Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: January 19, 2018

A. Newton, Ed.
ARIN
C. Martinez-Cagnazzo, Ed.
LACNIC
D. Shaw
AFRINIC
T. Bruijnzeels
RIPE NCC
B. Ellacott
APNIC

July 18, 2017

RPKI Multiple "All Resources" Trust Anchors Applicability Statement
draft-rir-rpki-allres-ta-app-statement-02

Abstract

This document provides an applicability statement for the use of multiple, over-claiming 'all resources' (0/0) RPKI certificate authorities (CA) certificates used as trust anchors (TAs) operated by the Regional Internet Registry community to help mitigate the risk of massive downstream invalidation in the case of transient registry inconsistencies.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 19, 2018.

Table of Contents

1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Introduction

The RPKI is a hierarchical cryptologic system that uses X.509 certificates to match and validate holdership of Internet number resources. This validation follows the allocation change from IANA to an RIR, to an NIR or LIR, and ending with end users who make use of the address block. Since these allocations can be cryptographically validated, this can then be tied to assertions made by the holder of those number resources. As an improvement of this system, the RPKI was updated to add validation of origin routing announcements via ROAs. These ROAs can then be independently and cryptographically validated by third parties to assure themselves that the origin of the announcement as seen in the actual routing system is valid.

Since this system is envisioned to be used by network operators and ISPs to determine their routing decisions, there is a goal to be 100% correct 100% of the time. This goal could be achieved if the system was contained in a static environment where there is little or no movement of holdership changes from one organization to another of number resources. Unfortunately, this state cannot be achieved today, as movement of number resouces from from organization to organization is becoming common largely due to IPv4 scarcity.

Unfortunately, this state of 100% correctness at all times is infeasible in a model where separate entities are operating independently, yet rely critically on each others' perfect synchronisation at all times.

Because the current validation mechanism is all-or-nothing, any inconsistency at all at a high apex CA has the potential to invalidate a large number of additional Internet Number Resources. The higher the apex, and the larger the total set of INRs maintained by the CA, the greater the impact of even a small inconsistency.

As resources do change at high apex CAs for a variety of reasons, the likelihood of a small inconsistency is non-zero. And the likelihood of a transitional inconsistency is moderate. Due to the distributed nature of the RPKI repository mechanism, even if all CAs were able to operate in perfect synchronicity at all times, there is a reasonable likelihood that a given validating client may witness a temporarily inconsistent state of the system as a whole. A risk of wide-spread invalidity therefore exists as a very high impact and moderate likelihood event.

This brittleness in the RPKI validation rules has been identified and presented by the current RPKI TA operators to the IETF. A solution has also been proposed ([I-D.ietf-sidr-rpki-validation-reconsidered]), a solution that would allow for accidental over-claiming only to invalidate the resource that is incorrectly listed and allow the remaining to continue to be valid. As the implementation and deployment of solutions to this problem will occur according to timelines outside the control of the current TA operators, the workaround proposed in the present draft provides an acceptable trade-off.

3. Applicability to reduce overclaiming possibilities

The consequences of an RIR over-claiming are grave given that every ISP within their certificate would be invalidated. If routing was to be reliant on RPKI at this point, all routes announced by those ISPs below the affected RIR certificate would cease to work.

To mitigate risk and alleviate this threat, each RIR will move from a Trust Anchor that reflects their current holdings only, to one that reflects all holdings (e.g. 0/0). This will then ensure that over-claiming can not occur at a RIR level when dealing with transfers from one RIR to another. RPKI validators will not see the five Trust anchors from the RIRs as over-claiming and validation can proceed normally.

For those who may want to audit the RIRs to ensure that RIRs are not allocating the same IP addresses in separate regions, this can be done by matching the inventory of each RIR ([NROSTATS]) that is provided by the RIRs with the certificates issued by the RIRs within the RPKI.

Note that there will be minor changes from time to time to account for movements from IP address holdings that are in flight from one RIR to another and that transient overlaps can, and probably will, occur as inter-RIR transfers become more and more common.

4. Normative References

[I-D.ietf-sidr-rpki-validation-reconsidered]
Huston, G., Michaelson, G., Martinez, C., Bruijnzeels, T., Newton, A., and D. Shaw, "RPKI Validation Reconsidered", draft-ietf-sidr-rpki-validation-reconsidered-06 (work in progress), July 2016.

[NROSTATS]
"NRO Extended Stats File", July 2016, <https://www.nro.net/wp-content/uploads/apnic-uploads/delegated-extended>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

Authors' Addresses

Andrew Newton (editor)
ARIN
Chantilly VA
United States

Email: andy@arin.net

Carlos Martinez-Cagnazzo (editor)
LACNIC
Montevideo
Uruguay

Email: carlos@lacnic.net

Daniel Shaw
AFRINIC
Cybercity Ebene
Republic of Mauritius

Email: daniel@afrinic.net

Tim Bruijnzeels
RIPE NCC
Amsterdam
Netherlands

Email: tim@ripe.net

Byron Ellacott
APNIC
Brisbane
Australia

Email: bje@apnic.net