Routing Protocol Security Requirements
Internet-Draft
Expires: January 20, 2006

B. Christian, Ed.
KMC Telecom Solutions
T. Tauber, Ed.
Comcast

July 19, 2005

BGP Security Requirements
draft-ietf-rpsec-bgpsecrec-02

Status of this Memo

Copyright Notice

Abstract

The security of BGP, the Border Gateway Protocol, is critical to the proper operation of large-scale internetworks, both public and private. While securing the information transmitted between two BGP speakers is a relatively easy technical matter, securing BGP, as a routing system, is more complex. This document describes a set of requirements for securing BGP, including securing peering relationships between BGP speakers, and authenticating the routing

information carried within BGP.

1. Introduction

1.1 System Description

BGP is described in RFC1771 [3], and, more recently, in an updated specification, as a path-vector routing protocol. BGP speakers typically exchange information about reachable destinations (expressed as address prefixes) in an internetwork through pairwise peering sessions. Once this information has been exchanged, each BGP speaker locally determines a loop free path to each reachable destination, based on local policy, policy indicators (or policies) carried in the update, and the AS_PATH data carried in the BGP UPDATE messages.

Each BGP speaker represents an Autonomous System (AS). All of the BGP speakers within an AS operate under a common administrative policy.

1.2 Threats

Violations of security for network and information systems generally fall under one of the three categories as defined in RFC 2196 [1]:

- Unauthorized access to resources and/or information
- Unintended and/or unauthorized disclosure of information
- Denial of service

A number of attacks can be realized which, if exploited, can lead to one of the above mentioned security violations. Attacks against communications are typically classified as passive attacks or active wiretapping attacks. Passive attacks are ones where an attacker simply observes information traversing the network, violating confidentiality or identifying a means of engaging in further attacks. Active attacks are ones where the attacker modifies data in transit. Such attacks include replay attacks, message insertion, message deletion, and message modification attacks. Some attacks may be effected by sending data from any where in the Internet. Other active attacks require a "man-in-the-middle" capability, i.e., the attacker must be in a position where traffic passes through an attacker-controlled device. Attacks against BGP may be used by an attacker to facilitate a wide variety of active or passive wiretapping attacks.

Attacks that do not involve direct manipulation of BGP, and the information contained within BGP, are outside the scope of this document.

Because ASes are autonomous in their operation, it is not possible to mandate secure operation by all ASes, nor would it be advisable to assume such operation. Thus the primary goal of BGP security measures is to provide data to AS operators to enable BGP speakers to reject advertisements (UPDATE messages) that are not valid. For example, UPDATE messages that represent erroneous binding of prefixes to an origin AS, or that advertise invalid paths (as defined later in this document) should be rejected. Because BGP peering sessions take place in the context of TCP, the authentication and integrity guarantees usually association with TCP need to be provided in the face of possible active wiretapping attacks. Using the terminology established in RFC 3552 [2], these peering sessions should be afforded data origin and peer entity authentication and connection-oriented integrity.

Security for subscriber traffic is outside the scope of this document, of BGP security in general. IETF standards for subscriber data security, e.g., IPsec, TLS, and S/MIME should be employed for such purposes. While adoption of BGP security measures may preclude certain classes of attacks on subscriber traffic, these measures are not a substitute for use of subscriber-based security mechanisms of the sort noted above.

1.3 Areas to secure

There are two primary points where BGP may be secured. If we examine the system description presented above those points are as follows.

- The session between two BGP speakers can be secured such that the BGP data received by the BGP speakers can by cryptographically verified to have been transmitted by the peer BGP speaker. There are several existing IETF standards to choose from to ensure that this system functions with greater effectiveness than the current system. Examples include IPsec and TLS.

- The originator and the propagators of prefix information may have their routing preference, such as the LOCAL_PREF Attribute, information verified such that the intent of their preferences with respect to a specific prefix is preserved.

There are also several questions we can ask about the information contained within a received update.

- Is the originating Autonomous System authorized to propagate the prefix we have received?

- Does the AS_PATH, received via an UPDATE, represent a viable path through the network?

The verification of AS_PATH validity falls into two distinct categories. These categories are ordered from least to most rigorous.

- Does the AS_PATH specified actually exist as a path in the network topology and, based on the AS_PATH, is it possible to traverse that path to reach a given prefix? This AS_PATH Feasibility Check will be referred to later in this document.

- Has the update actually travelled the path?

