УДК 004.056

Я. А. Бекенева
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Анализ актуальных типов DDoS-атак и методов защиты от них

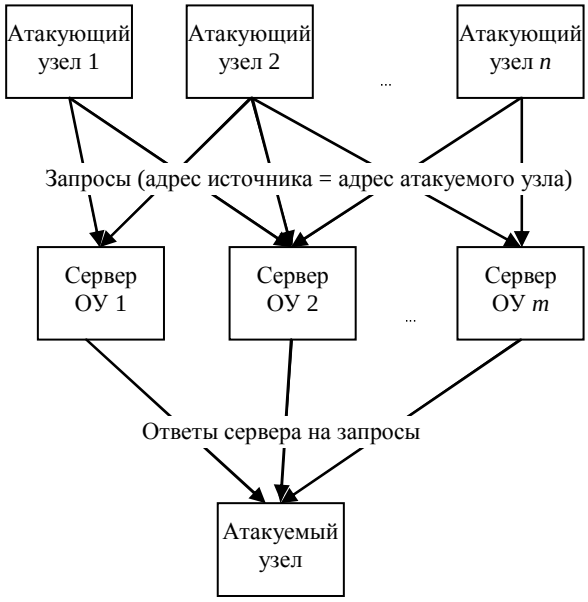
Представлен анализ наиболее актуальных типов атак, основанных на отражении и усилении трафика. Приведены методы, рекомендуемые для предотвращения таких атак, а также существующие методы защиты от них. Выявлены преимущества и недостатки этих методов. Поставлены дальнейшие цели по разработке новых методов защиты.

DDoS-атака, DNS, NTP, SSDP, SNMP, методы защиты от DDoS-атак, RRL, RAD

DDoS-атака – распределенная атака типа «отказ в обслуживании» различных интернет-сервисов. При успешном совершении подобных атак на сервер он перестает отвечать на легитимные запросы от пользователей. Крупным DDoS-атакам подвергаются сайты правительства и органов власти, сайты ведущих IT-корпораций Amazon, Yahoo, Microsoft и т. д. Эти мощные корпорации, имеющие огромные ресурсы, не всегда могут справиться с атаками и отразить нападение.

Согласно отчету [1] количество проводимых DDoS-атак неуклонно возрастает. Мировые лидеры по информационной безопасности [2] ставят необходимость обнаружения DDoS-атак и противостояния им как первостепенную задачу в своих исследованиях и разработках. Это свидетельствует о том, что разработка и внедрение методов защиты от DDoS-атак – актуальная задача. В настоящее время одним из наиболее популярных типов DDoS-атак являются атаки, основанные на отражении и усилении вредоносного трафика. При разработке новых универсальных методов защиты от атак такого типа первоочередной задачей является анализ протоколов, которые могут быть использованы для реализации подобных атак. Помимо этого необходим анализ уже существующих методов защиты от атак, осуществляющих отражение трафика с использованием различных протоколов. В статье представлены результаты проведенного анализа и сделанные на его основе выводы.

Атаки, основанные на отражении и усилении трафика. На рисунке представлена общая схема реализации атак с отражением и усилением трафика.



Отражение трафика достигается отправкой на определенные серверы (на рисунке обозначены как серверы ОУ) запроса, где IP-адреса источника подменяются на IP-адрес жертвы. В качестве таких серверов, в зависимости от типа реализуемой атаки, могут использоваться как крупные серверы, такие, как DNS-серверы, NTP-серверы, так и

пользовательские устройства. Эффект усиления достигается за счет того, что генерируются такие запросы, ответы на которые по объему в разы превосходят сами запросы. Это позволяет злоумышленникам совершать массированные атаки, не имея в своем распоряжении большого количества ресурсов.

Коэффициент усиления (КУ) при этом определяется как

$$КУ = \frac{Размер_{ответа}}{Размер_{запроса}}.$$

Очевидно, что такие атаки не могут совершаться с использованием протоколов, основанных на TCP, так как процесс трехэтапного рукопожатия исключает возможность подмены адреса. В работе [3] было выявлено 14 популярных протоколов, которые могут использоваться для реализации атак с усилением трафика. Все эти протоколы работают на базе протокола UDP.

