Internet Engineering Task Force (IETF)
Request for Comments: 8206
Updates: 8205
Category: Standards Track
ISSN: 2070-1721

W. George
Neustar
S. Murphy
PARSONS, Inc.

September 2017

BGPsec Considerations for Autonomous System (AS) Migration

Abstract

This document discusses considerations and methods for supporting and securing a common method for Autonomous System (AS) migration within the BGPsec protocol.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8206.

Table of Contents

1. Introduction

A method of managing a BGP Autonomous System Number (ASN) migration is described in RFC 7705 [RFC7705]. Since it concerns the handling of AS_PATH attributes, it is necessary to ensure that the process and features are properly supported in BGPsec [RFC8205] because BGPsec is explicitly designed to protect against changes in the BGP AS_PATH, whether by choice, by misconfiguration, or by malicious intent. It is critical that the BGPsec protocol framework be able to support this operationally necessary tool without creating an unacceptable security risk or exploit in the process.

1.1. Requirements Language

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.

1.2. Documentation Note

This document uses ASNs from the range reserved for documentation as described in RFC 5398 [RFC5398]. In the examples used here, they are intended to represent Globally Unique ASNs, not ASNs reserved for private use as documented in Section 10 of RFC 1930 [RFC1930].

2. General Scenario

This document assumes that the reader has read and understood the ASN migration method discussed in RFC 7705 [RFC7705] including its examples (see Section 2 of the referenced document), as they will be heavily referenced here. The use case being discussed in RFC 7705 [RFC7705] is as follows: For whatever the reason, a provider is in the process of merging two or more ASes, where eventually one subsumes the other(s). BGP AS confederations [RFC5065] are not enabled between the ASes, but a mechanism is being used to modify BGP’s default behavior and allow the migrating Provider Edge (PE) router to masquerade as the old ASN for the Provider-Edge-to-Customer-Edge (PE-CE) eBGP (external BGP) session, or to manipulate the AS_PATH, or both. While BGPsec [RFC8205] does have a method to handle standard confederation implementations, it is not applicable in this exact case. This migration requires a slightly different solution in BGPsec than for a standard confederation because unlike in a confederation, eBGP peers may not be peering with the "correct" external ASN, and the forward-signed updates are for a public ASN, rather than a private one; so, there is no expectation that the BGP speaker would strip the affected signatures before propagating the route to its eBGP neighbors.

In the examples in Section 5.4, AS64510 is being subsumed by AS64500, and both ASNs represent a Service Provider (SP) network (see Figures 1 and 2 in RFC 7705 [RFC7705]). AS64496 and 64499 represent end-customer networks. References to PE, CE, and P routers mirror the diagrams and references in RFC 7705.

3. RPKI Considerations

The methods and implementation discussed in RFC 7705 [RFC7705] are widely used during network integrations resulting from mergers and acquisitions, as well as network redesigns; therefore, it is necessary to support this capability on any BGPsec-enabled routers/ASNs. What follows is a discussion of the potential issues to be considered regarding how ASN migration and BGPsec [RFC8205] validation might interact.

One of the primary considerations for this document and migration is that service providers (SPs) rarely stop after one

merger/acquisition/divestiture; they end up accumulating several legacy ASNs over time. Since SPs are using migration methods that are transparent to customers and therefore do not require coordination with customers, they do not have as much control over the length of the transition period as they might with something completely under their administrative control (e.g., a key roll). Because they are not forcing a simultaneous migration (i.e., both ends switch to the new ASN at an agreed-upon time), there is no incentive for a given customer to complete the move from the old ASN to the new one. This leaves many SPs with multiple legacy ASNs that don't go away very quickly, if at all. As solutions were being proposed for Resource Public Key Infrastructure (RPKI) implementations to solve this transition case, the WG carefully considered operational complexity and hardware scaling issues associated with maintaining multiple legacy ASN keys on routers throughout the combined network. While SPs who choose to remain in this transition phase indefinitely invite added risks because of the operational complexity and scaling considerations associated with maintaining multiple legacy ASN keys on routers throughout the combined network, saying "don't do this" is of limited utility as a solution. As a result, this solution attempts to minimize the additional complexity during the transition period, on the assumption that it will likely be protracted. Note that while this document primarily discusses service provider considerations, it is not solely applicable to SPs, as enterprises often migrate between ASNs using the same functionality. What follows is a discussion of origin and path validation functions and how they interact with ASN migrations.