2. Underlying Assumptions regarding BGP

In order to properly identify security requirements it is important to articulate the fundamental aspects of BGP as related to security requirements. The following list presents the basic parameters and application concepts of BGP that are assumed by this document.

- Peer Communication: BGP traffic travels over TCP between peers, so BGP speakers assume the TCP data delivery guarantees of TCP in a benign environment. This includes ordered, error-free delivery of application traffic from a peer identified by an IP address, plus integrity of the control aspects of TCP. From a security perspective, these guarantees need to be enforced in the context of possible active wiretapping.

- Routing and Reachability: BGP is a protocol used to convey routing and reachability information both internal and external to an Autonomous System. Typically, interior BGP (iBGP) is used to distribute prefix reachability information in conjunction with an IGP and is used by a distinct network administrative entity to convey internal routing policy regarding external and internal information. Exterior BGP (eBGP) is typically used to distribute route/prefix reachability information between two distinct routing entities and is used to signal eBGP preferences and policy decisions.

- Inter-AS UPDATE Message assumptions: When an AS distributes reachability information to a peer it is done with the intent of affecting routing decisions by the peer. For example, an AS-A sends peer AS-B a less specific advertisement and peer AS-C a "more" specific advertisement. This prefix distribution decision may have been made to provide a means for failure resolution between AS-A and AS-C. However, it should be noted that while AS-A tries to influence the routing decisions of AS-B and downstream ASes, AS-A is only providing inputs to a local decision by AS-B, a decision that is very much influenced by AS-B's local policy over which AS-A has no control. Update messages are sent between AS peers with the implicit assumption that those messages will be forwarded to others. A notable exception to this assumption is the use of various policy based mechanisms between peers such as the NO-EXPORT community. In this document an important aspect of the UPDATE message to note is that the specific UPDATE message itself is typically not re-transmitted. Instead, the specific UPDATE message is regenerated continually as it passes from BGP speaker to BGP speaker. Furthermore, UPDATE messages have no mechanism for freshness (e.g. timestamps or sequence numbers). This indicates that messages may appear valid at any point in the life of a BGP peering session. While the

AS_PATH information is typically transitive it is, currently, not clearly mandated and many times is removed for various utilitarian reasons.

- It is important to note that while preference regarding routing can be explicity managed with direct peers it is markedly more difficult to influence routing decisions with ASes not directly adjacent.

- Inter-AS withdrawal message assumptions: The processing model of BGP RFC1771 [3] indicates that only the peer advertising NLRI information may withdraw it. There are several instances where a withdrawal may occur. Typical reasons for withdrawal include the determination of a better path, peer session failure, or local policy change. There is no specified mechanism for indicating, to an external peer, the reason for a route withdrawal. Each withdrawal received from a valid peering session must be taken at face value. There is no existing method to ensure that an AS will properly propagate withdrawal messages received from its external peers nor do mechanisms exist to ensure that old UPDATES are not re-propagated.

- AS_PATH assumptions: Aside from the use of AS_SET, the AS_PATH is typically considered to be an ordered list of the Autonomous Systems that an update has traversed. In most cases the rightmost AS in the list is the origin AS, or at least the AS responsible for the management of the NLRI information associated with the first AS. Specifications state that the AS topology MUST be loop free. This indicates that updates received from an external peer which contain the local AS will be rejected. The prepending of AS information for received updates and transmitted updates is generally permitted and is common practice. Prepended AS information on inbound advertisements (where the external peers AS is prepended) and outbound advertisements (where the local AS number is prepended) is a commonly used method to effect forwarding changes. Prepending a peer AS on inbound reception is accomplished for internal routing and forwarding management while prepending one's own AS on outbound advertisement is typically accomplished to effect forwarding and routing changes in external networks. The common practice is to prepend (possibly multiple) instances of either one's own AS number or that of the neighbor from which an update was heard. Another practice, according to some operators, involves inserting a remote AS number, in order to cause the update to be dropped by that AS so that traffic will not traverse a given path. Though this practice appears to be unintended in the design in BGP, anecdotal evidence is that its use is not totally insignificant. While such a practice can be beneficial to legitimate operators, it presents a strong potential

for misuse. A proposed security system SHOULD address how to either address this concern or give specific information on this topic for consideration by the Operational community.

- Route Origination: BGP speakers may originate routes based on various internal and external data. An Autonomous System should only originate a prefix to its external peers if that prefix has been somehow allocated to the administrators of that system, or authorized by the prefix holders.