В настоящее время для реализации атак с усилением трафика наибольшей популярностью пользуются такие протоколы, как DNS и NTP.

Постепенно набирают популярность атаки, основанные на других протоколах. Например, атаки, основанные на протоколе SSDP: в первом квартале 2014 г. таких атак было произведено всего 3, а в четвертом их число достигло 83 000. В первом квартале 2015 г. число таких атак выросло до 126 000, а во втором квартале атаки этого типа заняли второе место в общем рейтинге атак, уступив только SYN-Flooding [1], [2]. Мощность подобных атак была достаточно велика.

Рассмотрим подробнее типы атак, которые пользуются наибольшей популярностью, а также предлагаемые методы защиты от них.

DNS-атаки. DNS-атака представляет собой своеобразный классический тип атак, основанных на отражении трафика, а также использующих усиление трафика. Эти атаки осуществляются уже несколько лет и при этом продолжают оставаться популярными среди злоумышленников. Атака по протоколу DNS реализуется, как правило, генерацией запроса в формате #dig @SERVER_IP NS, где SERVER_IP – IP-адрес сервера. Размер запроса составляет 17 байт, размер же всего пакета – 60 байт. На данную команду сервер отвечает подсказкой в виде адресов корневых DNS-серверов, при этом размер ответа составляет 360 байт, а размер всего пакета – 402 байт.

Как правило, максимальная длина пакетов DNS ограничена размером 512 байт для уровня приложений. Однако существуют расширенные DNS (EDNS) [4], которые позволяют отправлять и принимать пакеты DNS большего размера, если такое расширение поддерживается и отправителем, и получателем. Таким образом, злоумышленники могут прибегать к использованию EDNS. Используя записи типа OPT, злоумышленники могут включать дополнительную запись длиной 11 байт. Если сервер не поддерживает EDNS или если ответ не превышает стандартную длину 512 байт, размер ответа остается тем же. В таком случае использование EDNS приведет к снижению коэффициента усиления. Однако если сервер поддерживает EDNS, то ответ большого размера может существенно превзойти запись OPT и увеличить коэффициент усиления.

NTP-атаки. Протокол NTP стал использоваться для реализации атак с отражением трафика значительно позже, чем DNS. Высокий коэффициент усиления послужил росту популярности атак этого типа. Кроме того, в 2014 г. атака максимальной мощности была реализована именно по протоколу NTP [2]. Для выполнения атаки с использованием протокола NTP на публичные NTP-серверы отправляются запросы с командой get monlist. Адрес источника при этом заменяется адресом узла-жертвы. Ответом на эту команду является список из 600 IP-адресов, обращавшихся к серверу. В результате размер ответа во много раз превышает исходный запрос (на загруженных серверах на запрос в 234 байт возвращается ответ в 48 Кбайт), что позволяет многократно усилить объем трафика, генерируемого в сторону системы-жертвы. Проблему усугубляет то, что команда get monlist выполняется без аутентификации.

SSDP-атаки. Протокол SSDP является основой протокола обнаружения Universal plug-and-play. Атака такого типа осуществляется в 2 этапа. Сначала злоумышленник отправляет широковещательный запрос M-SEARCH, на который откликаются доступные устройства UPnP. Далее отправляется множество запросов M-SEARCH, где адрес источника подменяется адресом компьютера-жертвы, на каждый из которых доступное устройство отправляет ответ. Размер ответа зависит от размера описания устройства, однако коэффициент усиления в среднем принято считать около 30 [3]. В отличие от атак DNS и NTP, где в качестве отражателя трафика используются круп-

ные серверы, атака SSDP предполагает использование устройств, которые принадлежат рядовым пользователям. Они, в свою очередь, могут даже не подозревать, что их мобильные телефоны, факсы или принтеры принимают участие в распределенной атаке. Большинство владельцев таких устройств не имеют информации о том, какие настройки следует применить, чтобы предотвратить использование своих устройств в атаке.

