Передача данных в сетях с динамической рандомизацией адресного пространства

© К.Н. Кравцов
Нижегородский государственный технический университет им. Р.Е. Алексеева,
Нижний Новгород
kirill@kravtsov.biz

Аннотация

Разрабатывается метод передачи данных с повышенной устойчивостью к прослушиванию трафика и распределенным атакам типа «отказ в обслуживании» на участников сессии передачи информации. Способ основан на предложенной модели динамической рандомизации адресного пространства сети (convoluted multiaddress networks). Такой подход к организации адресного пространства сетей позволяет изолировать узлы сети от нежелательного трафика путем скрытия физического адреса от неавторизованных пользователей. Предложенный метод предлагает рассматривать IP адрес сервера, не как его уникальный идентификатор, а как некоторую псевдослучайную величину, которая устанавливается динамически для каждого пакета каждого потока трафика от легитимных клиентов. В результате, атакующий терминал не может получить доступ к серверу, так как ему недоступен текущий временный адрес сервера и алгоритм его смены. В работе рассматривается модель передачи трафика в таких сетях и пример реализации прототипа.

Введение

Компьютерные сети, построенные на базе стека протоколов TCP/IP, подвержены различным типам сетевых атак, например, атакам типа «отказ в обслуживании» (DoS), IP спуфинг, прослушивание трафика и так далее (более подробная классификация приведена в статье [3]). В рамках этого исследования, обсуждаются методы предотвращения сетевых атак типа «отказ в обслуживании» и прослушивания трафика. Однако, разрабатываемый метод может быть так же применен для защиты от атак других типов, в ходе которых атакующие терминалы создают отдельные потоки трафика от потоков сообщений легитимных (авторизованных) пользователей.

Распределенные атаки типа «отказ в обслуживании» остаются одной из главных угроз в современных сетях, размер и частота таких нежелательных воздействий на сетевое оборудование растет с каждым годом. Такие атаки характеризуются, как явные попытки предотвратить легитимное использование службы. Результат здесь достигается путем специальных действий атакующей стороны, результатом которых становится исчерпывание ограниченных ресурсов жертвы атаки. Согласно [6], такие действия могут быть классифицированы по двум типам: семантические (semantic) и насыщающие полосу пропускания (flood, brute-force). В ходе таких действий, к серверу-жертве подключается не только легитимный клиент, использующий пропускную способность канала связи для посылки необходимого трафика, но и ботнет, т.е. большое число одновременно посылающих запросы терминалов. Поскольку увеличение потока запросов здесь создается увеличением числа терминалов, то какой бы уровень производительности сервера не был достигнут, начиная с некоторого числа ботов, создаваемый ими поток запросов превысит допустимый уровень для любого сервера.

В литературе предложено множество методов предотвращения DDoS атак. Согласно различным принципам, эти подходы можно разделить на следующие группы: по местоположению установки (близко к источникам, близко к серверу-жертве, в рамках транзитной сетевой инфраструктуры [9]); по типу алгоритма анализа и фильтрации трафика [8], другие классификации и примеры методов так же приведены в статьях [4] и [1].

Однако, можно заключить, что большая часть существующих подходов к решению проблем сетевой безопасности основаны на широком спектре алгоритмов анализа и фильтрации трафика. Такие методы используют реактивную стратегию: система защиты анализирует трафик, пытается детектировать DDoS атаку и, затем, фильтрует нежелательные пакеты. Здесь сетевой адрес сервера

Труды XVII Международной конференции DAMDID/RCDL'2015 «Аналитика и управление данными в областях с интенсивным использованием данных», Обнинск, 13-16 октября 2015

является его уникальным идентификатором, поэтому, ботнет может инициировать поток трафика на этот сервер, который достигнет узла назначения, если не будет отфильтрован установленным методом предотвращения атак. Таким образом, решения в этой области работают с прямым трактом между источниками трафика и точкой его назначения. В этом исследовании, разрабатывается альтернативный подход, заключающийся в том, что устойчивость к атакам достигается рандомизацией тракта передачи сообщений с помощью специальной адресной политики, в рамках которой сетевой адрес является лишь временным условным идентификатором сервера.

Необходимо заметить, что разрабатываемый метод не является широко применимой техникой «ручного» перескока IP-адреса (IP hopping), когда адрес атакуемого сервера меняется в ходе DDoS атаки на какой-либо другой IP-адрес на глобальном уровне (включая DNS серверы). В таких условиях, DDoS атака может быть переключена на новый адрес, так как он публично известен.

