Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 9, 2017

G. Huston
G. Michaelson
APNIC
C. Martinez
LACNIC
T. Bruijnzeels
RIPE NCC
A. Newton
ARIN
D. Shaw
AFRINIC
July 8, 2016

RPKI Validation Reconsidered
draft-ietf-sidr-rpki-validation-reconsidered-06

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 Internet Number Resources (INRs) of each certificate in the validation path are "encompassed" by INRs 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 since the INRs of each certificate are encompassed by those of 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. 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. A certificate is said to "over-claim" if it includes INRs not contained in the INRs of the CA that issued the certificate in question.

It may also happen that a child CA does not voluntarily request a Shrunken (reduced scope) resource certificate when resources are being transferred or reclaimed by the parent. Furthermore operational errors that may occur during management of RPKI databases also may create CA certificates that, temporarily, no longer encompass all of the INRs of subordinate certificates. Finally, some types of attacks against a CA (or repository operators) may result in certificates that over-claim, until the attack is discovered and remediated, c.f. Section 2.5 of[adverse actions].

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; by recursion the embedded Certificate 4 used for ROA1 is also invalid. And ROA1 is invalid because the specified prefix contained in the ROA 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 should 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, since the assertion it makes was not affected by the reduced scope of CA1's certificate.

4. An Amended RPKI Certification Validation Process

4.1. Verified Resource Sets

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 over-claiming certificate appeared near the apex of the RPKI hierarchy, as this would invalidate the entirety of the sub-tree located below this point.

Stephen Kent 7/14/2016 2:08 PM
Deleted: occurred

The changes proposed here to the validation procedure in [RFC6487] do not change the probability of this problem arising, but they do limit the impact to just the over-claimed resources. This revised validation algorithm is intended to avoid causing CA certificates to be treated as completely invalid as a result of over-claims. However, these changes are designed to not degrade the security offered by the RPKI. Specifically, ROAs and router certificates will be treated as valid only if all of the resources contained in them are encompassed by all superior certificates along a path to a trust anchor.

The way this is achieved conceptually is by maintaining Verified Resource Set (VRS) for each certificate that is separate from the INRs found in the [RFC3779] resource extension in the certificate.

4.2. Changes to existing standards

4.2.1. Resource Certificate Path Validation

The following is an amended specification to be used in place of section 7.2 of [RFC6487].

The following algorithm is employed to validate CA and EE resources certificates. It is modeled on the path validation algorithm from [RFC5280], but modified to make use of the IP Address Delegation and AS Identifier Delegation Extensions from [RFC3779].

There are two inputs to the validation algorithm:

1. a trust anchor

2. a certificate to be validated

The algorithm is initialized with two new variables for use in the RPKI: Validated Resource Set-IP (VRS-IP) and Validated Resource Set-AS (VRS-AS). These sets are used to track the set of INRs (IP address space and AS Numbers) that are considered valid for each CA certificate. The VRS-IP and VRS-AS sets are initially set to the IP Address Delegation and AS Identifier Delegation values, respectively, from the trust anchor used to perform validation.

This path validation algorithm verifies, among other things, that a prospective certification path (a sequence of n certificates) satisfies the following conditions:

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

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

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

d. for all 'x' in {1, ..., n}, certificate 'x' is valid.

Certificate validation requires verifying that all of the following conditions hold, in addition to the certification path validation criteria specified in Section 6 of [RFC5280].

1. The signature of certificate x (x>1) is verified using the public key of the issuer's certificate (x-1), using the signature algorithm specified for that public key (in certificate x-1).

2. The current time lies within the interval defined by the NotBefore and NotAfter values in the Validity field of certificate x.

3. The Version, Issuer, and Subject fields of certificate x satisfy the constraints established in Section 4.1-4.7 of [RFC6487].

4. Certificate x contains all the extensions that MUST be present, as defined in Section 4.8 of [RFC6487]. The value(s) for each of these extensions MUST be satisfy the constraints established for each extension in the respective sections. Any extension not identified in Section 4.8 MUST NOT appear in certificate x.

5. Certificate x MUST NOT have been revoked, i.e., it MUST NOT appear on a CRL issued by the CA represented by certificate x-1

6. Compute the VRS-IP and VRS-AS set values as indicated below:

   * If the IP Address Delegation extension is present in certificate x, compute the intersection of the resources between this extension and the value of the VRS-IP computed for certificate x-1. This becomes the new value of VRS-IP.

   * If the IP Address Delegation extension is absent in certificate x, set the value of VRS-IP to NULL.