SNMP-атаки. SNMP представляет собой протокол, предназначенный для управления устройствами в сети. Для реализации атаки с помощью этого протокола используют запросы с командой GetBulk, которая автоматизирует получение большого объема данных, преимущественно табличных. При этом размер запроса GetBulk составляет около 87 байт, в то время как ответ содержит около 60 000 байт фрагментированных данных.

Chargen-атаки. Стандартная UDP-атака Chargen также может осуществляться как атака с отражением и усилением трафика. Для этого требуется отправить запрос малого размера на 19 UDP-порт узла, используемого для отражения, при этом размер ответа будет иметь максимально возможный размер. Несмотря на то, что этот тип атаки существует уже достаточно давно, он попрежнему находится в числе наиболее часто реализуемых типов атак.

QOTD (Quote of the day) – атака с использованием этого протокола реализуется способом, похожим на Chargen. Для осуществления атаки требуется установить соединение с сервером, поддерживающим протокол QOTD, через UDP-порт 17. Сервер возвращает произвольное короткое сообщение. Обычно оно выбирается случайным образом из списка известных цитат. Популярность атак такого типа весьма невысока.

NetBios – протокол для работы в локальных сетях на персональных ЭВМ также может быть использован для реализации атак посредством запроса о конфигурации сети. Коэффициент усиления такой атаки невелик (по оценкам [3] составляет около четырех), поэтому данные атаки не пользуются популярностью.

В качестве средств усиления трафика могут быть использованы peer-to-peer-сервисы для распространения файлов (уязвимыми считаются такие протоколы, как BitTorrent и Kad), peer-to-peer-ботсети (ZeroAccess, Sality, Gameover), а также игровые серверы, такие, как Quake 3 и Steam. Эти протоколы достаточно редко используются для реализации атак, однако не следует забывать о присущих им уязвимостях и по возможности бороться с ними. Ежегодные отчеты показывают, что атаки того или иного типа, долгое время оставаясь в тени, быстро набирают популярность, а мощность, которая достигается за счет их реализации, может оказаться весьма высока.

В работе [5] отмечается, что в качестве средства усиления трафика могут использоваться сервисы, предназначенные для обмена голосовыми сообщениями, такие, как Skype. Авторы показывают, что протоколы SIP и VoIP имеют определенные уязвимости, что также позволяет использовать их для реализации атак.

Механизмы защиты от DDoS-атак. Методы защиты от DDoS-атак можно условно классифицировать по двум признакам. Первый признак – расположение механизма защиты в сети. Методы защиты могут подразделяться на применяемые у источника, на стороне жертвы, а также на промежуточных узлах сети. Методы, объединяющие различные схемы защиты и обеспечивающие их взаимодействие, обычно называют гибридными [6]. Принято считать, что гибридные методы обеспечивают лучшую защиту от атак, нежели отдельные методы защиты, работающие самостоятельно на различных участках сети.

Второй признак – время применения метода. Механизмы, применяемые до наступления атаки, относятся к методам предотвращения [7]. Методы, используемые во время атаки, относятся к группе обнаружения атаки и идентификации источника. После обнаружения атаки применяются методы реакции на атаку. Наилучшим вариантом является предотвращение атаки. Оно может быть достигнуто на всех этапах пути трафика, начиная от источника атаки и заканчивая обработкой данных на стороне атакуемого сервера. Зачастую используются комбинированные средства предотвращения (IPS) и обнаружения атак (IDS) – IPDS.

