Network Working Group R. Gagliano
Internet-Draft K. Patel
Intended status: Standards Track B. Weis
Expires: December 7, 2012 Cisco Systems
June 5, 2012

BGPSEC router key rollover as an alternative to beaconing
draft-rogaglia-sidr-bgpsec-rollover-01

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.

Comment: Better not to start the abstract with a negative statement.

Suggested wording for the abstract:
In the BGPSEC protocol operation, router certificates have a NotValidAfter time and they expire at that time, and hence key rollover and re-propagation of updates become necessary. In addition, key rollover mechanism can also be used as a tool for providing some degree of protection against replay attacks in BGPSEC. This draft document attempts to specify the operational details in BGPSEC of the router key rollover mechanism for refreshing the keys as well as replay-attack mitigation albeit in a limited sense.

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 with expire time in the update messages that was proposed for replay attack mitigation in an earlier version (02-draft) of the BGPSEC protocol specification. ~~proposed by the BGPSEC base documents to protect a BGPSEC attribute against a re-play~~replay~~ attack. ~~ However, there are a number of operational details to be considered if the expire time field in the BGPSEC Signature List Block attribute ~~is ~~were ~~removed~~not used.

This document details a possible key rollover process in BGPSEC and explores the operational environment ~~where ~~in which key rollovers could be used ~~as a protection~~for some degree of mitigation against ~~a re-play~~replay ~~attach ~~attacks ~~against ~~in BGPSEC
.

3. Key rollover in BGPSEC

Here we attempt to describe ~~T~~the key rollover process in BGPSEC.~~ has not been well defined yet.~~
~~However, this ~~Key rollover mechanism in BGPSEC will be a mandatory process due to ~~some of ~~the following ~~causes~~reasons:

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 a 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~~So it imperative 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~~would utilize the key provisioning mechanisms [cite: draft-ietf-sidr-rtr-keying ?] that ~~would~~ are expected to be in place. The key provisioning mechanisms for BGPSEC are not yet documented in a final form as the work is still in progress[cite: draft-ietf-sidr-rtr-keying ?] . 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) Question: What is a reference? Is this mentioned in draft-ietf-sidr-rtr-keying? . This protocol will allow BGPSEC code to include automatic re-keying scripts with minimum development cost.

Explain first the two possibilities: Shared private key across the whole AS and distinct private key for each router.
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~~ approach by adopting [I-D.ietf-pkix-cmc-serverkeygeneration]

~~If we work under the assumption~~Assuming that an automatic mechanism will exist to rollover a ~~BGPSEC~~ AS resource certificates, a possible ~~process~~ approach for the operation of the key rollover process for BGPSEC could be as follows:

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 the certificate published ~~on the correspondent~~in the RPKI repository. ~~This~~ The details of this process and the time take for this process will vary ~~in every~~depending on the environment as it will depend on where the keys are located (either in every router or on a centralized server), if the RPKI Certificate Authority (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 ?? What is it? Is this work in progress? Reference?.)

2. ~~Stage~~ Staging Period: ~~A stage~~ sStaging period ~~will be required~~ is the time from ~~the~~ when ~~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~~ that measure the RPKI data propagation times. Design documents [reference] mention RPKI end-to-end propagation time objectives ~~a~~ with lower limit on the order of of 24 hours. If rollovers ~~will~~ need be done frequently and if we want to ~~avoid~~mitigate delays due to the the ~~stage~~ staging 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 and routers around the globe would already have all the new {public key, SKI, AS} triple~~s.~~

3. Twilight: ~~At this moment,~~Twilight occurs when the BGP speaker that ~~uses the key~~has passed the staging period ~~been rolled-over will~~ stops 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~~ re-propagation and re-origination of updates may generate a great number of BGP UPDATE messages. To reduce the instantaneous work load on the BGP speaker as well as its neighbors, the re-propagation of updates may be jittered in time. The jittering may be done at the scale of prefixes or– ~~In any given BGP SPEAKER,~~ the Twilight moment may be scheduled at different times for ~~every~~ different peers. ~~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 in a CRL or due to the expiration of the
certificate's ~~validation~~validity (based on NotValidAfter field), the RPKI cache servers around the globe
will need to communicate to ~~its~~ their RTR peers that the OLD
certificate's public key is ~~not~~ no longer valid. This can be accomplished by a ~~(rtr~~ RTR cert withdrawal
message that can be potentially defined when the RPKI-rtr protocol is extended for BGPSEC~~)~~ (Note: RPKI-rtr protocol is currently defined only for origin validation). It is also not documented yet what will be a router's
reaction to a RTR cert withdrawal message but it should include the
removal of any RIB ~~entry~~ entries that ~~includes~~ include a BGPSEC attribute signed
with that key and the generation of WITHDRAWs (either implicit or explicit) for the ~~the correspondent~~ affected BGP prefixes.
~~WITHDRAWS (either implicit or explicit)~~.

