УДК 004.77, 004.56

ИСПОЛЬЗОВАНИЕ СТАТИСТИЧЕСКИХ ДАННЫХ О ПОВЕДЕНИИ ПОЛЬЗОВАТЕЛЕЙ НА РЕСУРСЕ ДЛЯ БОРЬБЫ С DDOS-АТАКАМИ

Акуляков А.А.
Научный руководитель — канд. техн. наук, доц. А.С.Кузнецов
Институт космических и информационных технологий СФУ

Введение

DDoS-атака (Distributer Denial of Service) — это атака на компьютерную систему с целью вызова отказа обслуживания, то есть такая атака, целью которой является предотвращение предоставления сервиса конечным пользователям системы.

В настоящее время данный вид атак крайне популярен и особенно в Российском сегменте интернета. Целью злоумышленников обычно является устранение конкурента с рынка или же шантаж.

DDoS-атаки могут быть условно разделены на два типа:

1. атаки на сервер. Суть таких атак заключается в генерации большого числа запросов, целью которых является создание искусственной нагрузки на веб-сервер и сервер баз данных, которая в конечном итоге должна привести к аварийному завершению работы (например, по исчерпанию доступной оперативной памяти) или же к отказу в обслуживании легитимных клиентов (превышение интервалов ожидания ответа от сервера). Реализация может различаться
2. атаки на канал. Целью этого типа атак является заполнение сетевого канала большим количеством паразитного трафика. Часто такие атаки реализуются через большое количество запросов некоторого статического ресурса достаточно большого размера, например изображения

Существует несколько методов противодействия DDoS-атакам.

Первый заключается в наращивании количества серверов и пропускной способности канала. Он является наиболее результативным и может успешно применяться для отражения как атак на сервера, так и атак на канал. Однако недостатком этого метода является его стоимость и задержка на подключение оборудования.

Второй метод предполагает фильтрацию паразитных запросов. Он в большей степени ориентирован на защиту от атак на сервера. Для защиты от атак на канал так же может применяться, но менее эффективен в зависимости от реализации атаки. Фильтрация запросов достаточно дешева, может быть быстро развернута в случае атаки, но возможны ошибки, при которых запросы легитимных пользователей будут отфильтрованы.

Третий метод является комбинацией двух предыдущих. При этом наиболее активно наращивают пропускную способность канала, а параметры фильтрации выставляют таким образом, что бы минимизировать вероятность ложного срабатывания.

Целью настоящей работы является разработка метода борьбы с DDoS-атаками с использованием статистических данных о поведении пользователей на ресурсе.

Постановка задачи

Имеется абстрактный веб-сервер и некоторое веб-приложение, развернутое на нем. В каждый конкретный момент времени доступны логи веб-сервера.

Определяют два класса запросов: легитимный запрос(запрос от легитимного

пользователя, то есть запрос, не подлежащий фильтрации, блокированию) и паразитный запрос(атакующий запрос, то есть блокируемый запрос).

В этом случае, задача фильтрации сводится к задаче классификации поступающих запросов согласно классам, определенным выше.

Анализ задачи и определение общего вида решения

При решении задачи фильтрации присутствуют две весьма существенных проблемы.

Во-первых, атаки чаще всего носят индивидуальный характер. Злоумышленники анализируют атакуемый сайт, исследуют программное обеспечение и инфраструктуру, на основании чего вырабатывают вектор атаки.

Во-вторых, невозможно получить или предугадать информацию об атаке до ее начала, то есть до момента атаки имеется информативная выборка, представляющая действия исключительно легитимных пользователей.

Существует два потенциальных решения:

1. получение «отрицательной» обучающей выборки во время атаки
2. использование исключительно «положительной» выборки

Первое решение имеет очевидные недостатки, так как возможна неработоспособность на начало атаки и требуется формирование «негативной» выборки, которое предполагает участие человека.

Второе решение с одной стороны менее эффективно, так как использует меньше информации, но с другой стороны оно не зависит от типа атаки, а следовательно менее чувствительно к изменению атакующей стратегии, не требует присутствия человека.

В данной работе рассматривается исключительно второе решение. Фактически его смысл заключается в формировании, на основании статистических данных, шаблона поведения легитимных пользователей на ресурсе. Все запросы, не попадающие под сформированный шаблон, блокируются.

Определение информативных признаков

Наиболее важным источником информации являются логи веб-сервера. Из логов веб-сервера может быть извлечена следующая информация: ip-адрес клиента(инициатора запроса), время запроса(время поступления запроса на сервер), время обработки запроса, тип запроса, адрес запроса(ресурс, к которому происходит обращение), юзер-агент(тип и версия веб-браузера), статус запроса.

Используя информацию о юзер-агенте, можно ввести такой показатель запроса, как актуальность юзер-агента. Действительно, ведь зачастую у большинства пользователей установлена достаточно современная версия браузера, к тому же многие браузеры имеют автоматические механизмы обновлений.

