УДК 004.738.5.772

В.И. Никонов

Методы защиты информации в распределенных компьютерных сетях с помощью алгоритмов маршрутизации

Рассмотрен альтернативный метод защиты информации при её передаче в распределенных сетях в условиях воздействия преднамеренных атак. Основанный на применении разработанного приложения «маршрутизируемый сервис» позволяет решать поставленную задачу защиты без применения алгоритмов шифрования. Смоделированы сетевые атаки на сервис, даны оценки вероятностям реализации атак. Выполнена апробация «маршрутизируемого сервиса» на распределенной сети. Произведен анализ построенной защиты.

Ключевые слова: распределенные сети, сетевые протоколы, сетевые атаки, маршрутизируемый сервис, мультиплексирование трафика, Интернет.

Настоящая работа продолжает исследование [1], которое посвящено разработке алгоритмов разделения данных в распределенных сетях. Данный метод выступает в качестве альтернативы снижению вычислительных затрат при использовании шифрования.

Разнообразие угроз, воздействующих на информацию в распределенных сетях, объясняется сложной структурой последних. Сетевые атаки многогранны и определяются рядом факторов: целью злоумышленника, объектом воздействия, архитектурой сегмента сети.

В настоящее время существует достаточно много работ, посвященных классификации и описанию сетевых атак. Например, в исследованиях профессора Avinasha Kaka, в том числе [2], разбираются угрозы, подстерегающие трафик в TCP/IP сетях.

Наиболее распространен класс так называемых активных сетевых атак, для осуществления которых злоумышленнику необходимо напрямую совершить взаимодействие с некоторой системой, являющейся частью сети. Набор инструментов столь же широк: создание перегрузок серверов, эксплуатация недостатков протоколов, использование уязвимостей программного обеспечения. В международной литературе по вопросам информационной безопасности примеры таких атак можно встретить под названиями «sniffing», «flooding», «smurf», «spoofing», «hijacking» и др.

Существующие меры по снижению угроз атак эффективны, но, как правило, узко специализированы. Например, применение криптографических инструментов протокола IpSec делает перехват TCP/IP-пакетов нецелесообразным, но никак не противодействует атакам, вызывающим значительную загрузку на некоторых участках пути следования трафика.

Автором разработан принципиально иной подход к повышению устойчивости системы при целенаправленных воздействиях активного характера.

Одним из видов активных сетевых атак является класс атак, основанных на снифинге [2]. Приведем пример одной из них.

Злоумышленник, обладая знаниями, что некоторая организация регулярно передает данные из A в G, может довольно точно определить маршрут от A до G в момент времени Δt и осуществить перехват на каком-нибудь из участков следования трафика (рис. 1).

A, B, C, D, E, F, G – пока следует понимать как некоторые узловые сервера, необходимые для пространственного представления маршрута следования трафика. Так, A – Интернет-шлюз организации. Производя посылку трассировочных пакетов, злоумышленник в момент времени Δt определил маршрут следования трафика (показано пунктиром) и произвел атаку на подконтрольном маршрутизаторе, расположенном на участке BF.

Автором разработан «маршрутизируемый сервис» S_M передачи данных через распределенные сети. S_M – клиент-серверное приложение, позволяющее пользователю передавать данные специфичным маршрутом. Характер маршрута определяется базой критериев S_M. Среди них, например, такие как скорость доставки, надежность, безопасность и т.д. В данной статье приведено описание работы, посвященной исследованию критерия безопасности передачи. В рамках же всего проекта рассматривались и остальные.

В роли маршрутизаторов для S_M выступает некоторое множество доверенных серверов распределенной сети. Под доверенным сервером будем понимать некоторый многофункциональный сервер распределенной сети, к которому злоумышленник не имеет доступа.

