2008 Математические основы компьютерной безопасности № 2(2)
DOI 10.17223/20710410/2/18
УДК 681.3

О ЦЕНТРАЛИЗОВАННОМ ТЕРРИТОРИАЛЬНО-РАСПРЕДЕЛЁННОМ АНАЛИЗЕ СЕТЕВОГО ТРАФИКА

В.В. Лапшин

Томский государственный университет

E-mail: alter@mail.tsu.ru

Предлагается метод централизованного территориально-распределённого анализа сетевого трафика. Излагаются приёмы захвата, доставки, анализа и принятия решений. Сообщается о реализации метода и полученных экспериментальных результатах.

Ключевые слова: *сетевой трафик*, *захват трафика*, *анализ.*

С широким распространением Интернет возникли разные задачи, связанные с безопасностью сетей. Одной из этих задач является качественный анализ трафика по различным критериям оценок. В настоящее время качественный анализ с применением штатного аппаратного и программного обеспечения весьма затруднён. Главными причинами являются кратный рост пропускной способности сетей на базе Ethernet и архитектура ядер операционных систем, которая не приспособлена к транспортировке пакетов из пространства ядра в пространство пользовательского процесса при высокой скорости поступления пакетов. В данной работе предлагается способ использования захвата пакетов без потерь с интерфейса Ethernet с возможностью предоставления их прикладной программе, транспортировки в центр анализа из нескольких точек сбора трафика и анализа протоколов на основе полученных данных. В центре анализа трафика, создавая различные критерии анализа, можно строить распределённые системы выявления и блокирования DDoS-атак, несанкционированной сетевой активности, атак на сетевые службы, документирования сетевых сообщений, а также прочих задач информационной безопасности.

1. Проблема захвата IP-пакетов на скоростях 100 Мбит/с и выше

Современные операционные системы общего назначения (GNU/Linux, FreeBSD, Windows 2000/XP на Intel-совместимом аппаратном обеспечении) довольно легко справляются с захватом трафика на скоростях 10 Мбит/с и ниже через стандартный интерфейс библиотеки libpcap [1] (winpcap [2] для Windows). Количество необходимых операций для этого покрывается существующими мощностями аппаратного обеспечения. При захвате более высокоскоростного трафика наблюдается ситуация потери пакетов. Причиной этого является недостаточная вычислительная мощность ЭВМ, с одной стороны, и архитектура операционной системы – с другой, которая никогда не предполагала высокой (в пике до 1488000 переключений из контекста ядра в пространство пользователя и обратно при скорости 1 Гбит/с) интенсивности при передаче пакетов из пространства ядра в пространство пользователя.

Потеря пакетов при захвате чревата в первую очередь для процесса дальнейшего декодирования TCP/IP-сессий и других сеансовых соединений. В случае потери одного пакета процесс автоматизированного разбора протокола не может продолжить работу ввиду выпавшего необходимого участка данных. В этом случае вся последующая информация из данной сессии не может быть использована. Именно по этой причине недопустима потеря даже одного пакета.

С целью исправить ситуацию с большим количеством потерянных пакетов сторонними исследователями предложены разные варианты решения: libpcap-mmap [3], nCap [4] (исходные тексты в настоящее время не доступны, несмотря на некогда открытую лицензию), PF_RING [5]. Все они ориентированы на применение в рамках ядра Linux. Тем не менее ни одна из технологий не включена в стандартное ядро Linux. Организовав дистрибутив с интегрированной технологией PF_RING, можно добиться 100%-го захвата пакетов в 1Гбит/с-ethernet сети. Имея этот дистрибутив, можно быстро разворачивать точки захвата трафика. С его применением отпадает необходимость вручную накладывать заплатки и интегрировать технологию PF_RING в операционную систему.

