Литература

1. Баричев С. Г., Гончаров В. В., Серов Р. Е. 2.4.2. Стандарт AES. Алгоритм Rijdael // Основы современной криптографии — 3-е изд. — М.: Диалог-МИФИ, 2011. — С. 30—35. — 176 с.
2. Гатчин Ю. А., Коробейников А. Г. Основы криптографических алгоритмов. Учебное пособие. — СПб.: СПбГИТМО(ТУ), 2002.

А.А. Фирсова, И.В. Константинов

МЕХАНИЗМ ДЛЯ ПРОТИВОДЕЙСТВИЯ DDOS-АТАКАМ, НАПРАВЛЕННЫЙ НА КЛИЕНТОВ ДИФФЕРЕНЦИРОВАННЫХ УСЛУГ

(Поволжский государственный университет
телекоммуникаций и информатики)

Сети с дифференцированным обслуживанием (DiffServ) обеспечивают гарантию качества обслуживания (QoS) методом распределения трафика по фиксированному числу ранее существовавших классов. Атаки типа DoS/DDoS на клиентов DiffServ становятся все более целенаправленными и требуют меньшей пропускной способности, чем текущие атаки, из-за ограничений пропускной способности для каждого клиента и класса, которые должны быть наложены для обеспечения гарантий качества обслуживания. В этой статье представлена техника отражения DDoS-атаки на клиенте DiffServ посредством динамической модификации заголовков пакетов. Этот механизм позволяет сети DiffServ отличать легитимный трафик от вредоносного трафика, но не требует криптографической обработки для каждого пакета и не увеличивает размер пакета.

Дифференцированный сервис обеспечивает QoS без сохранения информации о состоянии каждого потока в основных маршрутизаторах. Пограничные маршрутизаторы контролируют трафик, входящий в сеть, классифицируя и обрабатывая его, чтобы он соответствовал определенному агрегату поведения на основе соглашения об уровне обслуживания (SLA) между источником и поставщиком DiffServ. Основные маршрутизаторы не отслеживают состояние отдельных потоков. Они несут ответственность только за пересылку на основе маркировки, присвоенной каждому пакету при его поступлении в сеть.

DDoS-атаки пытаются искусственно истощить ресурсы поставщика услуг, такие как пропускная способность, память или циклы процессора. Большинство DDoS-атак основаны на одной и той же концепции. Злоумышленник компрометирует группу нецелевых хостов и заставляет их отправлять поток трафика на целевую систему. Этот лавинный трафик потребляет полосу пропускания на канале к цели, вызывая переполнение очереди на канале. Адреса источников в заголовках пакетов обычно изменяются, чтобы предотвратить обнаружение скомпрометированных узлов.

Известные методы противодействия DDoS-атакам, например, Ingress Filtering, IP Traceback, Distributed Filtering и т. д. Общим недостатком этих методов является необходимость взаимодействия сторонних маршрутизаторов или хостов, чтобы меры защиты были эффективными. Противостоять DDoS-атаке необходимо, останавливая ее у источника или у поставщика услуг Интернета. Без знания истинного источника атаки все пакеты должны рассматриваться как допустимые на сетевом уровне. Однако IP сам по себе не обеспечивает надежного способа для получателя определить настоящий источник входящих пакетов, поскольку поле адреса источника может быть легко подделано. Расширение заголовка аутентификации (AH) к протоколу IP является хорошим средством проверки источника потока трафика, но криптографическая обработка пакетов, необходимая для IP AH, плохо масштабируется и может потребовать слишком больших вычислительных ресурсов для реализации при сохранении гарантий QoS. Кроме того, IP AH требует вставки дополнительного поля заголовка в каждый пакет. Это может привести к фрагментации пакетов, что негативно скажется на QoS.

Основываясь на этом наблюдении, разработан механизм, с помощью которого провайдер может уведомлять клиентов, когда их трафик не соответствует профилю, указанному в SLA. Полученный в результате механизм обладает преимуществами:

- не требует криптографической обработки каждого пакета,
- не увеличивает вероятность фрагментации пакетов,
- оказывает небольшое влияние или вообще не влияет на способность провайдера гарантировать QoS.

Рассмотрим случай, где в проводной сети клиент находится всего в одном переходе от входного маршрутизатора, домен DiffServ также сможет фильтровать трафик на основе входящего канала. Злоумышленник не сможет залить поддельный трафик, используя адрес источника этого клиента, так как уже заявлено, что сам клиент не может быть скомпрометирован. Из этого следует, что никакая атака невозможна, если клиент не находится более чем в одном переходе от назначенного ему входного маршрутизатора. Однако это неверно, если соединение клиента с входным маршрутизатором является беспроводным каналом, поскольку сама среда передачи не защищена. Можно сделать предположение, что пропускная способность пути между клиентским шлюзом и входным маршрутизатором достаточно велика, чтобы злоумышленник не смог провести атаку с потреблением полосы пропускания против входного маршрутизатора или клиентского шлюза. Кроме того, предположим, что злоумышленник не имеет возможности производить мониторинг трафика клиента и не может изменять, задерживать или уничтожать пакеты во время передачи.