3.1. Origin Validation

Route Origin Validation as defined by RFC 6480 [RFC6480] does not require modification to enable AS migration, as the existing protocol and procedure allow for a solution. In the scenario discussed in RFC 7705 [RFC7705], AS64510 is being replaced by AS64500. If there are any existing routes originated by AS64510 on the router being moved into the new ASN, new Route Origination Authorizations (ROAs) for the routes with the new ASN should be generated, and they should be treated as new routes to be added to AS64500. However, we also need to consider the situation where one or more other PEs are still in AS64510 and are originating one or more routes that may be distinct from any that the router under migration is originating. PE1 (which is now a part of AS64500 and instructed to use "Replace Old AS" as defined in [RFC7705] to remove AS64510 from the path) needs to be able to properly handle routes originated from AS64510. If the route now shows up as originating from AS64500, any downstream peers' validation check will fail unless a ROA is *also* available for AS64500 as the origin ASN. In addition to generating a ROA for 65400 for any prefixes originated by the router being moved, it may be

necessary to generate ROAs for 65400 for prefixes that are originating on routers still in 65410, since the AS replacement function will change the origin AS in some cases. This means that there will be multiple ROAs showing different ASes authorized to originate the same prefixes until all routers originating prefixes from AS64510 are migrated to AS64500. Multiple ROAs of this type are permissible per Section 3.2 of RFC 6480 [RFC6480] so managing origin validation during a migration like this is merely applying the defined case where a set of prefixes are originated from more than one ASN. Therefore, for each ROA that authorizes the old ASN (e.g., AS64510) to originate a prefix, a new ROA MUST also be created that authorizes the replacing ASN (e.g., AS64500) to originate the same prefix.

3.2. Path Validation

BGPsec path validation requires that each router in the AS path cryptographically sign its update to assert that "every Autonomous System (AS) on the path of ASes listed in the UPDATE message has explicitly authorized the advertisement of the route to the subsequent AS in the path" (see Section 1 of RFC 8205 [RFC8205]). Since the referenced AS-migration technique explicitly modifies the AS_PATH between two eBGP peers who are not coordinating with one another (are not in the same administrative domain), no level of trust can be assumed; therefore, it may be difficult to identify legitimate manipulation of the AS_PATH for migration activities when compared to manipulation due to misconfiguration or malicious intent.

3.2.1. Outbound Announcements (PE-->CE)

When PE1 is moved from AS64510 to AS64500, it will be provisioned with the appropriate keys for AS64500 to allow it to forward-sign routes using AS64500. However, there is no guidance in the BGPsec protocol specification [RFC8205] on whether or not the forward-signed ASN value is required to match the configured remote AS to validate properly. That is, if CE1’s BGP session is configured as "remote AS 64510", the presence of "local AS 64510" on PE1 will ensure that there is no ASN mismatch on the BGP session itself, but if CE1 receives updates from its remote neighbor (PE1) forward-signed from AS64500, there is no guidance as to whether the BGPsec validator on CE1 still considers those valid by default. Section 6.3 of RFC 4271 [RFC4271] mentions this match between the ASN of the peer and the AS_PATH data, but it is listed as an optional validation, rather than a requirement. We cannot assume that this mismatch will be allowed by vendor implementations, so using it as a means to solve this migration case is likely to be problematic.

3.2.2. Inbound Announcements (CE-->PE)

Inbound is more complicated, because the CE doesn't know that PE1 has changed ASNs, so it is forward-signing all of its routes with AS64510, not AS64500. The BGPsec speaker cannot manipulate previous signatures and therefore cannot manipulate the previous AS path without causing a mismatch that will invalidate the route. If the updates are simply left intact, the ISP would still need to publish and maintain valid and active public keys for AS 64510 if it is to appear in the BGPsec_PATH signature so that receivers can validate that the BGPsec_PATH signature arrived intact/whole. However, if the updates are left intact, this will cause the AS path length to be increased, which is unacceptable as discussed in RFC 7705 [RFC7705].

4. Requirements

In order to be deployable, any solution to the described problem needs to consider the following requirements, listed in no particular order. BGPsec:

- MUST support AS migration for both inbound and outbound route announcements (see Sections 3.2.1 and 3.2.2), without reducing BGPsec's protections for route path.

- MUST NOT require any reconfiguration on the remote eBGP neighbor (CE).

- SHOULD NOT require global (i.e., network-wide) configuration changes to support migration. The goal is to limit required configuration changes to the devices (PEs) being migrated.