2. О физических средствах захвата IP-трафика

Существует по крайне мере два подхода в методе захвата. Безболезненный метод заключается в прозрачном внедрении точки захвата трафика. Прозрачный метод позволяет сделать это без какого-либо изменения структуры сети, без установки дополнительных маршрутизаторов, без вмешательства в порядок работы пользователей. Реализовать это можно путём установки аппаратного зеркала ethernet-порта (такого, как nTap

[6], nMirror [7]) с подсоединением зеркальных выводов (для принимаемого и передающегося трафика, так как обычно ethernet-порты – полнодуплексные) к двум сетевым картам, где и будет производиться захват трафика. Под пиковой нагрузкой будем подразумевать ситуацию, когда канал загружен полностью и все захваченные пакеты должны быть проанализированы. Альтернативным механизмом может служить сетевой концентратор (hub). В этом случае достаточно будет одной сетевой карты для сбора принимаемого и передаваемого трафика.

При пиковой нагрузке к аппаратуре захвата должны быть подсоединены ещё две сетевые карты или одна, но более высокой производительности. Производительность последней должна быть не ниже удвоенной производительности менее скоростной. Таким образом, при использовании данной схемы удастся прозрачно и без нарушения работы сети произвести необходимые действия. Минусом метода является необходимость дополнительного подвода канала удвоенной ёмкости для передачи информации в центр анализа.

Второй метод может быть внедрён на базе маршрутизатора с операционной системой GNU/Linux. Работая в штатном режиме, ядро может быть дополнено функциональностью технологий PF_RING, после чего с произвольного порта может быть осуществлён захват пакетов. Недостаток метода состоит в том, что сетевые карты не должны быть произвольного производителя, так как применяемые технологии могут работать только с фиксированным числом сетевых карт, но обычно в маршрутизаторах на базе GNU/Linux установлены соответствующие карты от Intel или Broadcom (или иных подходящих марок). Кроме этого, минусом является необходимость обновления ядра после штатного системного обновления (так как оно с большой вероятностью заменит ядро и модифицированную библиотеку libpcap, и далее высокоскоростной захват пакетов без потерь будет невозможен), а также перерыв в работе при плановых перезагрузках сервера.

3. О необходимости централизованного пункта сбора и анализа трафика

Как показано выше, высокоскоростной трафик удаётся собрать в отдельных высокоскоростных участках сети. Но так как точек сбора может быть несколько, было бы не рационально в каждой устанавливать программное обеспечение по его анализу. Кроме этого, могли бы возникнуть многочисленные коллизии ввиду того, что один и тот же трафик может проходить через несколько точек сбора. Соответственно встаёт задача транспортировки захваченного трафика в центр сбора и его обработки. В целом можно отметить два пути: штатным образом через сеть Интернет, либо специализированным выделенным каналом, который одним концом подключен к точке сбора трафика, другим – напрямую к центру анализа трафика. В первом случае необходимо защитить при транспортировке трафик от третьих сторон, чтобы иметь уверенность в аутентичности и конфиденциальности при дальнейшем анализе.

Проверка вероятностного симметричного шифра libpssc на современном оборудовании показала, что он способен шифровать два потока по 100 Мбит/с. Libpssc представляет собой реализацию класса вероятностных поточных шифров, построенных на базе симметричных криптосхем в поточных режимах, описанных в работах [8, 9]. Использование других алгоритмов (AES, например) может предоставить возможность шифровать и более скоростной (1 Гбит/с) трафик. При транспортировке через выделенный канал защита может производиться как физическим, так и криптографическим методами. Таким образом, будем считать, что в описанных случаях трафик доставляется в центр анализа в полном объёме и недоступным для третьих лиц способом.

4. О возможном временном сохранении трафика

В случае временного перерыва связи с центром в пунктах сбора могут быть использованы накопители на жестких магнитных дисках для временного хранения информации (на криптографически-защищённых файловых системах или разделах). Криптографическая защита носителей предусматривается для случая возможной кражи или выемки несанкционированной стороной. После восстановления связи ранее записанная информация передаётся для анализа.

Протокол передачи представляет собой простой протокол, работающий через TCP-сессию. Соединение инициирует узел сборки трафика. Перед отправкой захваченных пакетов они подвергаются криптографическому преобразованию. В пункте приёма происходит обратная операция. Пункт приёма трафика по этому же каналу может передавать корректирующие сведения по поводу маски захвата трафика. Устанавливая маску, которая соответствует только интересующему трафику, можно снизить расходы ресурсов, связанных с транспортировкой трафика. Таким образом, в центр анализа будет доставлен только интересующий трафик.

