

## 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.

#### Тезисы

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 вставки 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 обеим 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 обеим 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 реализаций 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 будут передаваться. Более важно обеспечение полного контроля приложения над передачей сигнатур и предотвращение возможности их удаления хостами, не понимающими данную опцию.

### 3.0 Синтаксис

Формат предлагаемой опции показан на рисунке.

Сигнатура MD5 всегда имеет размер 16 байтов и опция будет включаться в каждый сегмент соединения.

```
+-----+-----+-----+
| Kind=19 |Length=18| сигнатура MD5 ... |
+-----+-----+-----+
|
+-----+-----+-----+
|
+-----+-----+-----+
|
+-----+-----+-----+
```

## 4.0 Некоторые предположения

### 4.1 Не связанные с соединением сегменты сброса

Не связанные с соединением сегменты сброса (connectionless reset) будут игнорироваться получателем, поскольку отправитель таких сегментов не знает ключа и, следовательно, не сможет указать корректную сигнатуру сегмента. Это означает, например, что попытки соединения со стороны узла TCP, генерирующего сигнатуры, с портом, который не прослушивается, будут завершаться тайм-аутом, а не отказом. Подобно этому, сегменты сброса, генерируемые TCP в ответ на сегменты, переданные в просроченное соединение, также будут игнорироваться. Это может вызывать некоторые проблемы при работе, поскольку сегменты сброса помогают протоколу BGP быстрее детектировать выход партнера из строя.

### 4.2 Производительность

Вопросы производительности могут послужить препятствием использованию этой опции. Эксперименты на тестовых реализациях показали, что при использовании процессора с частотой 100 МГц в R4600 генерация простого сегмента ACK занимает в среднем 0,0268 мсек, а генерация сигнатуры для сегмента данных размером 4096 байтов занимает в среднем 0,8776 мсек. Эти значения применимы как для приемной стороны, так и для передающей, поскольку в обоих случаях производится расчет 16-байтовой сигнатуры.

### 4.3 Размер заголовка TCP

Как и для прочих опций, добавляемых в каждый сегмент, размер опции MD5 должен учитываться в значении MSS<sup>1</sup>, предлагаемом другой стороне на этапе организации соединения. В частности, размер заголовка, вычитаемый из значения MTU (независимо от того, связано ли значение MTU с передающим интерфейсом или является минимальным для IP значением MTU = 576 байтов), увеличивается по крайней мере на 18 байтов.

Следует принимать во внимание и общий размер заголовка. Заголовок TCP указывает начало сегмента данных с помощью 4-битового поля, которое показывает общий размер заголовка (включая опции) в 32-байтовых словах. Это означает, что общий размер заголовка и опций не может превышать 60 байтов – на опции остается 40 байтов.

В качестве конкретного примера рассмотрим используемые по умолчанию заголовки 4.4BSD для передачи сведений о масштабировании окна и временную метку на этапе организации соединения. Наиболее загруженным является стартовый пакет SYN, передаваемый первым в соединении. При использовании сигнатуры MD5 пакет SYN будет содержать в своем заголовке:

- 4-байтовую опцию MSS;
- 4-байтовую опцию масштабирования размера окна (3 байта опции дополняются до 4 в 4.4BSD);
- 12-байтовую временную метку (4.4BSD дополняет эту опцию в соответствии с RFC 1323 Appendix A);
- 18-байтовую сигнатуру MD5;
- 2-байтовое поле завершения списка опций для выравнивания по 32-битовой границе.

Таким образом, суммарный размер заголовка составляет 40 байтов.

### 4.4 MD5 в качестве алгоритма хэширования

К моменту выпуска первого варианта этого документа (он имел другое название) в алгоритме MD5 была обнаружена уязвимость для атак с целью поиска коллизий [Dobb] и возникли сомнения в его достаточной надежности для предлагаемого здесь использования.

В данном документе по-прежнему указывается алгоритм MD5, однако, в силу того, что опция уже используется на практике, в нее не включено поле типа алгоритма, чтобы впоследствии можно было заменить алгоритм без смены номера опции. В исходном документе также не было задано поле типа, поскольку оно потребовало бы по крайней мере 1 байта и полный размер опции стал бы не менее 19 байтов (которые могли бы дополняться до 20 реализациями TCP), что могло бы оказаться неприемлемым с учетом ограниченности размера заголовка.

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.

<sup>1</sup>Максимальный размер сегмента. Прим. перев.

## 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<sup>1</sup>, April 1992.

[RFC1323] Jacobson, V., Braden, R., and D. Borman, "TCP Extensions for High Performance", RFC 1323<sup>1</sup>, 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

E-Mail: [ahh@cisco.com](mailto:ahh@cisco.com)

### Перевод на русский язык

**Николай Малых**

[nmalykh@protocols.ru](mailto:nmalykh@protocols.ru)

### Полное заявление авторских прав

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

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS 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.

<sup>1</sup>Перевод этого документа имеется на сайте [www.protocols.ru](http://www.protocols.ru). Прим. перев.