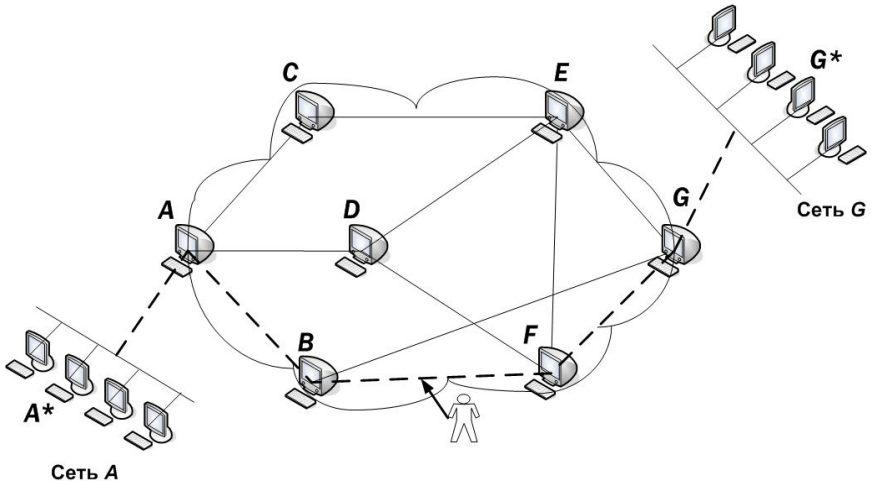

Рис. 1. Работа протоколов маршрутизации между A и G в момент Δt. Возможный вариант атаки на участке BF

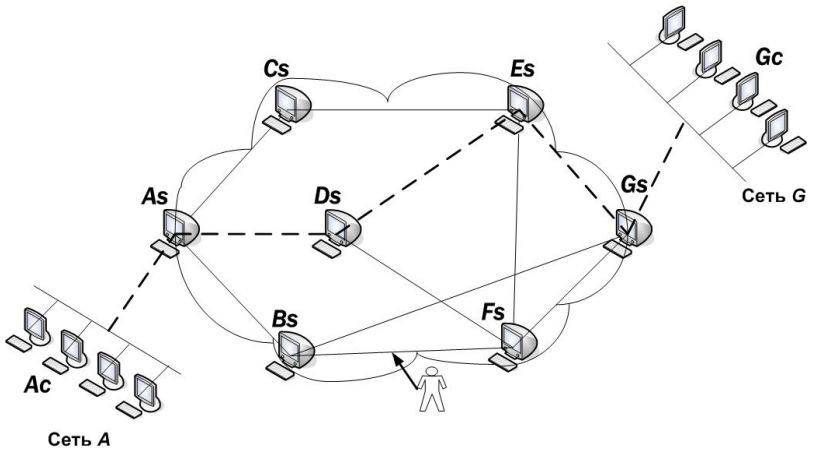

Рис. 2. Изменение маршрута трафика за счет использования доверенных серверов D_S, E_S

На доверенных серверах A_S, B_S, C_S, D_S, E_S, F_S, $G_S \in F$ устанавливается серверная часть сервиса – S_{MS}, выполняющая автоматическую «интеллектуальную» маршрутизацию трафика. Обозначим F – множество всех доверенных серверов с S_{MS}, а F_i – конкретный доверенный сервер $i \in [1,n]$. S_{MC} – приложения клиентской части сервиса. S_{MC} устанавливается на компьютерах пользователей и предоставляет пользователям диалог для инициализации процесса передачи данных с участием F_i [3].

На рис. 2 показано, что использование S_M позволило избежать прохождения трафиком подконтрольного злоумышленнику участка. Данное решение S_M (итоговый маршрут) является вероятностным с вероятностью принятия p_j, $0 < p_j \le 1, j \in [1, k]$, где k – количество различных маршрутов от A_S до G_S на графе с вершинами A_S, B_S, C_S, D_S, E_S, F_S, G_S и ребрами, определяемыми текущей топологией сети. Расчет значений p_j будет рассмотрен далее.