В протоколе передачи предусмотрена возможность сжатия информации для снижения необходимого объёма полосы пропускания канала. В случае применения алгоритмов сжатия информации для текстовых и немультимедийных протоколов возможно экономить в среднем до 70 % пропускной способности канала.

5. Центр анализа и принятия решений

Предполагается, что центр анализа является защищённым от присутствия третьих лиц объектом. На его площадке ввиду отсутствия необходимости скрывать перехваченный трафик от третьих лиц происходит обратная процедура – расшифрование. Поток информации поступает на анализ произвольным средствам реа-

гирования, которые, руководствуясь заложенной в них логикой, принимают те или иные решения. Предполагается, что модули средств реагирования могут быть подключены (или отключены, заменены) в процессе работы системы через механизм подключаемых библиотек. Загрузка (отключение) одних модулей не влияет на работу других модулей. Одним из стандартных механизмов в этом процессе является блок сбора TCP/IP-сессий libnids [10] (основан на ядре Linux-2.0) из поступающих пакетов. Основной задачей данного механизма является получать данные TCP/IP-сессий из набора TCP-пакетов. В нём специально заложены средства учёта полученных дублируемых пакетов, возможных ввиду ненулевой вероятности прохождения одного и того же пакета через несколько точек сбора. Поэтому возникающие потоки являются уникальными и не дублируют друг друга. К особенностям механизма можно отнести возможность успешной дефрагментации поступающих пакетов, высокую надёжность и устойчивость против попыток злоумышленников блокировать сборку TCP/IP-сессий.

Получение TCP/IP-сессий не является достаточным для разбора произвольных протоколов. Далее могут использоваться специальные средства распознавания конкретных протоколов (HTTP, FTP, SMTP, POP3, ICQ и др.) и модули анализа трафика для должного реагирования на возникающие события.

6. Планы на будущее

Целью дальнейшего исследования является изучение методов оптимального построения математических алгоритмов распознавания и реагирования на (распределённые) DoS-атаки, проверка работоспособности метода на скоростях 10 Гбит/с и изучение вопроса об изменении производительности и масштабируемости при смене блока сбора TCP/IP-сессий на блоки из других ОС семейства BSD [11] и современной версии ядра Linux 2.6. Также не безынтересна перспектива использования в точках захвата ОС FreeBSD с разработкой аналога технологии PF_RING для сетевой подсистемы Netgraph, что поможет отказаться от поддержки специализированного дистрибутива на базе GNU/Linux и использовать стандартную ОС с подключаемым модулем ядра.

Заключение

В рамках апробирования предложенной схемы созданы специализированный дистрибутив на базе ОС GNU/Linux с интегрированной технологией PF_RING и программа приёма и передачи захваченного трафика в центр обработки. При транспортировке используются потоковые вероятностные криптосистемы, однако криптографические преобразования ими не ограничены. Программа приёма трафика с точек сбора производит обратную процедуру и предоставляет подключаемым средствам анализа необходимый интерфейс для обращения к нему. Таким образом, разработав соответствующие механизмы распознавания и реагирования и применяя предлагаемую систему в рамках ISP, возможно осуществить массовую защиту Web-сайтов от DDoS-атак, а также решать иные задачи компьютерной безопасности на множестве географически-распределённых точек присутствия узлов сбора трафика.

ЛИТЕРАТУРА

1. http://www.tcpdump.org/
2. http://www.winpcap.org/
3. http://public.lanl.gov/cpw/
4. http://www.nmon.net/nCap.html
5. http://www.ntop.org/PF_RING.html
5. http://www.nmon.net/nTap.html
6. http://www.nmon.net/nMirror.html
7. *Агибалов Г.П.* Вероятностные схемы симметричного поточного шифрования над конечным полем // Вестник ТГУ. Приложение. 2005. № 14. С. 39 – 42.
8. *Колегов Д.Н.* Общая схема вероятностной поточной шифрсистемы // Вестник ТГУ. Приложение. 2006. № 17. С. 112 – 114.
9. http://libnids.sourceforge.net/
10. http://ru.wikipedia.org/wiki/BSD