УДК 681.324

И.В. Рубан, А.А. Смирнов

Харьковский университет Воздушных Сил имени Ивана Кожедуба, Харьков

ВОЗМОЖНОСТИ ПО ИСПОЛЬЗОВАНИЮ ЗАГОЛОВКОВ ПАКЕТОВ СЕТЕВОГО УРОВНЯ БАЗОВОЙ МОДЕЛИ СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ OSI/ISO В КАЧЕСТВЕ СТЕГОКОНТЕЙНЕРА

В данной статье рассмотрены возможности по использованию заголовков пакетов сетевого уровня модели OSI/ISO в качестве стегоконтейнера. Описаны наиболее распространённые методы ip-стеганографии. Предложен и описан новый метод сетевой стеганографии – «метод опций». Обоснована целесообразность использования особенностей протоколов сетевого уровня модели OSI/ISO в качестве стегоконтейнера.

Ключевые слова: *сетевая стеганография, стеганографический канал, стегоконтейнер.*

Вступление

В последнее время приобрели популярность методы, когда скрытая информация передается через компьютерные сети с использованием особенностей работы протоколов передачи данных. Такие методы получили название "сетевая стеганография" [1]. Этот термин впервые ввел Кжиштоф Джипйорски (Krzysztof Szczypiorski) в 2003 году. Типичные методы сетевой стеганографии включают изменение свойств одного из сетевых протоколов. Кроме того, может использоваться взаимосвязь между двумя или более различными протоколами с целью более надежного сокрытия передачи секретного сообщения[1, 2].

Сетевая стеганография охватывает широкий спектр методов, в частности:

– WLAN стеганография основывается на методах, которые используются для передачи стеганограмм в беспроводных сетях (Wireless Local Area Networks). Практический пример WLAN стеганографии – система HICCUPS (Hidden Communication System for Corrupted Networks) [2]. В основе этих методов, лежат присущие беспроводным сетям недостатки, которые могут вызывать неисправимые искажения в энергетических характеристиках транслируемых сигналов. В результате могут появляться «неправильные» пакеты (пакеты, контрольная сумма которых не соответствует заявленной в заголовке сегмента транспортного уровня). Для реализации такого рода методов, необходимо располагать актуальной статистикой сетевой активности в пользуемой среде, чтобы не вызывать аномальной сетевой активности.

– LACK (Lost Audio Packets Steganography) стеганография – скрытие сообщений во время разговоров с использованием IP-телефонии. Например: использование пакетов, которые задерживаются, или намеренно повреждаются и игнорируются приемником (прикладной программой), но не стеганографическим приложением [3].

В связи с тем, что самым распространённым в интернете является стек протоколов TCP/IP, то целесообразным является организация стеганографических каналов (СГК) именно на его базе.

Основная часть

Под сетевой стеганографией на сетевом уровне модели OSI (далее ip – стеганография), понимается группа методов сетевой стеганографии, в которых стегоконтейнером могут являться неиспользуемые места в заголовках и полях данных ip – дейтаграмм.

Метод DF. Одним из примеров использования полей заголовков является метод, основанный на модификации полей «identification» и «fragment-offset» при установленном флаге «DF» (don'tfragment – не фрагментировать). Если установлен флаг DF, модуль IP не станет фрагментировать дейтаграмму. Вместо этого дейтаграмма отбрасывается и по протоколу ICMP генерируется сообщение об ошибке – «необходима фрагментация, но установлен флаг запрета фрагментации», которое посылается отправителю пакета. Если IP-дейтаграмма была фрагментирована, то каждый фрагмент становится отдельным пакетом со своим собственным IP-заголовком. Такие пакеты маршрутизируются независимо, и, как следствие, фрагменты дейтаграммы могут приходить в точку назначения с нарушением их очередности. Однако в IP-заголовках фрагментов содержится вся необходимая информации для их правильной сборки в пункте назначения.

