Network Working Group R. White
Internet-Draft Cisco Systems
Expires: December 17, 2006 June 15, 2006

Architecture and Deployment Considerations for Secure Origin BGP (soBGP)

draft-white-sobgp-architecture-02

Status of this Memo

Copyright Notice

Abstract

There is a great deal of concern over the security of internetworks built using the Border Gateway Protocol to provide routing information to autonomous systems connected to the internetwork. This draft provides an architecture for a secure distributed registry of routing information to address these concerns. The draft begins with an overview of the operation of this system, and then follows with various deployment scenarios, starting with what we believe will be the most common deployment option.

1. Motivation

2. Overview

There are two fundamental pieces of a routing system that need to be secured:

- Adjacencies between devices running the routing protocol.
- Information carried within the routing protocol.

While security between [BGP] speakers has been addressed in a number of ways, including cryptographic authentication [BGP-MD5] and limiting the attack radius through TTL mechanisms [GTSH], security for the information carried within BGP is not considered a solved problem.

This draft proposes a possible solution to securing the information within BGP, using the certificates and protocol extensions proposed in [SOBGP-BGPTRANSPORT], [SOBGP-CERTIFICATE], and [SOBGP-RADIUS].

3. General Theory

soBGP provides a secure registry mechanism against which a BGP speaker can check:

- The authorization of the AS listed as the originating AS in any received update to advertise reachability to the prefix listed in the update.
- The validity of the AS Path contained in the update.

A valid AS Path, in this document, is a path that has the following attributes:

- Each autonomous system listed in the AS Path is an actual participant in the internetwork.
- Each pair of autonomous systems listed in the AS Path are actually interconnected.
- Starting from the first autonomous system (the origin AS), and passing through each autonomous system listed in the AS Path, actually results in reaching the advertising peer's AS.

As shown in [PATH-CONSIDER], it isn't possible to verify an AS more than one AS hop away has authorized the advertisement of specific reachability information based on the AS Path. The concept of policy, and soBGP's interaction with policy, is considered more fully in a later section in this draft.

soBGP operates by distributing a set of signed certificates, described in [SOBGP-CERTIFICATE], containing the information required to validate the two pieces of information given above. These certificates MAY be distributed using the mechanisms described in [SOBGP-BGPTRANSPORT], or some other mechanism. Once these certificates have been received and processed (signatures validated, etc, as described in [SOBGP-CERTIFICATE], they form a database containing:

- A listing of IP address blocks and the AS authorized to originate them.
- Policies related to specific prefixes and blocks of addresses.
- A list of autonomous systems connected to each autonomous system within the internetwork. This connection list is used to build a graph of AS interconnectivity within the internetwork, as described in the section Building the AS Connectivity Graph, below.

This effectively forms a secure registry of routing information which can be used to check the validity of routing information received from BGP peers. This database is termed the "authorization database." No assumption about the location of the authorization database is made within this document.

As BGP updates are processed, a security preference is assigned to each prefix, as described further in the Security Preference section of this document. BGP update processing is described in the Receiving and Processing Updates section of this document.

4. soBGP Operation

Each section below provides detailed information on some aspect of soBGP operation.

4.1. Building the AS Connectivity Graph

Each ASPolicycert advertised by a member of the internetwork contains a list of the autonomous systems the advertising AS is connected to, along with possible policy information about that connection. From this information, a graph of AS connectivity within the internetwork is built.

Any AS can be used as the starting point for building this graph, thus multiple disconnected graphs (representing section of the internetwork running soBGP and providing interconnection information) are possible. If every AS within the internetwork is providing interconnection information, one graph can be built containing all

the internetwork's interconnections.

The process of creating this graph is:

- Begin with the local AS, or any AS for which an ASPolicycert is available.
- Examine the list of connected autonomous systems advertised by the current AS.
- Examine the ASPolicycert of each AS the current AS is advertising as connected, and determine if that AS is advertising a connection back to the current AS. This is termed the two way connectivity check.
- If the two way connectivity check passes, the connection SHOULD be added to the interconnection graph, and marked as trustable.
- If the two way connectivity check fails, the connection MAY be added to the interconnection graph, but marked so a lower security preference will be assigned to routes containing this AS pair in their AS Path.
- Apply any policies indicated by either of the two autonomous systems in their ASPolicycert. This could include, for instance, noting the connected autonomous system MUST NOT be used for transiting traffic.
- Repeat this process for each ASPolicycert in the authorization database.