To summarize, ~~T~~the proposed rollover mechanism will depend on the existence of an
automatic provisioning ~~process~~mechanism [cite: draft-ietf-sidr-rtr-keying ?] for BGPSEC certificates.~~,~~ ~~it~~ It will also
require a staging mechanism as described above that would have a response time ~~given~~ determined by RPKI propagation time ~~of~~ (expected to be around

24 hours. ~~and~~ Further, the rollover mechanism will cause significant BGP update churn due to the need for re-origination and re-propagation of prefixes routes that are affected due to ~~it will generate BGP UPDATES for all prefixes in the~~
router ~~been~~ re-keying.

The first two steps (i.e. New Certificate Pre-Publication and ~~Stage~~Staging
Period) ~~could~~ can be performed well ahead of time (i.e. in anticipation for an emergency key rollover) so that ~~happen ahead of time from the rest of the process as~~
a network operator~~s~~ ~~could~~ may be well prepared to quickly re-generate new updates when an emergency situation arises. The operator also tries to render the old updates invalid by issuing CRL for the old certificate, but this process takes RPKI propagation time (~ 24 hours). ~~itself to accelerate a future key~~
~~roll-over.~~

4. BGPSEC key rollover as a ~~measure~~ mechanism for mitigating ~~against~~ replay~~s~~ attacks in BGPSEC

The mechanism that has been considered so far in the SIDR WG for mitigating replay attacks is to use an Expire Time field in the BGPSEC updates [draft-ietf-sidr-bgpsec-protocol-01]. The originating BGPSEC speaker would set a value in the Expire Time field specifying the time when the origin’s signature would expire. Let us call this mechanism the Expire Time method. This is an explicit way of setting an expiry time in the update itself and thus contrasts with the key rollover approach where the update expire time is not in the update but implicitly in the router cert. The benefit of the Expire Time method is that it allows old BGPSEC updates to expire automatically at the chosen Expire Time intervals, and also the BGPSEC updates are refreshed (i.e. beaconed) periodically within the Expire Time interval. The Expire Time has the following pros and cons:

Pros of the Expire Time method:

1. The network operator is assured that if there is an emergency and they need to withdraw prefixes sent on a certain peering link, then their previously prefix announcements towards that peer would be invalid after the Expire Time that was set in those previous updates.

2. The re-origination and re-propagation of BGPSEC updates can be performed at the granularity of individual prefixes. That is, if only one prefix need to be withdrawn, then only that prefix can be withdrawn without need to re-propagate all the other prefixes. Also, if the peering relationship with one peer has gone sour, then prefix WITHDRAWs can be sent only to that peer and there is no need to simultaneously re-generate BGPSEC updates towards other peers.

3. The Expire Time method does not produce any churn in the global RPKI system.

Cons of the Expire Time method:

1. There is a possibility that a network operator may aggressively set the Expire Time too low (order of minutes) and beacon too often at the expense of overloading BGPSEC speakers in other ASes. The Expire Time units can be made granular in principle (say, 24 hour granularity) but still there is no guarantee that a router vendor and a network operator would not collude to change that to a much finer granularity.

2. The Expire Time field is built into the update format and hence is native to the BGPSEC protocol. Expire Time granularity needs to be specified at the time of deployment, and it is hard to change that granularity later such need is felt.

Due to the cons mentioned above, the community has been looking for an alternative. One alternative is a mechanism based on key rollover that is the topic of this draft document. It is attractive because this mechanism would be more advantageous provided the network operators can live with a window of replay-attack protection that is on the order of 24 hours (or a few days in the worst case). The 24 hours to up to few days range of window of protection for replay attacks is tied to how fast the CRLs of old router certs can propagate in the global RPKI system to update all

Relying Parties (RPs). We will now describe in further detail the replay-attack protection mechanism based on key rollover.

