Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: October 17, 2013

R.G.M. Gagliano
K.P. Patel
B.W. Weis
Cisco Systems

April 15, 2013

BGPSEC router key rollover as an alternative to beaconing
draft-ietf-sidr-bgpsec-rollover-02

Abstract

BGPSEC will need to address the impact from regular and emergency rollover processes for the BGPSEC End-Entity (EE) certificates that will be performed by Certificate Authorities (CAs) participating at the Resource Public Key Infrastructure (RPKI). This document provides general recommendations for that process and specifies how this process is used to control BGPSEC's window of exposure to replay attacks.

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 October 17, 2013.

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 a router's key pair (or pairs), issuing the corresponding new End-Entity certificate and (if the old certificate is still valid) revoking the old certificate. This process will need to happen at regular intervals, normally due to local policies at each network. This document provides general recommendations for that process that Certificate Practice Statements (CPS) documents MAY reference.

When a router receives (or creates depending of the key provisioning mechanism to be selected) a new key pair, this key pair will be used to sign new BGP UPDATE messages that are originated or that transit through the BGP speaker. Additionally, the BGP speaker MUST refresh its outbound BGP UPDATE messages to update its respective BGPSEC attribute by including the correspondent signature performed with the new key. When the rollover process finishes, the old BGPSEC certificate (and its key) will not longer be valid and thus any BGP UPDATE that includes a BGPSEC attribute with a signature performed by

the old key will be invalid. Consequently, if the router do not refresh its outbound BGP UPDATE messages, routing information may be lost after the rollover process is finished.

As a key rollover process invalidates BGP UPDATE messages signed with the old key, frequent key rollover processes could be used to control BGPSEC's window of exposure to replay attacks as required by [I-D.ietf-sidr-bgpsec-reqs]. This document explores the operational environment to achieve this goal.

In [I-D.ietf-sidr-rtr-keying], the "operator-driven" method is introduced and it enables that a key pair could be shared among different BGP Speakers. In this scenario, the roll-over of the correspondent BGPSEC certificate will impact all the BGP Speakers sharing the same private key.

3. Key rollover in BGPSEC

A BGPSEC EE certificate (as any X.509 certificate) will required a rollover process due to causes such as:

BGPSEC scheduled rollover: BGPSEC certificates have an expiration date (NotValidAfter) that requires a frequent rollover process. The validity period for these certificates is typically expressed at the CA's CPS document.

BGPSEC certificate fields changes: Information contained in a BGPSEC certificate (such as the ASN or the Subject) may need to be changed.

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

In most of these cases (probably excepting when the key has been compromised), it is possible to generate a new certificate without changing the key pair. This practice simplifies the rollover process as the correspondent BGP speakers do not even need to be aware of the changes to its correspondent certificate. However, not replacing the certificate key for a long period of time increases the risk that the certificate key may be compromised.

3.1. A proposed process for BGPSEC key rollover

The BGPSEC key rollover process should be dependent of the key provisioning mechanisms that would be in place. The key provisioning mechanisms for BGPSEC are not yet fully documented (see [I-D.ietf-sidr-rtr-keying] as a work in progress document). We will

assume that an automatic provisioning mechanism will be in place. (A possible provisioning mechanism is the Enrollment over Secure Transport (EST) [I-D.ietf-pkix-est]). That protocol will allow BGPSEC code to include automatic re-keying scripts with minimum development cost.

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 a new certificate. In order to accomplish this goal, the new key pair and certificate will need to be generated and published at the appropriate RPKI repository publication point. The details of this process will vary as they depend on whether the keys are assigned per-BGP speaker or shared, whether the keys are generated on each BGP speaker or in a central location and wether the RPKI repository is locally or externally hosted.

2. Staging Period: A staging 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 operations. RPKI repository design documents mention a lower limit of 24 hours (NOTE: need reference only one I found is the ops document). If rollovers will be done frequently and we want to avoid the stage period, an administrator can always provision two certificate for every router. In this case when the rollover operation is needed, the relying parties around the globe would already have the new keys. A staging period may not be possible to implement during emergency key rollover, in which case routing information may be lost.

