Network Working Group
Internet-Draft
Intended status: Informational
Expires: March 28, 2014

R. Bush
Internet Initiative Japan

September 24, 2013

RPKI Local Trust Anchor Use Cases
draft-ymbk-lta-use-cases-00

Abstract

There are a number of critical circumstances where a localized routing domain needs to augment or modify the Global RPKI. This document attempts to outline a few of them.

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 March 28, 2014.

Table of Contents

1. Introduction

Today RPKI-based Origin Validation, [RFC6811], relies on widespread deployment of the Global Resource Public Key Infrastructure (RPKI), [RFC6480]. In the future, RPKI-based Path Validation, [I-D.lepinski-bgpsec-overview], will be even more reliant on the Global RPKI.

But there are critical circumstances in which a local, well-scoped, administrative and/or routing domain will need to augment and/or modify their internal view of the Global RPKI.

This document attempts to lay out a few of those use cases. It is not intended to be autoritative, complete, or to become a standard. It merely tries to lay out a few critical examples to help scope the issues.

2. Suggested Reading

It is assumed that the reader understands the RPKI, see [RFC6480], the RPKI Repository Structure, see [RFC6481], Route Origin Authorizations (ROAs), see [RFC6482], and Ghostbusters Records, see [RFC6493].

3. What is 'Local'

The RPKI is a distributed database containing certificates, CRLs, manifests, ROAs, and Ghostbusters Records as described in [RFC6481]. Policies and considerations for RPKI object generation and maintenance are discussed elsewhere.

Like the DNS, the Global RPKI presents a single global view, although only a loosely consistent view, depending on timing, updating, fetching, etc. There is no 'fix' for this, it is not broken, it is the nature of distributed data with distributed caches.

There are critical uses of the RPKI where a local administrative and/or routing domain, e.g. an end-user site, a particular ISP or content provider, a geo-political region, ... may wish to have a special view of the RPKI.

For the purposes of this exploration, we refer to this localized view as a 'Local Trust Anchor', mostly for historical reasons, but also because implementation would likely be the local distribution of one or more specialized trust andchors, [RFC6481].

4. Example Uses

Carol, a RIPE member, is a victim of the "Dutch Court Attack" (someone convinces a Dutch court to force the RIPE/NCC to remove or modify records) and we all want to save the ability to route to Carol's network(s). There is need for some channel through which we can exchange some local trust command and data gorp necessary to create patches local to all our caches.

Bob has a multi-AS network under his administration and some of those ASs use private ([RFC1918]) or 'borrowed' US military space, and he wishes to certify them for use in his internal routing.

Alice runs the root trust for a large organization where upper management has the router geeks pointing their competitors' prefixes to pictures of kittens and unicorns, and Alice is responsible for making the CA hierarchy have validated certificates for those redirected resources and the rest of the internet.

5. Notes

In these examples, it is ultimately the ROAs, not the certificates, which one wants to modify. But one can't just hack new ROAs as one does not have the private keys needed to sign them. Hence one has to first hack the 3779 certificates.

But we should not lose sight of the goal that it is the ROAs and Ghostbuster Records which need re-issuing under the new 3779 certificates.

Further, since we're not the NSA, GCHQ, ..., we can not assume that we can reissue down from the root trust anchor at the IANA or from the RIRs' certificates. So we have to create a new trust anchor

which, for ease of use, will contain the new/hacked certificates and ROAs as well as the unmodified remainder of the Global RPKI.

And, because Alice, Bob, and Carol want to be able to archive, reproduce, and send to friends the data necessary to recreate their hacks, there will need to be a formally defind set of data which is input to a well-defind process to take an existing Global RPKI tree and produce the desired modified re-anchored tree.

6. Security Considerations

These use cases are all about violating global security, albeit within a constrained local context.

7. IANA Considerations

This document has no IANA Considerations.

8. Acknowledgments

The author wishes to thank Rob Austein.

9. References

9.1. Normative References

[RFC6481] Huston, G., Loomans, R., and G. Michaelson, "A Profile for Resource Certificate Repository Structure", RFC 6481, February 2012.

[RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", RFC 6482, February 2012.

[RFC6493] Bush, R., "The Resource Public Key Infrastructure (RPKI) Ghostbusters Record", RFC 6493, February 2012.

[RFC6811] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", RFC 6811, January 2013.

9.2. Informative References

[I-D.lepinski-bgpsec-overview]
Lepinski, M. and S. Turner, "An Overview of BGPSEC", draft-lepinski-bgpsec-overview-00 (work in progress), March 2011.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC4271] Rekhter, Y., Li, T., and S. Hares, "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, February 2012.

Author's Address

Randy Bush
Internet Initiative Japan
5147 Crystal Springs
Bainbridge Island, Washington 98110
US

Email: randy@psg.com