~~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~~replay ~~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~~Replay attack window requirement

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

Having said the above, we do realize that in some cases replay protection may be important even without topology change. Consider the following example. Let us say I am multi-homed two ISPs A and B. I depref my prefix announced to ISP B by prepending because ISP A has been charging me less. But starting today, ISP A has become more expensive. So I now try to depref my prefix to ISP A (make the path longer by prepending) and prefer my inbound traffic to come via ISP B. But ISP A is greedy; suppresses my new deprefed update and continues to attract 100% of my traffic via him! That is an example of replay attack without there being any topology change.

Note: The key rollover mechanism can be shown to be effective to mitigate the above type of replay attack (or any replay attack), except that the window of vulnerability is about 24 hours (or, may a few days in the worst case). That is a limitation but it is much better than no protection or perhaps other expensive protections.

The BGPSEC Ops [draft-ymbk-bgpsec-ops] document gives some ~~ideas~~ guidance regarding ~~of~~ requirements for the admissible ~~re-~~replay ~~play~~ attack vulnerability window 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~~ Can key rollover provide ~~us a~~ adequate ~~similar~~ protection against ~~re-play~~replay attacks. ~~without the need for beaconing?~~

Comment: I think we cannot say that key rollover has no “beaconing” because the router does have to anticipate expiry due to NotValidAfter and “beacon” (i.e. re-originate and/or re-propagate) in advance of that, even if it is once a year.

The answer we feel is ~~that~~ YES when the vulnerability window requirement is in the order of about 24 hours (or may a few days in the worst case), ~~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~~NotValidAfter time ~~as your timestamp~~is being used as the equivalent of Expire Time to protect against replay attacks. However, the use of frequent key rollovers comes with an additional administrative cost as well as churn in the RPKI system and also some risks if the process fails. As ~~documented~~ mentioned 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 so that new updates can be propagated quickly in the event of an emergency such as a peering relationship change or a key compromise. The old prefix updates (which are now vulnerable to replay) will expire when the old cert’s NotValidAfter time is reached. ~~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~~ be 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 with frequency that is determined by the desired replay vulnerability window. Consequently, the transit BGPSEC certificate is expected to be much longer living than the origin BGPSEC certificate.

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

1. Does not require the strictly periodic and frequent beaconing that is characteristic of the Expire Time method [ietf-sidr-bgpsec-protocol-01]. It may be noted that there is beaconing required (though much less) in some form even for the key rollover method in order to re-propagate and/or re-originate BGPSEC updates before NotValidAfter time of a router cert is reached. However, there appears to be much lower chance of abuse by too frequent re-propgation/re-origination in the case of key rollover as compared to that for the Expire Time method.
2. All ~~timestamps~~ expire time policies are managed by use of appropriate routers certs and CRLs in the RPKI and also the policies are maintained in the RPKI.

3. Additional administrative cost is paid by ~~the~~ a provider that ~~wants~~ ~~to~~ protects its infrastructure (from ill effects of relay of prefix announcements) based on a level of tolerance (vulnerability window) of their choice. This refers to the key rollover management process and update re-propagation that needs to be administered by that provider. However, the provider's choice has an impact felt by other ASes or RPs in terms the extra work due to more churn in the RPKI or due to more BGPSEC churn attributable to that provider.

4. Can be implemented in coordination with planned topology changes by either origin ASes or transit ASes. ~~(if~~ If I am changing providers, I do key rollover and perform all necessary functions such as re-propagate/re-originate my prefix updates, etc.~~)~~

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

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

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

2. ~~Minimum~~ Replay-attack vulnerability window size is lower bounded by RPKI propagation time to RPKI Caches ans all RPs. If pre-provisioning (i.e. having two pre-staged certs) is~~done ahead of time~~, it means 24 hours minimum ~~in paper~~vulnerability based on some rough current estimates [reference]. However, more experimentation and measurements ~~is~~ are needed as and when when RPKI and cache servers are more ~~massively~~ widely deployed.

3. Increases the dynamic of RPKI repository and the RPKI as well as BGPSEC churn for RPs.

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

Comment: Need to add some more reference as identified in some places the revised text.

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