Напомним, что в процессе передачи с помощью S_M данные проходят через некоторое число доверенных серверов, равное f (для примера на рис. 2 f = 3). Выбор каждого следующего сервера происходит динамически. Учитывая приведенное выше определение таблиц маршрутизации для S_{MS}, выбор каждого следующего сервера описывает гипергеометрическое распределение HG(c; a_i, n, c).

Параметры распределения: n – число всех используемых доверенных серверов; c = 1, в случае использования инструмента мультиплексирования трафика c>1. a_i – число недоступных для F_i серверов из числа всех серверов (определяется из динамической таблицы маршрутизации M_i).

Но далее логично считать, что недоступные серверы не участвуют в выборке на каждом из этапов передачи.

Таким образом, итоговый маршрут трафика от отправителя до получателя при использовании S_M и f доверенных серверов (из n-доступных) будет выбран с вероятностью

$$p_j = \binom{n-a_0}{c} \times \binom{n-1-a_1}{c} \times \ldots \times \binom{n-f-a_f}{c},\ j \in [1,\ k]; \tag{1}$$

a_i – число недоступных серверов для F_i в момент выбора F_{i+1} доверенного сервера на $i + 1$ шаге.

$$a_i = n - \sum_{w=1}^{n} m_{iw}. \tag{2}$$

Если мультиплексирование не используется, то

$$p_j = \binom{n-a_0}{c} \times \binom{n-1-a_1}{c} \times \ldots \times \binom{n-f-a_f}{c} = \frac{1}{n-a_0} \times \frac{1}{n-1-a_1} \times \ldots \times \frac{1}{n-f-a_f}. \tag{3}$$

Разобьем все сетевые атаки, которым может подвергнуться разработанная система, на два класса: атаки на трафик между «смежными» серверами и атаки непосредственно на доверенные сервера F_i. Понятие «смежности» определяется динамически для каждого сеанса передачи, например, «смежными» являются серверы F_t и F_{t+1}, выбранные на i и i+1 этапе передачи, $t \in [1,\ n]$, $i \in [1,\ f]$.

Оценим вероятность реализации атаки первого класса P_{A1}, когда злоумышленник контролирует участок между доверенными серверами F_t и F_{t+1}. При неизвестном пространственном расположении F_i считаем атаку успешной, если при работе сервиса S_M передатчики F_t и F_{t+1} были выбраны на i и i+1 этапе передачи, $t \in [1,\ n]$, $i \in [1,\ f]$.

$$P_{A1} = \frac{2}{n-a_0} \times \frac{1}{n-1-a_1} + \frac{2}{n-1-a_1} \times \frac{1}{n-2-a_2} + \ldots + \frac{2}{n-(f-1)-a_{f-1}} \times \frac{1}{n-f-a_f}. \tag{4}$$

Формула (4) легко распространяется на случай подконтрольных злоумышленнику участков между s-доверенными серверами F_t, F_{t+1}, …, F_{t+s}. Приближения (4) при известных соотношениях параметров n, f и a_i рассматриваются в [3].

Представим второй, более широкий класс атак в виде неординарного (группового) потока событий, т.е. последовательности событий, наступающих одно за другим в случайные промежутки времени.

Тот факт, что в один момент времени может поступить несколько угроз различных видов или одного вида, но с разных источников, определяет неординарность потока.

Обозначим ω – количество успешно атакованных серверов в единицу времени (интенсивность).

Тогда вероятность того, что за время t будут реализованы атаки на m-доверенных серверов (из n доступных) описывается распределением Пуассона:

$$P_{A2}(m,t) = \frac{(\omega \cdot t)^m}{m!} \mathrm{e}^{-(\omega \cdot t)}. \tag{5}$$

Для оценки ω воспользуемся результатами, полученными в [4]. Авторы этой работы использовали специальные СОВ-сенсоры (система обнаружения вторжений) для регистрации разных видов сетевых атак на веб-серверы. Результаты работы СОВ-сенсоров представлены на рис. 3.