- Originating a route without the ability to forward the traffic associated with that route is, in most cases, in conflict with the intent of the BGP specification, notable exceptions include:

  * Deployments that make extensive use of separate route servers and forwarding devices

  * Deployments that use the propagation of prefixes in order to effectively block high bandwidth attacks against specific IP addresses (and the associated oversubscription of resources).

- Aggregation and de-aggregation: According to RFC1771 [3], if a BGP speaker chooses to aggregate a set of more specific prefixes into a less specific prefix then the ATOMIC_AGGREGATE attribute SHOULD be set. This creates a significant potential loophole in an attempt to secure BGP based on the RFC specifications.

3. Operational Requirements

We have determined, through discussion with several large internetwork operators and equipment vendors, that the following attributes are important to the ongoing performance of interdomain routing systems such as BGP.

3.1 Convergence speed

Convergence speed is a major concern to many operators of large scale internetworking systems. Networks, and internetworks, are carrying ever increasing amounts of information that is time and delay sensitive; increasing convergence times can adversely affect the usability of the network, and the ability of an internetwork to grow. BGP's convergence speed, with a security system in operation, SHOULD be equivalent to BGP running without the security system in operation. This includes the preservation of optimizations currently used to produce acceptable convergence speeds on current hardware, including update packing, peer groups, and others. Two types of verification MAY be offered for the NLRI and the AS_PATH in order to allow for a selection of optimizations:

- Contents of the UPDATE message SHOULD be authenticated in real-time as the UPDATE message is processed.

- The route information base MAY be authenticated periodically or in an event-driven manner by scanning the data and verifying the originating AS and the validity of the AS_PATH list.

All BGP implementations that implement security MUST utilize at least one of the above methods for validating routing information. Real time verification is preferred in order to prevent transitive failures based on periodic or event-driven scan intervals.

3.2 Incremental deployment

We will not be able to deploy a newly secured BGP protocol instantaneously and will be unable to dictate a partitioning of large ASes by network operators. Because of this, there are several requirements that any proposed mechanism to secure BGP must consider.

- A BGP security mechanism MUST enable each BGP speaker to configure use of the security mechanism on a per-peer basis.

- MUST provide backward compatibility in the message formatting, transmission, and processing of routing information carried through a mixed security environment. Message formatting in a fully secured environment MAY be handled in a non-backward

compatible fashion though care must be taken to ensure when traversing intermediate routers which don't support the new format.

- In an environment where both secured and non-secured systems are interoperating a mechanism MUST exist for secured systems to identify whether an originator intended the information to be secured.

3.3 Conditions for initialization

A key factor in the robust nature of the existing internal and external relationships maintained in todays Internet provider space is the ability to maintain and return to a significantly converged state without the need to rely on systems external to the routing system (the physical equipment that is performing the forwarding). In order to ensure the rapid initialization and/or return to service of failed nodes it is important to reduce reliance on external systems to the greatest extent possible. Therefore, proposed systems SHOULD NOT require connections to external systems, beyond those directly involved in peering relationships, in order to return to full service. Proposed systems MAY require post initialization synchronization with external systems in order to synchronize security information.

3.4 Local controls for secure UPDATE acceptance

Each secured environment may have different levels of requirements in terms of what is acceptable or unacceptable. In environments that require strict security it may not be acceptable to temporarily route to a destination while waiting for security verification to be performed. However, in many commercial environments the rapidity of route installation may be of paramount importance; in order to facilitate the more common occurence of route withdrawal due to network failure. Based on the two divergent requirements, the following criteria apply.

- The security system MUST support a range of possible outputs for local determination of the trust level for a specific route so that routing preference and policy can be applied to its inclusion in the RIB. Any given route should be trustable to a locally configured degree, based on the completeness of security information for the update and other factors.

- The security system SHOULD allow the operator to determine whether the speed of convergence is more important than security operations, or security operations are more important than the

speed of convergence. This facilitates the incremental deployment of security on systems not designed to support increased processing requirements imposed by the security system.