The resulting graph is called the internetwork graph.

4.2. Validating Routing Information (The Security Preference)

soBGP provides a two tier evaluation of routes. In the first stage, a BGP speaker evaluating received routing information would discard all routing information found to be false, or not accurately representing the internetwork as it exists. Routing information not meeting this criteria SHOULD be discarded, as indicated in the processing steps outlined below.

In the second tier, the BGP speaker assigns a Security Preference to the received routing information, indicating a locally significant trust level determined by examining the received routing information. The amount by which the Security Preference is increased or decreased for any operation described in this draft is locally significant to the autonomous system. This allows the operator provide a finer granularity of security policy, from dropping routing information deemed invalid through simply preferring routes the operator deems "more secure."

The operator MAY configure a lower bound. Routes with Security Preferences under this lower bound SHOULD be discarded. Any of the

following methods may be used to implement the Security Preference within an autonomous system:

- o Assign the value of the Security Preference to any of the attributes used in the [BGP] decision process. Care must be taken with attributes for which the lower value is preferred.
- o Use a Cost Community [COST] and its associated methods to consider the Security Preference at any step in the Decision Process [BGP] without overloading other attributes. Care must be taken as the lowest value in a Cost Community is preferred.

Several basic rules apply to all BGP speakers either evaluating the security level of received routing information, or using the Security Preference to determine which path to install in the local RIB:

- o The method selected to implement the Security Preference MUST be consistent through the local autonomous system.
- o All devices processing routes against soBGP information MUST use the same mechanisms and values of the Security Preference to ensure consistent routing within the autonomous system.
- o The Security Preference value may be used to select among different routes for the same prefix; the higher value MUST be preferred.

The process described below does not rule out additional policies added locally, or in some future draft. For each route (prefix/ attribute pair) within a given BGP UPDATE message:

- o The local authorization database is examined, and the Authcert with the longest prefix length encompassing the range of addresses described by the prefix is chosen. If there is no entry in the local authorization database which encompasses the range of addresses described by the prefix, then the route is said to be unverified. The Security Preference SHOULD be set to a level indicated by local policy.
- o If there is an AS_SET in the AS_PATH, the following process MAY be followed for each AS_SET:
  - * For each AS in the AS_SET, examine the set of PrefixPolicycerts advertised by that AS.
  - * If a PrefixPolicycert is found authorizing at least one of the autonomous systems in the AS_SET to advertise some component of the prefix, the Security Preference MAY be increased or left at its current value.
  - * If a PrefixPolicycert is not found authorizing at least one of the autonomous systems in the AS_SET to advertise some component of the prefix, the Security Preference MAY be decreased or left at its current value.

    - If a path exists from the aggregator to each AS listed in the AS_SET, the Security Preference MAY be increased or left at its current value.
    - If a path does not exist from the aggregator to each AS listed in the AS_SET, the Security Preference MAY be decreased or left at its current value.
- If there is an AS_SET in the AS_PATH, it is disregarded in all further processing. The first AS contained in the AS_PATH not contained in the AS_SET is considered the originator of the route for the remainder of the processing.
- The second hop in the AS_PATH attribute is examined.
    - If the second hop in the AS_PATH is advertised as connected by the originating AS, the Security Preference for this prefix SHOULD be increased.
    - If the second hop in the AS_PATH is not advertised as connected by the originating AS, the Security Preference for this prefix SHOULD be decreased.
    - If the second hop in the AS_PATH is not advertised as connected by the originating AS and the originator's policy indicates the second hop MUST be validated, the prefix SHOULD be removed from further consideration.
- The AS_PATH attribute is compared to the internetwork graph.
    - If a series of two way verified pairwise peerings exists, beginning with the first AS listed in the AS_PATH, and ending in the advertising AS, the Security Preference SHOULD be increased.
    - If a series of pairwise peerings exists, beginning with the first AS listed in the AS_PATH, and ending in the advertising AS, the Security Preference MAY be increased. This case allows for the inclusion of one-way advertised AS interconnections in the graph.
    - If the AS_PATH described is not contained within the internetwork graph, and the originator indicated the AS_PATH MUST be checked, the prefix SHOULD be removed from further consideration.
    - Otherwise, the Security Preference SHOULD be decreased.
- The Authcert chosen at the first step is examined.
    - If the authorized AS in the Authcert matches the originating AS in the AS_PATH, the Security Preference SHOULD be increased.
    - If the authorized AS in the Authcert does not match the originating AS in the AS_PATH, the prefix SHOULD be removed from further consideration.

