Network Working Group
Internet-Draft
Intended status: Best Current Practice
Expires: June 14, 2018

B. Weis
R. Gagliano
Cisco Systems
K. Patel
Arrcus, Inc.

December 11, 2017

BGPsec Router Certificate Rollover
draft-ietf-sidrops-bgpsec-rollover-04

Abstract

Certification Authorities (CAs) within the Resource Public Key Infrastructure (RPKI) manage BGPsec router certificates as well as RPKI certificates. The rollover of BGPsec router certificates must be carefully performed in order to synchronize the distribution of router public keys with BGPsec Update messages verified with those router public keys. This document describes a safe rollover process, as well as discussing when and why the rollover of BGPsec router certificates are necessary. When this rollover process is followed the rollover will be performed without routing information being lost.

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 June 14, 2018.

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Introduction

In BGPsec, a key rollover (or re-key) is the process of changing a router's BGPsec key pair (or key pairs), issuing the corresponding new BGPsec router 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 policies of the local network. This document describes a safe rollover process that results in a BGPsec receiver always having the needed verification keys. Certificate Practice Statements (CPS) documents may reference this memo. This memo only addresses changing of a router's BGPsec key pair within the RPKI. Refer to [RFC6489] for a procedure to rollover RPKI Certification Authority key pairs.

When a router receives or creates a new key pair (using a key provisioning mechanism), this key pair will be used to sign new BGPsec updates [RFC8205] that are originated or that transit through the BGP speaker. Additionally, the BGP speaker will refresh its outbound BGPsec Update messages to include a signature using the new key (replacing the old key). When the rollover process finishes, the old BGPsec router certificate (and its key) will no longer be valid, and thus any BGPsec Update that includes a signature performed by the old key will be invalid. Consequently, if the router does not refresh its outbound BGPsec Update messages, previously sent routing information may be treated as unauthenticated after the rollover process is finished. It is therefore extremely important that new BGPsec router certificates have been distributed throughout the RPKI before the router begin signing BGPsec updates with a new private key.

It is also important for an AS to minimize the BGPsec router key rollover interval (i.e., the period between the time when an AS distributes a BGPsec router 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 updates signed with a new private key in order to invalidate BGPsec updates signed with the old private key. In particular, if the AS suspects that a stale BGPsec update is being distributed instead of the most recently signed attribute it can cause the stale BGPsec updates to be invalidated by completing a key rollover procedure. The BGPsec router 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 suppression of BGP WITHDRAW messages or replay of BGP UPDATE messages, such as controlling BGPsec's window of exposure to such attacks. The BGPsec router certificate 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 multiple BGP speakers. In this scenario, the rollover of the correspondent BGPsec router certificate will impact all the BGP speakers sharing the same private key.

3. Key rollover in BGPsec

A BGPsec router 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 BGPsec router certificate.

Scheduled rollover: BGPsec router certificates have an expiration date (NotValidAfter) that requires a frequent rollover process to refresh certificates or issue new certificates. The validity period for these certificates is typically expressed in the CA's CPS document.

Router certificate field changes: Information contained in a BGPsec router certificate (such as the ASN or the Subject) may need to be changed.

Emergency router key rollover: Some special circumstances (such as a compromised key) may require the replacement of a BGPsec router certificate.

Protection against withdrawal suppression and replay attacks: An AS may determine that withdrawn BGPsec updates are being propagated instead of the most recently propagated BGPsec updates. Changing the BGPsec router signing key, distributing a new BGPsec router certificate, and revoking the old BGPsec router certificate will invalidate the replayed BGPsec updates.

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 BGP speakers receiving BGPsec Updates do not even need to be aware of the change of certificate. However, not replacing the certificate key for a long period of time increases the risk that a compromised router private key may be used by an attacker to deliver unauthorized or false BGPsec Updates. Distributing the old public key in a new certificate is NOT RECOMMENDED when the rollover event is due to a compromised key, or when it is suspected that withdrawn BGPsec updates are being distributed.

3.1. Rollover Process

The key rollover process is dependent on the key provisioning mechanisms adopted by an AS [I-D.ietf-sidr-rtr-keying]. An automatic provisioning mechanism such as EST will allow router key management procedures to include automatic re-keying methods with minimum development cost.