- MUST NOT lengthen the AS path during migration.

- MUST operate within existing trust boundaries, e.g., can't expect remote side to accept pCount=0 (see Section 4.2 of RFC 8205 [RFC8205]) from untrusted/non-confederation neighbor.

5. Solution

As noted in Section 4.2 of RFC 8205 [RFC8205], BGPsec already has a solution for hiding ASNs where increasing the AS path length is undesirable. So a simple solution would be to retain the keys for AS64510 on PE1 and forward-sign towards CE1 with AS64510 and pCount=0. However, this would mean passing a pCount=0 between two ASNs that are in different administrative and trust domains such that it could represent a significant attack vector to manipulate BGPsec-signed paths. The expectation for legitimate instances of pCount=0 (to make a route server that is not part of the transit path

invisible) is that there is some sort of existing trust relationship between the operators of the route server and the downstream peers such that the peers could be explicitly configured by policy to accept pCount=0 announcements only on the sessions where they are expected. For the same reason that things like "Local AS" [RFC7705] are used for ASN migration without end-customer coordination, it is unrealistic to assume any sort of coordination between the SP and the administrators of CE1 to ensure that they will by policy accept pCount=0 signatures during the transition period; therefore, this is not a workable solution.

A better solution presents itself when considering how to handle routes coming from the CE toward the PE, where the routes are forward-signed to AS64510, but will eventually need to show AS64500 in the outbound route announcement. Because both AS64500 and AS64510 are in the same administrative domain, a signature from AS64510 forward-signed to AS64500 with pCount=0 would be acceptable as it would be within the appropriate trust boundary so that each BGP speaker could be explicitly configured to accept pCount=0 where appropriate between the two ASNs. At the very simplest, this could potentially be used at the eBGP boundary between the two ASNs during migration. Since the AS_PATH manipulation described above usually happens at the PE router on a per-session basis and does not happen network-wide simultaneously, it is not generally appropriate to apply this AS-hiding technique across all routes exchanged between the two ASNs, as it may result in routing loops and other undesirable behavior. Therefore, the most appropriate place to implement this is on the local PE that still has eBGP sessions with peers expecting to peer with AS64510 (using the transition mechanisms detailed in RFC 7705 [RFC7705]). Since that PE has been moved to AS64500, it is not possible for it to forward-sign AS64510 with pCount=0 without some minor changes to the BGPsec behavior to address this use case.

AS migration is using AS_PATH and remote AS manipulation to act as if a PE under migration exists simultaneously in both ASNs even though it is only configured with one global ASN. This document describes applying a similar technique to the BGPsec signatures generated for routing updates processed through this migration machinery. Each routing update that is received from or destined to an eBGP neighbor that is still using the old ASN (64510) will be signed twice, once with the ASN to be hidden and once with the ASN that will remain visible. In essence, we are treating the update as if the PE had an internal BGP hop and the update was passed across an eBGP session between AS64500 and AS64510, configured to use and accept pCount=0, while eliminating the processing and storage overhead of creating an actual eBGP session between the two ASNs within the PE router. This will result in a properly secured AS path in the affected route updates, because the PE router will be provisioned with valid keys

for both AS64500 and AS64510. An important distinction here is that while AS migration under standard BGP4 is manipulating the AS_PATH attribute, BGPsec uses an attribute called the "Secure_Path" (see Section 3.1 of RFC 8205 [RFC8205]) and BGPsec-capable neighbors do not exchange AS_PATH information in their route announcements. However, a BGPsec neighbor peering with a non-BGPsec-capable neighbor will use the information found in the Secure_Path to reconstruct a standard AS_PATH for updates sent to that neighbor. Unlike in the Secure_Path where the ASN to be hidden is still present but ignored when considering the AS path (due to pCount=0), when reconstructing an AS_PATH for a non-BGPsec neighbor, the pCount=0 ASNs will not appear in the AS_PATH at all (see Section 4.4 of RFC 8205 [RFC8205]). This document is not changing existing AS_PATH reconstruction behavior, merely highlighting it for clarity.

The procedure to support AS migration in BGPsec is slightly different depending on whether the PE under migration is receiving the routes from one of its eBGP peers ("inbound" as in Section 3.2.2) or destined toward the eBGP peers ("outbound" as in Section 3.2.1).