4.3. Validating Received BGP UPDATES

As BGP UPDATES are received, they MAY be processed at one of several points:

- Each prefix may be validated according to the process outlined in Validating Routing Information before they are installed in the ADJ-RIB-IN.
- Each prefix may be validated according to the process outlined in Validating Routing Information after they are installed in the ADJ-RIB-IN, but before they are considered in the BGP Best Path calculation.
- Each prefix may be validated according to the process outlined in Validating Routing Information after they are run through the Best Path algorithm, but before they are installed in the local RIB.
- Routes may be installed in the local RIB, and then validated using the process outlined in Validating Routing Information. Once validation is accomplished, the local RIB and routes advertised to BGP peers may need to be adjusted.

4.4. Requirements for Systems Running soBGP

This section describes requirements for autonomous systems running soBGP, requirements for BGP speakers forming external adjacencies from within such autonomous systems, and devices exchanging soBGP certificates.

- Any peering session along the border of an autonomous system running soBGP SHOULD be authenticated through some means such as [BGP-MD5], IPsec ([ESP], [AH]), or through some other current, effective means of protecting BGP sessions from being hijacked, or otherwise abused.
- Any peering session along which soBGP certificates are exchanged SHOULD be authenticated through some means such as IPsec ([ESP, [AH]), or through some other current, effective means of protecting these sessions from being hijacked, or otherwise abused.
- For each received route, the last (most recently added) autonomous system MUST be compared to the autonomous system of the BGP speaker advertising the route. If the last (most recently added) AS in the AS Path does not match the autonomous system of the transmitting speaker, the route MUST be discarded.

When soBGP is supported, a BGP speaker MUST have access to the authorization database. Possible methods of access include:

- Have a local copy of this authorization database, and perform the checks described later in this document against that local database.
- Pass received routing information to a locally maintained server for validation against that server's copy of the authorization database. [SOBGP-RADIUS] describes one such possible access mechanism, although others are possible.

- Accept filters built from a copy of the authorization database contained on a locally maintained server.

4.5. Logging Requirements

Any system valildating received routing information using an soBGP database built using the mechanisms described in this draft SHOULD log:

- Any change in the Security Preference of any processed route, and the reason for the change in Security Preference.
- Any route that is discarded from further processing, and the reason for the discarding of the route.
- Any route that is marked as unverified.
- The verification of any certificate received by an soBGP speaker.
- Failure to verify any certificate received by an soBGP speaker, and why the certificate failed to be verified.

5. soBGP Deployment

This section begins by describing what we believe to be the most practical deployment of this secure registry of routing information. Following sections describe some other deployment options that may prove useful in some situations, or may prove to be more practical than the deployment outlined in this section.

5.1. Deploying soBGP on Distributed Registry Servers

This deployment scenario works within three constraints:

- It may not be not desirable to combine routing and cryptographic processing of soBGP certificates on the same device.
- The system should be distributed, using as few centralized resources as possible.
- Trust relationships should be based on existing business and working relationships, rather than building new relationships specifically for securing the routing system.

Assume we have a small internetwork, as shown below:

```
S1 - - - - - - - - - - -S2 - - - -S3
10.1.1.0/24---A---B-----C---D-----E---F
| AS65000            | AS65001 | AS65002
```

In this network, we assume each AS has an soBGP server locally within their AS, marked as S1, S2, and S3, above. These servers are interconnected to distribute the certificates described in [SOBGP-CERTIFICATE] between them (possibly using the mechanism outlines in

[SOBGP-TRANSPORT], but other transport mechanisms are possible).

