Метод обнаружения несанкционированного копирования Ethernet-трафика киберобъектов

С. А. Петренко

Повсеместное внедрение стандарта Ethernet в локальных, LAN и федеральных, MAN сетях критически важных объектов поднимает целый ряд вопросов, связанных с обеспечением конфиденциальности и целостности передаваемых данных, а также доступности сервиса в целом. Одним из таких вопросов является встроенная в большое число моделей активного сетевого оборудования стандарта Ethernet возможность пересылать копию передаваемого трафика на рабочую станцию, отличную от получателя. Заявляемая разработчиками устройств исключительно как средство отладки и мониторинга, данная возможность, тем не менее, является весьма серьезной угрозой для конфиденциальности любых передаваемых по сети Ethernet данных, будь то файлы, мгновенные сообщения или, например, трафик IP-телефонии.

Высокая степень опасности указанной угрозы вызвана тем фактом, что при получении злоумышленником прав на изменение конфигурации оборудования его действия, направленные на копирование («ответвление») трафика на нецелевой порт, не будут иметь практически никаких демаскирующих признаков (в отличие от атак вида «MAC-storm» или «ARP poisoning», направленных на те же цели). Просмотр администратором безопасности настроек оборудования, если он будет проводиться регулярно и иметь одной из целей проверку отсутствия несанкционированных ответвлений трафика, несомненно, выявит подобные злоупотребления. Однако данный путь трудно формализуем в случае использования разнородного оборудования, а следовательно, для достаточной периодичности проверок потребует неприемлемых затрат времени.

Давайте рассмотрим возможный метод автоматического контроля отсутствия несанкционированного ответвления Ethernet-трафика. Ме-

тод предполагает использование типовых протоколов и стандартов сетевой статистики (SNMP и аналогичных) на периодической основе с целью обнаружения корреляций между объемами защищаемого трафика и трафика по нецелевым портам. Для значительного повышения быстродействия и точности метода предлагается в моменты проведения измерений корреляций генерировать между защищаемыми абонентами фиктивный сетевой трафик в объемах, достаточных для быстрого и достоверного обнаружения ответвлений, однако, не превышающий в совокупности порог пропускной способности канала.

1. Существующие варианты технологии ответвления трафика

В настоящее время наибольшее распространение получили следующие технологии и стандарты ответвления Ethernet-трафика, способные послужить для злоумышленника средством несанкционированного доступа к передаваемым данным.

Технология *зеркальных* (*mirror*) *портов* на коммутаторах (другие наименования — *Tap ports, SPAN ports — Switched Port ANalyzer*), представляет собой возможность настройки одного или нескольких портов коммутатора на получение полной копии сетевого трафика, проходившего через тот или иной порт. В зависимости от программного обеспечения, управляющего коммутатором, порт, настраиваемый в зеркальный режим, может как становиться выделенным (прекращать штатное функционирование), так и оставаться вполне работоспособным портом коммутатора. Второй вариант еще больше повышает шансы успешного маскирования ответвления, например, в том случае, когда злоумышленник является штатным сотрудником компании (инсайдером) и использует для зеркалирования свой «рабочий» порт коммутатора. Большинство коммутаторов, обладающих функциональностью зеркалирования портов, поддерживают возможность ответвления в один и тот же зеркальный порт сразу нескольких коммутируемых информационных потоков (см. рис. 1).