Так же, исследователями было предложено несколько методов динамической смены адреса сервера (рандомизации его адреса). Например, статья [7] предлагает метод динамической смены IP-адреса сервера в соответствии со псевдослучайным законом, известным только авторизованным клиентам. Но, по сравнению с методом, предлагаемым в текущем исследовании, такая смена обеспечивается только во время активной DDoS атаки глобально для всех клиентских сессий одновременно с достаточно большим периодом смены адреса (порядка 5 минут).

Метод динамической рандомизации адресного пространства предложен в статье [2] и предполагает, что случайным образом выбирается некоторый IP-адрес из глобального пула IP-адресов и эта замена происходит напрямую на защищаемом сервере. Таким образом, реализация основывается на специальной конфигурации DHCP сервера, что значительно ограничивает область применения метода.

1 Математическая модель передачи трафика в сетях с адресацией

Основная идея исследования состоит в декомпозиции отображения мгновенной интенсивности трафика $A_x^{out}(t) \to A_y^{in}(t)$ из узла с адресом *x* в узел с адресом *y* на три отображения: отображение $in(x,i)$ исходящего трафика в сетевое адресное пространство, автоморфизма *m(n,R),* сетевого адресного пространства, где *n* – задержка передачи данных в сети, *R* - функция подстановки на множестве пар адресов и отображения $out(j,y)$ из сетевого адресного пространства во входящий трафик. Моделью сетевого адресного пространства будем считать двумерную таблицу адресации с числом строк и столбцов, равным размеру адресного

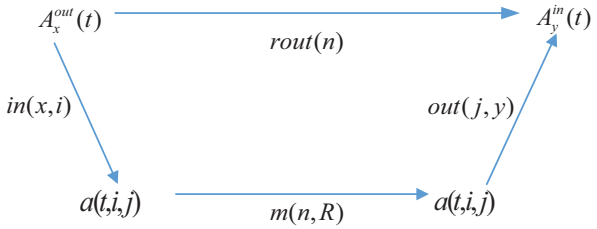

Рис. 1. Модель передачи трафика в сетях с адресацией

пространства сети. Эта модель приведена на рис. 1. Элементами $a(t,i,j)$ таблицы в каждый момент времени являются значения интенсивности трафика, адресованного из адреса *i* в адрес *j*.

При этом отображение $rout(n): A_x^{in}(t) = A_y^{out}(t-n)$ обеспечивает прямую трансляцию трафика из адреса источника *x* в адрес получателя *y* с задержкой на *n* единиц времени.

Отображение $in(x,i)$ определяет адрес *i* источника *x* в сети:

$$in(x,i): a(t,i,j) = A_x^{out}(t)$$

Отображение $out(j,y)$ определяет, какому получателю *y* соответствует сетевой адрес *j*:

$$out(j,y): A_x^{in}(t) = a(t,i,j)$$

Отображение сетевого адресного пространства в себя (автоморфизм) *m(n,R)* определяется параметром задержки и подстановкой $(i,j) \leftarrow R(i,j)$, т.е.

$$m(n,R):\ a(t,i,j) = a(t-n, R(i,j))$$

Покажем, при каких подстановках R построенная диаграмма отображений является коммутативной. Тривиальное решение заключается в подстановке вида:

$$R(i,j) = (i,j)$$

Соответственно отображения $in(x,i)$ и $out(j,y)$ определяются следующим образом

$$in(x,i): a(t,x,y) = A_x^{in}(t); \qquad out(j,y): A_y^{out}(t) = a(t,x,y)$$

Очевидно, что тривиальное решение не единственно. Рассмотрим случай, когда подстановка не тривиальна, а значение второго аргумента определяется некоторой функцией *f(j)*:

$$R(i,j) = \big(i, f(j)\big);\ \ out(j,y): y = f(j)$$

Это решение соответствует трансляции адреса получателя (NAT).

Еще одним решением является использование подстановки с функцией $hi(t,j)$, зависящей от времени *t*:

$$R(i,j) = \big(i, hi(t,j)\big);\ \ out(j,y): y = ho(t,j); hi(.,.) = ho(.,.)$$

Будем называть этот случай адресным хоппингом. Здесь мы ввели две функции хоппинга – хоппинг источника $hi(t,j)$ и хоппинг получателя $ho(t,j)$. Если эти функции одинаковые, то коммутативность диаграммы отображений также сохраняется.