4. Infrastructure Requirements

In the case that proposed BGP security mechanisms make use of a security infrastructure to distribute authenticated data that is an input to routing decisions. Such data may be needed to verify whether a given AS is authorized to originate an advertisement for a specified prefix, whether an given organization is the recognized holder of a block of address space or of an AS number, etc. Any infrastructure used to distribute data in support of BGP security is subject to the following criteria:

- It MUST be resilient to attacks on the integrity of the data it contains.
- It MUST enable network operators to verify the origin of the data.
- It MUST be sufficiently available so as to not degrade the existing pace of network operations.
- It SHOULD not introduce new organizational entities that have to be trusted in order to establish the authenticity of the data.

5. The Trust Model

In discussion with the operations community, concerns have emerged regarding the viability of a security system which requires agreement on a hierachical trust model dependent on a single root. Current operational practice has many providers engaging in bilateral agreements which local policy choices remaining sacrosanct. The viability of a solution may well rest on the business imperatives of the provider community which may be unwilling to surrender their percieved autonomy or unable to come to communal agreement on this topic.

In other environments, deployments may require an authority which has been decided by law or other institutional mandate. Moreover, these two deployment types (single-rooted heirarchy or arbitrary association) may "touch" (i.e. be part of the same co-extensive BGP topology).

Solutions MUST account for these differing types of deployments.

If two internetworks using differing trust models are interconnected they MUST be able to interoperate using locally determined levels of trust to compensate for differences in their trust models. Some acknowledgement is made that this requirement might render it difficult to discern an attack from a difference in trust model or implementation. Any proposed solution MUST mitigate this risk.

6. The AS_PATH Attribute and NLRI Authentication

BGP distributes routing information across the Internet (between BGP speakers) using BGP UPDATE messages. The UPDATE message contains withdrawn routes, path attributes and one or more NLRIs (Network Layer Reachability Information is synonymous with advertised prefix). For the remainder of this section, we will focus on the AS_PATH Attribute and the NLRI. Attributes such as local pref are locally specific and, as such, are protected by BGP session security.

The AS_PATH for specific prefixes may be protected in any proposed security system in four ways:

- Authorization of Originating AS: For the purposes of authorization of the originating AS, verifiable means that it is possible to determine the authorization of the originator of a specific prefix (or block of IP addresses) relative to the organization that holds the prefix.

- Announcing AS Check: For all BGP peers, a BGP Implementation MUST ensure that the first element of the AS_PATH list corresponds to the locally configured AS of the peer from which the UPDATE was received.

- AS_PATH Feasibility Check: The AS_PATH list MUST correspond to a valid list of autonomous systems according to the first verification category listed in the "Areas to Secure" Section above.

- Update Transit Check: Routing information carried through BGP SHOULD include information that can be used to verify the readvertisement or modification by each autonomous system through which the UPDATE has passed. This check is somewhat more rigorous than the "verifiable list of autonomous systems" above.

Both checks SHOULD be made available to operators who MAY employ more rigorous checks according to the needs of the deployment.

There are many ways in which a differential between the speed of prefix/AS path attribute propagation and the information validating the the prefix/AS_PATH attribute information can be exploited to attack the routing system on a temporary basis. These types of attacks are dominantly exploitative of the time it takes to follow the withdrawal of a route via an update. As a result of this potential for temporary disruption, BGP security solutions MUST propagate security information at the same rate as the BGP announcements and withdrawals propagate.

The following items are required to propagate at the same rate:

- the distribution of key information used by individual actors within the system, including the keys used by individual autonomous systems to sign certificates and other objects,

- the distribution of information about the AS(es) authorized to advertise a given block of IP addresses (or an address space),

- the distribution of information about connectivity between autonomous systems and about autonomous system polcies.

Note that in today's operational Internet, the first two pieces of information, or their analogues, are not a part of the BGP routing system per se (e.g. information in Routing or Address regisistries.) They are consulted by operators on an inconsistent basis and do are not consulted in real time by the routing system. The third piece of information is explicitly carried in the routing system and inconsistently expressed and consulted by operators. However, the ability to change the connectivity in real time is an important feature of the current Internet.

7. Address Allocation and Advertisement

As part of the regular operation of the Internet, addresses that are allocated to one organization may be, and are quite commonly, advertised by different organizations. Common reasons for this practice include multi-homing and route reduction for the purposes of resource conservation (e.g aggregation). There are two modes of delegation:

- A BGP speaker and listener have chosen to restrict the amount of received prefixes for the listener. The listener has chosen to honor route announcements sent in a summary fashion by the speaker.

- Address space that is being delegated is part of a larger allocation that is owned by an autonomous system. The owner then delegates the smaller block to another AS for purposes of advertisement. This mode is commonly observed in multi-homing.