A safe BGPsec router key rollover process is as follows.

1. New Certificate Publication: The first step in the rollover mechanism is to publish the new certificate. If required, a new key pair will be generated for the BGPsec router. A new certificate will be generated and the certificate 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-BGPsec speaker or shared among multiple BGPsec speakers, whether the keys are generated on each BGPsec 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 router public keys. However, if an administrator has not previously provisioned the next certificate then a staging period may not be possible to implement during emergency key rollover. If there is no staging period, routing may be disrupted due to the inability of a BGPsec router to validate BGPsec updates signed with a new private key.

3. Twilight: At this moment, the BGPsec speaker holding the rolled-over private key will stop using the old key for signing and start using the new key. Also, the router will generate appropriate refreshed BGPsec updates just as in the typical operation of refreshing out-bound BGP polices. This operation may generate a great number of BGPsec updates. A BGPsec speaker may vary the Twilight moment for every peer in order to distribute the system load (e.g., skewing the rollover for different peers by a few minutes each would be sufficient and effective).

4. Certificate Revocation: This is an optional step, but SHOULD be taken when the goal is to invalidate BGPsec updates signed with the old key. Reasons to invalidate old BGPsec updates include: (a) the AS has reason to believe that the router signing key has been compromised, and (b) the AS needs to invalidate already propagated BGPsec updates signed with the old 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. Alternatively, the CA will just let the old certificate 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 no longer valid (e.g., using the

RPKI-Router Protocol described in [RFC8210]). A router's reaction to a message indicating withdrawal of a router key in the RPKI-Router Protocol SHOULD include the removal of any RIB entries (i.e., BGPsec updates) signed with that key and the generation of the corresponding BGP WITHDRAWALs (either implicit or explicit).

This rollover mechanism depends on the existence of an automatic provisioning process for BGPsec router certificates. It requires a staging mechanism based on the RPKI propagation time (typically a 24 hour period at the time this document was published), and an AS is REQUIRED to re-sign all originated and transited BGPsec updates that were previously signed with the old key.

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 perform its subsequent key rollover in an efficient and timely manner.

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

4. BGPsec router key rollover as a measure against replay attacks

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. The timestamp approach was originally proposed for BGPsec [I-D.sriram-replay-protection-design-discussion] but later dropped in favor of the key rollover approach. This section discusses the use of using a key rollover as a measure to mitigate replay attacks.

4.1. BGP UPDATE window of exposure requirement

The need to limit the vulnerability to replay attacks is described in [RFC7353] Section 4.3. 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 is no topology change at all, then no security threat comes from a replay of a BGPsec update because the signed information is still valid.

The BGPsec Operational Considerations document [RFC8207] gives some idea of requirements for the size of the window of exposure to replay

attacks. It states that the requirement will be in the order of a day or longer.

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

Since the window requirement is on the order of a day (as documented in [RFC8207]) and the BGP speaker performing re-keying is the edge router of the origin AS, it is feasible to use key rollover to mitigate replays. In this case it is important to complete the full process (i.e., the old and new certificates do not share the same key). By re-keying, an AS is letting the BGPsec router certificate validation time be a type of "timestamp" to mitigate 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 ensure that the public key corresponding to the new router certificate will be available to validate the corresponding BGPsec updates when received.

If a transit AS also originates BGPsec updates for its own prefixes and it wishes to mitigate replay attacks on those prefixes, then the transit AS SHOULD be provisioned with two unique key pairs and certificates. One of the key pairs is used to sign BGPsec updates for prefixes originated from the transit AS, and can have a replay protection policy applied to it. The other key pair is used to sign BGPsec updates in transit and SHOULD NOT have replay protection policy applied to it. Because the transit AS is not likely to know or care what is the policy of origin ASes elsewhere, there is no value for the transit AS to perform key rollovers to mitigate replay attacks against prefixes originated elsewhere. If the transit AS were instead to perform replay protection for all updates that it signs, its key rollover process would generate a large number of BGPsec UPDATE messages, even in the complete Default Free Zone (DFZ). Therefore, it is best to let each AS independently manage the replay attack vulnerability window for the prefixes it originates.