Кроме отраслевых стандартов для ответвления/перехвата трафика широко используются внутренние протоколы и соглашения производителей активного сетевого оборудования. Так, например, лидер в области телекоммуникационного оборудования компания Cisco System Inc. внедряет (на устройствах разного уровня) сразу 3 дополнительных

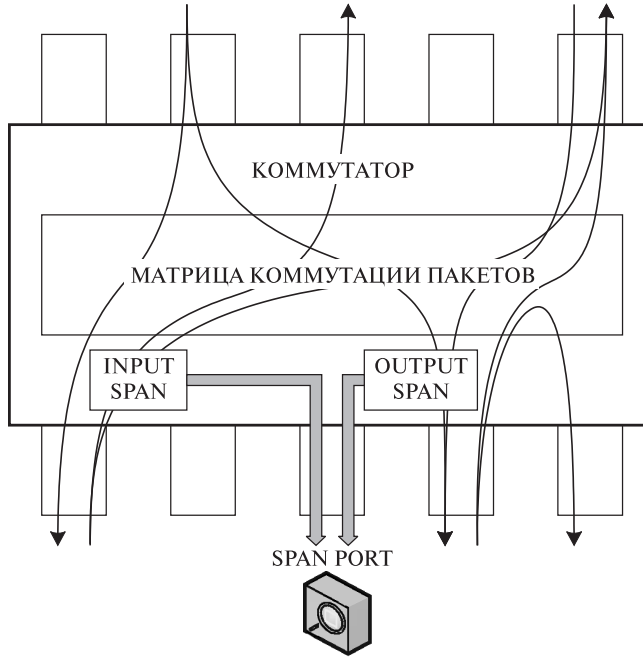

Рис. 1. Зеркалирование портов

протокола, расширяющих функциональность базовой технологии зеркалирования портов:

- *RSPAN* (*Remote SPAN*), ориентированный на передачу захваченного трафика через цепочку устройств в отдельном VLAN-е (снимая необходимость конфигурирования SPAN-портов на каждом из них);
- *ERSPAN* (*Encapsulated Remote SPAN*), инксапсулирующий на прослушивающем коммутаторе пакеты захваченного трафика в пакеты протокола GRE, что позволяет доставлять их далее по IP-сети без ограничения на дальность передачи (получатель может находиться, например, в любой точке сети INTERNET);
- *IP Traffic Export*, расширяющий технологию ответвления трафика на устройства 3-го уровня модели OSI — маршрутизаторы, и позволяющий перенаправить копию любого IP-трафика, прошедшего через маршрутизатор, на любое устройство, подключенное к нему либо напрямую (канал «точка-точка») либо через сеть Ethernet (в заголовках перенаправляемых пакетов изменяется только MAC-адрес получателя).

2. Существующие средства сбора сетевой статистики

Унифицированные (не подразумевающие прямой доступ к конфигурации устройства из командной строки) методы контроля за режимом работы активного оборудования основаны на мониторинге консолидированной (обобщенной) статистики работы устройства:

- на общесистемном уровне (загрузка ЦП устройства, размер таблицы динамической коммутации/маршрутизации, средняя длина очередей пакетов и т. п.);
- на физическом уровне модели OSI (количество принятых и переданных байт или пакетов по каждому из физических портов, распределение длин пакетов и т. п.);
- на канальном уровне модели OSI (статистика по байтам и пакетам, идущим от определенного MAC-адреса, или к определенному MAC-адресу, или в матричном виде для пары «MAC-отправитель — MAC-получатель», например, RMON(6));
- на сетевом уровне модели OSI — только для маршрутизаторов — (статистика по байтам и пакетам, идущим от определенного IP-адреса, или к определенному IP-адресу, или в матричном виде для пары «IP-отправитель — IP-получатель», например, RMON(15), NetFlow от компании Cisco Systems Inc. или sFlow (RFC3176) от компании Hewlett-Packard).

Наибольшее распространение среди протоколов, поддерживающих в т. ч. и передачу консолидированной статистики сетевого оборудования, получил SNMP — Simple Network Management Protocol (v.1. — RFC1157, v.2 — RFC1901.RFC1910). В настоящее время протокол SNMP с базовыми возможностями по консолидированной статистике общесистемного и физического уровня реализован в подавляющем большинстве моделей активного сетевого оборудования.