These two modes lead to a single common requirement: Any BGP Security solution MUST support the ability of an address block holder to declare (in a secure fashion) the AS(es) that the holder authorizes to originate routes to its address block(s) or any portion thereof regardless of the relationship of the entities.

An associated delegation criteria is the requirement to allow for non-BGP IP end user implementations. As a result, all secured BGP implementations MUST allow for the contemporaneous origination of a route for a prefix by more than one AS.

8. Logging

In order to facilitate auditing and troubleshooting, a logging capability MUST be implemented which will indicate both negative and positive event behaviors. This data SHALL be for consumption of the AS operating the device which is producing the logs and MAY be combined with data from other ASes or devices with different implmentations within the same AS for purposes of event correlation and tracking. Here follow some considerations in this regard:

The data generated by logging may be very large depending on the number of peers, the number of prefixes received, the authentication model used, and routing policies. As such, efficient data structures and storage mechanisms MUST be developed to allow for an effective means of reproducing incidents and outages

Path and NLRI attributes MUST be logged using a standard format. The format MUST be scalable with the amount of data logged and the frequency of log generation. The frequency of log generation should be controllable by the operator. The logging mechanisms for the tracked information MUST be standardized across all platforms. Logging ability both on and off line is considered highly desirable.

9. NLRI and Path Attribute Tracking

The ability for a receiver to know exactly who originated and forwarded a routing update is a desirable trait. In order to rapidly identify attack points and parties at fault for route table disruption, it is important to be able to track and log prefix origination information along with associated security information.

This capability can be afforded by implementation of the aforementioned directive that any security system SHOULD provide a method to allow the receiver of an update to verify that the originator is actually authorized to originate the update, and that the AS's listed in the AS_PATH actually forwarded the update.

10. Transport Layer Protection

Transport protection is an important aspect of BGP routing protocol security. The potential to create a linked transport/NLRI/AS_PATH authentication mechanism should not be overlooked and may provide for the accelerated deployment of a BGP security system. Current security mechanisms for BGP transport (e.g. TCP-MD5 [4] and GTSM [6]) are inadequate and require significant operator interaction to maintain a respectable level of security.

Transport protection systems SHOULD function as a component of the BGP routing protocol security mechanism. This includes the use of the same key generation/management systems as the rest of the security system.

Any proposed security mechanism MUST include provisions for securing both internal BGP and external BGP peering sessions.

11. Key Management

Current implementations and deployments of TCP-MD5 [4] exhibit serious shortcomings with regard of key management as described in RFC 3562 [5] which involve key generation, handling, and distribution.

Key maintenance can be especially onerous to the operators. The number of keys required and the maintenance of keys (update/withdraw/renew) has had an additive effect as a barrier to deployment. Thus automated means of managing keys, to reduce operational burdens, MUST be available throughout BGP security systems. These security systems MUST be resistant to compromise of session-level or device-level keys, i.e., the security implications of such compromises MUST be limited.

12. References

[1] Fraser, "RFC 2196 - Site Security Handbook", September 1997.

[2] Rescorla, Korver, and Internet Architecture Board, "RFC 3552 - Guidelines for Writing RFC Text on Security Considerations", July 2003.

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

[4] Heffernan, "RFC 2385 - Protection of BGP Sessions via the TCP MD5 Signature Option", August 1998.

[5] Leech, "RFC 3562 - Key Management Considerations for the TCP MD5 Signature Option", July 2003.

[6] Gill, Heasley, and Meyer, "RFC 3682 - The Generalized TTL Security Mechanism (GTSM)", February 2004.

Authors' Addresses

Blaine Christian (editor)
KMC Telecom Solutions
1545 U.S. Highway 206
Bedminster, NJ 07921
US

Tony Tauber (editor)
Comcast
27 Industrial Avenue
Chelmsford, MA 01824
US

Email: ttauber@1-4-5.net

Appendix A. Acknowledgements

The following individuals contributed to the development and review of this draft. Steve Kent, Russ White, Sandy Murphy, Jeff Haas, Bora Akyol, Susan Hares, Mike Tibodeau, Thomas Renzy, Kaarthik Sivakumar, Tao Wan, Radia Perlman, and Merike Kaeo.

This draft was developed based on conversations with various network operators including Chris Morrow, Jared Mauch, Tim Battles, and Ryan McDowell.

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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