УДК 004.056

Скрытые каналы передачи информации

Виктор АЛЕКСЕЕВ

Viktor M. ALEKSEEV

Алексеев Виктор Михайлович *– доктор технических наук, профессор кафедры управления и защиты информации Российского университета транспорта (МИИТ), Москва, Россия.*

Covert Channels of Information Transfer

(текст статьи на англ. яз. – English text of the article – p. 54)

В статье рассмотрены вопросы организации скрытых каналов передачи информации с помощью встроенных агентов в операционные системы. Современное состояние исследований в данной области науки, сравнение с мировым уровнем показывают, что отсутствуют теоретические разработки анализаторов скрытых каналов, а также программно-аппаратная реализация их моделей. Автор предлагает свой подход к созданию анализаторов скрытых каналов на основе методов самоорганизации, а также алгоритм сетевых операций, позволяющий выполнять функции перепутывания пакетов с целью разрушения процесса передачи информации по скрытым каналам.

Ключевые слова: каналы информации, корпоративная сеть, скрытый канал, анализатор, тайный агент, пакет, перцептрон.

Обзор публикаций по скрытой передаче информации показал, что проблема исследования этой сферы является актуальной. Скрытые агенты, поставляемые в современных операционных системах (ОС), выполняют различные задачи по сбору данных с компьютеров через, казалось бы, безобидные приложения. Объёмы памяти, занимаемые операционными системами, растут значительно, а функции практически остаются прежними. Это косвенно доказывает то, что внутри операционных систем на базе приложений присутствуют тайные агенты-организаторы, скрытые агенты по передаче информации. Приложения – необходимый инструмент для сбора информации, легально установленный на персональных компьютерах, коммуникаторах, серверах и других вычислительных средствах [1–3, 6, 7]. Причём с обновлением ОС одновременно обновляются и тайные агенты.

Технология работы скрытых каналов основана на следующем принципе. Скрытое программное обеспечение (агенты) не позволяет себя контролировать, так как непосредственно располагается в ядре операционной системы. Тайный агент начинает действовать от команды извне,

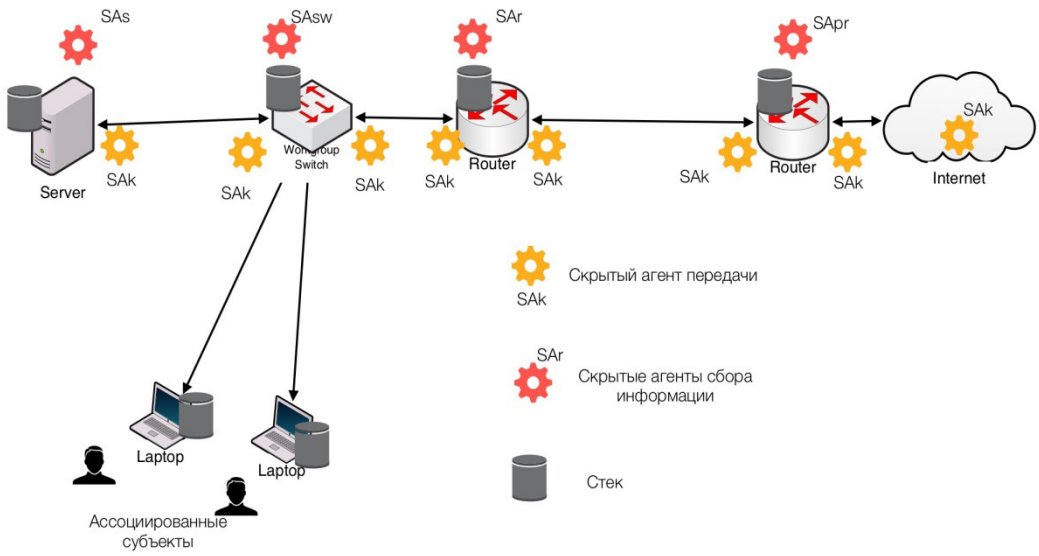

Рис. 1. Структурная схема формирования скрытых каналов: SAs, sw, r, pr – скрытые агенты, отвечающие за сбор данных с сетевых устройств и формирование объёма передаваемой информации; SA_k – скрытый агент передачи информации по одному из признаков или их комбинации.

а следовательно, в системе должны быть организованы скрытые каналы доставки управляющей команды. Занимаются этим агенты-организаторы. Передача и приём их информации осуществляют по тем же каналам, которые использует и общая корпоративная сеть предприятия. Процесс поначалу идёт посредством оборудования локальной сети: точки доступа, коммутаторы, защитные экраны, маршрутизаторы. Передача информации по скрытым каналам происходит далее через оборудование оператора связи, где основными звеньями становятся сервера и маршрутизаторы.

Иначе говоря, через канал связи от внешнего источника к нелегальному агенту должна быть передана информация, объём которой зависит от типа решаемых задач. Но если такая операция будет замечена, то «закладку» можно тут же уничтожить. Ясно, что передача информации автомату такого агента осуществляется через ту же входную последовательность, что и информация компьютерной системе (КС). За работой КС наблюдает некий субъект U, который не видит скрытого управления агентом и располагает некоторой информацией относительно текущего состояния КС и поданного на вход задания.

