Санкт-Петербург, ул. Седова, 80, телефон (812) 449-0770, факс (812) 449-0771, E-mail: info@bilim.com

Network Working Group
Request for Comments: 3514
Category: Informational

S. Bellovin
AT&T Labs Research
1 April 2003

Флаг безопасности в заголовке IPv4

The Security Flag in the IPv4 Header

Статус документа

Документ содержит информацию, предназначенную для сообщества Internet. Документ не задает какого-либо стандарта Internet. Допускается свободное распространение данного документа.

Авторские права

Тезисы

Межсетевые экраны (брандмауэры), пакетные фильтры, системы детектирования вторжений (IDS) и другие системы такого рода часто сталкиваются с трудностями при попытках отличить “злонамеренные” пакеты от пакетов, которые просто представляются не совсем обычными. Данный документ определяет для заголовков Ipv4 флаг безопасности (security flag), позволяющий легко различать эти две разновидности пакетов.

1. Введение

Межсетевые экраны [CBR03], пакетные фильтры, системы IDS и другие системы подобного типа часто сталкиваются с трудностями при попытке различить пакеты “злонамеренного” содержания от пакетов: просто представляющихся не совсем обычными. Эта проблема сильно затрудняет идентификацию пакетов. Для решения проблемы мы определяем флаг безопасности (security flag) или бит evil (дурной бит) в заголовке пакетов IPv4 [RFC791]. В нормальных (не злонамеренных) пакетах этот бит устанавливается в 0, тогда как для пакетов, используемых при атаках, флаг безопасности имеет значение 1.

1.1. Терминология

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с RFC 2119 [RFC2119].

2. Синтаксис

Единственным свободным битом заголовка IP является старший бит поля смещения фрагмента. Следовательно, выбор этого бита может быть сделан без согласования с IANA.

Схема использования бита evil показана на рисунке:

```
 0
+-+
|E|
+-+
```

В соответствии с настоящим документом бит может принимать следующие значения:

0x0 нулевое значение бита говорит о том, что пакет не имеет злонамеренного характера. Хостам, элементам сети и др. устройствпам **следует** предполагать, что такие пакеты безвредны и **не следует** принимать каких-либо защитных действий[1].

0x1 значение 1 говорит о том, что пакет является злонамеренным. Системам, обеспечивающим свою безопасность, **следует** принять меры по самозащите от таких пакетов. Системы, не обеспечивающие собственной безопасности, **могут** “падать”, пропускать такие пакеты внутрь системы и т. п.

3. Установка бита Evil

Существует множество способов установки бита evil. Программы, применяемые для организации атак, могут использовать подходящий интерфейс API для установки этого бита. Системы, не обеспечивающие иных механизмов установки дурного бита, **должны** обеспечивать такой интерфейс API, а программы, служащие для организации атак, **должны** использовать этот бит.

Многоуровневые операционные системы, не обеспечивающие безопасности, могут использовать специальные уровни для организации атак; бит evil **должен** по умолчанию устанавливаться для пакетов, исходящих из программ, которые работают на уровне организации атак. Однако система **может** обеспечивать интерфейс API, позволяющий сбрасывать бит evil для пользователя, обычно занимающегося атаками на другие компьютеры, если он, паче чаяния, решит заняться конструктивной деятельностью.

[1] Отметим, что эта часть спецификации уже реализована во многих операционных системах общего назначения.

Фрагменты, которые могут сами по себе представлять опасность **должны** передаваться с установленным битом evil. Если пакет с установленным битом evil фрагментируется промежуточным маршрутизатором и отдельные фрагменты не представляют самостоятельной опасности, для таких фрагментов бит evil **должен** быть сброшен при фрагментации. В процессе сборки фрагментов бит evil **должен** быть восстановлен.

Для сокрытия атак иной раз используются промежуточные системы. В передаваемых таким системам пакетах, которые направлены в атакуемую систему **следует** устанавливать бит evil.

Некоторые приложения занимаются "рукоблудием" со своими пакетами. Если такие пакеты являются частью атаки, приложение **должно** самостоятельно устанавливать бит evil.

В сетях, защищенных брандмауэрами в качестве аксиомы рассматривается допущение о том, что атакующие всегда находятся на внешней стороне межсетевого экрана. Следовательно, для хостов, находящихся с внутренней стороны брандмауэра, **недопустимо** устанавливать бит evil в каких бы то ни было пакетах.

Поскольку устройства NAT [RFC3022] изменяют пакеты, таким устройствам **следует** устанавливать бит evil во всех измененных пакетах. "Прозрачным" proxy-системам для http и электронной почты **следует** устанавливать бит evil в пакетах откликов для хостов добропорядочных клиентов.