Each server then processes the certificates as described in [SOBGP-CERTIFICATE], and either provides a set of filters or a mechanism through which the eBGP peering routers can authenticate routing information, such as described in [SOBGP-RADIUS]. This deployment technique provides BGP route validation that is:

- Fully Distributed: A local server (or a set of servers) builds the required databases based on received certificates, and distributes certificates throughout the routing system.
- Locally Controlled: Each local server (or set of servers) is maintained and managed by autonomous systems participating in the internetwork.
- Based on Existing Business Relationships: Peering autonomous systems also peer their soBGP servers, so the system uses existing business relationships to provide the deployment and long term maintenance of the system.
- Very Little Impact on the Existing Routing System: The current processing and distribution of routing information through [BGP] isn't impacted in any way. The only additional requirements on existing equipment are to compare the routing information to the database results provided by the local servers (i.e., receiving and processing filter lists, through [SOBGP-RADIUS], or through some other mechanism).

5.2. Certificate Processing on Edge Peering Routers

soBGP can also be deployed entirely within BGP speakers at the edge of an Autonomous System (AS).

```
         +-(eBGP)-+           +-(eBGP)-+
         |        |           |        |
         v        v           v        V

         A--------B-----C-----D--------E

                  ^           ^
                  |           |
                  +--(iBGP)---+
```

In this network, A is sending certificates it has learned from other sources to B using the mechanisms described in [SOBGP-BGPTRANSPORT]. B is passing these certificates to D via iBGP, and D is passing these certificates to E via eBGP. Each edge router, B and D, process these certificates locally, building the databases required to validate received routing information from them.

B has two choices with regard to the certificates it receives from D. It can assume these certificates have been validated before they were transmitted by D, or it can assume these certificates were not validated before being transmitted by D. If B assumes D is validating certificates before transmitting them, then B can place any certificates received from D, an iBGP peer, directly into its local databases. If B assumes D is not validating certificates before transmitting them, then B can validate any received certificates before placing them in its local database. These two options are determined within the autonomous system, and do no impact soBGP's inter-AS operation, nor the overall system operation.

5.3. Multihoming Deployment

Multihoming presents a special challenge to the deployment of soBGP within a large scale internetwork.

```
           (---------)            (---------)
          (  AS65401  )          (  AS65402  )
         (             )        (             )
          (           )          (           )
            (---A---)              (---B---)
                |                      |
                 \                    /
                  \-----+      +-----/
                        |      |
                     (--C------D--)
                    (              )
                     (   No-AS    )
                      (----------)
```

Assume No-AS has obtained a block of addresses, 10.1.1.0/24, from AS65401, and would like to advertise that same block of addresses through AS65402. Since No-AS has no AS number, it cannot generate any soBGP certificates, and must rely on its upstream providers to work out the security impact in some way. The simplest solution would be, of course, for No-AS to obtain an AS number, and fully participate in soBGP, but barring that, what other solutions are there?

- AS65401 could issue a certificate allowing AS65402 to originate just the prefix in question, 10.1.1.0/24. AS6402 could then advertise this certificate.
- AS65401 could list AS65402 in the certificate covering 10.1.1.0/24 as an authorized originator for this address space (as multiple authorized originators are allowed).

These options are also applicable to the case where No-AS receives an

address allocation, perhaps provided with a certificate as described in [RFC3779]. No-AS can use these certificates, provided by the authorizing entity to create and sign Authcerts containing the autonomous system number of each of its service providers (or two Authcerts, one for each service provider).

5.4. Proxy Advertisement of Certificates

Note there is no requirement for a given entity which originates routes into the routing system to actually originate the corresponding certificates required for the correct origination of the route to be validated, and the AS Path attached to the route to be verified.

```
                   (-----------------)
                  ( Other Third Party )
                    (---------------)
                     /              \
                    /                \
           (---------)            (---------)
          (  AS65401  )          (  AS65402  )
         (             )        (             )
          (           )          (           )
            (---A---)              (---B---)
                |                       |
                 \                     /
                  \-----+      +-----/
                        |      |
                     (--C------D--)
                    (              )
                     (  AS65403   )
                      (----------)
```

In this case, AS65401, AS65402, or some other third part may actually advertise the certificates necessary for AS65403 to originate validated routes.

