Network Working Group M. Behringer
Internet-Draft Cisco Systems Inc
Intended status: Informational July 10, 2008
Expires: January 11, 2009

BGP Session Security Requirements
draft-ietf-rpsec-bgp-session-sec-req-01.txt

Status of this Memo

Abstract

The document "BGP security requirements" (draft-ietf-rpsec-bgpsecrec) specifies general security requirements for BGP. However, specific security requirements for single BGP sessions, i.e., the connection between two BGP peers, are only touched on briefly in the section "transport layer protection". This document expands on this particular aspect of BGP security, defining the security requirements between two BGP peers.

Table of Contents

1. Introduction and Problem Statement

The document "BGP security requirements" [I-D.ietf-rpsec-bgpsecrec] specifies general security requirements for BGP. However, specific security requirements for single BGP sessions, i.e., the connection between two BGP peers, are only touched on briefly in the section "transport layer protection". This document expands on this particular aspect of BGP security, defining the security requirements between two BGP peers.

It is important to note that security requirements between BGP peers are not limited to the BGP protocol itself or a particular layer of the OSI stack. Crafted ICMP messages for example may have an impact on an established BGP session: An ICMP port unreachable, referring to the BGP port on the peer router, would tear down the BGP session, if no additional security measures are taken to prevent this. A similar effect can be achieved with ICMP source quench messages. Some of the mechanims currently employed to secure a BGP session are on the TCP layer (e.g., MD5), some on the IP layer (e.g., GTSM). This document provides an overall, practical view on the security requirements for BGP sessions, not limited to the BGP protocol.

Previous work in this area includes most notably the following documents:

- "Protection of BGP Sessions via the TCP MD5 Signature Option" [RFC2385]
- "Key Management Considerations for the TCP MD5 Signature Option" [RFC3562]
- "Key Change Strategies for TCP-MD5" [RFC4808]
- "The Generalized TTL Security Mechanism (GTSM)" [RFC5082]
- "Problem Statement and Requirements for a TCP Authentication Option" [I-D.bellovin-tcpsec]
- "The TCP Authentication Option" [I-D.ietf-tcpm-tcp-auth-opt].
- "BGP Security Requirements" [I-D.ietf-rpsec-bgpsecrec]
- "Generic Security Requirements for Routing Protocols" [I-D.ietf-rpsec-generic-requirements]
- "An Attack Tree for the Border Gateway Protocol" [I-D.ietf-rpsec-bgpattack]
- "Automated key selection extension for the TCP Enhanced Authentication Option" [I-D.weis-tcp-auth-auto-ks]
- "Backbone Infrastructure Attacks and Protections" [I-D.savola-rtgwg-backbone-attacks]

Current implementations of BGP include a combination of some of these mechanisms. However, while the security level achieved with these is probably currently acceptable for most providers, they pose some operational challenges which limit the effectiveness of BGP point to point security. Current problems with BGP session security (between

BGP peers) include:

- o The use of static keys, which tend to be changed infrequently, and often not at all. [RFC3562] states that keys SHOULD be changed at least every 90 days. However, the relative complexity of changing MD5 keys on all BGP peering sessions, specifically when securing sessions to routers maintained by two different organisations, means that keys are often not changed at all. This makes long term brute force attacks feasible.
- o The key change process needs to be coordinated between both sides of the BGP session, making this an operationally expensive exercise.
- o The keys are typically chosen by humans, and expressed in ASCII; therefore, the entropy is typically small, making the keys easier to guess. [RFC3562] outlines this problem.
- o Dependence on the MD5 algorithm, which brings two problems: MD5 is not considered strong enough for the future. ([RFC4278] states that "the IESG believes that [RFC2385], though adequate for BGP deployments at this moment, is not strong enough for general use".) And, security architectures should also allow a choice of algorithms, to have an alternative in case serious vulnerabilities are discobered in an algorithm.
- o Where confidentiality of BGP routing information is required, this can only be achieved today by securing the BGP session with IPsec. Other ways to provide confidentiality may be required in the future.