Разумеется, можно построить другие отображения, сохраняющие коммутативность, но

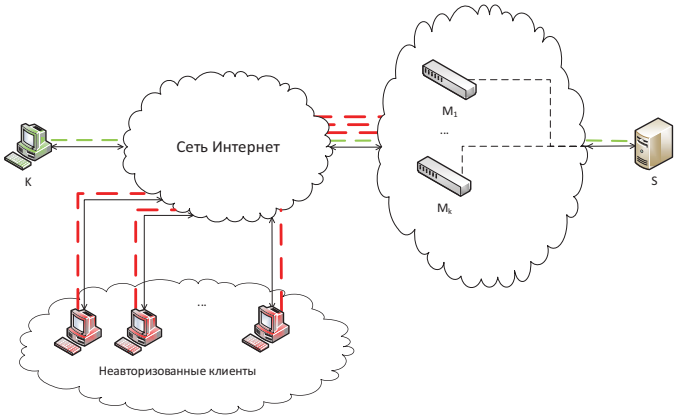

Рис. 2. Схема DDoS атаки на сеть с динамической адресацией

для нашего приложения этих случаев оказывается достаточно.

Рассмотрим теперь случай нескольких источников и одного получателя. Рассматривая исходные отображения для каждой пары источник – получатель *(x, y)*, можно видеть, что интенсивность трафика в узле одного получателя *y* от нескольких источников $x \in X$ может рассматриваться как аддитивная величина:

$$A_y^{out}(t) = \sum_{x \in X} rout(n_x) A_x^{in}.$$

Для противодействия распределенным атакам нас будет интересовать, какая адресная политика в сети, представленная в предложенной нами модели, будет приводить к случаю, когда аддитивность будет нарушена следующим образом: интенсивность трафика от одного выделенного (легитимного) источника x_1 полностью передается выбранному получателю y, тогда как для других источников $x \in X$, $x \neq x_1$, адресующихся этому же получателю, интенсивность доставленного трафика будет ослаблена в заданное число *K* раз.

Покажем, что задача имеет решение с помощью следующего определения отображений:

$$in(x,i): a(t,i,j) = A_x^{in}(t); R(i,j) = (i, hi(t,i);$$
$$out(j,y): y = ho(t,j),$$
$$hi(t,k) = ho(t,k)\ \forall (t,k)\ if x = x_1\ else\ hi(t,k) \neq ho(t,k)$$

Действительно, трафик от легитимного источника x_1 будет передан по сети в соответствие с коммутативностью диаграммы отображений без изменений. Для других источников x передача трафика будет происходить только для моментов времени, когда значения функций хоппинга $hi(t,j)$ и $ho(t,j)$ совпадут. Таким образом, если не существует моментов времени, в которые эти функции совпадают, интенсивность трафика от соответствующего источника для получателя *y* будет равна нулю. Если в некоторые моменты времени значения функций хоппинга совпадут, то в эти моменты времени трафик нелигитимных источников будет передан получателю *y*. Ослабление трафика в среднем будет определяться следующим отношением:

$K = \frac{|Tm|}{|Th|}$, где $|T_m|$ - мощность множества моментов времени передачи сообщения, $|T_h|$ – мощность множество моментов времени, на которых совпадают значения хоппинговых функций.

2 Метод построения сети с динамической рандомизацией адресного пространства

Рассмотрим функционирование сети с динамической рандомизацией адресного пространства, детально рассмотренный в статьях [10] и [5]. В результате применения такого метода, сервер обладает повышенной устойчивостью к распределенным атакам типа «отказ в обслуживании» и перехвата трафика. Данная техника, основанная на модели, приведенной выше, получила название IP Fast Hopping. Архитектура сети с динамической рандомизацией адресного пространства приведена на рис. 2.

Способ защиты сервера от распределенных атак типа «отказ в обслуживании» и перехвата трафика, основанный на прыгающей адресации ресурса, заключается в том, что реальный IP адрес защищаемого терминала (IP_R) не является публично доступной информацией (например, DNS серверы содержат записи не о нем, а об IP адресе некоторого сервера авторизации IP_A). Чтобы получить доступ к серверу S, клиент K должен пройти авторизацию на предмет того, является ли он доверенным для этого сервиса. Если авторизация пройдена успешно, то клиенту сообщается пул IP адресов $IP_r = \{IP_1, IP_2, \ldots, IP_n\}$ и ключ генерации псевдослучайной последовательности адресов для осуществления прыгающей адресации (идентификатор сессии) R. Так как эти данные сообщаются клиенту некоторым сервером-менеджером только на этапе установки соединения, то возможные перерывы в работе сервера-менеджера не влияют существенным образом на работу всей сети в целом (в особенности, уже подключенных клиентов). Так же на этом этапе клиенту задается «инициальный» IP адрес защищенного ресурса IP_0, который используется на уровнях выше сетевого для сохранения существующей логики работы вышестоящих протоколов и технологий. Шлюзы подсетей доступа

устройств к серверу являются основными структурными элементами предлагаемой архитектуры, которые поддерживают постоянные сеансы обмена сообщениями, и такая процедура авторизации и установки расширенных защищенных соединений сервера и клиента может быть выполнена на этапе первоначального конфигурирования сети или ее элементов. В данной работе под расширенными защищенными соединениями будем понимать сессии передачи данных между терминалом клиента и сервером, которые осуществляются при помощи динамической смены адресов назначения и отправителя передаваемых пакетов.