Фрагментация в IP выполняется независимо от транспортного уровня модели OSI. Не смотря на такую «прозрачность», фрагментация может привести к нежелательным последствиям, которые сказываются на уровнях выше IP. Дело в том, что из-за потери одного фрагмента потребуется передать повторно всю дейтаграмму, а поскольку в самом протоколе IP не предусмотрены таймаут и повторная передача, то эти функции должны быть возложены на более высокие уровни. Протокол TCP осуществляет повторную передачу по таймауту, а UDP — нет.

Если окажется, что потерян некоторый фрагмент сегмента TCP, то по таймауту будет повторена передача всего сегмента TCP. Повторная передача отдельного фрагмента ip-дейтаграммы невозможна в принципе. Действительно, если фрагментацию произвел не хост источника дейтаграммы, а один из промежуточных маршрутизаторов, то источник не может знать, каким именно образом было выполнено разбиение на фрагменты. Уже по одной этой причине желательно принимать меры для предотвращения фрагментации.

Фрагментация пакетов в IP является штатной ситуацией, поэтому использование ранее указанных полей заголовков ip-пакетов в качестве стегоконтейнера является вполне целесообразным методом для организации скрытого канала связи. Важно понимать, что при правильном выборе размера пакета возможно добиться выполнения условия 1.

$$L \le PMTU, \qquad (1)$$

где L – длина пакета; MTU – maximum transmission unit (максимальный размер полезного блока данных одного пакета); PMTU – MTU трассы от источника до конечного адресата пакета.

$$PMTU = \min MTU_i, \qquad (2)$$

где $\min MTU_i$ – минимальное значение MTU среди интерфейсов маршрута, по которому пройдёт пакет.

При выполнении условия (1) необходимость фрагментации пакетов на интерфейсах маршрута отсутствует. Это означает, что поля «identification», «flags», «fragmentoffset» обрабатываться промежуточными маршрутизаторами не будут. В таком случае, при использовании этих полей в качестве стегоконтейнера, информация встроенная в него будет передана без изменений. Ёмкость такого стегоконтейнера может составлять до 32 бит.

Метод опций. На современном этапе «метод DF», является единственным описанным методом сетевой стеганографии, применяемый на сетевом уровне модели OSI. Но следует отметить, что могут существовать и другие поля заголовка ip – дейтаграммы, которые возможно использовать для организации скрытых каналов обмена информацией в информационно-телекоммуникационных сетях (ИТКС). К таким полям относятся опции IPv4, размер которых может достигать 40 байт. К подходящим опциям, необходимо отнести следующие: «запись маршрута», «временной штамп», «маршрутизация от источника». Общей чертой перечисленных опций является выделение достаточного (до 40 октетов) места в заголовке ip – пакета для их реализации.

Поле опций является необязательным, а их поддержка должна реализоваться во всех модулях IP (на хостах и шлюзах). Использование опций определяется для отдельной дейтаграммы, а не для реализации модуля [4]. Теоретическая основа «метода опций» описана на примере опций «запись маршрута» и «временной штамп».

При использовании в качестве стегоконтейнера поля для записи промежуточных узловых устройств (опция «запись маршрута» или RecordRoute (RR)), возможно достигнуть размера контейнера до 37 байт. Опция RR предназначена для записи в заголовок дейтаграммы ip-адресов выходных интерфейсов маршрутизаторов, маршрутизируемых данную дейтаграмму. При использовании данной опции представляется возможным записать до 9 ip-адресов. Это связано с тем, что в ip-дейтаграмме отведено до 40 байт для описания опций, 3 из которых – заголовок опции RR [4] (рис. 1).

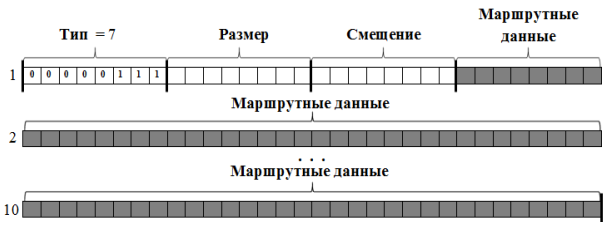

Рис. 1. Вид поля опции «Запись маршрута»

Опция начинается с поля типа опции (7), за которым следует поле длины, учитывающее Type=7 полный размер опции (тип, размер, смещение, маршрутные данные). Третий октет содержит указатель

на октет, с которого начинается следующая область записи маршрута. Смещение отсчитывается от начала опции, поэтому значение указателя не может быть меньше 4. Отправляющий дейтаграмму хост должен обеспечить достаточное пространство (размер опции) для записи адресов на пути к получателю. В исходной дейтаграмме поля адресов должны иметь нулевые значения.