This document lists the requirements for BGP session security, with the goal to provide a guideline for flexible, operationally manageable, and secure algorithms for BGP session protection.

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in [RFC2119].

2. The Threat Model

The threat model presented here is based on the document "Generic Threats to Routing Protocols" [RFC4593], which explains generic threats to routing protocols. That document provides a categorization and classification of threat sources, threat actions, threat consequences, threat consequence zones, and threat consequence periods.

Security threats to point to point BGP sessions can be classified with the following parameters:

- Threat source: Any host in the Internet that can reach one of the BGP peers. (By using The Generalized TTL Security Mechanism (GTSM) [RFC5082] the threat source must be within the configured IP hop count, in the ideal case directly connected.) A threat source can also be a wire tap agent, either passively listening to the BGP session, or actively modifying BGP data in transit.
- Threat action: Sending of forged BGP packets, or sniffing BGP traffic.
- Threat consequence: Break of confidentiality by wire tapping, break of integrity by faking BGP messages or hijacking a session, or denial of service, for example by sending fake RST packets, terminating a BGP session abnormally.
- Threat consequence zones: The BGP peering session itself, the BGP tables on the affected peers, or potentially larger areas of the BGP routing system.
- Threat consequence period: Depending on the attack and the implemented counter measures, a threat might be preliminarily mitigated by changing the MD5 key, unless it is a threat against MD5 itself, in which case the threat period is indefinite.

Threats not considered in this document include:

- Attacks from legitimate BGP speakers, in other words, attacks from other BGP speakers, which are trusted (implicitly or explicitly). The source of the attack in this case could be either a misconfiguration, or an attacker gaining illegitimate access to a router, for example through SSH brute force attacks.

The document "Backbone Infrastructure Attacks and Protections" [I-D.savola-rtgwg-backbone-attacks] describes general attack forms against backbones, not limited to the BGP protocol. It provides useful background information to this threat model.

3. BGP Session Security Requirements

3.1. BGP Speaker Identity

A BGP speaker MUST have a unique identity to present to its peer. This serves as a base for subsequent security mechanisms, such as peer authentication. At this moment this identity is tied to the IP address used for the BGP peering session. This address can be either the IP address of a loopback interface, or a physical interface.

Any point to point security mechanism for BGP MUST refer to and use a specific BGP ID. This ID MUST be unique for the BGP peers, it SHOULD be unique within an autonomous system, and it MAY be globally unique.

A BGP speaker SHOULD be capable of using different IDs to different

peers, because a single router identity (the same ID for all peers) may not be sufficient from an operational point of view. For example internally a provider may want to use address space which should not be seen from or accessible to the outside of his network. Alternatively, a provider who uses private address space [RFC1918] inside his network for iBGP sessions, may want to use public address space for eBGP sessions on the same router.

Although currently the IP address used for the BGP peering is used as an identifier, it is entirely possible to use an alternative BGP ID, for example based on public/private key pairs, or the HIP architecture [RFC4423]. The document "AS-wide Unique BGP Identifier for BGP-4" [I-D.ietf-idr-bgp-identifier] for example proposes a 4-byte unsigned, non-zero integer as an identity, which should be unique in the autonomous system.

Note that this document does not mandate or recommend the use of a particular type of BGP ID, nor does it discuss the differences between the various approaches. It only specifies the generic requirements for BGP IDs.

3.2. Peer Authentication

A BGP speaker MUST have a way to authenticate messages from its peer. Currently this is achieved by [RFC2385] derived mechanisms, however, several alternatives are conceivable and partly under discussion, for example [I-D.ietf-tcpm-tcp-auth-opt]. Also IPsec [RFC4301] provides peer authentication, as does TLS [RFC4346] or SSH [RFC4251]. (Note: Key management is discussed below.)

3.3. Integrity

A BGP speaker MUST have methods to ensure integrity of messages in transit, to avoid insertion of fake messages in the transport layer. This requirement is currently addressed by RFC 2385-derived mechanisms. However, new methods should avoid the operational issues mentioned in the introduction of that RFC. It MUST be possible to use various algorithms, either statically by specifying the algorithms used for integrity services, or by dynamic negotiation. (Note: Key management is discussed below.)