Некоторые хосты занимаются сканированием других хостов для проверки системы детектирования вторжений. Если такие сканирование осуществляется с исследовательскими целями, в пакетах сканирования **недопустима** установка бита evil. Если же сканирование осуществляется с добрвми намерениями, но сканируемых хост использует систему IDS, бит evil **следует** устанавливать.

4. Обработка бита Evil

Устройства типа межсетевых экранов **должны** отбрасывать все пакеты с установленным битом evil. Отбрасывание пакетов со сброшенным битом evil **недопустимо**. Отброшенные пакеты следует отмечать в соответствующей переменной MIB.

Достаточно серьезные проблемы связаны с системами детектирования попыток вторжения (IDS). Эти системы отличаются склонностью к ложной трактовке как нормальных, так и злонамеренных пакетов, поэтому IDS **должны** использовать вероятностные методы трактовки значений бита evil. Если бит evil установлен, следует использовать подходящий генератор случайных чисел [RFC1750] для трактовки этого бита. Если же бит evil сброшен, генератор случайных чисел позволяет определить не следует ли все-таки считать этот пакет злонамеренным.

Используемый по умолчанию вероятностный метод трактовки дурного бита зависит от типа IDS. Основанные на анализе сигнатур системы IDS отличаются низким уровнем ложных срабатываний, но достаточно часто пропускают реальные атаки. Для установки и сброса параметров вероятностного метода **должен** обеспечиваться административный интерфейс.

Маршрутизаторам, не включенным в систему обеспечения безопасности, **не следует** проверять значение бита evil. Это позволяет повысить скорость обработки пакетов в маршрутизаторах.

Как было указано выше, обработка злонамеренных пакетов хостом зависит от используемой операционной системы, однако все хосты должны реагировать на этот бит в соответствии со своей природой.

5. Связанные работы

Хотя в этом документе определяется только бит evil для протокола Ipv4, существуют и другие механизмы (протоколы) для выполнения злокозненных операций. Ниже кратко рассмотрены некоторые из таких возможностей.

Для протокола IPv6 [RFC2460] злонамеренные действия могут выполняться в двух вариантах. Вариант hop-by-hop используется для пакетов, нарушающих работу сети (например, пакеты DdoS). Вариант end-to-end используется для атак на отдельные хосты. В любом случае опция содержит 128-битовый индикатор силы, показывающий степень способности пакета, и 128-битовый индикатор типа, который описывает конкретный тип атаки.

Некоторые протоколы канального уровня (в частности, протоколы оптической коммутации) позволяют полностью обходить маршрутизаторы (и, следовательно, межсетевые экраны). Следовательно, для индикации злонамеренных действий на канальном уровне **должна** использоваться та или иная схема (например, поляризация злобных действий).

Пакеты атак DDoS помечаются специальным кодом diffserv.

Для злонамеренных действий через Web и системы электронной почты определяется специальный тип MIME. Другие типы MIME допускается включать в злокозненную секцию – это позволяет упростить обработку текстовыми процессорами документов с макровирусами и другим враждебным кодом.

6. Требования IANA

Данный документ определяет поведение систем обеспечения безопасности для значений 0x0 и 0x1 бита evil. Поведение систем при других значениях этого бита может быть определено только по согласованию с IETF [RFC2434].

7. Вопросы безопасности

Корректная работа механизмов обеспечения безопасности в значительной степени зависит от трактовки бита evil. Если некорректно работающая компонента не устанавливает evil = 1 в тех случаях, когда это требуется, межсетевые экраны не смогут выполнять свою работу подобающим образом. Если же дурной бит имеет значение 1, когда этого не должно быть, могут возникать отказы в работе того или иного сервиса.

8. Литература

[CBR03] W.R. Cheswick, S.M. Bellovin, and A.D. Rubin, "Firewalls and Internet Security: Repelling the Wily Hacker", Second Edition, Addison-Wesley, 2003.

[RFC791] Postel, J., "Internet Protocol", STD 5, RFC 791[2], September 1981.

[2] На сайте http://www.protocols.ru можно найти перевод этого документа на русский язык. *Прим. перев.*

[RFC1750] Eastlake, D., 3rd, Crocker, S. and J. Schiller, "Randomness Recommendations for Security", RFC 1750, December 1994.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119[3], March 1997.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC3022] Srisuresh, P. and K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", RFC 3022, January 2001.

9. Адрес автора

Steven M. Bellovin

AT&T Labs Research

Shannon Laboratory

180 Park Avenue

Florham Park, NJ 07932

телефон: +1 973-360-8656

EMail: bellovin@acm.org

Перевод на русский язык

Николай Малых
BiLiM Systems
nmalykh@bilim.com

10. Полное заявление авторских прав

Подтверждение

Поддержка функций RFC Editor обеспечивается Internet Society.

[3] На сайте www.protocols.ru можно найти перевод этого документа на русский язык. *Прим. перев.*