Представим ω как сумму интенсивностей конечного числа различных видов успешных атак, например таких, как спуфинг, «человек посередине», флуд и др. В статье [5] предлагается классификация атак, которая охватывает 14 признаков атак и представляется их численная оценка. Таким образом,

$$\omega = \sum_{i=1}^{k} \omega_i = \sum_{i=1}^{k} p_i \cdot h_i; \tag{6}$$

p_i – вероятность реализации атаки i-го вида, h_i – количество атак i-го вида, $i \in [1,\ k]$.

Как показали авторы [4], практически невозможно дать точную оценку ω, т.к. ее величина зависит от многих факторов: времени наблюдения, расположения сервера, функционального назначения сервера и др.

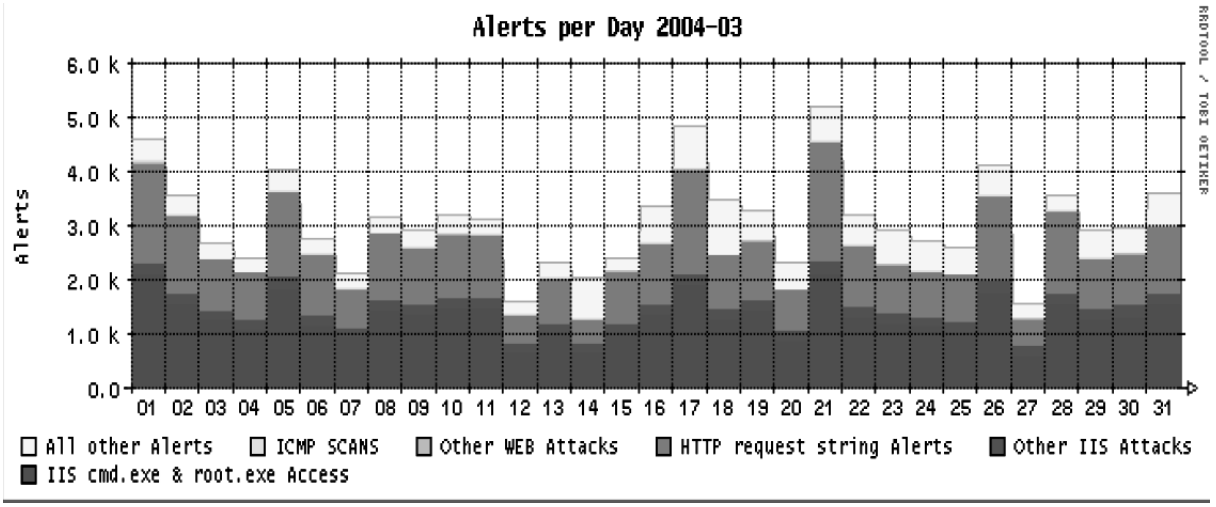

Рис. 3. Интенсивность различных видов атак на наблюдаемые веб-серверы, опубликованная в работе Dörges – Gellert – Kossakowski

Спроектируем модель потока атак, не зависящего от вышеперечисленных факторов (рис. 4). В этой схеме смоделирован ординарный поток атак, модель группового потока строится аналогичным образом.