3.4. Confidentiality

A BGP speaker MAY have mechanisms to encrypt BGP messages in transit, thus providing confidentiality. This service is rarely used today, but since BGP is used increasingly for more applications, amongst which for example signaling security measures, it is conceivable that the need for confidentiality for BGP sessions will increase. If

confidentiality services are provided, they MUST allow for different crypto algorithms, and negotiation of which algorithm to use. (Note: Key management is discussed below.)

3.5. Anti-Replay

A BGP speaker MUST have methods to detect and prevent replay of messages, to avoid for example an attacker saving a session reset message, and replaying it later, to produce a denial of service attack.

3.6. Availability and Restricting IP Reachability

A BGP speaker SHOULD have mechanisms to protect the BGP session against denial of service attacks, targeting the availability of the BGP session. More specifically, a BGP speaker SHOULD have mechanisms to drop non-session packets efficiently (with minimum CPU impact, specifically before any crypto operations). This includes access control lists (ACL) on layer 3/4 and possibly layer 2, providing easy protection against some forms of attack. It also includes TTL based mechanisms such as proposed in [RFC5082]. Any reachability restriction of these types MUST be carried out before more CPU intensive tasks such as crypto operations, to be effective against denial of service attacks.

Fragmentation attacks can bypass layer 4 ACLs, by fragmenting packets in a way that no fragment is recognized by the ACL. (Note that layer 4 ACLs still provide operationally useful filtering, and should therefore be supported.) Fragmentation cannot occur on a single-hop BGP session, therefore a BGP speaker MUST have the capability to drop fragments on a single-hop BGP session. On multi-hop BGP sessions fragmentation should not occur, if the network has been correctly designed, therefore a BGP speaker SHOULD also be capable of dropping fragements on a multi-hop BGP session. Also on other, related, protocols fragmentation needs to be specially considered, since it can bypass some forms of ACLs.

The document "Service Provider Infrastructure Security" [I-D.ietf-opsec-infrastructure-security] provides an overview of best practices regarding infrastructure protection, and is useful background material.

3.7. Key Management and Operational Considerations

Some of the requirements above may, in turn, require mechanisms that employ shared keys between the BGP peers. Currently, statically-defined and manually configured keys are used for this purpose. [RFC3562] explains possible shortcomings of such keys, and gives

recommendations to improve security. Key selection is also discussed in [I-D.weis-tcp-auth-auto-ks], as an extension to [I-D.ietf-tcpm-tcp-auth-opt].

For any new mechanism aimed at securing BGP sessions it is highly desirable to use automated key generation and negotiation mechanisms, based on the BGP speaker identity.

Mechanisms based on key lists with defined life times for keys, for example as defined by the document "Authentication-Key Rollover mechanism for Routing and Management Protocols" [I-D.viswanathan-keyrollover] may be acceptable if there are good reasons to avoid automated key negotiation.

3.8. Logging and Alerting

To be able to detect attempts of security breaks, BGP speakers MUST have be able to produce related alerts or logging messages. General considerations to logging apply here: There should be summarization of events, to avoid for example a message to be sent for each packet that is not authenticated. When available, secure syslog should be used to guarantee delivery of those messages to the management center.

3.9. General Considerations

For many of the above mentioned security requirements there are a vast range of protocol and implementation options, with varying degrees of effective security. While strong security is desirable, there are several considerations to be taken into account for a BGP implementation:

- o Efficient use of system resources: Stronger security mechanisms may require more system resources (CPU, memory, bandwidth) than more light-weight versions, or the unprotected BGP protocol. A security mechanism may lead to an excessively higher exposure to denial of service attacks than the unprotected protocol, or another security mechanims.When considering security mechanisms, the "cost" in terms of system resources should be taken into account.
- o Ease of configuration: Complicated configurations increase the likelihood for misconfigurations, with potential security vulnerabilities. BGP security mechanisms should therefore be easy to configure, where "easy" referes to both the length of the configuration, as well as the complexity of it.

