Secure Inter-Domain Routing
Internet-Draft
Intended status: Best Current Practice
Expires: January 4, 2015

D. Mandelberg
BBN Technologies

July 3, 2014

Simplified Local internet nUmber Resource Management with the RPKI
draft-dseomn-sidr-slurm-01

Abstract

The Resource Public Key Infrastructure (RPKI) is a global authorization infrastructure that allows the holder of Internet Number Resources (INRs) to make verifiable statements about those resources. Internet Service Providers (ISPs) can use the RPKI to validate BGP route origination assertions. Some ISPs locally use BGP with private address space or private AS numbers (see RFC6890). These local BGP routes cannot be verified by the global RPKI, and SHOULD be considered invalid based on the global RPKI (see RFC6491). The mechanisms described below provide ISPs with a way to make local assertions about private (reserved) INRs while using the RPKI's assertions about all other INRs.

Table of Contents

1. Introduction 2
1.1. Terminology 3
2. Validation Output Filtering 3
3. Locally Adding Assertions 4
4. Configuring SLURM 4
5. Combining Mechanisms 5
6. IANA Considerations 6
7. Security Considerations 6
8. Acknowledgements 6
9. References 6
9.1. Informative References 6
9.2. Normative References 7
Appendix A. Example SLURM File 7
Author's Address 8

1. Introduction

The Resource Public Key Infrastructure (RPKI) is a global authorization infrastructure that allows the holder of Internet Number Resources (INRs) to make verifiable statements about those resources. For example, the holder of a block of IP(v4 or v6) addresses can issue a Route Origination Authorization (ROA) [RFC6482] to authorize an Autonomous System (AS) to originate routes for that block.

Internet Service Providers (ISPs) can then use the RPKI to validate BGP routes. However, some ISPs locally use BGP with private address space ([RFC1918], [RFC4193], [RFC6598]) or private AS numbers ([RFC1930], [RFC6996]). These local BGP routes cannot be verified by the global RPKI, and SHOULD be considered invalid when using the RPKI. For example, [RFC6491] recommends the creation of ROAs that would invalidate routes for reserved and unallocated address space.

This document specifies two new mechanisms to enable ISPs to make local assertions about some INRs while using the RPKI's assertions about all other INRs. These mechanisms support the second and third use cases in [I-D.ietf-sidr-lta-use-cases]. The second use case describes use of [RFC1918] addresses or use of public address space not allocated to the ISP that is using it. The third use case describes a situation in which an ISP publishes a variant of the RPKI hierarchy (for its customers). In this variant some prefixes and/or AS numbers are different from what the RPKI repository system presents to the general ISP population. The result is that routes for consumers of this variant hierarchy will be re-directed (via routing).

Both mechanisms are specified in terms of abstract sets of assertions. For Origin Validation [RFC6483], an assertion is a tuple of {IP prefix, prefix length, maximum length, AS number} as used by rpki-rtr [RFC6810]. Output Filtering, described in Section 2, filters out any assertions by the RPKI about locally reserved INRs. Locally Adding Assertions, described in Section 3, adds local assertions about locally reserved INRs. Note that both of these mechanisms can later be extended to cover any assertions made by the RPKI for use in BGPSEC [I-D.ietf-sidr-bgpsec-protocol].

In general, the primary output of an RPKI relying party is the data it sends to routers over the rpki-rtr protocol. The rpki-rtr protocol enables routers to query a relying party for all Origin Validation assertions it knows about (Reset Query) or for an update of only the changes in Origin Validation assertions (Serial Query). The mechanisms specified in this document are to be applied to the result set for a Reset Query, and to both the old and new sets that are compared for a Serial Query. Relying party software MAY modify other forms of output in comparable ways, but that is outside the scope of this document.

This document is intended to supersede [I-D.ietf-sidr-ltamgmt] while focusing only on local management of private INRs. Another draft [I-D.kent-sidr-suspenders] focuses on the other aspects of local management.

1.1. Terminology

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 [RFC2119].

2. Validation Output Filtering

To prevent the global RPKI from affecting routes with locally reserved INRs, a relying party is locally configured with a list of IP prefixes and/or AS numbers that are used locally, and taken from the reserved INR spaces. Any Origin Validation assertions where the IP prefix is equal to or subsumed by a locally reserved IP prefix, are removed from the relying party’s output. Any Origin Validation assertions where the IP prefix contains a locally reserved IP prefix are removed and the relying party software SHOULD issue a warning.

3. Locally Adding Assertions

Each relying party is locally configured with a (possibly empty) list of Origin Validation assertions. This list is added to the relying party's output.