В данной статье рассмотрим механизм, который позволит входному маршрутизатору домена DiffServ отличать действительные пакеты от вредоносных на основе цифровой подписи. Определим подпись пакета как комбинацию поля адреса источника и одного или нескольких других полей в заголовке IP. Такой механизм основан на возможности клиента изменить созданную под-

пись. Предполагается, что злоумышленник сможет наблюдать за трафиком, проходящим между клиентом и доменом DiffServ, и что он сможет дать указание источникам лавинной рассылки имитировать любые изменения в подписях пакетов, которые он наблюдает. Поэтому однократного изменения заголовков недостаточно. Изменения должны вноситься на периодической основе и должны выполняться быстрее, чем злоумышленник может их продублировать.

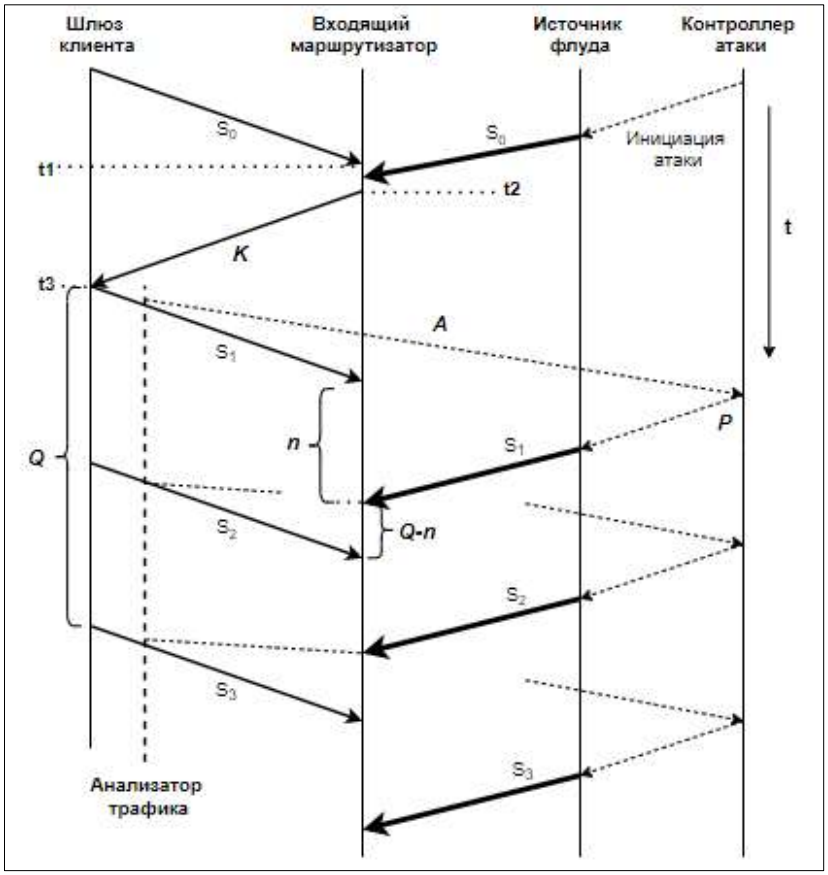

Рис. 1. Схема работы механизма противодействия DDoS-атак

На Рис.1 представлена временная диаграмма, показывающая последовательность действий, связанных с работой предлагаемого механизма.

Когда входной маршрутизатор помечает пакет, исходящий от клиента DiffServ, как не соответствующий профилю, он регистрирует источник и время (t1) отбрасывания. Когда частота маркировки вне профиля превышает предварительно установленный порог (t2), маршрутизатор отправляет клиенту сообщение обратной связи (K). После получения (t3) клиент начнет изменять подпись своих пакетов. Входной маршрутизатор будет использовать эти изменения для идентификации действительных пакетов. Он отбрасывает все пакеты с недействительной подписью. Обратная связь маршрутизатора с клиентом состоит из сгенерированного маршрутизатором начального ключа для алгоритма, который генерирует последовательность подписей. Клиент и маршрутизатор могут независимо вычислить, какой должна быть правильная подпись, используя этот алгоритм и специальный ключ. Алгоритм может быть хорошо известен до тех пор, пока используемый начальный ключ остается секретным. Начальный ключ

будет зашифрован с использованием общего секретного ключа и обеспечен цифровой подписью. Начальный ключ используется для создания новых подписей вместо общего секретного ключа, чтобы избежать компрометации секретного ключа из-за чрезмерного использования. Цифровая подпись обеспечивает аутентификацию сообщения обратной связи, поэтому злоумышленники не смогут создать DDoS, подделав эти сообщения. Также необходимо шифрование полезной нагрузки, поскольку злоумышленник может отслеживать трафик, проходящий между клиентом и доменом DiffServ.