Методы, основанные на механизмах фильтрации. Существует множество методов предотвращения DDoS-атак. Для этого очень часто исследователи предлагают различные механизмы фильтрации, например Ingress/Egress filtering [8] , SAVE [9], Hop-Count filtering [10], Route-based filtering [11] и др. Фильтрация является весьма эффективным способом выявления подмены IP-адреса, что особенно актуально в тех случаях, когда используется усиление или отражение атаки. Различные методы фильтрации, применяемые

на разных этапах продвижения трафика, представляют собой мощный инструмент для выявления фактов подмены адреса. Наибольшее распространение получил метод Ingress/Egress filtering, так как он позволяет выявить подмену IP-адреса и заблокировать вредоносный пакет еще до того, как он покинет локальную сеть. На основе методов фильтрации трафика были созданы более сложные гибридные механизмы защиты, такие, как TRACK [12], Active Internet Traffic Filtering (AITF) [13], StopIt [14] и др. Эти методы выявляют вредоносный трафик и отправляют на маршрутизаторы запросы на фильтрацию пакетов от подозрительного источника. Каждый из этих методов применяет различные схемы обнаружения вредоносного трафика и различные методы фильтрации. Однако не все методы ориентированы на случаи подмены адреса. Так, например, метод StopIt применяет фильтрацию на ближайшем к источнику трафика маршрутизаторе. При этом реальный путь трафика не отслеживается, и запрос на блокировку поступает к источнику, адрес которого указан в подозрительном пакете в качестве адреса отправителя. В том случае, если использовалась подмена адреса, будет осуществляться фильтрация от источника, который на самом деле может быть легитимным пользователем. Таким образом, следует уделять внимание проблеме подмены адреса и тем способам фильтрации и отслеживания реального пути трафика, которые позволяют ее выявить. Тем не менее, данные методы можно успешно использовать в составе комплексных решений по противодействию атакам.

Математические методы и методы интеллектуального анализа данных. Помимо уже описанных методов для анализа трафика могут быть реализованы механизмы защиты на основе математических методов, например определение энтропии [15].

В последние годы активно разрабатываются методы защиты, основанные на различных алгоритмах интеллектуального анализа данных. В качестве примеров можно привести механизмы на основе метода ближайших соседей (kNN) [16], обучаемых нейронных сетей [17]. Такие методы могут быть применимы и для противодействия атакам, использующим отражение трафика и его усиление. Интеллектуальные способы анализа данных позволяют выявить различные девиации трафика, а также подозрительное поведение клиентов. Сложность заключается в том, что обучение нейронных сетей, например, может занять весьма продолжительное время.

В работе [18] была предложена статистическая модель обнаружения DDoS-атак, осуществляемых по протоколу TCP. Модель анализирует флаги в заголовке каждого пакета и сравнивает реальный трафик с заданным шаблоном нормального трафика. Отклонения от шаблонного трафика расцениваются как аномалия.

Метод, представленный в работе [19], основан на принципе асимметрии трафика в случае атаки. В качестве шаблона нормального трафика принята схема симметричного обмена запросами клиента и ответами сервера. В случае значительного повышения количества входящих запросов или ответов на запросы, которые не могут быть корректно обработаны, нарушается симметрия трафика, и такая ситуация расценивается как атака. Стоит отметить, что анализ симметричности трафика предлагается также в качестве метода борьбы с атаками, основанными на отражении трафика и его усилении, так как при данных атаках асимметрия трафика является значительной и такую атаку становится легко выявить.

Метод защиты одноранговых сетей от различных атак, направленных на инфраструктуру компьютерной сети, представлен в работе [20]. Предлагаемый механизм защиты устанавливается на пограничном маршрутизаторе сети, на которую направлена атака. Метод обнаружения атаки основан на статистическом анализе трафика и его сопоставлении с шаблонным трафиком. После обнаружения атаки используется схема маркировки пакетов с целью выявления источника атаки и блокировки трафика от него. Такая схема представляет собой один из эффективных методов защиты и в случае, когда используется подмена адреса, так как отслеживается реальный путь трафика, а не выполняется блокировка трафика от указанного в пакете отправителя.

Механизмы защиты от атак, использующих отражение трафика. Рассмотрим механизмы защиты, разработанные непосредственно для атак, основанных на отражении и усилении трафика.

