Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: February 7, 2013

R. Gagliano
K. Patel
B. Weis
Cisco Systems

August 6, 2012

BGPSEC router key rollover as an alternative to beaconing
draft-sidr-bgpsec-rollover-00

Abstract

The current BGPSEC draft documents do not specifies a key rollover process for routers. This document describes a possible key rollover process and explores its impact to mitigate replay attacks and eliminate the need for beaconing in BGPSEC.

Status of this Memo

Copyright Notice

Table of Contents

1. Requirements notation

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. Introduction

In BGPSEC, a key rollover (or re-keying) is the process of changing the router's key pair, issuing the correspondent new End-Entity certificates and revoke the old certificate. This process will need to happen at regular intervals normally due to local policies at each network.

During a rollover process, a router needs to generate BGP UPDATE messages in order to signal the new key to be used to its neighbors. So, intuitively, a frequent key rollover process has similar effects as the beaconing process proposed by the BGPSEC base documents to protect a BGPSEC attribute against a re-play attack. However, there are a number of operational details to be considered if the expire time field in the BGPSEC attribute is removed.

This document details a possible key rollover process in BGPSEC and explores the operational environment where key rollovers could be used as a protection against a re-play attach against BGPSEC

3. Key rollover in BGPSEC

The key rollover process in BGPSEC has not been well defined yet. However, this will be a mandatory process due to some of the following causes:

BGPSEC scheduled rollover: BGPSEC certificates have an expiration date (NotValidAfter). Although it is possible to generate a new certificate without changing the key pair, it is normally good practice to adopt the policy of using a new key pair in every rollover event.

BGPSEC certificate fields changes: A BGPSEC certificate field's information (such as the ASN or the Subject) may need to be changed. The normal process requires the rollover of the old certificate with a new key pair and the revocation of the old certificate.

BGPSEC emergency rollover Some special circumstances (such as a compromised key) may require the rollover of a BGPSEC certificate.

It should be clear at this point that a key rollover process is required for BGPSEC. The next section describes how this process may be implemented.

3.1. A proposed process for BGPSEC key rollover

The BGPSEC key rollover process should be very tighten to the key provisioning mechanisms that would be in place. The key provisioning mechanisms for BGPSEC are not yet documented. We will assume that such an automatic provisioning mechanism will be in place (a possible provisioning mechanism when the private key lives only inside the BGP speaker is the Enrollment over Secure Transport (EST). This protocol will allow BGPSEC code to include automatic re-keying scripts with minimum development cost.

When the same private key is shared by different routers, a mechanism to distribute the private key will need to be implemented. A possible solution may include the transmission of the private key over a secure channel. The PKIX WG has started work on this sense by adopting [I-D.ietf-pkix-cmc-serverkeygeneration]

If we work under the assumption that an automatic mechanism will exist to rollover a BGPSEC certificate, a possible process could be:

1. New Certificate Pre-Publication: The first step in the rollover mechanism is to pre-publish the new public key. In order to

accomplish this goal, the new key pair and certificate will need to be generated and published on the correspondent RPKI repository. This process will vary in every environment as it will depend on where the keys are located (either in every router or on a centralized server), if the RPKI CA is hosted at the ISP or at an external party (i.e. needs to use the RPKI provisioning protocol) and finally if the repository is also local or hosted (i.e. will need to use the RPKI-Repository protocol.)

2. Stage Period: A stage period will be required from the time a new certificate is published in the RPKI global repository until the time it is fetched by RPKI caches around the globe. The exact minimum staging time is not clear and will require experimental results from RPKI. Design documents mention a lower limit of 24 hours. If rollovers will be done frequently and we want to avoid the stage period in case of emergency rollover needs, an administrator can always provision two certificate for every router. In this case when the rollover operation is needed, the cache servers around the globe would already have the new keys.

3. Twilight: At this moment, the BGP speaker that uses the key been rolled-over will stop using the OLD key for signing and start using the NEW key. Also, the router will generate appropriate BGP UPDATES just as in the typical operation of refreshing out-bound BGP polices. This operation may generate a great number of BGP UPDATE messages. In any given BGP SPEAKER, the Twilight moment may be different for every peer in order to distribute the system load.

4. CRL Publication: As part of the rollover process, a CA MAY decide that it will publish the serial number of the OLD BGPSEC certificate on its CRL. It may also be the case that the CA will just let the certificate to expire and not update its CRL.

5. RPKI-Router Protocol Withdrawal: Either due to the inclusion of the OLD certificate serial number or the expiration of the certificate's validation, the RPKI cache servers around the globe will need to communicate to its RTR peers that the OLD certificate's public key is not longer valid (rtr withdrawal message). It is not documented yet what will be a router's reaction to a RTR withdrawal message but it should include the removal of any RIB entry that includes a BGPSEC attribute signed with that key and the generation of the correspondent BGP WITHDRAWS (either implicit or explicit).

The proposed rollover mechanism will depend on the existence of an automatic provisioning process for BGPSEC certificates, it will require a staging mechanism given by RPKI propagation time of around

24hours and it will generate BGP UPDATES for all prefixes in the router been re-keying.