6. Other Considerations

In this section, we move from specific deployment scenarios to other deployment considerations, such as key generation and protection, and memory utilization/impact.

6.1. Certificate Generation and Private Key Protection

There is only one private/public key pair per autonomous system; certificates are generated as determined by local policy and as

required to account for changes in the network. Since the entity's private key is not used in any part of the operations verifying received information, or in generating information to transmit to other devices, these certificates could be generated on some secure central system in the AS, and the results, containing only public keys, can be transmitted throughout the network.

Securing the private key of each entity should be relatively easy in this environment, since the location of the private key can be carefully constrained; no device other than the system which generates the required certificates needs use of the private key.

6.2. Impact on Performance and Memory Utilization

Detailed performance and memory utilization characteristics of soBGP will be the subject of future investigation. However, as this is an important area of consideration, we present some suggested analysis below. (In other words, this is a guess).

In terms of memory, each device running soBGP will need to store:

- o Each of the Entitycerts Received. The maximum number of Entitycerts within the routing system would be the number participating autonomous systems multiplied by the number of outstanding Entitycerts from each autonomous system.
- o Each of the ASPolicycerts Received. The number of ASPolicycerts within the system will probably be similar to the number of Entitycerts within the system.
- o Each of the PrefixPolicycerts Received. The number of PrefixPolicycerts within the system will depend on the number of address blocks each participant in the routing system advertises, and could double during key rollover.

Performance will depend on the cryptographic processing requirements imposed by the certificate signature methods, as described in [SOBGP-CERTIFICATE]. However, all of this additional memory and processing would most likely be required on a distributed soBGP server, rather than on routers themselves.

The primary impact on routers and routing protocol convergence will be the memory and processing requirements added from the additional route filters or processing as required by the deployment technique used.

6.3. soBGP Impact on Internetwork Convergence

We generally assume that adding a security infrastructure on top of an operating system will dramatically decrease the performance of

that system. However, much depends on the system being modified, itself, and how closely to perfectly efficient that system already performs. We've already examined, in prior sections, the impact of soBGP on memory and processor utilization in devices running these extensions, but we've not examined the impact of soBGP on another aspect of an internetwork's operation, convergence time. In this section, we will examine some possible side effects of deploying soBGP using the following small internetwork as an example.

```
+--B--C--D--+
|           |
A---E---F---G---K
|           |
+-----H-----+
```

In this network, assume that:

- o A prefers the path through {H,G} to K.
- o E prefers the path through {F,G} to K.
- o B prefers the path through {C,D,G} to K.

In this network, if the link from G to K fails:

- o A will first receive a withdraw from H, and begin to prefer the path through {E,F,G} to K.
- o A will then receive a withdraw from E, and begin to prefer the path through {C,D,E,G} to K.
- o A will finally receive a withdraw from C, and remove the route to K from its local tables.

This processing pattern is well documented through multiple studies in the operations of [BGP] in large scale internetworks. The most obvious answer to resolve this problem is for G to include some sort of information in its withdraw indicating the nature of the failure, so A can directly remove all paths through the link {G,K} on receiving the first withdraw. This is more problematic than it appears, however, because [BGP] is designed for protocol efficiency, and withdraws are often removed from the internetwork, along with any information they might contain, at an early point in the convergence process.

The mechanism soBGP uses to build a graph of the interconnections between the autonomous systems in the internetwork, however, provide another place where this sort of direct information about changes in the topology of the internetwork can be distributed. If this network were running soBGP, G would be able to reissue its certificate claiming connectivity to K, or use some specific policy indicator to note the link {G,K} has failed. On receiving this certificate, all

the autonomous systems could remove all routes with the link {G,K} in their AS Paths, and the network would converge with much less distribution and processing of routing information.

We believe there are probably several performance enhancements that may be gained through the laying of a connectivity graph on top of the current [BGP] provided view of an internetwork. These types of efficiency gains may overcome or fully offset the added costs of deploying soBGP as a security system.