Субъект U не видит в состоянии s скрытый канал $X \to Y$ тогда и только тогда, когда $I_s(X, Y) \to \mathrm{Is}(X, Y|Z)$ [3, 5, 8]. Данное заключение интерпретируется следующим образом. Если C получает сообщение $z \in Z$ и не хочет, чтобы этот факт был замечен субъектом U, то информационный поток от X к Y должен оставаться таким же, как и в случае, когда скрытой передачи по каналу $X \to Z$ просто нет.

В формировании скрытого канала участвуют нелегальные агенты серверов, коммутаторов, маршрутизаторов. Наиболее рационально контролировать появление скрытых каналов передачи информации на оборудовании с большими очередями: коммутаторах и маршрутизаторах, обязательным атрибутом которых является наличие стека пакетов, куда они отправляются и откуда могут извлекаться недостающие пакеты в случае их отсутствия в информационном потоке. Именно таким образом из текущего информационного потока и стека пакетов происходит формирование последовательности в скрытом канале (рис. 1).

Работа анализатора информационного потока на основе перцептрона [4] базируется на анализе ситуации по сформированным решающим правилам в пространстве заданных признаков. Особенность анализатора заключается в том, что требуется распознать комбинацию из существующих

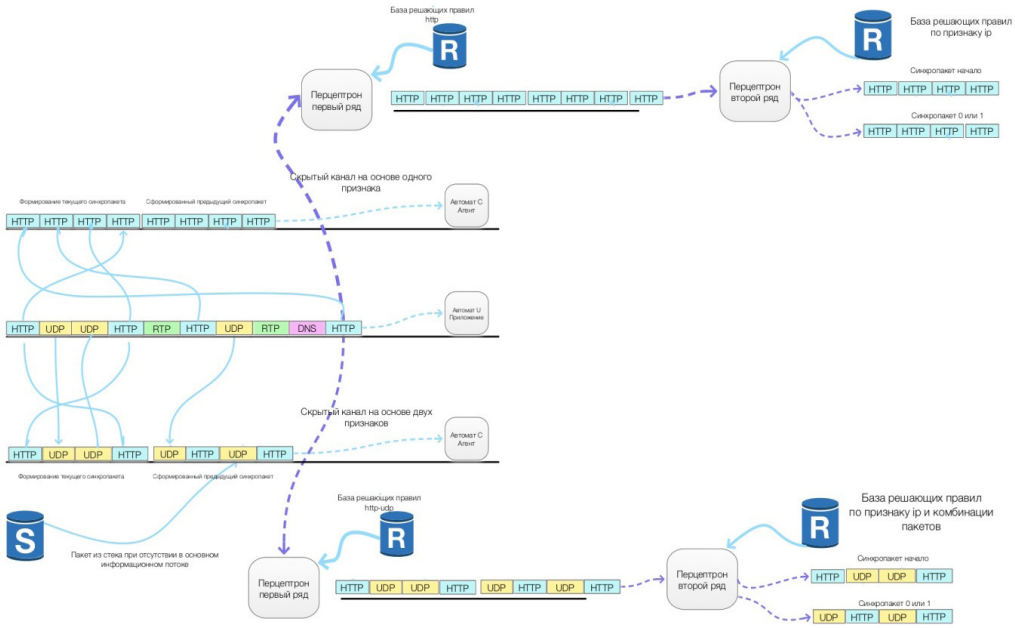

Рис. 2. Формирование информационного потока по признакам.

параметров. Для реализации скрытого канала возможно использование синхронизирующих последовательностей, обозначающих начало и конец передачи информационного потока (соответственно используются синхропакеты начала и окончания). Организатором любой передачи является тайный агент-посредник. Повторяемость некоторых комбинаций служит признаком, что существует скрытая передача.

Однорядный перцептрон в случае применения одного признака для передачи информации по скрытому каналу содержит возможные комбинации пакетов, упорядоченных по некоторому признаку, например по протоколу. В варианте применения двух признаков решающие функции будут содержать два признака и так далее (рис. 2).

Формирование скрытого канала при использовании двух признаков происходит следующим образом. В качестве признака может использоваться заранее заданная последовательность i_p-адресов для определённых протоколов (HTTP-UDP или любая другая пара, например HTTP-RTCP). Необходимо отметить, что создание скрытой последовательности может быть основано на порядке расположения пакетов. Следовательно, перцептрон должен содержать в базе решающих правил комбинации расположения пакетов, как в приведённом примере: UDP и HTTP.

Последовательность пакетов разделяется на потоки по протоколам, при этом в каждом потоке может формироваться скрытый канал. В случае последовательности из двух признаков синхропоток рождается из последовательностей пакетов двух протоколов.

На рис. 2 показаны два случая формирования скрытых каналов на пакетах одного протокола и пакетах двух протоколов. Во втором случае решающие правила должны учитывать то, что комбинация расстановки пакетов может быть использована и для формирования синхропакетов скрытых каналов.