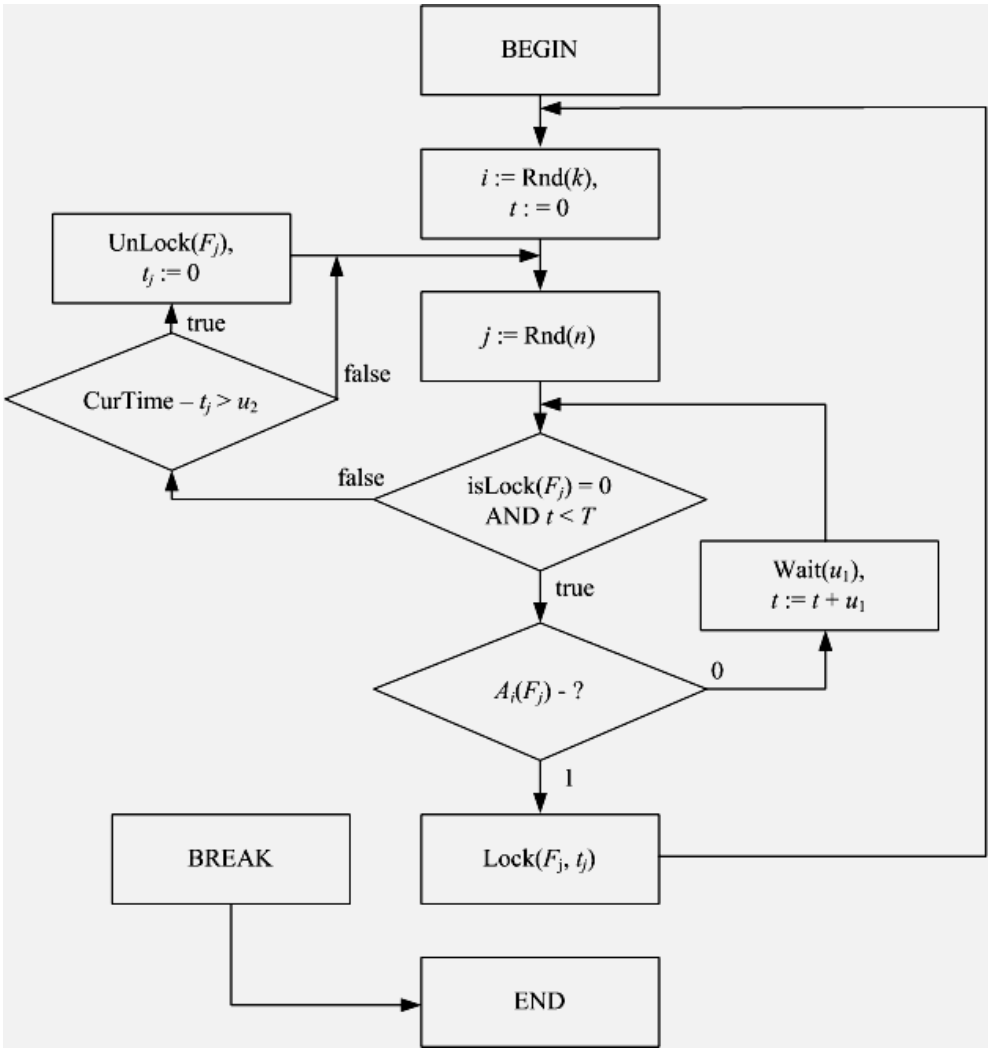

Рис. 4. Блок-схема алгоритма генерации потока атак на доверенные сервера

Приведем обозначения переменных и процедур, используемых в схеме.

Переменные: n – количество доверенных серверов в сети; k – количество видов атак; T – время действия выбранного вида атаки; u_1 – время ожидания в случае неудачного исхода атаки; u_2 – время блокировки доверенного сервера в случае успешного исхода атаки; F – доверенный сервер; p_i – вероятность реализации атаки i-го вида; i, j, t, t_j – вспомогательные переменные; CurTime – текущее время.

Процедуры и функции: Rnd(x) – генерация случайного целого числа на интервале $[1;x]$, $x >= 1$; Unlock(F_j) – разблокировать сервер F_j; $A_i(F_j)$ – исход эксперимента «атака на сервер F_j», определяемого дискретной случайной величиной с распределением «вероятность принять значение 1 (успех) равна p_i, вероятность принять значение 0 (неудача) равна $1 - p_i$»; Wait(x) – пауза на время x; isLock(F_j) – возвращает статус сервера F_j (доступен; заблокирован); Lock(F_j, x) – заблокировать F_j и вернуть текущее время в переменную x.