Общий механизм предотвращения отражения трафика RAD (Reflector Attack Defense) предлагается в [21]. В основе метода используется message authentication code (MAC). Когда тот или иной узел отправляет запрос, он помещает MAC в отведенное поле. В ответе на это сообщение размещается тот же самый MAC, что и в запросе. Узел,

получив ответ на запрос, сверяет MAC из отправленного им запроса и MAC из полученного ответа. Если MAC совпадают, сообщение принимается. В противном случае считается, что ответ представляет собой отраженный трафик и сообщение отклоняется.

В настоящее время разработано множество методов защиты от DNS-атак.

В работе [22] в основе метода защиты DAAD (DNS Amplification Attacks Detector) лежит тот факт, что при атаке DNS атакуемый узел получает большое количество ответов на отправленные ранее запросы. Авторы предлагают вести базу адресов DNS-серверов, на которые отправлялись запросы от того или иного узла. Все получаемые ответы должны проверяться, и если входящий пакет действительно является ответом на запрос, он будет принят. Если же с узла, которому адресован ответ, не отправлялся DNS-запрос на данный сервер, такой пакет должен быть отклонен. Данный метод весьма эффективен, однако следует помнить, что ведение подобных баз требует большого объема ресурсов.

В работе [23] предлагается установка предварительного DNS-резольвера и создание туннеля, использующего протоколы IPSec или SSL, между предварительным резольвером и DNS-резольвером на стороне организации. Все запросы DNS проходят исключительно через туннелированный канал связи и не могут поступить напрямую из внешних источников. Отмечается, что основная фильтрация DNS-ответов должна осуществляться провайдером услуг интернет-связи после соответствующего запроса от организации. Туннелирование в данном случае играет лишь вспомогательную роль.

В работе [24] предлагается механизм RRL (Response Rate Limiting), направленный на ограничение числа уникальных ответов от DNS-сервера. Этот механизм защиты используется на стороне DNS-сервера и анализирует исключительно исходящий трафик, полностью игнорируя входящий. Суть метода заключается в том, что адреса, на которые был отправлен ответ, записываются. При этом задается ограничение числа ответов сервера на каждый адрес. Если это число превышено, ответы на данный адрес больше не высылаются. Такой метод эффективен для снижения потока вредоносного трафика от сервера, но при этом существует вероятность ошибки первого рода. Однако следует помнить, что не всегда владельцы DNS-серверов готовы прибегать к использованию таких механизмов. Ведение базы адресов требует определенных ресурсов. Кроме того, не всегда владельцы таких серверов обеспокоены тем, что их серверы используются для осуществления атак, а также не всегда замечают увеличение нагрузки на сервер в периоды их использования для реализации атак.

В работе [25] предлагается метод FB (Flow-based), основанный на выявлении девиации трафика относительно шаблонного. Анализируется количество входящих пакетов по протоколу DNS и их размер. Если количество и размер пакетов превышают заданные значения, такая ситуация расценивается как атака. При этом автор отмечает, что в ситуациях, когда осуществляется атака, но при этом анализируемые параметры не превышают пороговых значений, трафик считается легитимным. Таким образом, процент ошибок второго рода в отдельных случаях может быть весьма высок. Данный метод, тем не менее, весьма перспективен при соответствующей доработке.

В таблице приведен общий сравнительный анализ рассмотренных методов защиты.

Метод	Место внедрения	Достоинства	Недостатки
RAD	На стороне атакуемого узла	Высокая точность обнаружения вредоносного трафика	Необходимость хранения запросов и соответствующих им MAC до получения ответа. Необходимость размещения сервером MAC в ответе на запрос
DAAD	На стороне атакуемого узла	Достаточно высокая точность обнаружения вредоносного трафика	Необходимость ведения базы данных, потребление большого объема ресурсов
Туннелирование	На стороне атакуемого узла	Безопасная передача данных	Предлагаемый метод играет вспомогательную роль, так как основная фильтрация осуществляется интернет-провайдером
RRL	На стороне сервера	Снижение потока вредоносного трафика	Необходимость ведения баз данных на сервере. Вероятность ошибки первого рода
FB	На стороне атакуемого узла	Достаточно высокая точность обнаружения вредоносного трафика	В отдельных случаях процент ошибок второго рода достаточно высок

Следует отметить, что рассмотренные методы были разработаны для противодействия атакам, реализуемым с помощью протокола DNS. Что касается атак, реализуемых по другим рассмотренным протоколам, то, например, основным средством предотвращения популярных в последние несколько лет атак по протоколу NTP является отключение команды мониторинга на стороне серверов. В настоящее время данную уязвимость имеют версии ntpd до 4.2.7p25 включительно, в выпуске 4.2.7p26 и выше команда monlist отключена. Иных мер, направленных на борьбу с отраженным трафиком, поступающим по протоколу NTP, до настоящего времени не предлагалось.