6.4. Aggregation

Aggregation is a diificult problem within any system attempting to validate routes in an internetwork running BGP. The primary purpose of aggregation is to remove information from the routing system, and information removed from the system cannot be validated or verified. This appears to be a simple observation, but it has a number of far reaching impacts.

```
(    AS1    )  (AS4) (AS5)
10.1.0.0/24----A-----+
                     |
(    AS2    )        |  (AS5)
10.1.1.0/24----------B----C
                     |
(    AS3    )        |
10.1.2.0/24----------+
```

In this small internetwork, B could be:

- o Reoriginating 10.1.0.0/22 towards C. This means that rather than building a BGP aggregate, B is simply generating 10.1.0.0.0/22 locally, and filtering all longer prefix components of this aggregate. This is a common, normally recommended, practice, in many situations. In this case, C will receive 10.1.0.0/22 with an AS Path of {B}.
- o Aggregating 10.1.0.0/22, using the aggregation procedure described in [BGP]. In this case, B will generate an AS Set containing the contributing autonomous system numbers. In this case, C will receive 10.1.0.0/22 with an AS Path of {(1,2,3),4}

If B is reoriginating 10.1.0.0/22, C will not know this route is an aggregate, and MUST treat the route as it does any other received routing information.

If B is building an AS SET, C can examine the aggregator (the first AS listed after the AS Path), and treat this AS as the originating AS, verifying the route as it does any other received routing information. If the internetwork's local policy rules require all

participants to run soBGP, and does not allow any AS to filter soBGP certificates, C can also use the AS interconnection graph to verify B is actually connected to each AS listed in the AS Set.

7. Incremental Deployment of soBGP

One of the primary concerns with any security system is the ability of users to incrementally deploy the system without impacting current network operations. As the security system is deployed, it should provide greater security. In theory, the amount of additional security offered verses the additional work required should be fairly balanced.

There are two aspects of incremental deployment that need to be considered:

- The impact of some of the participants in the system deploying the security system, but not all participants deploy the system.
- The impact of some part of the system being deployed widely, but not all of the system.

7.1. Not All Connected Networks Participate

The first consideration in incremental deployment of soBGP is asking what happens if all of the autonomous systems in an internetwork don't run soBGP. Is there any advantage to partial deployments of soBGP in this sense?

Throughout this section, we will assume soBGP certificates are received by all autonomous systems running soBGP, even if they are separated by multiple hops which are not running soBGP. This is not an unreasonable assumption, since soBGP certificates can be shared in multiple ways, including multihop BGP sessions across non-participating autonomous systems.

Assume we have the following small internetwork, what impact will incrementally deploying soBGP through this network have?

```
(AS1) (AS2) (AS3) (AS4             )
  A-----B-----C-----D---10.1.1.0/24
```

Assume AS3 and AS4 deploy soBGP, but not AS1 and AS2; is there any value in this partial deployment? When AS3 receives routes from AS4, it can verify AS4 is authorized to advertise 10.1.1.0/24. Further, any routes AS3 forwards to AS4 from AS1 or AS2 can be validated, to some degree, by AS4. The AS Path can be checked to make certain AS2 is actually connected to AS3 (since AS3 is advertising its

connectivity to AS3). If some route is advertised from AS2 showing an AS hop in the middle of those two autonomous systems, it can be safely discarded by AS4 as an invalid AS Path.

We can make an alternate assumption, that AS1 and AS4 have deployed soBGP, while AS2 and AS3 have not. In this case, what gains would be made by deploying soBGP? Assume Router A receives a route from Router B with an AS Path of {B,C,D}. If Router A has access to Router D's certificates, it can:

- Check the origin AS (the first AS in the AS Path, in this case AS4) is authorized to advertise the address space (in this case 10.1.1.0/24).
- Check the first hop in the AS Path (in this case AS3) is actually attached to AS4, as advertised by AS4.
- Since Router A knows it is connected to AS2, through B, it can also validate the last AS listed in the AS Path.

There is some gain, then, in deploying soBGP in both of these situations. The gain is obviously more in the second scenario than the first.

7.2. Deploying Parts of soBGP

The second question concerning incremental deploying is if implementing some part of soBGP, without the remainder, would be useful. This question is generally placed in the context of validating the origination authorization of routes, and possibly the first hop in the AS Path, but not the entire AS Path.