3. Twilight: At this moment, the BGP speaker that hold the private key that has 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 (due to the need to refresh BGP outbound policies). In any given BGP SPEAKER, the Twilight moment may be different for every peer in order to distribute the system load (probably in the order of minutes to avoid reaching any expiration time).

4. Certificate Revocation: This is an optional step. As part of the rollover process, a CA MAY decide to revoke the OLD certificate by publishing its serial number on the CA's CRL. On the other

side, the CA will just let the OLD certificate to expire and not revoke it. This chose will depend on the reasons that motivated the rollover process.

5. RPKI-Router Protocol Withdrawals: Either due to the revocation of the OLD certificate or to the expiration of the OLD certificate's validation, the RPKI relying parties around the globe will need to communicate to their 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 WITHDRAWALs (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 based on the RPKI propagation time of around 24hours, and it will generate BGP UPDATES for all prefixes in the router been re-keyed.

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

When a new BGPSEC certificate is generated without changing its key, steps 3 (Twilight) and 5 (RPKI-Router Protocol Withdrawals) SHOULD not be executed.

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

There are two typical generic measures to mitigate replay attacks in any protocol: the addition of a timestamp or the addition of a serial number. Currently BGPSEC offers a timestamp (expiration time) as a protection against re-play attacks of BGPSEC attributes. The process requires all BGP Speakers that originate a BGP UPDATE to re-advertise ("beacon") the message before it expires. This requirement changes a long standing BGP operational practice and the community has been searching for alternatives.

4.1. BGPSEC Replay attack window requirement

In [I-D.ietf-sidr-bgpsec-reqs] Section 4.3, the need to limit the vulnerability to replay attacks is described. One important comment is that during a windows of exposure, a replay attack is effective only if there was a downstream topology change that makes the signed AS path not longer current. In other words, if there have been no

topology changes, no security threat comes from a replay of a BGP UPDATE message (the signed information is still valid)

The BGPSEC Ops document [I-D.ietf-sidr-bgpsec-ops] gives some ideas of requirements for the size of the BGPSEC windows of exposure to replay attacks. At that document, it is stated that for the vast majority of the prefixes, the requirement will be in the order of days or weeks. For a very small but critical fraction 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 the key rollover process earlier described provide a similar protection against replay attacks without the need for beaconing?

The answer is that YES when the window requirement is in the order of days and the BGP speaker re-keying is the edge router of the origin AS and the full process is completed (i.e. the OLD and NEW certificate do not share the same key). 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 risk.

For a transit AS that also originates BGP UPDATES for its own prefixes, the key rollover process may generate a large number of UPDATE messages (even the complete Default Free Zone or 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 (for prefixes originated in its AS) should be rolled-over frequently as a means of limiting replay attach windows. The transit BGPSEC certificate is expected to be longer living than the origin BGPSEC certificate.

Advantage of Re-keying as replay attack protection mechanism:

1. Does not require beaconing

2. All expiration policies are maintained in RPKI

3. Most of the additional administrative cost is paid by the provider that wants to protect its infrastructure (RP load will increase as there is a need to validate more BGPSEC certificates)

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 replay attack protection mechanism:

1. More administrative load due to frequent rollover, although how frequent is still not clear. Some initial ideas in [I-D.ietf-sidr-bgpsec-ops]

2. Minimum window size bounded by RPKI propagation time to RPKI caches for new certificate and CRL (2x propagation time). If pre-provisioning done ahead of time the minimum windows size is reduced (to 1x propagation time for the CRL). However, more experimentation is needed when RPKI and RPs are more massively deployed.

3. Increases dynamics and size 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.

[RFC6489] Huston, G., Michaelson, G., and S. Kent, "Certification Authority (CA) Key Rollover in the Resource Public Key Infrastructure (RPKI)", BCP 174, RFC 6489, February 2012.

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-pkix-est]
Pritikin, M., Yee, P., and D. Harkins, "Enrollment over Secure Transport", draft-ietf-pkix-est-02 (work in progress), July 2012.

[I-D.ietf-sidr-bgpsec-ops]
Bush, R., "BGPsec Operational Considerations", draft-ietf-sidr-bgpsec-ops-05 (work in progress), May 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-rtr-keying]
Turner, S., Patel, K., and R. Bush, "Router Keying for BGPsec", draft-ietf-sidr-rtr-keying-00 (work in progress), May 2012.

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