В целом, в качестве основной меры борьбы с атаками, основанными на отражении, рекомендуется отключать те функции серверов, которые могут использоваться для реализации атак, а также закрывать неиспользуемые порты. Такое решение, на первый взгляд, кажется самым простым и действенным, однако не все владельцы серверов по тем или иным причинам следуют этой рекомендации. Применительно к устройствам, принадлежащим пользователям, решить эту проблему становится сложнее. Статистика проведенных атак свидетельствует о том, что популярные типы атак, основанных на отражении, попрежнему легко реализовать. Несмотря на то, что, например, поддержка команды get_monlist была отключена в новых версиях протокола NTP, атаки данного типа продолжают занимать одну из лидирующих позиций. Это свидетельствует, в том числе, и о том, что не все владельцы NTP-серверов обновляют версии протокола до более безопасных, а значит, не все заботятся о предотвращении атак, в которые могут быть вовлечены их серверы.

В статье были рассмотрены протоколы, которые могут использоваться для реализации отражения трафика и его усиления. Проведенный анализ показал, что достаточно большое количество протоколов, основанных на протоколе UDP, имеют те или иные уязвимости, позволяющие реализовать отражение трафика.

Рассмотренные методы защиты от атак преимущественно были разработаны для противодействия атакам, реализуемым с помощью протокола DNS. Идеи, лежащие в основе этих методов, могут быть использованы для других типов атак, а сами методы модифицированы и применены для более широкого круга атак. Однако заметным недостатком таких методов будет высокое потребление ресурсов памяти для хранения записей, особенно при отслеживании трафика одновременно по нескольким протоколам. Тем не менее, они могут стать полезными в борьбе с новыми типами атак, против которых еще не были разработаны и внедрены методы защиты.

Растущая мощность атак, основанных на усилении трафика, а также количество таких атак свидетельствуют о том, что необходима разработка новых эффективных средств защиты компьютерных сетей. Остается нерешенной проблема фильтрации исходящего трафика на стороне сервис-провайдеров, что по-прежнему делает возможной подмену адреса источника. Многообразие протоколов, которые могут быть использованы для реализации атак, показывает необходимость поиска универсальных методов обнаружения возможных атак, использующих отражение и усиление. Не следует забывать о том, что потенциально опасные протоколы, на сегодняшний день находящиеся в тени, в ближайшем будущем могут стать инструментом для реализации массированных атак. Таким образом, следует не только уделить внимание уязвимостям, присущим популярным в настоящее время протоколам, но и разработать схемы противодействия как существующим, так и потенциально возможным атакам.

В качестве дальнейшей цели ставится задача проведения серии экспериментов по оценке эффективности существующих методов защиты для атак с различными сценариями. В том числе планируется проведение экспериментов по оценке эффективности методов защиты от DNS-атак, модифицированных для работы с другими протоколами, используемыми для реализации атак, основанных на отражении трафика. Полученные результаты будут учитываться при разработке новых методов защиты от атак, в основе которых лежат механизмы отражения и усиления вредоносного трафика.

Статья подготовлена в рамках проекта «Организация научных исследований» основной части государственного плана Министерства образования России.

СПИСОК ЛИТЕРАТУРЫ

1. Сайт DDoS AND WEB APPLICATIONS ATTACKS, 2015. URL: https://www.stateoftheinternet.com/downloads/pdfs/resources-web-security-2015-q2-ddos-webapp-stats-infographic.pdf.