5.1. Outbound (PE-->CE)

When a PE router receives an update destined for an eBGP neighbor that is locally configured with AS-migration mechanisms as discussed in RFC 7705 [RFC7705], it MUST generate a valid BGPsec signature as defined in RFC 8205 [RFC8205] for _both_ configured ASNs. It MUST generate a signature from the new (global) ASN forward-signing to the old (local) ASN with pCount=0, and then it MUST generate a forward signature from the old (local) ASN to the target eBGP ASN with pCount=1 as normal.

5.2. Inbound (CE-->PE)

When a PE router receives an update from an eBGP neighbor that is locally configured with AS-migration mechanisms (i.e., the opposite direction of the previous route flow), it MUST generate a signature from the old (local) ASN forward-signing to the new (global) ASN with pCount=0. It is not necessary to generate the second signature from the new (global) ASN because the Autonomous System Border Router (ASBR) will generate that when it forward-signs towards its eBGP peers as defined in normal BGPsec operation. Note that a signature is not normally added when a routing update is sent across an iBGP (internal BGP) session. The requirement to sign updates in iBGP represents a change to the normal behavior for this specific AS-migration scenario only.

5.3. Other Considerations

In the inbound case discussed in Section 5.2, the PE is adding BGPsec attributes to routes received from or destined to an iBGP neighbor and using pCount=0 to mask them. While this is not prohibited by BGPsec [RFC8205], BGPsec-capable routers that receive updates from BGPsec-enabled iBGP neighbors MUST accept updates with new (properly formed) BGPsec attributes, including the presence of pCount=0 on a previous signature, or they will interfere with this method. In a similar fashion, any BGPsec-capable route-reflectors in the path of these updates MUST reflect them transparently to their BGPsec-capable clients.

In order to secure this set of signatures, the PE router MUST be provisioned with valid keys for _both_ configured ASNs (old and new), and the key for the old ASN MUST be kept valid until all eBGP sessions are migrated to the new ASN. Downstream neighbors will see this as a valid BGPsec path, as they will simply trust that their upstream neighbor accepted pCount=0 because it was explicitly configured to do so based on a trust relationship and business relationship between the upstream and its neighbor (the old and new ASNs).

Additionally, Section 4 of RFC 7705 [RFC7705] discusses methods in which AS migrations can be completed for iBGP peers such that a session between two routers will be treated as iBGP even if the neighbor ASN is not the same ASN on each peer’s global configuration. As far as BGPsec is concerned, this requires the same procedure as when the routers migrating are applying AS-migration mechanisms to eBGP peers, but the router functioning as the "ASBR" between old and new ASN is different. In eBGP, the router being migrated has direct eBGP sessions to the old ASN and signs from old ASN to new with pCount=0 before passing the update along to additional routers in its global (new) ASN. In iBGP, the router being migrated is receiving updates (that may have originated either from eBGP neighbors or other iBGP neighbors) from its downstream neighbors in the old ASN and MUST sign those updates from old ASN to new with pCount=0 before sending them on to other peers.

5.4. Example

The following example will illustrate the method being used above. As with previous examples, PE1 is the router being migrated, AS64510 is the old ASN, which is being subsumed by AS64500, the ASN to be permanently retained. 64505 is another external peer, used to demonstrate what the announcements will look like to a third-party peer that is not part of the migration. Some additional notation is used to delineate the details of each signature as follows:

The origin BGPsec Signature Segment takes the form:
sig(Target ASN, (pCount,...,Origin ASN), NLRI) key.

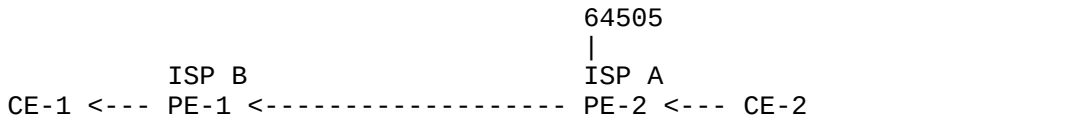
Intermediate BGPsec Signature Segments take the form:
sig(Target ASN,...,(pCount,...,Signer ASN),...,NLRI) key.

(pCount,...,ASN) refers to the new Secure_Path Segment added to the BGPsec_PATH attribute by the ASN (Origin ASN or Signer ASN).

"Equivalent AS_PATH" refers to what the AS_PATH would look like if it was reconstructed to be sent to a non-BGPsec peer, while the Securedpath shows the AS path as represented between BGPsec peers.