- soBGP Authcerts could be advertised or published (for instance, on a Web page), to provide authorization for each origin AS to advertise specific address blocks. These certificates could be self signed, in the most relaxed case, or signed by the entity authorizing the AS to advertise the address block.
- soBGP PrefixPolicycerts could be advertised or published (for instance, on a web page), to provide authorization and first hop checking for received routes. The Authcert within the PrefixPolicycert contains the information required to validate the origin's authorization to originate a route. The list of MAY TRANSIT autonomous systems contained in the PrefixPolicycert would provide the ability to check the first hop in the AS Path of any received route.
- soBGP PrefixPolicycerts and ASPolicycerts could be advertised to provide authorization to advertise a route from within an address block, and also provide the ability to validate the first hop in the AS Path. The Authcert, within the PrefixPolicycert, contains the information required to validate the origin's authorization to

originate a route. The list of connected autonomous systems within the ASPolicycert provides the information required to validate the first hop in the AS Path of any received route.

Any of these modes of operation could be mixed with a full deployment of soBGP, and provides checks for the first hop and origination of received routes.

8. Policy Interactions with soBGP

Beyond simply securing the information contained within the routing database [BGP] builds, it's also desirable to have a secure mechanism for an autonomous system to advertise policy information. For instance, an autonomous system may not want a specific peer to transit traffic, or an originator may want routing information to be advertised only to a specific number of AS hops away from the origin.

The sections below examine some various policies of this type, and possible solutions within soBGP.

8.1. Indicating Do Not Transit

In the following small internetwork, A would like to enforce a policy preventing C from transiting traffic from B to A.

```
     A-------B--------D
     |       |
     +---C---+
```

A may attempt to prevent C from transiting traffic from B to A by advertising its routing information to C in such a way that C cannot readvertise that routing information to B. The problem with this approach is that B must assume the lack of specific routing information from C indicates A has a local policy forbidding C from transiting traffic to A. Unfortunately, because of the nature of address space assignment, aggregation, filtering, and other factors, B cannot make this assumption. For instance, C may receive a superset of the routing information A is advertising, and advertise those routes to B instead, in which case A will find there's no effective way to enforce its policy towards C.

We find, however, that the interconnection graph laid on top of the routing information transmitted by each autonomous system provides a point where A may communicate its nontransit policy towards C directly to B. Using its ASPolicycert, A may indicate B is not a transit AS, allowing B to mark routes with the AS pair {B,A} in their AS Path with a lower security preference, or possibly even discarding

such routing information altogether.

This is a simple application of the policies available in the soBGP certificates; more complex policies may be expressed through similar means. The certificates described in [SOBGP-CERTIFICATE] are built so policies may be added in the future, as well.

9. Acknowledgements

A large number of people contributed to this draft either by contributing text, ideas, or comments; we've tried to include all of them here (but might have missed a few): James Ng, Tim Gage, Alvaro Retana, Dave Cook, Brian Weis, Iljitsch van Beijnum, Bora Akyol, Tony Li, Sue Hares, and Victor P. Long.

10. Security Considerations

11. IANA Considerations

12. References

12.1. Normative References

[BGP] Rekhter, Y. and T. Li, "A Border Gateway Protocol 4 (BGP-4)", RFC 1771, March 1995.

[SOBGP-CERTIFICATE]
Weiss, B., "Secure Origin BGP (soBGP) certificates", draft-weis-sobgp-certificates-01.txt (work in progress), October 2003.

12.2. Informative References

[COST] Retana, A. and R. White, "BGP Custom Decision Process", draft-retana-bgp-custom-decision-00.txt (work in progress), October 2002.

[PATH-CONSIDER]
White, R., "Considerations in Validating the Path in Routing Protocols", draft-white-pathconsiderations-02.txt (work in progress), April 2004.

[SOBGP-BGPTRANSPORT]
Ng, J., "Extensions to BGP Transport soBGP certificates",

draft-ng-sobgp-bgp-extensions-01.txt (work in progress), April 2004.

[SOBGP-RADIUS]
Lonvick, C., "RADIUS Attributes for soBGP Support", draft-lonvick-sobgp-radius-04.txt (work in progress), February 2004.

Author's Address

Russ White, editor
Cisco Systems

Email: riw@cisco.com

Intellectual Property Statement

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.