3. Основные принципы способа, ограничения и допущения

Обнаружение несанкционированного копирования Ethernet-трафика в направлении нецелевых портов в активном сетевом оборудовании может быть реализовано несколькими способами в зависимости от воз-

можностей программного обеспечения, под управлением которого работает устройство. Так, например, очевидно, что в тех случаях, когда это возможно, наиболее достоверное и быстрое подтверждение факта копирования может дать консолидированная статистика матричного вида (с разбивкой по отправителю и получателю), такая как, например, RMON(6), RMON(15) или NetFlow. Однако, данный подход нельзя назвать универсальным, т. к. во-первых, для случая базового ответвления сетевого трафика на 2-м уровне (технология SPAN) дублирующий трафик не попадает ни в одну из матриц статистики (его MAC-адреса отправителя и получателя не изменены, а следовательно, выделить его в матрице 2-го уровня модели OSI невозможно), во-вторых, многие версии программного обеспечения полностью игнорируют дублирующий трафик при подсчете матричной статистики.

Предлагаемый метод основан на наблюдении за консолидированной статистикой физического уровня, а именно — количеством байт, переданных по определенному физическому интерфейсу устройства. Указанный статистический датчик реализован во всех версиях программного обеспечения, поддерживающего протокол SNMP. Дублирующий трафик учитывается этим датчиком в большинстве реализаций.

В стандарте RFC1213, описывающем минимально требуемый набор SNMP-датчиков, он определен в абсолютном варианте (подсчитывая количество байт, прошедших через интерфейс с момента его инициализации — чаще всего запуска устройства). В нескольких стандартах производителей телекоммуникационного оборудования реализация датчика дополнена уже вычисленным значением среднего исходящего трафика по интерфейсу за некоторый интервал времени (1 секунду, 5 секунд, 1 минуту). Этот вариант повышает точность исчисления границ интервала, т. к. устраняет ошибку, связанную с длительностью доставки и обработки SNMP-запроса/ответа.

В случае активации на оборудовании опции копирования трафика по той или иной технологии между объемами перехватываемого и выходящего трафика по SPAN-порту будет наблюдаться статистическая корреляция. В общем случае она может быть «зашумлена» трафиком, выходящим из SPAN-порта, но не являющимся дубликатом перехваченного (в том случае, когда SPAN-порт остается невыделенным и выполняет штатные функции для абонента). Данный факт может значительно усложнить (замедлить) процесс обнаружения корреляций, если поток перехватываемого трафика невелик по сравнению со штатным

трафиком SPAN-порта. Это приводит к вопросу о модификации способа путем активного воздействия (провокации) в отношении анализируемой системы. Генерация между защищаемыми абонентами фиктивного сетевого трафика в объемах, превосходящих статистические отклонения «шума» SPAN-порта, превращает задачу обнаружения в сходящуюся за вполне определенный временной интервал.

4. Математическая модель принятия решения

Обнаружение корреляции между объемом исходящего трафика на определенном интерфейсе устройства и передаваемыми фиктивными сообщениями представляет собой задачу детектирования на выходе канала связи с аддитивными помехами двоичного сигнала с априорно известными значениями для «0» и «1». Нулевому значению сигнала соответствует отсутствие дублирующего трафика, единичному — его присутствие, а шумам — штатный трафик SPAN-порта.

Максимально эффективное детектирование сигнала достигается при наибольшем разнесении по амплитуде значений сигнала для «0» и «1». Поскольку уровень «0» соответствует отсутствию трафика, увеличение расстояния между уровнями возможно только за счет увеличения объема контролируемого трафика. Однако, чрезмерная генерация фиктивного трафика может негативно сказаться на работоспособности самой коммутирующей системы, в связи с чем возникает вопрос об оптимальном объеме генерируемого потока. Проведем расчет этой величины, исходя из следующих соображений и допущений.