Note: The representation of Signature Segment generation is being simplified here somewhat for the sake of brevity; the actual details of the signing process are as described in Sections 4.1 and 4.2 of [RFC8205]. For example, what is covered by the signature also includes Flags, Algorithm Suite Identifier, NLRI length, etc. Also, the key is not carried in the update; instead, the Subject Key Identifier (SKI) is carried.

Before Merger



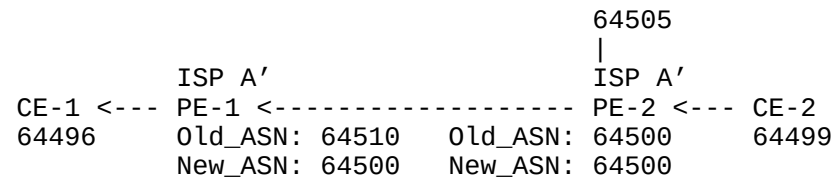
CE-2 to PE-2: sig(64500, (pCount=1,...,64499), N)K_64499-CE2
Equivalent AS_PATH=(64499)
Securedpath=(64499)
length=sum(pCount)=1

PE-2 to 64505: sig(64505,...,(pCount=1,...,64500),...,N)K_64500-PE2
sig(64500, (pCount=1,...,64499), N)K_64499-CE2
Equivalent AS_PATH=(64500,64499)
Securedpath=(64500,64499)
length=sum(pCount)=2

PE-2 to PE-1: sig(64510,...,(pCount=1,...,64500),...,N)K_64500-PE2
sig(64500, (pCount=1,...,64499), N)K_64499-CE2
Equivalent AS_PATH=(64500,64499)
Securedpath=(64500,64499)
length=sum(pCount)=2

PE-1 to CE-1: sig(64496,...,(pCount=1,...,64510),...,N)K_64510-PE1
sig(64510,...,(pCount=1,...,64500),...,N)K_64500-PE2
sig(64500, (pCount=1,...,64499), N)K_64499-CE2
Equivalent AS_PATH= (64510,64500,64499)
Securedpath=(64510,64500,64499)
length=sum(pCount)=3

Migrating, route flow outbound PE-1 to CE-1



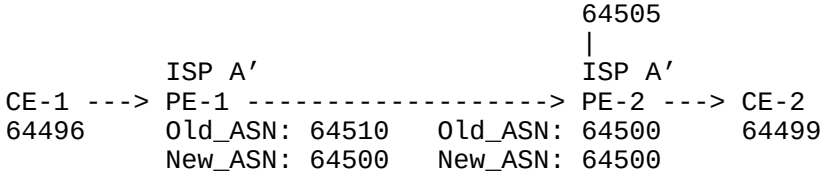

```
CE-2 to PE-2:  sig(64500, (pCount=1,...,64499), N)K_64499-CE2
               Equivalent AS_PATH=(64499)
               Securedpath=(64499)
               length=sum(pCount)=1

PE-2 to 64505: sig(64505,...,(pCount=1,...,64500),...,N)K_64500-PE2
               sig(64500, (pCount=1,...,64499), N)K_64499-CE2
               Equivalent AS_PATH=(64500,64499)
               Securedpath=(64500,64499)
               length=sum(pCount)=2

PE-2 to PE-1:  sig(64500, (pCount=1,...,64499), N)K_64499-CE2
               Equivalent AS_PATH=(64499)
               Securedpath=(64499)
               length=sum(pCount)=1
#PE-2 sends to PE-1 (in iBGP) the exact same update
#as it received from AS64499.


PE-1 to CE-1:  sig(64496,...,(pCount=1,...,64510),...,N)K_64510-PE1
               sig(64510,...,(pCount=0,...,64500),...,N)K_64500-PE2 (*)
               sig(64500, (pCount=1,...,64499), N)K_64499-CE2
               Equivalent AS_PATH=(64510,64499)
               Securedpath=(64510, 64500 (pCount=0),64499)
               length=sum(pCount)=2 (length is NOT 3)
#PE-1 adds the Secure_Path Segment in (*) acting as AS64500
#PE-1 accepts (*) with pCount=0 acting as AS64510,
#as it would if it received (*) from an eBGP peer
```