Работа приложения «маршрутизируемый сервис» была опробована на глобальной сети крупного предприятия, в полной мере моделирующей некоторую распределенную сеть. В [3] приведено описание процесса тестирования, представлен граф маршрутов следования трафика и вычислена вероятность реализации атаки при использовании в сети данного приложения. Исходя из полученных результатов, сделан вывод о соответствии практических результатов теоретическим представлениям работы сервиса S_M.

В формуле (1) показана возможность встраивания в S_M алгоритмов мультиплексирования. Таким образом, можно объединить два подхода к обеспечению безопасности передаваемой информации: с одной стороны, снизить вероятность доступа злоумышленника к используемым каналам связи, а с другой – применить логическое преобразование информации. В качестве варианта логического преобразования в [1] разработана система, выполняющая разделение данных по нескольких разнесенным каналам передачи так, что с физической точки зрения перехват всех частей затруднителен и сложность восстановления исходной последовательности без какой-либо ее отдельной части максимальна. В данной работе в системе разделения данных выделяются три основных элемента: мультиплексор, демультиплексор и передатчики. По выполняемым функциям передатчики близки к доверенным серверам S_M. Данный факт создает хорошие предпосылки для интеграции двух систем.

В результате выполнения исследовательских работ разработан алгоритм динамической маршрутизации трафика. На основе данного алгоритма разработан метод защиты конфиденциальности информации в распределенных сетях – приложение «маршрутизируемый сервис». Выработаны основные компоненты, необходимые для функционирования системы. Даны оценки вероятностям реализации сетевых атак на передаваемую информацию в случае применения «маршрутизируемого сервиса». Произведена апробация сервиса на глобальной сети предприятия.

Использование «маршрутизируемого сервиса» S_M для передачи данных через распределенные сети позволяет значительно снизить вероятность реализации класса активных сетевых атак злоумышленника без использования каких-либо инструментов шифрования.

Литература

1. Ефимов В.И. Система мультиплексирования разнесенного TCP/IP трафика / В.И. Ефимов, Р.Т. Файзуллин // Вестник Том. гос. ун-та. – 2005. – № 14. – С. 115–118.

2. Kak A. Port Scanning, Vulnerability Scanning, and Packet // Computer and Network Security. – 2008. – № 23. – P. 29–38.

3. Никонов В.И. Маршрутизируемый сервис передачи данных через распределенные сети // Научная сессия ТУСУР–2009: матер. докл. Всерос. науч.-техн. конф. студентов, аспирантов и молодых ученых. 12–15 мая 2009 г.: В 5 ч. – Ч. 1. – Томск: В-Спектр, 2009. – С. 92–95.

4. Dörges T. A Network of IDS Sensors for Attack Statistics / T. Dörges, O. Gellert, K. Kossakowski // Praxis der Informationsverarbeitung und Kommunikation. – 2004. – № 27. – P. 202–208.

5. Paulauskas N. Computer System Attack Classification / N. Paulauskas, E. Garšva // Electronics and Electrical Engineering. – 2006. – № 2(66). – P. 84–87.

Никонов Вячеслав Игоревич
Аспирант, ассистент преподавателя каф. средств связи и информационной безопасности ОмГТУ
Тел.: +7-904-322-24-95, (381-2) 56-59-38
Эл. почта: vi.nikonov@gmail.com

Nikonov V.I.
Network attacks on routed traffic

The article describes the questions, concerning information transfer through public distributed networks under deliberate attacks. In order to answer this question, the author has developed «routed service» of data transmission through the distributed networks, allowing to increase information safety. The author has simulated network attacks to the service and has calculated estimated probabilities of attacks. As a result «routed service» has been tested on the distributed network.
Keywords: distributed networks, network protocols, network attacks, routed service, traffic multiplexing, Internet.