Пусть штатный трафик обследуемого порта является стационарным и имеет нормальный закон распределения $p_0(x)=N(m,\sigma)$. Тогда трафик обследуемого порта при наличии ответвленного трафика объема q имеет распределение $p_1(x)$, идентичное $p_0(x)$, но смещенное на q единиц вправо — $p_1(x) = N(m + q,\sigma)$. В случае, если ответвление трафика вызывает увеличение его объема (например, при дополнении GRE-заголовком) под величиной q будем понимать итоговую величину на выходе порта, а истинное значение генерируемого фиктивного трафика корректировать (уменьшать) на величину дополнительных данных.

При наличии n наблюдений задача принятия решения сводится к статистической задаче о выборе из двух простых гипотез. Для нор-

мального закона распределения наиболее мощным критерием для проверки гипотезы является условие

$$t_\alpha \le \sqrt{n}\,\frac{\bar{x} - m}{\sigma}, \tag{1}$$

где $\Phi(-t_\alpha) = \alpha$, α — вероятность ошибки I-го рода, заключающейся в принятии решения о наличии несанкционированного копирования, при том что фактически оно не производилось; $\bar{x}$ — наблюдаемое среднее значение величины x.

Для данного критерия количество испытаний n^*, необходимых для того, чтобы ошибки I-го и II-го рода не превышали некоторых заранее заданных величин (α и β), должно удовлетворять неравенству

$$n^* \ge \sigma^2 \frac{\left(\Phi^{-1}(\alpha) + \Phi^{-1}(\beta)\right)^2}{q^2}. \tag{2}$$

Ограничения на величину q сверху зададим, исходя из требований минимального негативного воздействия на коммутирующую систему, следующим образом. Пусть каждый факт превышения суммарным (штатным + фиктивным) трафиком пропускной способности канала в текущем отсчете увеличивает количество требуемых испытаний на 1. Физический смысл этого соображения в том, что в случае переполнения полосы пропускания значение, снятое в следующем интервале, будет иметь некорректное значение, при этом величина ошибки достаточно сложно определима из-за отсутствия информации о правилах «сброса» избыточного трафика в коммутационной матрице устройства. Вероятность данного события $P(x > b)$ при пропускной способности канала b для случайной величины x, распределенной по закону $p_1(x) = N(m + q, \sigma)$, равна

$$P(x > b) = 1 - \Phi\left(\frac{b - (m + q)}{\sigma}\right), \tag{3}$$

что приводит к итоговому неравенству для граничного значения количества $t(q)$ временных интервалов, требуемых для анализа:

$$t(q) = \sigma^2 \frac{\left(\Phi^{-1}(\alpha) + \Phi^{-1}(\beta)\right)^2}{q^2} \Bigg/ \Phi\left(\frac{b - (m + q)}{\sigma}\right). \tag{4}$$