После установки соединения клиент начинает обмениваться сообщениями с сервером по его «инициальному» IP-адресу. При этом адрес назначения каждого следующего отправляемого пакета определяется терминалом клиента динамически из полученного пула адресов путем расчета специальной хэш-функции, которая отображает метку времени передаваемого IP пакета t_n и идентификатора текущей расширенной защищенной сессии R на номер адреса n во множестве адресов IP_r:

$$n = f(t_n, R)$$

Таким образом, осуществляется изменение адреса получателя IP пакетов, отправляемых от клиента к серверу, с фиксированного «инициального» адреса на виртуальный, рассчитанный по псевдослучайному закону.

Подчеркнем, что пул IP адресов IP_r не содержит адреса сервера, защита которого осуществляется посредством предлагаемого метода. Этот набор формируется из адресов, которые принадлежат одному или нескольким высокопроизводительным маршрутизаторам M_k в изолированных подсетях устройств. При создании расширенного защищенного соединения, каждому из маршрутизаторов M_k сообщается идентификатор новой сессии и адрес клиента, с которым должно поддерживаться расширенное соединение. После получения маршрутизатором пакета от клиента K, производится расчет хэш-функции $f(t_n, R)$, отображающей идентификатор этой сессии R, и метку времени полученного пакета t_n. Если рассчитанный IP адрес совпадает с адресом назначения принятого пакета, то этот пакет перенаправляется на реальный адрес ресурса. В противном случае пакет отбрасывается. Ответы ресурса подвергаются такой же процедуре, но не с адресом назначения пакета, а с адресом отправителя.

В итоге получается, что, для внешнего наблюдателя сессии передачи данных между сервером и авторизованным клиентом IP адрес сервиса регулярно меняется (для исходящих от пользователя пакетов меняется IP адрес назначения, а для входящих – адрес отправителя). Замена IP адреса защищаемого сервера происходит с каждым инкрементом значения метки времени пакета. Предсказание IP адреса назначения следующего пакета крайне затруднено для стороннего терминала (так как ему неизвестен идентификатор сессии и реальный адрес сервера) и зависит от параметров псевдослучайной последовательности, по закону которой изменяется виртуальный адрес защищенного сервера для данного конкретного терминала доверенного пользователя. В итоге, нелегитимный клиент не только не может инициировать атаку на защищенный сервер, но и процесс анализа прослушанного трафика пользователя оказывается затруднен ввиду того, что пакеты этого клиента отправляются не какому-то определенному адресу, а большому количеству различных адресов в сети интернет.

3 Реализация механизма динамической смены IP адреса сервера

В качестве простейшего примера реализации механизма псевдослучайной смены IP-адресов сетевых устройств рассмотрим его реализацию в виде модуля ядра операционной системы GNU/Linux. В этом случае, для применения предложенной системы достаточно установить на маршрутизаторы, построенные на базе операционной системы GNU/Linux (или подобной ей), разработанный модуль ядра.

Ядро Linux содержит в себе встроенный межсетевой экран (брандмауэр) – Netfilter, который осуществляет фильтрацию и перенаправление пакетов, согласно установленным пользователем набором правил при помощи утилиты iptables. Данный межсетевой экран поддерживает 5 цепочек правил: для начальной обработки пакетов (PREROUTING), для входящих пакетов (INPUT), транзитных пакетов (FORWARD), исходящих пакетов (OUTPUT) и окончательной обработки исходящих пакетов POSTROUTING.

Основная идея реализации предлагаемого в данной статье метода заключается в следующем: при установке расширенного защищенного соединения, утилита netfilter добавляет новый набор правил в цепочку PREROUTING для каждого маршрутизатора, участвующего в поддержке процесса обмена пакетами между сервером и клиентом по алгоритму прыгающей адресации. Этот новый набор правил осуществляет проверку того, что полученный пакет адресован на корректный виртуальный IP адрес сервера. Если поле адреса назначения удовлетворяет этому условию, то пакет будет перенаправлен на физический адрес защищаемого сервера, иначе пакет будет отброшен. Для всех отправляемых сервером клиенту пакетов этот же набор правил будет осуществлять замену IP адреса источника на корректный виртуальный адрес сервера для конкретного значения метки времени этого пакета.