4. Configuring SLURM

Relying party software SHOULD support the following configuration format for Validation Output Filtering and Locally Adding Assertions. The format is defined using the Augmented Backus-Naur Form (ABNF) notation and core rules from [RFC5234] and the rules <IPv4address> and <IPv6address> from Appendix A of [RFC3986]. Each <del> command specifies an INR to use for Validation Output Filtering. Each <add> command specifies an assertion to use for Locally Adding Assertions. See Appendix A for an example SLURM file.

```
SLURMFile = header *line

header = %x53.4c.55.52.4d SP "1.0" CRLF ; "SLURM 1.0"

line =  *WSP [comment] CRLF
      / *WSP command [ 1*WSP [comment] ] CRLF

comment = "#" *(VCHAR / WSP)

command = add / del

add = %x61.64.64 1*WSP IPprefixMaxLen 1*WSP ASnum

del = %x64.65.6c 1*WSP inr

inr = IPprefix / ASnum

IPprefix = IPv4prefix / IPv6prefix

IPprefixMaxLen = IPv4prefixMaxLen / IPv6prefixMaxLen

IPv4prefix = IPv4address "/" 1*2DIGIT

IPv6prefix = IPv6address "/" 1*3DIGIT

; In the following two rules, if the maximum length component is
; missing, it is treated as equal to the prefix length.
IPv4prefixMaxLen = IPv4prefix ["-" 1*2DIGIT]
IPv6prefixMaxLen = IPv6prefix ["-" 1*3DIGIT]

ASnum = 1*DIGIT
```

5. Combining Mechanisms

In the typical use case, a relying party uses both output filtering and locally added assertions. In this case, the resulting assertions MUST be the same as if output filtering were performed before locally adding assertions. I.e., locally added assertions MUST NOT be removed by output filtering.

If a relying party chooses to use both SLURM and Suspenders [I-D.kent-sidr-suspenders], the SLURM mechanisms MUST be performed on the output of Suspenders.

6. IANA Considerations

TBD

7. Security Considerations

The mechanisms described in this document provide an ISP additional control over its own network. Care should be taken in how that control is used.

8. Acknowledgements

The author would like to thank Stephen Kent for his guidance and detailed reviews of this document.

9. References

9.1. Informative References

[I-D.ietf-sidr-bgpsec-protocol]
Lepinski, M., "BGPSEC Protocol Specification", draft-ietf-sidr-bgpsec-protocol-08 (work in progress), November 2013.

[I-D.ietf-sidr-lta-use-cases]
Bush, R., "RPKI Local Trust Anchor Use Cases", draft-ietf-sidr-lta-use-cases-01 (work in progress), June 2014.

[I-D.ietf-sidr-ltamgmt]
Reynolds, M., Kent, S., and M. Lepinski, "Local Trust Anchor Management for the Resource Public Key Infrastructure", draft-ietf-sidr-ltamgmt-08 (work in progress), April 2013.

[I-D.kent-sidr-suspenders]
Kent, S. and D. Mandelberg, "Suspenders: A Fail-safe Mechanism for the RPKI", draft-kent-sidr-suspenders-01 (work in progress), March 2014.

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

[RFC1930] Hawkinson, J. and T. Bates, "Guidelines for creation, selection, and registration of an Autonomous System (AS)", BCP 6, RFC 1930, March 1996.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, October 2005.

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

[RFC6483] Huston, G. and G. Michaelson, "Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs)", RFC 6483, February 2012.

[RFC6491] Manderson, T., Vegoda, L., and S. Kent, "Resource Public Key Infrastructure (RPKI) Objects Issued by IANA", RFC 6491, February 2012.

[RFC6598] Weil, J., Kuarsingh, V., Donley, C., Liljenstolpe, C., and M. Azinger, "IANA-Reserved IPv4 Prefix for Shared Address Space", BCP 153, RFC 6598, April 2012.

[RFC6810] Bush, R. and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol", RFC 6810, January 2013.

[RFC6890] Cotton, M., Vegoda, L., Bonica, R., and B. Haberman, "Special-Purpose IP Address Registries", BCP 153, RFC 6890, April 2013.

[RFC6996] Mitchell, J., "Autonomous System (AS) Reservation for Private Use", BCP 6, RFC 6996, July 2013.

9.2. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

Appendix A. Example SLURM File

```
SLURM 1.0

# Reserve 192.0.2.0/24 and 2001:DB8::/32 for local use.
del 192.0.2.0/24
del 2001:DB8::/32

# Allow either 65536 or 65537 to originate routes to 192.0.2.0/24.
add 192.0.2.0/24 65536
add 192.0.2.0/24 65537

add 2001:DB8::/48-52 65536 # 65536 originates 2001:DB8::/48 and
                           # sub-prefixes down to length 52.
add 2001:DB8:0:42::/64 65537 # However, 65537 originates
                             # 2001:DB8:0:42::/64.
add 2001:DB8:1::/48 65537 # 65537 also originates 2001:DB8:1::/48
```

Author’s Address

David Mandelberg
BBN Technologies
10 Moulton St.
Camridge, MA 02138
US

Email: david@mandelberg.org