Network Working Group   R. Gagliano
Internet-Draft   K. Patel
Intended status: Standards Track   B. Weis
Expires: September 22, 2016   Cisco Systems
                                                         March 21, 2016

                  BGPsec Router Certificate Rollover
                  draft-ietf-sidr-bgpsec-rollover-05

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). Rollovers of BGPsec
   EE certificates must be carefully managed in order to synchronize
   distribution of router public keys and the usage of those pubic keys
   by BGPsec routers. This document provides general recommendations
   for that process, as well as describing reasons why the rollover of
   BGPsec EE certificates might be necessary.

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 September 22, 2016.

carefully, as they describe your rights and restrictions with respect
to this document. Code Components extracted from this document must
include Simplified BSD License text as described in Section 4.e of
the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.

Table of Contents

1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "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.
Certificate Practice Statements (CPS) documents MAY reference these
recommendations. This memo only addresses changing of a router's key
pair within the RPKI. Refer to [RFC6489] for a procedure to rollover
RPKI Certificate Authority key pairs.

When a router receives or creates a new key pair (depending on the
key provisioning mechanism to be selected), this key pair will be
used to sign new BGPsec_Path attributes

[I-D.ietf-sidr-bgpsec-protocol] that are originated or that transit
through the BGP speaker. Additionally, the BGP speaker MUST refresh
its outbound BGPsec Update messages to include a signature using the
new key (replacing the replaced key). When the rollover process
finishes, the old BGPsec certificate (and its key) will not longer be
valid and thus any BGPsec Update that includes a BGPsec_Path
attribute with a signature performed by the old key will be invalid.
Consequently, if the router does not refresh its outbound BGPsec
Update messages, routing information may be treated as
unauthenticated after the rollover process is finished. It is
therefore extremely important that the BGPsec router key rollover be
performed such that the probability of new router EE certificates
have been distributed throughout the RPKI before the router begin
signing BGPsec_Path attributes with a new private key.

It is also important for an AS to minimize the BGPsec router key
rollover interval (i.e., in between the time an AS distributes an EE
certificate with a new public key and the time a BGPsec router begins
to use its new private key). This can be due to a need for a BGPsec
router to distribute BGPsec_Path attributes signed with a new private
key in order to invalidate BGPsec_Path attributes signed with the old
private key. In particular, if the AS suspects that a stale
BGPsec_Path attribute is being distributed instead of the most
recently signed attribute it can cause the stale BGPsec_Path
attribute to be invalidated by completing a key rollover procedure.
The BGPsec rollover interval can be minimized when an automated
certificate provisioning process such as Enrollment over Secure
Transport (EST) [RFC7030]) is used.

The Security Requirements for BGP Path Validation [RFC7353] also
describes the need for protecting against the replay of BGP UPDATE
messages, such as controlling BGPsec's window of exposure to replay
attacks. The BGPsec rollover method in this document can be used to
achieve this goal.

In [I-D.ietf-sidr-rtr-keying], the "operator-driven" method is
introduced, in which a key pair can 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

An BGPsec EE certificate SHOULD be replaced when the following events
occur, and can be replaced for any other reason at the discretion of
the AS responsible for the EE certificate.

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.

BGPsec signature anti-replay protection An AS may determine stale
       BGPsec_Path attributes signed by the AS are being propagated
       instead of the most recently signed BGPsec_Path attributes.
       Changing the BGPsec router signing key, distributing a new
       BGPsec EE certificate for the router,and revoking the old
       BGPsec EE certificate will invalidate the replayed BGPsec_Path
       attributes.

In some of these cases it is possible to generate a new certificate
without changing the key pair. This practice simplifies the rollover
process as the corresponding 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 router private key may be compromised. Distributing
the OLD public key in a new certificate is NOT RECOMMENDED when the
rollover event is due to the key has been compromised or stale
BGPsec_Path attribute signatures are being distributed.

3.1. A proposed process for BGPsec key rollover

The BGPsec key rollover process will be dependent on the key
provisioning mechanisms that are adopted by an AS. The key
provisioning mechanisms for BGPsec are not yet fully documented (see
[I-D.ietf-sidr-rtr-keying] as a work in progress document). It is
assumed that an automatic provisioning mechanism such as EST will be
in place as such a provisioning mechanism 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 RECOMMENDED process is as
follows.

1. New Certificate Publication: The first step in the rollover
    mechanism is to 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
whether 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 will be dictated by the conventional
    interval chosen between repository fetches. If rollovers will be
    done more frequently, an administrator can provision two
    certificates for every router concurrently with different valid
    start times. 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 holds 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 BGPsec_Path attributes just as in the
    typical operation of refreshing out-bound BGP polices. This
    operation may generate a great number of BGPsec_Path attributes
    (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, but SHOULD be
    taken when the goal is to invalidate signatures used with the OLD
    key. Reasons to invalidate OLD signatures include when the AS
    has reason to believe that the router signing key has been
    compromised, and when the AS needs to invalidate BGPsec_Path
    attribute signatures used with this key. 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 choice will depend on the reasons that motivated the
    rollover process.