2. Сайт ARBOR Networks Security Reports. URL: http://www.arbornetworks.com/resources.

3. Rossow C. Amplification hell: Revisiting network protocols for DDoS abuse // Symposium on Network and Distributed System Security (NDSS). 2014. URL: http://www.internetsociety.org/sites/default/files/01_5.pdf.

4. Damas J., Graff M. P. Vixie, Extension Mechanisms for DNS (EDNS (0)), 2013. URL: https://tools.ietf.org/html/rfc6891.

5. Shankesi R. Model-checking DoS amplification for VoIP session initiation // European Symposium on Research in Computer Security (ESORICS 2009), Saint-Malo, France. Springer Berlin Heidelberg, 2009. P. 390–405.

6. Zargar S. T., Joshi J., Tipper D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks // Communications Surveys & Tutorials. IEEE. 2013. Vol. 15, № 4. P. 2046–2069.

7. Peng T., Leckie C., Ramamohanarao K. Survey of network-based defense mechanisms countering the DoS and DDoS problems //ACM Computing Surveys (CSUR). 2007. Vol. 39, № 1. P. 3.

8. Ferguson P. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. 2000. URL: http://tools.ietf.org/html/rfc2827.html.

9. Li J. SAVE: Source address validity enforcement protocol // INFOCOM 2002. Twenty-First Annual Joint Conf. of the IEEE Computer and Communications Societies. Proceedings. IEEE. 2002. Vol. 3. P. 1557–1566.

10. Wang H., Jin C., Shin K. G. Defense against spoofed IP traffic using hop-count filtering // IEEE/ACM Transactions on Networking (ToN). 2007. Vol. 15, № 1. P. 40–53.

11. Chan E. Y. K. Intrusion detection routers: design, implementation and evaluation using an experimental testbed // Selected Areas in Communications. IEEE J. on. 2006. Vol. 24, № 10. P. 1889–1900.

12. Chen R., Park J. M., Marchany R. TRACK: A novel approach for defending against distributed denial-of-service attacks. 2006. URL: http://www.researchgate.net/profile/Jung-Min_Jerry_Park/publication/228471222_TRACK_A_Novel_Approach_for_Defending_Against_Distributed_Denial-of-Service_Attacks/links/0a85e53454bbb9ad32000000.pdf.

13. Argyraki K., Cheriton D. R. Scalable network-layer defense against internet bandwidth-flooding attacks // IEEE/ACM Transactions on Networking (TON). 2009. Vol. 17, № 4. P. 1284–1297.

14. Furfaro A. Modelling and simulation of a defense strategy to face indirect DDoS flooding attacks // Internet and Distributed Computing Systems Conf., Calabria, Italy. Springer International Publishing, 2014. P. 263–274.

15. Navaz A. S. S., Sangeetha V., Prabhadevi C. Entropy based anomaly detection system to prevent DDoS attacks in cloud // Intern. J. of Computer Applications. 2013. Vol. 62, № 15. P. 42–47.

16. Thwe Oo T. T., Phyu T. Analysis of DDoS Detection System based on Anomaly Detection System // Intern. Conf. on Advances in Engineering and Technology (ICAET'2014), Singapore, 2014. P. 315–319.

17. Kumar P. A. R., Selvakumar S. Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems // Computer Communications. 2013. Vol. 36, № 3. P. 303–319.

18. Tritilanunt S. et al. Entropy-based input-output traffic mode detection scheme for dos/ddos attacks // Communications and Information Technologies (ISCIT): Intern. Symp., Tokyo, 2010. P. 804–809.

19. Liu H., Sun Y., Kim M. S. Fine-grained DDoS detection scheme based on bidirectional count sketch // Computer Communications and Networks (ICCCN): Proc. of 20th Intern. Conf. on, Maui, Hawaii, 2011. P. 1–6.

20. Tariq U. Collaborative peer to peer defense mechanism for DDoS attacks // Procedia Computer Science. 2011. Vol. 5. P. 157–164.

21. Kline E. RAD: Reflector attack defense using message authentication codes // Computer Security Applications Conf. ACSAC'09, Annual, 2009. P. 269–278.