После получения сообщения обратной связи клиент аутентифицирует его, расшифровывает полезную нагрузку и использует начальный ключ для вычисления последовательности значений подписи, которые он будет использовать. Клиент немедленно начнет использовать значения в назначенных полях заголовков IP своих пакетов. Он будет переключаться на следующую сигнатуру (S_i) в последовательности через равные промежутки времени, обозначенные Q. Злоумышленник не будет знать, что представляет собой каждая новая сигнатура, пока не получит информацию от монитора, установленного на пути клиентского трафика (A). Когда он узнает новую сигнатуру, он может указать источникам лавинной рассылки изменить используемые ими сигнатуры (P). Время между получением входным маршрутизатором первого действительного пакета с новой подписью и получением первого атакующего пакета с той же подписью, обозначаемое n, является окном, в котором возможна полная аутентификация. Исходный ключ также используется для создания такой же последовательности значений подписи на маршрутизаторе. После отправки сообщения обратной связи маршрутизатор будет рассматривать все пакеты как действительные, пока не получит первый пакет с первой измененной подписью. Все последующие пакеты с неверной подписью отбрасываются, кроме первого пакета, полученного со второй подписью. При получении первого пакета со второй подписью маршрутизатор отбрасывает все последующие пакеты, не соответствующие второй подписи, в том числе помеченные первой подписью. Это предотвращает использование злоумышленником старых сигнатур для обхода применяемого механизма.

В данной статье продемонстрировано, как можно смягчить DDoS-атаки на клиентов DiffServ и обнаружить кражу услуг без криптографического анализа каждого пакета. Платой за выигрыш в эффективности является отсутствие полной гарантии отклонения вредоносных пакетов на входе. Считается, что DDoS-атаки и кража услуг — это скорее проблема гарантии QoS, чем проблема обеспечения безопасности. Предлагаемый механизм противодействия следует сочетать с другими протоколами безопасности, если требуются как гарантия QoS, так и обеспечение безопасности. Низкая стоимость делает его отличным вариантом в качестве независимого мониторинга возможных нарушений протоколов безопасности.

Литература

1. Боршевников А.Е. Сетевые атаки. Виды. Способы борьбы / А.Е. Боршевников / Междунар. науч. конф. «Современные тенденции технических наук». - Уфа, 2011. - 78 с.

2. Васин Н.Н. Моделирование атак посредника в сетях пакетной коммутации / Н.Н. Васин, А.А. Фирсова // Проблемы и перспективы внедрения инновационных телекоммуникационных технологий: сборник материалов VII Международной научно-практической очно-заочной конференции. - Оренбург, 2021. - 206 – 214 с.

3. Руководство по технологиям объединенных сетей. - 3-е изд. - М.: Вильямс, 2002. - 1039 с.: ил.

В.П. Цветов

ВЫБОР ПАРАМЕТРА РЕГУЛЯРИЗАЦИИ ПО ОБУЧАЮЩЕЙ ВЫБОРКЕ ПРИ РЕШЕНИИ ПЛОХО ОБУСЛОВЛЕННЫХ СИСТЕМ ЛИНЕЙНЫХ АЛГЕБРАИЧЕСКИХ УРАВНЕНИЙ

(Самарский университет)

Задачи решения плохо обусловленных систем линейных алгебраических уравнений (СЛАУ) возникают в различных прикладных областях научного знания. Мы будем рассматривать подобные СЛАУ в контексте задач цифровой радиосвязи, использующих системы неортогональных несущих сигналов.

$$AX = Y, \tag{1}$$

где

$$X = \begin{pmatrix} x_0 \\ \vdots \\ x_{N-1} \end{pmatrix}, \mathrm{Y} = \begin{pmatrix} y_0 \\ \vdots \\ y_{N-1} \end{pmatrix}, \; x_i \in 0..M, y_i \in \mathbb{R}, i \in 0..N-1,$$

$$A = (a_{ij}) = \left(cos\left(\frac{\pi ij}{N_0}\right) \right), i, j \in 0..N-1, N_0 > N.$$

СЛАУ (1) моделирует спектрально эффективные многочастотные защищенные системы радиосвязи, которые разрабатываются в последнее время [1-2]. Целочисленный интервал $0..M$ описывает конечное число состояний цифрового передающего устройства.

При наличии помех в канале связи вместо решения СЛАУ (1) приходится искать решение СЛАУ (2)

$$A\tilde{X} = \tilde{Y}, \tag{2}$$

где $\tilde{Y} = Y + \Delta$, а $\Delta = \begin{pmatrix} \delta_0 \\ \vdots \\ \delta_{N-1} \end{pmatrix}$ - вектор помех. Найденное решение СЛАУ (2) $\tilde{X} \in \mathbb{R}$ округляется методом ближайшего соседа и принимается за приближенное решение СЛАУ (1).