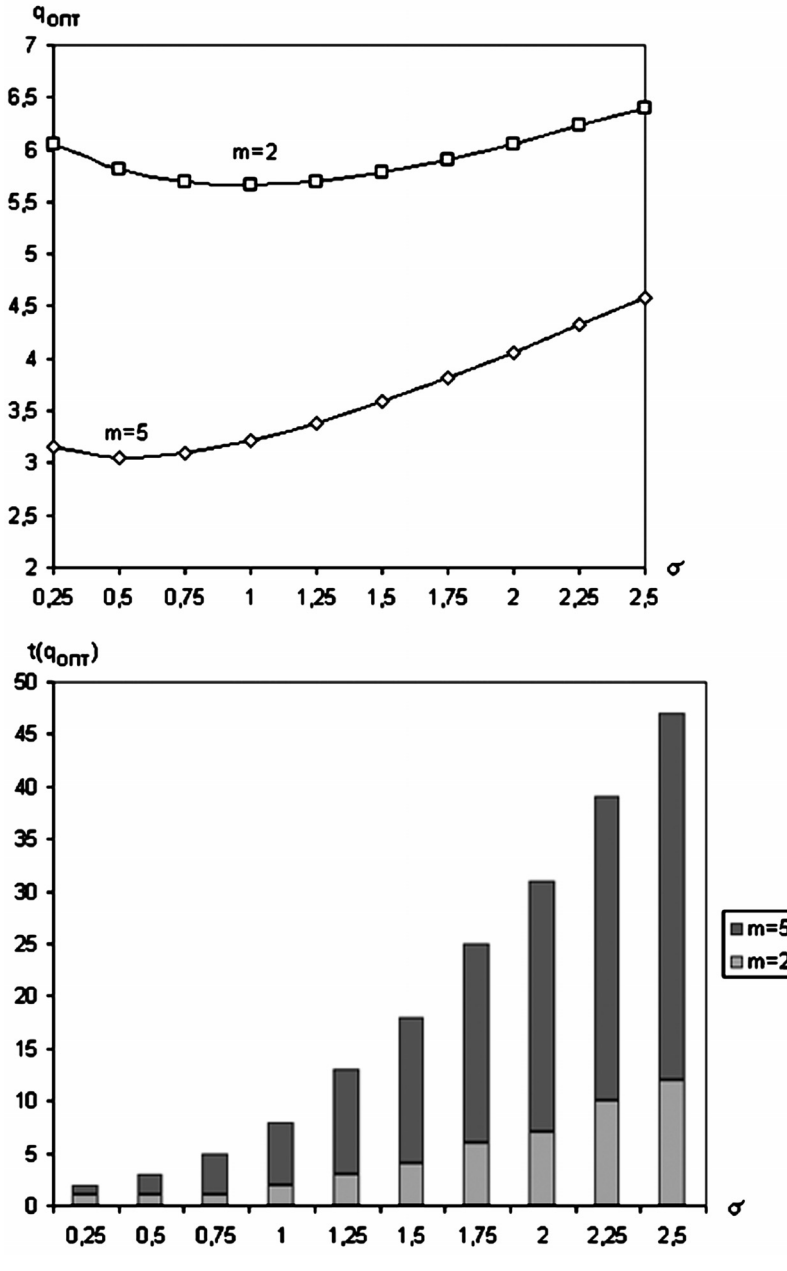

Рис. 2. Оценка полученного эффекта

Отыскание значения $q_{опт}$, доставляющего минимум функции $t(q)$, возможно численными методами. На графике приведены зависимости значения $q_{опт}(\sigma)$ для $\alpha = \beta = 0{,}001$, $b = 8{,}5$ (реальный порог пропускной способности типовых коммутирующих устройств) и величин штатного трафика SPAN-порта $m = 2$ и $m = 5$.

5. Заключение

Рассмотренный метод позволяет унифицированно обнаруживать несанкционированное копирование (ответвление) злоумышленником Ethernet-трафика на активном сетевом оборудовании киберобъектов с заранее заданным уровнем ошибки. Способ не требует изменения архитектуры сети и смены программного обеспечения на устройствах, т. к. использует широко распространенный протокол SNMP и анализирует датчики, ставшие его обязательной частью де факто в конце 90-х гг.

Дальнейшие перспективы развития метода заключаются в совершенствовании модели сетевого трафика (например, с помощью более точного описания логарифмически нормальным законом распределения с граничными условиями). Кроме того, представляется возможным расширить область применимости способа на компьютерные сети с нестационарными сетевыми потоками путем модификации схемы сбора статистических данных, например, чередуя интервалы подачи фиктивного трафика с интервалами «тишины», во время которых оцениваются текущие статистические характеристики шума.

Литература

1. *Мамаев М. А., Петренко С. А.* Технологии защиты информации в Интернете. Специальный справочник. СПб.: Питер, 2002. 848 с.: ил. (Специальный справочник).
2. RFC 1213. Management Information Base for Network Management of TCP/IP-based internets. 1991.
3. RFC 1901. Introduction to Community-based SNMP. V. 2. 1996.
4. Cisco Systems Inc. NetFlow Export Datagram Formats. 1997.
5. RFC 3176. sFlow: A Method for Monitoring Traffic in Switched and Routed Networks. 2001.