Заключение

Способы защиты серверов от DDoS атак и прослушивания трафика представляют научный и практический интерес. В этом исследовании, эти распространенные сетевые угрозы рассматриваются с альтернативной точки зрения. Обычно, исследователи работают над этой проблемой, как над проблемой безопасности единого прямого тракта (на физическом уровне, имеющего некоторое количество маршрутов). В таком случае, необходимо найти способ защиты концов такой «трубы» сообщений (путем создания брандмауэра) и/или способ защиты легитимных сообщений в этом тракте (при помощи фильтрации нежелательного трафика). Вместо этого, целью данного исследования стало изолирование и сокрытие такой «трубы» от атакующих терминалов (ботов). Очевидно, что это невозможно осуществить на практике на физическом уровне, но такая задача выполнима при рассмотрении сети как логического пространства взаимосвязанных узлов, местоположение каждого из которых определяется некоторым адресом (адресное пространство). Основная идея разрабатываемой технологии заключается в построении динамического адресного пространства, узлы которого находятся в движении в рамках этого пространства. Можно сказать, что на таком абстрактном уровне, участники сети станут уязвимыми к сетевым атакам в том случае, если каждый другой узел может однозначно определить местоположение жертвы в какой-либо момент времени в будущем. Предложенный метод предоставляет такую информацию только определенным узлам («авторизованным»), исключая все остальные. В статье продемонстрирован пример реализации обсужденной системы, который может быть применен в существующих вычислительных сетях, без изменения архитектуры или инфраструктуры глобальной сети интернет.

Литература

[1] Patel Ankita and Fenil Khatiwala, "Survey on DDoS Attack Detection and Prevention in Cloud," International Journal of Engineering Technology, Management and Applied Sciences, vol. 3, no. 2, pp. 43-47, 2015.

[2] S. Antonatos, P. Akritidis, E. P. Markatos, and K. G. Anagnostakis, "Defending Against Hitlist Worms Using Network Address Space Randomization," in Proceedings of the 2005 ACM Workshop on Rapid Malcode, Fairfax, VA, USA, 2005, pp. 30-40.

[3] Rajra Blessy and A J Deepa, "A Survey on Network Security Attacks and Prevention Mechanism," Journal of Current Computer Science and Technology, vol. 5, no. 2, pp. 1-5, 2015.

[4] B. B. Gupta, R. C. Joshi, and Manoj Misra, "Distributed Denial of Service Prevention Techniques," International Journal of Computer and Electrical Engineering, vol. 2, no. 2, pp. 268-276, 2010.

[5] Vladimir Krylov and Kirill Kravtsov, "DDoS attack and interception resistance IP fast hopping based protocol," in 23rd International Conference on Software Engineering and Data Engineering, SEDE 2014, New Orleans, 2014, pp. 43-48.

[6] Jelena Mirkovic and Peter Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Computer Communication Review, no. Volume 34 Issue 2, pp. 39 - 53, 2004.

[7] Prateek Mittal, Dongho Kim, Yih-Chun Hu, and Matthew Caesar, "Mirage: Towards Deployable DDoS Defense for Web Applications," 2012.

[8] K. Munivara Prasad, A. Rama Mohan Reddy, and K. Venugopal Rao, "DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms - A Survey," Global Journal of Computer Science and Technology, vol. 14, no. 7-E, pp. 15-32, 2014.

[9] Saman Taghavi Zargar, James Joshi, and David Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," Communications Surveys & Tutorials, IEEE, vol. 15, no. 4, pp. 2046 - 2069, 2013.

[10] Владимир Владимирович Крылов and Кирилл Николаевич Кравцов, "Защита IP-подсетей от DDoS-атак и несанкционированного доступа методом псевдослучайной смены сетевых адресов ," Вопросы Защиты Информации, no. 3, pp. 24-31, 2014.

Data Transmission in Networks with Address Space Dynamic Randomization

Kirill N. Kravtsov

The method ensuring increased DDoS and traffic eavesdropping resistance of data transmission sessions is demonstrated in this article. The technique is based on the suggested model of convoluted multiaddress networks. This approach provides a way to isolate network nodes from malicious traffic by hiding of physical node address from all unauthorized clients. Under the suggested method, server's IP address is not a unique identification, but a pseudorandom value which is calculated dynamically for each network packet from each traffic stream initiated by legitimate clients. In the result, malefactor is unable to acquire access to the server because the current network address and schedule of its change is unavailable. The model of traffic transmission in such networks and example of initial implementation is demonstrated in this paper.