Both efficient use of system resources and ease of configuration cannot be judged on their own, but rather represent additional variables to judge an overall BGP security implementation. In other

words, a highly secure, but also highly complex and resource-consuming solution may be less preferrable over a somewhat less secure but simple and light-weight solution. This has to be decided case-by-case.

4. Security Considerations

This document is entirely about security requirements for BGP point-to-point connections. No new security exposures are created by this document.

5. Acknowledgements

The author would like to thank Russ White, Alvaro Retana, Brian Weis, Carlos Pignataro, Stephen Kent, and Joe Touch for their feedback and support.

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

6.2. Informative References

[I-D.bellovin-tcpsec]
Bellovin, S., "Problem Statement and Requirements for a TCP Authentication Option", draft-bellovin-tcpsec-01 (work in progress), July 2007.

[I-D.ietf-idr-bgp-identifier]
Chen, E. and J. Yuan, "AS-wide Unique BGP Identifier for BGP-4", draft-ietf-idr-bgp-identifier-09 (work in progress), May 2008.

[I-D.ietf-opsec-infrastructure-security]
Lewis, D., "Service Provider Infrastructure Security", draft-ietf-opsec-infrastructure-security-01 (work in progress), April 2007.

[I-D.ietf-rpsec-bgpattack]
Convery, S., "An Attack Tree for the Border Gateway Protocol", draft-ietf-rpsec-bgpattack-00 (work in progress), April 2004.

[I-D.ietf-rpsec-bgpsecrec]
Christian, B. and T. Tauber, "BGP Security Requirements", draft-ietf-rpsec-bgpsecrec-09 (work in progress), November 2007.

[I-D.ietf-rpsec-generic-requirements]
McPherson, D., "Generic Security Requirements for Routing Protocols", draft-ietf-rpsec-generic-requirements-01 (work in progress), January 2005.

[I-D.ietf-tcpm-tcp-auth-opt]
Touch, J., Mankin, A., and R. Bonica, "The TCP Authentication Option", draft-ietf-tcpm-tcp-auth-opt-00 (work in progress), November 2007.

[I-D.savola-rtgwg-backbone-attacks]
Savola, P., "Backbone Infrastructure Attacks and Protections", draft-savola-rtgwg-backbone-attacks-03 (work in progress), January 2007.

[I-D.viswanathan-keyrollover]
Viswanathan, S., "Authentication-Key Rollover mechanism for Routing and Management Protocols", draft-viswanathan-keyrollover-00 (work in progress), October 2006.

[I-D.weis-tcp-auth-auto-ks]
Weis, B., Appanna, C., McGrew, D., and A. Ramaiah, "Automated key selection extension for the TCP Enhanced Authentication Option", draft-weis-tcp-auth-auto-ks-03 (work in progress), October 2007.

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC2385] Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option", RFC 2385, August 1998.

[RFC3562] Leech, M., "Key Management Considerations for the TCP MD5 Signature Option", RFC 3562, July 2003.

[RFC4251] Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Protocol Architecture", RFC 4251, January 2006.

[RFC4278] Bellovin, S. and A. Zinin, "Standards Maturity Variance Regarding the TCP MD5 Signature Option (RFC 2385) and the BGP-4 Specification", RFC 4278, January 2006.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4346] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

[RFC4423] Moskowitz, R. and P. Nikander, "Host Identity Protocol (HIP) Architecture", RFC 4423, May 2006.

[RFC4593] Barbir, A., Murphy, S., and Y. Yang, "Generic Threats to Routing Protocols", RFC 4593, October 2006.

[RFC4808] Bellovin, S., "Key Change Strategies for TCP-MD5", RFC 4808, March 2007.

[RFC5082] Gill, V., Heasley, J., Meyer, D., Savola, P., and C. Pignataro, "The Generalized TTL Security Mechanism (GTSM)", RFC 5082, October 2007.

Author's Address

Michael H. Behringer
Cisco Systems Inc
Village d'Entreprises Green Side
400, Avenue Roumanille, Batiment T 3
Biot - Sophia Antipolis 06410
France

Email: mbehring@cisco.com
URI: http://www.cisco.com

Full Copyright Statement

Intellectual Property