Когда модуль IP маршрутизирует дейтаграмму, он проверяет в ней наличие маршрутной записи. При наличии такой записи модуль помещает в нее свой адрес, известный в той среде, куда пересылается дейтаграмма, начиная со смещения, которое задано указателем, и увеличивая значение указателя на 4.

Если поле маршрутных данных уже заполнено (значение указателя превышает размер опции), дейтаграмма пересылается без дальнейшей записи маршрута. Если оставшегося пространства для записи маршрутных данных недостаточно для включения адреса, дейтаграмма рассматривается как ошибочная и отбрасывается. В таких случаях отправителю дейтаграммы может быть передано сообщение ICMP об ошибке в параметрах [5].

Следовательно, если на передающей стороне записать скрываемую информацию в поля, предназначенные для записи ip-адресов выходных интерфейсов, а для полей «смещение» и «размер» будет выполнено следующее условие, то эта дейтаграмма будет доставлена без изменений.

$$L_p > L_l, \qquad (3)$$

где L_p – октет маршрутных данных, начиная с которого будет обрабатываться следующий параметр, применяемый в опорной опции; L_l – значение размера опции (в октетах), с учетом полей типа и размера опции, а также октета указателя и собственно опции.

Для реализации описанного способа, необходимо иметь предустановленное программное обеспечение на стороне отправителя и получателя скрываемой информации. Ситуация при которой текущий маршрутизатор не сможет записать требуемую в опции информацию, является штатной для протокола IP [4].

Подобный подход возможно применить и к остальным опциям IP – SR (sourceroute – маршрутизация от источника), TS (timestamp – временной штамп), при выполнении условия (3). Для записи, необходимых данных для опций «маршрутизация от источника» и «запись маршрута» отводится 37 байт, а для опции «временной штамп» – 36 байт в каждой ip – дейтаграмме, что является ёмкостью такого стегоконтейнера.

Меньшая ёмкость стегоконтейнера, при использовании в качестве опорной, опции «временной штамп», обусловлена тем, что в четвёртом октете поля опции хранится информация, необходимая для выполнения назначения опции [4] (рис. 2).

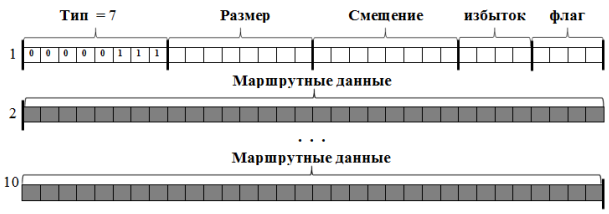

Рис. 2. Вид поля опции «временной штамп»

Поле «избыток» показывает количество маршрутизаторов, которые не смогли выполнить требуемую операцию. Поле «флаг», в зависимости от принимаемого значения, определяет:

0 – промежуточные маршрутизаторы должны записывать только временные метки, сохраняемые в последовательности 32-битовых слов;

1 – перед каждой меткой помещается IP-адрес регистрирующего метку модуля;

3 – поля адресов IP указываются заранее и модуль IP помещает временную метку только в том случае, когда адрес этого модуля указан следующим в списке адресов опции.

Выводы

Использование методов «ip стеганографии» не позволяет достигнуть приемлемой стойкости стегоканала за счёт того, что скрываемая информация передаётся в явном виде, а малая пропускная способность таких каналов, обусловлена редким применением описанных особенностей протокола IP.