Если попытаться сформировать на признаке X_1 последовательность из общего потока, то у субъекта U ничего не получится, так как пакеты перепутаны. Первый ряд перцептрона с двумя признаками будет иметь решающие функции:

$$R_j = \left(x_1^* - x_1\right)_j^2 + \left(x_2^* - x_2\right)_j^2,$$

где x^*_1 и x^*_2 – центральные значения признаков при обучении перцептрона (принимает числовое значение, соответствующее типу пакета DNS – 1, DHCP – 2, HTTP – 3 и т.д.).

Использование перцептрона позволяет создавать анализаторы скрытых каналов, работающих на нескольких признаках, при этом перцептрон должен быть многорядным.

Назначение второго ряда анализатора на базе перцептрона – анализ комбинаций пакетов протоколов, «несущих» определённые признаки, на основании которых должна осуществляться передача информации. Передача синхронизируется начальной и конечной комбинациями, составленными из пакетов протоколов в строго определённой последовательности (об этом заранее договариваются агенты передачи). Модель второго ряда перцептрона при использовании одного «несущего» протокола будет включать в себя (например, при наличии двух *ip*-адресов: ip_1 – логический ноль, ip_2 – логическая единица) возможные комбинации, указывающие на начало или окончание передачи информации. Например, при использовании комбинации из восьми пакетов модель содержит 256 вариантов реализации синхросигналов начала и окончания передачи.

С целью ускорения потока информации блок данных, заключённый между началом и окончанием процесса, передаётся логическими нулями и единицами, в качестве которых могут выступать, как указано ранее, *ip*-адреса. На выходе второго ряда перцептрона имеем следующую последовательность в моменты времени $[t_k]$:
$R^{нк}_j[t_k]$, $\{R^b_{i+1}[t_{k+1}],..., R^b_{i+1}[t_{k+j}],...,\}R^{нк}_m[t_{k+p}]$,
где $R^{нк}_j[t_k]$ – выход анализатора, обученный на синхропакет «начало передачи»;

$R^{нк}_m[t_{k+p}]$ – выход анализатора, обученный на синхропакет «окончание передачи»;

$R^b_{i+1}[t_{k+1}],..., R^b_{i+1}[t_{k+j}]$ – выходы анализатора, обученные на фиксацию логической единицы и нуля; формируются в блоке передаваемых данных.

Полученная последовательность представляет данные, идущие по скрытому каналу. При этом следует отметить, что их передача должна осуществляться в ограниченный временной интервал, чтобы не быть распознанной. И, кроме того, выявить вероятность существования скрытого канала без использования адекватных задаче анализаторов практически невозможно.

ЗАКЛЮЧЕНИЕ

Информация, полученная от анализатора скрытого канала, необходима, чтобы применить методы, позволяющие предотвратить возможность продолжения процесса с участием «нелегальных» агентов. Для реализации такой задачи предлагается исследовать методы перепутывания пакетов. Технически это требует значительных скоростей обработки информации, что предопределяет использование оптических интерфейсов, связывающих сервер перепутывания и буферное хранилище, куда временно помещаются пакеты. Причём алгоритм должен беспрепятственно пропускать определённые пакеты, которые нельзя перепутывать, иначе произойдёт нарушение работы сетевых устройств.

Таким образом, реализация анализатора на базе перцептрона для распознавания скрытых каналов позволяет существенно повысить эффективность борьбы с ними в корпоративном сегменте сетей.

ЛИТЕРАТУРА

1. Info Jett. [Электронный ресурс]: http://www.jetinfo.ru/jetinfo_arhiv/raspredelennye-ataki-na-raspredelennye-sistemy/o-kanalakh-skrytykh-potajnykh-pobochnykh-i-ne-tolko/2006. Доступ 10.01.2017.

2. Internet-technology. [Электронный ресурс]: http://www.internet-technologies.ru/articles/article_2826.html. Доступ 10.01.2017.

3. Грушко А. А. Скрытые каналы и безопасность информации в компьютерных системах // Дискретная математика.– 1998.– № 1.– С. 3–9.

4. Алексеев В. М. Система мониторинга информационной безопасности для высокоскоростного транспорта // Наука и техника транспорта.– 2016.– № 4.– С. 71–79.

5. Alcaraz C., Lopez J., Kim-Kwang, Choob R. Resilient interconnection in cyber-physical control systems: Computers & Security, Vol. 71, October 2017, pp. 2–14.

6. Osborn E., Simpson A. On small-scale IT user's system architectures and cyber security: A UK case study: Computers & Security, Vol. 70, September 2017, pp. 27–50.

7. Lei Ding, Jun Liu, Tao Qin, Haifei Li Internet traffic classification based on expanding vector of flow Computer Networks, October 2017, pp. 178–192.

8. Hongtao Sun, Chen Peng, Taicheng Yang, Hao Zhang, Wangli He Resilient control of networked control systems with stochastic denial of service attacks, Neurocomputing, October 2017, pp. 170–177.

Координаты автора: **Алексеев В. М.** – alekseevvm@ramber.ru.

Статья поступила в редакцию 14.07.2017, изменена 02.10.2017, принята к публикации 05.10.2017.