22. Kambourakis G. Detecting DNS amplification attacks // Critical Information Infrastructures Security. Springer Berlin Heidelberg, 2008. P. 185–196.

23. MacFarland D. C., Shue C. A., Kalafut A. J. Characterizing Optimal DNS Amplification Attacks and Effective Mitigation // Passive and Active Measurement Conf. New York: Springer International Publishing, 2015. P. 15–27.

24. Rozekrans T., Mekking M., de Koning J. Defending against DNS reflection amplification attacks // University of Amsterdam, Tech. Rep., Feb. 2013. URL: https://nlnetlabs.nl/downloads/publications/report-rrl-deko-ning-rozekrans.pdf.

25. Huistra D. Detecting Reflection Attacks in DNS Flows // 19thTwente Student Conference on IT. 2013. URL: http://referaat.cs.utwente.nl/conference/19/paper/7409/detecting-reflection-attacks-in-dns-flows.pdf.

Ya. A. Bekeneva
Saint Petersburg Electrotechnical University «LETI»

ANALYSIS OF DDoS-ATTACKS TOPICAL TYPES AND PROTECTION METHODS AGAINST THEM

In the paper an analysis of popular types of DDoS-attacks based on traffic reflection and traffic amplification is introduced. Existing methods for prevention and protection against such attacks are considered. Advantages and disadvantages of these methods are described. Necessity of new protection methods development is shown.

DDoS-attack, DNS, NTP, SSDP, SNMP, DDoS-attack protection, RRL, RAD

УДК 004.052.2

Р. Хаберланд, С. А. Ивановский, К. В. Кринкин
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Верификация объектно-ориентированных программ с динамической памятью на основе ссылочной модели

Предложен метод аксиоматичной верификации динамической памяти на основе логического языка программирования "Пролог" для объектно-ориентированных программ, использующих ссылочную модель памяти. Формально определены термины: куча, интерпретация кучи и рассмотрены формальные операции над кучами. Обобщенная реализация на Прологе разрешает преодолевать недостатки в выразимости. Сделаны предположения, что представленным подходом можно решить совокупность других актуальных проблем в той же области. Предполагаемая модель была проверена с помощью системы верификации [1], которая, в том числе, способна преобразовывать программы императивных языков с экземплярами классов в промежуточное представление.

Указатели, кучи, анализ псевдонимов, верификация динамической памяти

Разделяемые кучи. Реализация спецификации куч на Прологе может быть представлена различными моделями памяти, например глобальными графовыми моделями, моделями с функциями переходов или моделями с делением на кучи [2], [3]. В модели с делением на кучи используются «*распределенные кучи*» (модель согласной «Логики распределенной памяти» (ЛРП) [1]) с указанием связи вида «*а указывает на б*» или как «*а→б*», где «*а*» – идентификатор простого или объектного типа. Значением «*б*» может быть любое из предполагаемого (в том числе, объектного) домена T (см. далее). Это соответствие может быть представлено различными способами. В Прологе соответствие «*а→б*» представлено кортежами (*а*, *б*), например [(*h*2, 1), (*h*2, *h*3), (*h*3, 3)]. По определению, в модели ЛРП все кучи не пересекаются и не связаны между собой, кроме случая, когда такая связь задается дополнительным условием. Считается, что кучи могут иметь взаимосвязи. В этом случае необходимо определить связи между указателями явным образом в спецификации, как это сделано для указателей *h*1, *h*2 и *h*3 в приведенном ранее примере. Без ограничения общности можно считать, что определения куч с помощью ссылок достаточно, и ссылки на ссылки ради простоты далее не рассматриваются.

Определение кучи. Кучей является обобщенная и связанная графовая структура данных, которая располагается и меняется в динамической части памяти при запуске программы. Граф описывается типизированными ячейками памяти и связями между ними. Куча может иметь любое количество указателей (в том числе ни одного). Без ограничения общности, можно считать, что указатели определены либо стеком, либо кучей. Подкучей называем любой связный подграф.