Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 9, 2016

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

June 7, 2016

RPKI Validation Reconsidered
draft-ietf-sidr-rpki-validation-reconsidered-04

Abstract

This document proposes an update to the certificate validation procedure specified in RFC 6487 that reduces aspects of operational fragility in the management of certificates in the RPKI, while retaining essential security features.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document proposes an update to the certificate validation procedure specified in [RFC6487] that reduces aspects of operational fragility in the management of certificates in the RPKI, while retaining essential security features.

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, 198.51.100.0/24,
            2001:db8::/32, AS64496-AS64500

Certificate 2:
 Issuer TA,
 Subject CA1,
 Resources 192.0.2.0/24, 198.51.100.0/24, 2001:db8::/32

Certificate 3:
 Issuer CA1,
 Subject CA2,
 Resources 192.0.2.0/24, 2001:db8::/32

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. ROA1 is valid because the specified prefix is encompassed by the embedded EE certificate, as required by [RFC6482].

3. Operational Considerations

The allocations recorded in the RPKI change as a result of resource transfers and some types of operational errors. For example, the CAs involved in transfer might choose to modify CA certificates in an order that causes some of these certificates to "over-claim" temporarily. It may also happen that a child CA does not voluntarily request a shrunk resource certificate when resources are being transferred or reclaimed by the parent. Furthermore some types of operational errors that may occur during management of RPKI databases also may create CA certificates that, temporarily, no longer encompass all of the resources in subordinate certificates.

Consider the following sequence:

```
Certificate 1 (trust anchor):
 Issuer TA,
 Subject TA,
 Resources 192.0.2.0/24, 198.51.100.0/24,
           2001:db8::/32, AS64496-AS64500

Certificate 2:
 Issuer TA,
 Subject CA1,
 Resources 192.0.2.0/24, 2001:db8::/32

Certificate 3 (invalid):
 Issuer CA1,
 Subject CA2,
 Resources 192.0.2.0/24, 198.51.100.0/24, 2001:db8::/32

ROA 1 (invalid):
 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
```

Here Certificate 2 from the previous example was re-issued by TA to CA1 and the prefix 198.51.100.0/24 was 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 the embedded Certificate 4 used for ROA1 is also invalid. And ROA1 is invalid because the specified prefix is no longer encompassed by a valid embedded EE certificate, as required by [RFC6482]

However, it should be noted that ROA1 does not make use of any of the address resources that were removed from CA1's certificate, and thus it would be desirable if ROA1 could still be viewed as valid. Technically CA1 could re-issue a Certificate 3 to CA2 without 198.51.100.0/24, and then ROA1 would be considered valid according to [RFC6482]. But as long as CA1 does not take this action, ROA1 remains invalid. It would be preferable if ROA1 could be considered valid.

4. An Amended RPKI Certification Validation Process

4.1. Verified Resource Set

The problem described above can be considered as a low probability problem today. However the potential impact on routing security would be high if an overclaim occurred near the apex of the RPKI

hierarchy and would invalidate the entirety of the sub-tree located below this point.

The changes proposed here to the validation procedure in [RFC6487] do not change the probability of this problem, but limit the impact to just the overclaimed resources. This approach is intended to avoid causing CA certificates to be treated as completely invalid as a result of overclaims. However, these changes are designed to not degrade the security offered by the RPKI. Specifically, no ROAs or router certificates will be treated as valid if they contain only resources that are not encompassed by all superior certificates along a path to a trust anchor.

The way this is achieved conceptually is by maintaining a set of verified resources for each certificate that is separate from the set of resources found in the [RFC3779] resource extension on a certificate.

4.2. Changes to existing standards

4.2.1. Resource Certificate Path Validation

Step 6 of the Resource Certification Path Validation defined in section 7.2 of [RFC6487] currently has the following on the validation of resources contained in the [RFC3779] resource extension of certificates:

- The resource extension data is "encompassed" by the resource extension data contained in a valid certificate where this issuer is the subject (the previous certificate in the context of the ordered sequence defined by the certification path).

The following is an amended specification to be used in place of this text.

- The Relying Party MUST keep a Verified Resource Set for the certificate independent of the RFC3779 extension itself, that is built up using the following approach:

    * If the certificate under test is chosen as a Trust Anchor, then the Verified Resource Set of this certificate is equal to the RFC3779 resource extensions.

    * If the certificate under test not chosen as a Trust Anchor, the Verified Resource Set is found by comparing this certificate to its parent certificate (the previous certificate in the context of the ordered sequence defined by the certification path) in the following way:

  - 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 RFC 3779, the corresponding resources of this type should be taken from the parent certificate.

  - For resource extensions that do no use the "inherit" element, the intersection of the resources on this certificate and the Verified Resource Set of the parent certificate MUST be used. If any resources on this certificate are not encompassed by the Verified Resource Set of the parent certificate, a warning SHOULD be issued to help operators rectify this situation.

  - If the Verified Resource Set obtained this way is empty for all resource classes (IPv4, IPv6 and AS), then the certificate MUST be considered invalid.