Migrating, route flow inbound CE-1 to PE-1




```
CE-1 to PE-1:  sig(64510, (pCount=1,...,64496), N)K_64496-CE1
               Equivalent AS_PATH=(64496)
               Securedpath=(64496)
               length=sum(pCount)=1

PE-1 to PE-2:  sig(64500,...,(pCount=0,...,64510),...,N)K_64510-PE1 (**)
               sig(64510, (pCount=1,...,64496), N)K_64496-CE1
               Equivalent AS_PATH=(64496)
               Securedpath=(64510 (pCount=0),64496)
               length=sum(pCount)=1 (length is NOT 2)
#PE-1 adds the Secure_Path Segment in (**) acting as AS64510
#PE-1 accepts (**) with pCount=0 acting as AS64500,
#as it would if it received (**) from an eBGP peer
#PE-1, as AS64500, sends the update including (**) to PE-2 (in iBGP)

PE-2 to 64505: sig(64505,...,(pCount=1,...,64500),...,N)K_64500-PE2
               sig(64500,...,(pCount=0,...,64510),...,N)K_64510-PE1
               sig(64510, (pCount=1,...,64496), N)K_64496-CE1
               Equivalent AS_PATH=(64500,64496)
               Securedpath=(64500,64510 (pCount=0), 64496)
               length=sum(pCount)=2 (length is NOT 3)

PE-2 to CE-2:  sig(64499,...,(pCount=1,...,64500),...,N)K_64500-PE2
               sig(64500,...,(pCount=0,...,64510),...,N)K_64510-PE1
               sig(64510, (pCount=1,...,64496), N)K_64496-CE1
               Equivalent AS_PATH=(64500,64496)
               Securedpath=(64500, 64510 (pCount=0), 64496)
               length=sum(pCount)=2 (length is NOT 3)
```

6. IANA Considerations

This document does not require any IANA actions.

7. Security Considerations

RFC 7705 [RFC7705] discusses a process by which one ASN is migrated into and subsumed by another. Because this process involves manipulating the AS_Path in a BGP route to make it deviate from the actual path that it took through the network, this migration process is attempting to do exactly what BGPsec is working to prevent. BGPsec MUST be able to manage this legitimate use of AS_Path manipulation without generating a vulnerability in the RPKI route security infrastructure, and this document was written to define the method by which the protocol can meet this need.

The solution discussed above is considered to be reasonably secure from exploitation by a malicious actor because it requires both signatures to be secured as if they were forward-signed between two eBGP neighbors. This requires any router using this solution to be provisioned with valid keys for both the migrated and subsumed ASN so that it can generate valid signatures for each of the two ASNs it is adding to the path. If the AS's keys are compromised, or zero-length keys are permitted, this does potentially enable an AS_PATH shortening attack, but these are existing security risks for BGPsec.

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, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7705] George, W. and S. Amante, "Autonomous System Migration Mechanisms and Their Effects on the BGP AS_PATH Attribute", RFC 7705, DOI 10.17487/RFC7705, November 2015, <https://www.rfc-editor.org/info/rfc7705>.

[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>.

[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/rfc8105>.

8.2. Informative References

[RFC1930] Hawkinson, J. and T. Bates, "Guidelines for creation, selection, and registration of an Autonomous System (AS)", BCP 6, RFC 1930, DOI 10.17487/RFC1930, March 1996, <https://www.rfc-editor.org/info/rfc1930>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

[RFC5065] Traina, P., McPherson, D., and J. Scudder, "Autonomous System Confederations for BGP", RFC 5065, DOI 10.17487/RFC5065, August 2007, <https://www.rfc-editor.org/info/rfc5065>.

[RFC5398] Huston, G., "Autonomous System (AS) Number Reservation for Documentation Use", RFC 5398, DOI 10.17487/RFC5398, December 2008, <https://www.rfc-editor.org/info/rfc5398>.

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <https://www.rfc-editor.org/info/rfc6480>.

Acknowledgements

Thanks to Kotikalapudi Sriram, Shane Amante, Warren Kumari, Terry Manderson, Keyur Patel, Alia Atlas, and Alvaro Retana for their review comments.

The authors particularly wish to acknowledge Kotikalapudi Sriram, Oliver Borchert, and Michael Baer for their review and suggestions for the examples in Section 5.4, which made an important contribution to the quality of the text.

Additionally, the solution presented in this document is an amalgam of several Secure Inter-Domain Routing (SIDR) interim meeting discussions plus a discussion at IETF 85, collected and articulated thanks to Sandy Murphy.

Authors' Addresses

Wesley George
Neustar
45980 Center Oak Plaza
Sterling, VA 20166
United States of America

Email: wesgeorge@puck.nether.net

Sandy Murphy
PARSONS, Inc.
7110 Samuel Morse Drive
Columbia, MD 21046
United States of America

Phone: +1 443-430-8000
Email: sandy@tislabs.com