Advantages to re-keying as replay attack protection mechanism are as follows:

1. All expiration policies are maintained in the RPKI.

2. Much of the additional administrative cost is paid by the provider that wants to protect its infrastructure, as it bears the cost of creating and initiating distribution of new router key pairs and BGPsec router 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. The re-keying 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 key rollover).

Disadvantages to Re-keying as replay attack protection mechanism are as follows:

1. Frequent rollovers add administrative and BGP processing loads, although the required frequency is not clear. Some initial ideas are found in [RFC8207].

2. The minimum replay vulnerability is bounded by the propagation time for RPKI caches to obtain the new certificate and CRL (2x propagation time because first the new certificate and then the CRL need to propagate through the RPKI system). If provisioning is done ahead of time, the minimum replay vulnerability window size is reduced to 1x propagation time (i.e., propagation of the CRL). However, these bounds will be better understood when RPKI and RPs are well deployed, as well as the propagation time for objects in the RPKI is better understood.

3. Re-keying increases the dynamics and size of the RPKI repository.

5. IANA Considerations

There are no IANA considerations. This section may be removed upon publication.

6. Security Considerations

This document does not contain a protocol update to either the RPKI or BGPsec. It describes a process for managing BGPsec router certificates within the RPKI.

Routers participating in BGPsec will need to rollover their signing keys as part of conventional certificate management processes. However, because rolling over signing keys will also have an effect of invalidating BGPsec updates signatures, the rollover process must be carefully orchestrated to ensure that valid BGPsec updates are not treated as invalid. This situation could affect Internet routing. This document describes a safe method for rolling over BGPsec router certificates. It takes into account both normal and emergency key rollover requirements.

Additionally, the key rollover method described in this document can be used as a measure to mitigate BGP update replay attacks, in which an entity in the routing system is suppressing current BGPsec updates and replaying withdrawn updates. When the key used to sign the withdrawn updates has been rolled over, the withdrawn updates will be considered invalid. When certificates containing a new public key are provisioned ahead of time, the minimum replay vulnerability window size is reduced to the propagation time of a CRL invalidating the certificate containing an old public key. For a discussion of the difficulties deploying a more effectual replay protection mechanism for BGPSEC, see [I-D.sriram-replay-protection-design-discussion].

7. Acknowledgments

Randy Bush, Kotikalapudi Sriram, Stephen Kent and Sandy Murphy each provided valuable suggestions resulting in an improved document. Kotikalapudi Sriram contributed valuable guidance regarding the use of key rollovers to mitigate BGP update replay attacks.

8. References

8.1. Normative References

[I-D.ietf-sidr-rtr-keying]
Bush, R., Turner, S., and K. Patel, "Router Keying for BGPsec", draft-ietf-sidr-rtr-keying-14 (work in progress), October 2017.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

8.2. Informative References

[I-D.sriram-replay-protection-design-discussion]
Sriram, K. and D. Montgomery, "Design Discussion and Comparison of Protection Mechanisms for Replay Attack and Withdrawal Suppression in BGPsec", draft-sriram-replay-protection-design-discussion-09 (work in progress), October 2017.

[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, <https://www.rfc-editor.org/info/rfc6489>.

[RFC7030] Pritikin, M., Ed., Yee, P., Ed., and D. Harkins, Ed., "Enrollment over Secure Transport", RFC 7030, DOI 10.17487/RFC7030, October 2013, <https://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, <https://www.rfc-editor.org/info/rfc7353>.

[RFC8205] Lepinski, M., Ed. and K. Sriram, Ed., "BGPsec Protocol Specification", RFC 8205, DOI 10.17487/RFC8205, September 2017, <https://www.rfc-editor.org/info/rfc8205>.

[RFC8207] Bush, R., "BGPsec Operational Considerations", BCP 211, RFC 8207, DOI 10.17487/RFC8207, September 2017, <https://www.rfc-editor.org/info/rfc8207>.

[RFC8210] Bush, R. and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol, Version 1", RFC 8210, DOI 10.17487/RFC8210, September 2017, <https://www.rfc-editor.org/info/rfc8210>.

Authors' Addresses

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

Email: bew@cisco.com

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

Email: rogaglia@cisco.com

Keyur Patel
Arrcus, Inc.

Email: keyur@arrcus.com