

Защита сеансов BGP с использованием сигнатур MD5

Protection of BGP Sessions via the TCP MD5 Signature Option

Статус документа

В этом документе содержится спецификация протокола, предложенного сообществу Internet. Документ служит приглашением к дискуссии в целях развития и совершенствования протокола. Текущее состояние стандартизации протокола вы можете узнать из документа «Internet Official Protocol Standards» (STD 1). Документ может распространяться без ограничений.

Авторские права

Copyright (C) The Internet Society (1998). All Rights Reserved.

Замечание IESG

В этом документе описывается практика обеспечения безопасности протокола BGP от некоторых типов атак. Понятно, что эти меры не могут обеспечить должную безопасность в случаях согласованных атак.

Аннотация

В этом документе описывается расширение TCP для повышения уровня безопасности протокола BGP. Документ определяет новую опцию TCP для передачи цифровой подписи (digest) MD5 [RFC1321] в сегментах TCP. Такая подпись служит сигнатурой сегмента, включающей информацию, известную только конечным точкам соединения. Поскольку протокол BGP использует транспорт TCP, применение этой опции описанным в документе способом существенно снижает уровень риска для некоторых типов атак на BGP.

1.0 Введение

Основным мотивом добавления этой опции является стремление обеспечить протоколу BGP средства самозащиты против вставок обманных сегментов TCP в поток данных через соединение. Особую важность имеют случаи сброса (reset) соединений TCP.

Для обмана соединения в случае использования описанной здесь схемы атакующему нужно не только предсказать порядковые номера TCP, но и узнать пароль, включенный в цифровую подпись MD5. Этот пароль не передается в потоке соединения и реальная форма пароля определяется приложением. Пароль даже может быть сменен во время работы соединения, если эта замена согласована обеими сторонами (отметим, что для некоторых реализаций TCP смена пароля может приводить к возникновению проблем при повторе передачи).

Важно также отметить, что использование этой опции не требует согласования - каждый сайт волен сам решить, будет ли он использовать данную опцию.

2.0 Предложение

Каждый сегмент, передаваемый через соединение TCP, для защиты от подмены будет включать 16-байтовую сигнатуру MD5, которая создается путем применения алгоритма MD5 к элементам соединения в указанном ниже порядке:

1. псевдозаголовок TCP (в следующем порядке: IP-адрес отправителя, IP-адрес получателя, дополненный нулями номер протокола, размер сегмента);
2. заголовок TCP без учета опций с нулевым значением контрольной суммы;
3. данные сегмента TCP (при их наличии);
4. независимо заданный ключ или пароль, известный обоим сторонам соединения TCP и (по-видимому) связанный с соединением.

Заголовок и псевдозаголовок используют сетевой порядок байтов. Природа ключа не задана обдуманно, но он должен быть известен обоим сторонам соединения. Реализации TCP могут определять способ задания ключа.

При получении подписанного сегмента на приемной стороне заново рассчитывается его сигнатура с использованием тех же данных (и своего ключа), которая сравнивается с полученной сигнатурой. Наличие расхождений может приводить к отбрасыванию сегмента и соответствующему отклику в адрес отправителя. Рекомендуется также записывать информацию о таких событиях в журнальный файл.

В отличие от других расширений TCP (например, от опции Window Scale [RFC1323]) отсутствие данной опции в сегменте SYN,ACK не должно заставлять отправителя исключать сигнатуру из передаваемых сегментов. Такое согласование обычно требуется для предотвращения некорректного поведения некоторых реализации TCP в случаях присутствия этой опции в сегментах, отличных от SYN. Это не является проблемой данной опции, поскольку сегменты SYN,ACK, передаваемые на этапе организации соединения, не будут подписаны и, следовательно, будут игнорироваться. В результате соединение не будет организовано и отличные от SYN сегменты с этой опцией просто не

Это не мешает разработке аналогичных опций с использованием другого алгоритма хэширования (например, SHA-1). Поскольку большинство реализаций дополняют 18 байтов опции до 20, не возникает проблем с определением новой опции, включающей поле типа алгоритма.

Однако рассмотрение этих вопросов требует создания отдельного документа.

4.5 Конфигурация ключей

Следует отметить, что механизм конфигурирования ключей в маршрутизаторах может вносить ограничения на набор ключей, которые могут использоваться партнерами. Разработчикам настоятельно рекомендуется обеспечить поддержку по крайней мере ключей, представляющий собой строки печатных символов ASCII размером до 80 байтов.

5.0 Вопросы безопасности

В этом документе определяется достаточно слабый, но применяемый в современной практике механизм обеспечения безопасности для протокола BGP. Есть надежда на появление в будущем более сильных механизмов для решения этой проблемы.

6.0 Литература

[RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm," [RFC 1321](#), April 1992.

[RFC1323] Jacobson, V., Braden, R., and D. Borman, "TCP Extensions for High Performance", [RFC 1323](#), May 1992.

[Dobb] H. Dobbertin, "The Status of MD5 After a Recent Attack", RSA Labs' CryptoBytes, Vol. 2 No. 2, Summer 1996.
<http://www.rsa.com/rsalabs/pubs/cryptobytes.html>

Адрес автора

Andy Heffernan

cisco Systems

170 West Tasman Drive

San Jose, CA 95134 USA

Phone: +1 408 526-8115

EMail: ahh@cisco.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

Полное заявление авторских прав

Copyright (C) The Internet Society (1998). Все права защищены.

Этот документ и его переводы могут копироваться и предоставляться другим лицам, а производные работы, комментирующие или иначе разъясняющие документ или помогающие в его реализации, могут подготавливаться, копироваться, публиковаться и распространяться целиком или частично без каких-либо ограничений при условии сохранения указанного выше уведомления об авторских правах и этого параграфа в копии или производной работе. Однако сам документ не может быть изменён каким-либо способом, таким как удаление уведомления об авторских правах или ссылок на Internet Society или иные организации Internet, за исключением случаев, когда это необходимо для разработки стандартов Internet (в этом случае нужно следовать процедурам для авторских прав, заданных процессом Internet Standards), а также при переводе документа на другие языки.

Предоставленные выше ограниченные права являются бессрочными и не могут быть отозваны Internet Society или правопреемниками.

Этот документ и содержащаяся в нем информация представлены "как есть" и автор, организация, которую он/она представляет или которая выступает спонсором (если таковой имеется), Internet Society и IETF отказываются от каких-либо гарантий (явных или подразумеваемых), включая (но не ограничиваясь) любые гарантии того, что использование представленной здесь информации не будет нарушать чьих-либо прав, и любые предполагаемые гарантии коммерческого использования или применимости для тех или иных задач.