy@arin.net

Alain Aina
African Network Information Centre (AFRINIC)
11th Floor, Raffles Tower
Cybercity, Ebene
Mauritius

Phone: +230 403 51 00
Email: aalain@afrinic.net