Использование флага «DF» в заголовках дейтаграмм предлагается избегать за счёт вычисления подходящего PMTU. Если флаг всё же установлен, то опытные сетевые администраторы предпочитают снимать его с IP пакетов. Это связано с задержками, которые вносятся в связи с необходимостью обработки пакетов: отправка соответствующих ICMP сообщений об ошибке, невозможность обеспечить заявленный провайдером уровень обслуживания клиентов. Если флаг «DF» будет снят, то пакеты станет возможно фрагментировать и проблема исчезнет и провайдер обеспечит себе приемлемые потери ресурсов, направленные на фрагментацию. Например, в маршрутизаторах cisco можно это сделать штатными средствами.

Применение опций в ip-дейтаграмме является крайне редким, а в некоторых операционных системах отключено по умолчанию. Это связано с тем, что большинство дейтаграмм не содержат опций, то есть имеют фиксированную длину заголовка (20 байт), их обработка максимально оптимизирована именно для этого случая.

Появление опции прерывает этот скоростной процесс и вызывает стандартный универсальный модуль IP, способный обработать любые стандартные опции, но за счет существенной потери в быстродействии.

Ещё одним сдерживающим фактором, перед использованием ip опций, являются дополнительные угрозы информационной безопасности ИТКС, вносимые за счёт них. Основная опция, которая может быть использована нарушителем, – опция «маршрутизация от источника». Она позволяет отправителю пакета однозначно определить маршрут к адресату вместо того, чтобы разрешить каждому маршрутизатору по пути следования пакета использовать свои таблицы для решения задачи маршрутизации. Нарушитель может задействовать данную опцию, чтобы попытаться обойти защиту шлюза и направить пакеты в защищенную зону корпоративной компьютерной сети. Атаки, основанные на опциях протокола IP, проистекают из стандарта, а не его реализации. Возникновение новых атак такого рода маловероятно, поскольку весьма распространенной политикой является полное игнорирование IP-опций.

Список литературы

1. WojciechMazurczyk, Krzysztof Szczypiorski, Steganography of VoIP Streams, Warsaw University of Technology, Faculty of Electronics and Information Technology, Institute of Telecommunications, 15/19 Nowowiejska Str., 00-665 Warsaw, Poland.

2. Krzysztof Szczypiorski, HICCUPS: Hidden Communication System for Corrupted Networks, Warsaw University of Technology, Institute of Telecommunications, ul. Nowowiejska 15/19, 00-665 Warsaw, Poland.

3. TelecommunSyst. – DOI 10.1007/s11235-009-9245-y. LACK—a VoIP steganographic method. WojciechMazurczyk · JózefLubacz.

4. "Internet protocol – DARPA Internet Program Protocol Specification" RFC-791 USC/Information Sciences Institute, September 1981.

Поступила в редколлегию 27.08.2014

Рецензент: д-р физ.-мат. наук, проф. С.В. Смеляков, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

МОЖЛИВОСТІ ПО ВИКОРИСТАННЮ ЗАГОЛОВКІВ ПАКЕТІВ МЕРЕЖЕВОГО РІВНЯ БАЗОВОЇ МОДЕЛІ МЕРЕЖЕВОЇ ВЗАЄМОДІЇ OSI/ISO ЯК СТЕГОКОНТЕЙНЕРА

І.В. Рубан, А.О. Смирнов

У даній статті розглянуті можливості по використанню заголовків пакетів мережевого рівня моделі OSI/ISO як стегоконтейнера. Описані найбільш поширені методи ip – стеганографії. Запропонований і описаний новий метод мережевої стеганографії – «метод опцій». Обґрунтована доцільність використання особливостей протоколів мережевого рівня моделіOSI/ISOв якості стегоконтейнера.

Ключові слова: *мережева стеганографія, стеганографічний канал, стегоконтейнер.*

POSSIBILITIES TO USE NETWORK LAYER PACKET HEADERS OF INTERCONNECTION BASIC REFERENCE MODEL OSI/ISO AS STEGANOGRAPHY CONTAINER

I.V. Ruban, A.A. Smirnov

This article examines the possibilities of using the network layer packet headers of model OSI/ISO as steganography container. Describes the most common methods of ip - steganography. Proposed and describe a new method to network steganography - "method of options." The expediency of using the features of network layer model OSI/ISO as steganography container.

Keywords: *network steganography, steganography channel, steganography container.*