4.2.2. ROA Validation

Section 4 of [RFC6482] currently has the following text on the validation of resources on a ROA:

- The IP address delegation extension [RFC3779] is present in the end-entity (EE) certificate (contained within the ROA), and each IP address prefix(es) in the ROA is contained within the set of IP addresses specified by the EE certificate's IP address delegation extension.

The following is an amended specification to be used in place of this text.

- The Verified Resource Set of the end-entity (EE) certificate (contained within the ROA), contains each IP address prefix(es) in the ROA.

4.2.3. BGPsec Router Certificate Validation

BGPsec Router Certificate Validation is defined in section 3.3 of [I-D.ietf-sidr-bgpsec-pki-profiles]. Path validation defined section 7 of [RFC6487] is used as the first step in validation, and a number of additional constraints are applied.

We propose that the text of the following two additions:

- BGPsec Router Certificates MUST NOT include the IP Resource extension.

- BGPsec Router Certificates MUST include the AS Resource Identifier Delegation extension.

Is updated to the following:

- The Validated Resource Set of BGPsec Router Certificates MUST NOT include IP Resources.

- BGPsec Router Certificates MUST include the AS Resource Identifier Delegation extension and all AS resources included on this MUST be encompassed by the Validated Resource Set of the BGPsec Router Certificates.

4.3. An example

Consider the following example under the amended approach:

```
     Certificate 1 (trust anchor):
      Issuer TA,
      Subject TA,
      Resources 192.0.2.0/24, 198.51.100.0/24,
                2001:db8::/32, AS64496-AS64500

       Verified Resource Set: 192.0.2.0/24, 198.51.100.0/24,
                              2001:db8::/32, AS64496-AS64500
       Warnings: none

     Certificate 2:
      Issuer TA,
      Subject CA1,
      Resources 192.0.2.0/24, 2001:db8::/32, AS64496

       Verified Resource Set: 192.0.2.0/24,
                              2001:db8::/32, AS64496
       Warnings: none

     Certificate 3:
      Issuer CA1,
      Subject CA2,
      Resources 192.0.2.0/24, 198.51.100.0/24, AS64496

       Verified Resource Set: 192.0.2.0/24, AS64496
       Warnings: overclaim for 198.51.100.0/24

     ROA 1 (valid):
      Embedded Certificate 4 (EE certificate):
       Issuer CA2,
       Subject R1,
```

Resources 192.0.2.0/24

Verified resources: 192.0.2.0/24
Warnings: none

Prefix 192.0.2.0/24, Max Length 24, ASN 64496

ROA1 is considered valid because the prefix matches the Verified Resource Set on the embedded EE certificate, as required by RFC 6482.

ROA 2 (invalid):
Embedded Certificate 5 (EE certificate):
Issuer CA2,
Subject R2,
Resources 198.51.100.0/24

Verified resources: none
Warnings: overclaim for 198.51.100.0/24

Prefix 198.51.100.0/24, Max Length 24, ASN 64496

ROA2 is considered invalid because the prefix does not match the Verified Resource Set on the embedded EE certificate. The amended approach therefore 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.

BGPSec Certificate 1 (valid):
Issuer CA2
Subject ROUTER-64496
Resources AS64496

Verified resources: AS64496
Warnings: none

BGPSec Certificate 2 (invalid):
Issuer CA2
Subject ALL-ROUTERS
Resources AS64496-AS64497

Verified resources: AS64496
Warnings: overclaim for AS64497

BGPSec Certificate 2 is considered invalid because not ALL resources are part of the Verified Resource Set of this certificate. This problem can be mitigated by issuing separate certificates for each AS number.

5. Security Considerations

As far as the authors can see there are no real new problems introduced by this approach.

6. IANA Considerations

No updates to the registries are suggested by this document.

7. Acknowledgements

TBA.

8. References

8.1. Normative References

[I-D.ietf-sidr-bgpsec-pki-profiles]
Reynolds, M. and S. Kent, "A Profile for BGPsec Router Certificates, Certificate Revocation Lists, and Certification Requests", draft-ietf-sidr-bgpsec-pki-profiles-17 (work in progress), June 2016.

[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>.

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

[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>.

8.2. Informative References

[RFC3849] Huston, G., Lord, A., and P. Smith, "IPv6 Address Prefix Reserved for Documentation", RFC 3849, DOI 10.17487/RFC3849, July 2004, <http://www.rfc-editor.org/info/rfc3849>.

[RFC5398] Huston, G., "Autonomous System (AS) Number Reservation for Documentation Use", RFC 5398, DOI 10.17487/RFC5398, December 2008, <http://www.rfc-editor.org/info/rfc5398>.

[RFC5737] Arkko, J., Cotton, M., and L. Vegoda, "IPv4 Address Blocks Reserved for Documentation", RFC 5737, DOI 10.17487/RFC5737, January 2010, <http://www.rfc-editor.org/info/rfc5737>.

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