Stephen Kent 7/14/2016 2:09 PM
Deleted: this

Stephen Kent 7/14/2016 2:10 PM
Deleted: specification.

Stephen Kent 7/14/2016 2:10 PM
Deleted: this specification

* If the AS Identifier Delegation extension is present in certificate x, compute the intersection of the resources between this extension and the value of the VRS-AS computed for certificate x-1. This becomes the new value of VRS-AS.

* If the AS Identifier Delegation extension is absent in certificate x, set the value of VRS-AS to NULL.

* If x = n (i.e., this is the certificate being validated), then:

  1. If IP Address Delegation extension is present, it is replaced with the intersection of the values from that extension and the value of the VRS-IP (computed from certificate x-1.

  2. If an AS Identifier Delegation extension is present, it is replaced with the intersection of the values from that extension and the value of the VRS-IP (computed from certificate x-1.

* If an RP is caching the results of validation, these values MAY be stored along with the certificate, to facilitate incremental validation based on cached results.

If x is < n, return to step 1 above.

These rules allow a certificate to contain resources that are not present in (all of) the certificates along the path from the trust anchor to the certificate, and still be viewed as valid. If none of the resources in a CA certificate are present in all certificates along the path, no subordinate certificates could be valid. However, the certificate is not immediately rejected as this may be a transient condition. Not immediately rejecting the certificate does not result in a security problem because the associated VRS sets accurately reflect the resources validly associated with the certificate in question.

4.2.2. ROA Validation

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

o 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.

Stephen Kent 7/14/2016 2:12 PM
Deleted: current

Stephen Kent 7/14/2016 2:12 PM
Deleted: current

Stephen Kent 7/15/2016 11:15 AM
Comment [1]: Your message said that you wanted the algorithm to apply to EE certificates too, so I'm not sure why the text still focuses on CA certificates. I modified the text slightly to red uce the references to CA certificates.

Stephen Kent 7/14/2016 2:13 PM
Deleted: CA

Stephen Kent 7/14/2016 2:13 PM
Deleted: CA

Stephen Kent 7/14/2016 2:15 PM
Deleted: the

Stephen Kent 7/14/2016 2:16 PM
Deleted: on

Stephen Kent 7/14/2016 2:17 PM
Deleted: on

o The IP address delegation extension [RFC3779] is present in the end-entity (EE) certificate (contained within the ROA), and each IP address prefix in the ROA is contained within the VRS-IP set that is specified as the result of EE certificate validation.

Note that this ensures that ROAs can be valid only, if all IP address prefixes in the ROA are encompassed by all certificates along the path to the trust anchor used to verify it.

Operators MAY issue separate ROAs for each IP address prefix, so that the loss of on IP address prefix from the VRS-IP of any certificate along the path to the trust anchor would not invalidate authorizations for other IP address prefixes.

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,
```


Stephen Kent 7/15/2016 11:18 AM
Deleted: (es)

Stephen Kent 7/15/2016 11:18 AM
Deleted: an outcome

Stephen Kent 7/14/2016 2:17 PM
Deleted: the VRS-IP of

Stephen Kent 7/15/2016 11:17 AM
Comment [2]: I've modified the bgpsec pki profile text so that it calls for use of the validation procedure in 6487 OR ANY RFC THAT UPDATES THIS PROCEDURE.

Stephen Kent 7/14/2016 2:18 PM
Deleted: 4.2.3. BGPsec Router Certificate Validation ... [1]

```
      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: over-claim 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 invalid):
       Issuer CA2,
       Subject R2,
       Resources 198.51.100.0/24

        EE certificate is invalid due to over-claim for 198.51.100.0/24

        Prefix 198.51.100.0/24, Max Length 24, ASN 64496

       ROA2 is considered invalid because he embedded EE certificate is
       considered invalid.

     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

EE certificate is invalid due to over-claim for AS64497

This problem can be mitigated by issuing separate certificates for each AS number.

5. Security Considerations

The authors believe that the revised validation algorithm introduces no new security vulnerabilities into the RPKI.

6. IANA Considerations

No updates to the registries are suggested by this document.

7. Acknowledgements

The authors would like to thank Stephen Kent for reviewing and contributing to this document.

8. References

8.1. Normative References

[I-D.ietf-sidr-bgpsec-pki-profiles]
Reynolds, M., Turner, S., 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>.

[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>.

[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

Daniel Shaw
African Network Information Centre (AFRINIC)
11th Floor, Standard Chartered Tower
Cybercity, Ebene
Mauritius

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