5. RPKI-Router Protocol Withdrawals: At the expiration of the OLD
    certificate's validation, the RPKI relying parties around the
    globe will need to communicate to their router peers that the OLD
    certificate's public key is not longer valid (e.g., using the
    RPKI-Router Protocol described in [RFC6810]). It is not

documented yet what will be a router's reaction to a message with
the withdrawal bit set to 1 in the RPKI-Router Protocol, 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 24 hours, and it will generate BGPsec_Path attributes for all
prefixes in the router been re-keyed.

The first two steps (New Certificate Publication and Staging Period)
may happen in advance of the rest of the process. This will allow a
network operator to accelerate its subsequent 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. However neither BGP nor BGPsec provide either measure. This
section discusses the use of BGPsec Rollover as a measure to mitigate
replay attacks.

4.1. BGPsec Replay attack window requirement

In [RFC7353] Section 4.3, the need to limit the vulnerability to
replay attacks is described. One important comment is that during a
window of exposure, a replay attack is effective only in very
specific circumstances: there is a downstream topology change that
makes the signed AS path no longer current, and the topology change
makes the replayed route preferable to the route associated with the
new update. In particular, if there have been no topology change at
all, then no security threat comes from a replay of a BGPsec_Path
attribute because 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.

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

   Since the window requirement is in the order of a day (as documented
   in [I-D.ietf-sidr-bgpsec-ops]) and the BGP speaker re-keying is the
   edge router of the origin AS, it is feasible for a BGPsec Rollover to
   mitigate replays. In this case it is important to complete the full
   process (i.e. the OLD and NEW certificate do not share the same key).
   By re-keying an AS is letting the BGPsec certificate validation time
   be a sort of "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 BGPsec_Path attributes 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 BGPsec_Path attributes
   in transit and a second one to sign an BGPsec_Path attribute 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. All expiration policies are maintained in RPKI

   2. Much of the additional administrative cost is paid by the
       provider that wants to protect its infrastructure, as it bears
       the human cost of creating and initiating distribution of new
       router key pairs and router EE certificates. (It is true that
       the cost of relying parties will be affected by the new objects,
       but their responses should be completely automated or otherwise
       routine.)

   3. Can be implemented in coordination with planned topology changes
       by either origin ASes or transit ASes (e.g., if an AS changes
       providers, it completes a BGP Rollover)

   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
    provisioning is done ahead of time the minimum window 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.

5. IANA Considerations

No IANA considerations

6. Security Considerations

Several possible reasons can cause routers participating in BGPsec to
replace rollover their signing keys and/or signatures containing
their current signature verification key. Some reasons are due to
the usual key management operations reasons (e.g.,key exposure,
change of certificate attributes, due to policy). However BGPsec
routers also may need to change their signing keys and associated
certificate as an anti-replay protection.

The BGPsec Rollover method allows for an expedient rollover process
when router certificates are distributed through the RPKI, but
without causing routing failures due to a receiving router not being
able to validate a BGPsec_Path attribute created by a router that is
the subject of the rollover.

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,
            DOI 10.17487/RFC2119, March 1997,
            <http://www.rfc-editor.org/info/rfc2119>.

8.2. Informative References

[I-D.ietf-sidr-bgpsec-ops]
            Bush, R., "BGPsec Operational Considerations", draft-ietf-
            sidr-bgpsec-ops-07 (work in progress), December 2015.

   [I-D.ietf-sidr-bgpsec-protocol]
              Lepinski, M. and K. Sriram, "BGPsec Protocol
              Specification", draft-ietf-sidr-bgpsec-protocol-15 (work
              in progress), March 2016.

   [I-D.ietf-sidr-rtr-keying]
              Bush, R. and K. Patel, "Router Keying for BGPsec", draft-
              ietf-sidr-rtr-keying-10 (work in progress), November 2015.

   [RFC6489] Huston, G., Michaelson, G., and S. Kent, "Certification
              Authority (CA) Key Rollover in the Resource Public Key
              Infrastructure (RPKI)", BCP 174, RFC 6489,
              DOI 10.17487/RFC6489, February 2012,
              <http://www.rfc-editor.org/info/rfc6489>.

   [RFC6810] Bush, R. and R. Austein, "The Resource Public Key
              Infrastructure (RPKI) to Router Protocol", RFC 6810,
              DOI 10.17487/RFC6810, January 2013,
              <http://www.rfc-editor.org/info/rfc6810>.

   [RFC7030] Pritikin, M., Ed., Yee, P., Ed., and D. Harkins, Ed.,
              "Enrollment over Secure Transport", RFC 7030,
              DOI 10.17487/RFC7030, October 2013,
              <http://www.rfc-editor.org/info/rfc7030>.

   [RFC7353] Bellovin, S., Bush, R., and D. Ward, "Security
              Requirements for BGP Path Validation", RFC 7353,
              DOI 10.17487/RFC7353, August 2014,
              <http://www.rfc-editor.org/info/rfc7353>.

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 Drive
   San Jose, CA 95134
   CA

   Email: keyupate@cisco.com

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

      Email: bew@cisco.com