Тип запроса сам по себе является достаточно информативным показателем и может в чистом виде, без преобразований и обработки, характеризовать запрос.

Из еще не рассмотренной информации наиболее ценной является информация о ip-адресе клиента. Она позволяет определить географическое положение источника запроса. Действительно, в случае если приложение ориентировано на русскоговорящую аудиторию, то запросы из Латинской Америки или Африки с большой долей вероятности являются паразитными.

Оставшаяся информация фактически бесполезна, если не рассматривать ее персонализировано для каждого из клиентов, для каждой из сессий.

Задача группировки запросов относительно источников не так тривиальна, как может показаться на первый взгляд. Для однозначной идентификации источника можно использовать ip-адрес клиента. Однако следует учитывать использование протоколов

трансляции адресов, таких как NAT, что несомненно ухудшит результаты, так как в этом случае группа пользователей, использующих один ip-адрес, рассматривается как один клиент.

Для каждого из источников запросов могут быть введены следующие показатели:

- на основании локального времени запроса и времени обработки запроса можно определить количество одновременных запросов от источника, а так же суммарную частоту запросов
- используя информацию о типе запроса можно ввести показатель соотношения типов запросов
- анализируя адрес запроса можно ввести показатель среднего количества посещенных страниц пользователем за сеанс

В итоге можно выделить следующие информативные признаки:

- соответствие географической зоны запроса и языка приложения
- актуальность версии веб-браузера
- средняя частота запросов от одного клиента
- количество одновременных запросов от одного клиента
- соотношение количества запросов по типам(POST, GET, PUT...) за сеанс
- количество посещаемых страниц пользователем за сеанс работы
- среднее соотношение статических запросов к динамическим
- частота запросов к каждому из ресурсов

Построение шаблона поведения пользователей на ресурсе

Шаблон поведения пользователей на ресурсе задается через функцию принадлежности. Определим данную функцию как среднее значений функций принадлежности для каждого из информативных признаков.

$$F\left(\vec{x}\right)=\frac{1}{n}\sum_{i=1}^{n} f_i\left(x_i\right), \quad F\left(\vec{x}\right)\in[0;1],$$

где n - количество информативных признаков, $\vec{x}$ - вектор признаков, характеризующих источник запросов.

Имеется два вида информативных признаков.

Во-первых, это признаки независимые от сессии. Для данных признаков логично задать функцию принадлежности следующим образом:

$$f\left(x\right)=e^{\frac{-\left(m-x\right)^2}{2\sigma^2}}, \quad f\left(x\right)\in[0;1],$$

где m — математическое ожидание информативного признака, σ^2 - дисперсия.

Во-вторых, это информативные признаки на сессию. Эти признаки накапливаются по мере работы клиента с сервисом. Соответственно, данную особенность следует учитывать следующим образом — в случае если величина менее средней и функция принадлежности менее чем 0.5, то установить значение функции принадлежности равным 0.5, что идентифицирует неопределенность.

Фильтрация

Фильтрация реализуется через пороговое значение. В случае если оценка принадлежности пользователя меньше порога, то он считается злоумышленником и блокируется. Величина порога определяется минимизацией следующего выражения:

$$\left|(1-\alpha)-\frac{1}{n}\sum_{i=0}^{n}\theta\left(p-F\left(\overrightarrow{x_i}\right)\right)\right| = \min_{p},$$

где p – порог фильтрации, θ - единичная функция, α – желаемая погрешность фильтрации легитимных пользователей.

Тестирование

Для тестирования использовались 11 виртуальных машин под управлением гипервизора Microsoft Hyper-V. Одна из них выполняла роль атакуемого сервера, остальные случайным образом выполняли роль легитимных пользователей или\и роль атакующих источников запросов. Действия легитимных пользователей эмулировались посредством утилиты нагрузочного тестирования jMetter. DDoS-атака производилась посредством программного обеспечения LOIC. Соотношение атакующих источников запросов к легитимным пользователям составляло один к одному. Проводилось 100 экспериментов с различными стратегиями DDoS-атаки.

Тестирование показало следующие результаты:

- 88% легитимных пользователей фильтры, то есть ошибка фильтрации легитимных пользователей составляет12%
- 71% паразитных запросов блокируются, то есть ошибка фильтрации паразитных запросов составляет 29%
- метод не чувствителен к типу и стратегии атаки

Результаты

В результате работы был разработан и протестирован метод борьбы с DDoS-атаками с использованием статистических данных о поведении пользователей на ресурсе. Метод не требует участия человека, не чувствителен к типу и смене стратегии атаки.

Разработанный метод является уникальным в силу своей открытости и доступности сообществу. В настоящий момент существует ряд методов, однако эти методы скрыты от общественности и являются коммерческой тайной компаний, оказывающих услуги по обеспечению защиты от DDoS-атак.