Abstract

The Border Gateway Protocol, version 4, (BGP4) provides the means to advertise reachability for IP prefixes. This reachability information is propagated in a peer-to-peer topology. Sometimes routes are announced to peers for which the local peering policy does not permit. And sometimes routes are propagated indiscriminantly, once they have been accepted.

This document considers the situations that can lead to routes being leaked, and tries to find acceptable definitions for describing these scenarios.

The purpose of these definitions is to facilitate discussion on what a route leak is, and what the scope of the problem space for route leaks is. This, in turn, is intended to inform a requirements document for detection of (and prevention of) route leaks. And finally, the definitions and requirements are intended to allow proposed solutions which meet these criteria, and to facilitate evaluation of proposed solutions.

The fundamental objective is to "solve the route leaks problem".

Author’s Note

Intended Status: Standards track.

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.
1. Introduction

1.1. Rationale

This document describes two different schemes for implementing a solution for route leaks.

They represent different trade-offs between simplicity of implementation, versus embedding information. The information embedded can be inferred currently from a variety of sources, so the risk/cost of doing so is marginal.

Either solution would be adequate to solve the route leak problem.

Due to the requirement for mandatory establishment of peering link types, and cryptographic protection, the ideal time and place to implement this would be coincident with BGPSEC.

Including route leak protection with BGPSEC may be beneficial to the latter. It is more compelling to deploy a solution to both sets of problems, than to deploy a solution to one or the other alone.

1.2. Requirements

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].

1.3. Terminology

The reader is assumed to be familiar with the IETF.

2. Prefix Attribute Possibilities

If we presume that there are two possible colors for a prefix, then we have three ways to express those colors:

1. A single bit, with two possible values, always attached to a prefix.

2. An attribute whose presence signals one of the colors, and whose absence signals the other color.

3. The same as 2, but with the other color being signaled.

For sake of clarity, we will use a fairly universally understood pair of colors, "green" (meaning "proceed"), and "yellow" (meaning
"caution").

So, the three ways of marking the colors are:

- Use a green/yellow bit (green if 1, yellow if 0)
- Use a "green" attribute (green if present, yellow otherwise)
- Use a "yellow" attribute (yellow if present, green otherwise).

Since information is leaked for both the "green/yellow bit" and "yellow attribute", there is no reason to discuss the "yellow attribute" option. It is inferior to both other methods.

3. Encoding Color via Choice of Algorithm

Here, we are presuming that BGPSEC is in use on prefixes, and that BGPSEC includes an explicit algorithm identifier. Currently, the identifier only specifies which algorithm to use to validate the signature in the signature block.

This would be augmented so that for any given algorithm, two identifiers would be assigned. One would be the identifier signifying "Green", and the other would signify "Yellow". When sending a "green" route, the current "green" algorithm would be used. When sending a "yellow" route, the current "yellow" algorithm would be used. Validation would work as usual, with the additional ability to validate the color rules for preventing route leaks.

No additional changes to the structure of the BGPSEC protocol or wire format are needed.

However, there is the leak of information about transit relationships, which is unavoidable with this design.

Routes which violate the path coloring rules but otherwise validate, would be blocked. (They should not occur, but should be checked regardless.) Routes which do not validate under BGPSEC would be blocked regardless, also preventing a potential source of route leaks.

4. Encoding Color via a Second Signature Block

A signature block analogous to the AS-PATH signature block, would be included on any announcement that is "green". The local sender would add her signature to the signature block on these "green"
announcements. In addition, the new signature block would be sent across the "green/yellow" boundary to any Peer. However, when sending across the "green/yellow" boundary, would not add her signature to the block.

The recipient would be able to validate all the "green" signatures up to the sender, and if present, the sender’s signature as well. If the "green" signature does not include the sender, no more signatures can be attached. When sending to a "yellow" peer, the "green attribute" block is stripped (if present). The absence of a "green block" means the prefix is considered "yellow". This mechanism is not "free" in that more crypto calculations are needed, the structure of the BGPSEC attributes change, and more data is needed on each announcement within the "green" zone.

However, no information concerning relationships is leaked, beyond what the recipient can already infer. A transit provider already knows his/her customers, and their customers, etc.

From a scaling perspective, it should be noted that only customers’ prefixes require additional signatures, so the number of prefixes with those signatures is proportionally smaller. Signature validation is only done on the "green block" upon receiving a customer’s routes or a peer’s routes. This also minimizes the incremental cost.

Since it is physically impossible to promote a "yellow" route to a "green" route, because the originators "green" block is absent, this is a very strong mechanism for stopping route leaks. Validating link type versus color, after validation of any "green block" present, is sufficient to stop route leaks.

5. Security Considerations

None per se.

6. IANA Considerations

This document contains no IANA-specific material.

7. Acknowledgements

To be added later.
8. References

8.1. Normative References


8.2. Informative References


Author’s Address

Brian Dickson
Brian Dickson
703 Palmer Drive,
Herndon, VA  20170
USA

Email: brian.peter.dickson@gmail.com