The first two steps (New Certificate Pre-Publication and Stage Period) could happen ahead of time from the rest of the process as network operators could prepare itself to accelerate a future key roll-over.

4. BGPSEC key rollover as a measure against replays attacks in BGPSEC

There are two typical measures to mitigate replay attacks: addition of a timestamp or addition of a serial number. Currently BGPSEC offers a timestamp (expiration time) as a protection against re-play attacks of BGPSEC messages. The process requires all BGP Speakers that originate a BGP UPDATE to beaconing the message before its expiration time. This requirement changes a long standing BGP operation practice and the community have been searching for alternatives.

4.1. BGPSEC Re-play attack window requirement

In [I-D.ietf-sidr-bgpsec-reqs] Sections 3.7 and 4.3, the replay attack requirements are set. One important comment is that during the windows of exposure, a replay attack is only effective if there was a downstream topology change that makes the signed AS path not longer current. In other words, if there has been no topology changes, no security threat comes from a replay of a BGP UPDATE message.

The BGPSEC Ops document give some ideas of requirements for the re-play attack in BGPSEC. For the vast majority of the prefixes, the requirement will be in the order of days or weeks. For a very small fraction, but critical, of the prefixes, the requirement may be in the order of hours.

4.2. BGPSEC key rollover as a mechanism to protect against replay attacks

The question we would like to ask is: can key rollover provide us a similar protection against re-play attacks without the need for beaconing?

The answer is that YES when the window requirement is in the order of days and the router re-keying is the edge router of the origin AS. By using re-keying, you are letting the BGPSEC certificate validation time as your timestamp against replay attacks. However, the use of frequent key rollovers comes with an additional administrative cost and risks if the process fails. As documented before, re-keying should be supported by automatic tools and for the great majority of the Internet it will be done with good lead time to correct any inconvenient in the process.

For a transit AS that also originates its BGP UPDATES for its own prefixes, the key rollover process may generate a large number of UPDATE messages (even the complete DFZ). For this reason, it is recommended that routers in this scenario been provisioned with two

certificates: one to sign BGP UPDATES in transit and a second one to sign BGP UPDATE for prefixes originated in its AS. Only the second certificate should be frequently rolled-over. Consequently, the transit BGPSEC certificate is expected to be longer living than the origin BGPSEC certificate.

Advantage of Re-keying as re-play attack protection mechanism:

1. Does not require beaconing

2. All timestamps policies are maintained in RPKI

3. Additional administrative cost is paid by the provider that wants to protect its infrastructure

4. Can be implemented in coordination with planned topology changes by either origin ASes or transit ASes (if I am changing providers, I rollover)

5. Eliminates the discussion on who has the authority over the expiration time

Disadvantage of Re-keying as re-play attack protection mechanism:

1. More administrative load due to frequent rollover, although how frequent is still not clear.

2. Minimum window size bounded by RPKI propagation time to RPKI caches. If pre-provisioning done ahead of time, it means 24 hours minimum in paper. However, more experimentation is needed when RPKI and cache servers are more massively deployed.

3. Increases dynamic of RPKI repository

4. More load on RPKI caches, but they are meant to do this work.

5. IANA Considerations

No IANA considerations

6. Security Considerations

No security considerations.

7. Acknowledgements

We would like to acknowledge Randy Bush, Sriram Kotikalapudi, Stephen Kent and Sandy Murphy.

8. References

8.1. Normative References

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

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

[RFC5101] Claise, B., "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information", RFC 5101, January 2008.

[RFC5102] Quittek, J., Bryant, S., Claise, B., Aitken, P., and J. Meyer, "Information Model for IP Flow Information Export", RFC 5102, January 2008.

8.2. Informative References

[I-D.ietf-pkix-cmc-serverkeygeneration]
Schaad, J., Timmel, P., and S. Turner, "CMC Extensions: Server Key Generation", draft-ietf-pkix-cmc-serverkeygeneration-00 (work in progress), January 2012.

[I-D.ietf-sidr-bgpsec-reqs]
Bellovin, S., Bush, R., and D. Ward, "Security Requirements for BGP Path Validation", draft-ietf-sidr-bgpsec-reqs-03 (work in progress), March 2012.

[I-D.ietf-sidr-bgpsec-threats]
Kent, S. and A. Chi, "Threat Model for BGP Path Security", draft-ietf-sidr-bgpsec-threats-02 (work in progress), February 2012.

[I-D.ietf-sidr-origin-validation-signaling]
Mohapatra, P., Patel, K., Scudder, J., Ward, D., and R. Bush, "BGP Prefix Origin Validation State Extended Community", draft-ietf-sidr-origin-validation-signaling-00 (work in progress), November 2010.

[I-D.ietf-sidr-pfx-validate]
Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", draft-ietf-sidr-pfx-validate-01 (work in progress), February 2011.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

Authors' Addresses

Roque Gagliano
Cisco Systems
Avenue des Uttins 5
Rolle, VD 1180
Switzerland

Email: rogaglia@cisco.com

Keyur Patel
Cisco Systems
170 W. Tasman Driv
San Jose, CA 95134
CA

Email: keyupate@cisco.com

Brian Weis
Cisco Systems
170 W. Tasman Driv
San Jose, CA 95134
CA

Email: bew@cisco.com