УДК 681.324

И.В. Рубан, А.А. Смирнов

Харьковский университет Воздушных Сил имени Ивана Кожедуба, Харьков

МЕТОД СТЕГАНОГРАФИЧЕСКОЙ ПЕРЕДАЧИ ДАННЫХ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ НА ОСНОВЕ ГЕНЕРАЦИИ ISN TCP-СОЕДИНЕНИЙ

В данной статье предложен новый метод сетевой стеганографии, в основе которого лежит использование особенностей протокола TCP в качестве стегоконтейнера. Описан алгоритм работы метода и приведён пример передачи четырёх байтов данных.

Ключевые слова:*сетевая стеганография, стего, начальный номер последовательности.*

Введение

В условиях современных информационных войн, немаловажной является задача скрытной и надёжной передачи ценной информации. Это обуславливается как необходимостью получения конкурентоспособного преимущества над противником, так и для обеспечения собственной информационной безопасности [1]. В этом направлении хорошо зарекомендовали себя многие подходы по организации защищённых каналов связи, в основе которых лежат криптографические методы защиты информации. Но с ростом количества способов доступа к информации, постоянно растёт и количество атак на информационные ресурсы.

В последнее время приобрели популярность методы, когда скрываемая информация передается через информационно-телекоммуникационные сети (ИТКС) с использованием особенностей протоколов базовой модели сетевого взаимодействия OSI (Open System Inter connection). Такие методы получили название "сетевая стеганография".

При современных темпах развития инфраструктуры глобальных ИТКС [2], техническая возможность наличия сетевого стеганографического канала (СГК) имеется в подавляющем большинстве соединений.Известно, что протокол TCPявляется самым распространённым в сети интернет. В основе этого лежит открытость его описания в [3], выполненная в виде рекомендаций и не обязывающая к однообразной реализации в разных операционных системах (ОС), а также надёжность протокола. Исходя из описанных преимуществ протокола TCP, целесообразно использовать его свойства для разработки методов сетевой стеганографии.

Ещё одним стимулом для использования стеганографических каналов (СГК) для передачи важной информации в ИТКС, является высокая ресурсоёмкость стегоанализа таких стегоконтейнеров (СК)[4 – 6].

Средняя расчётная задержка сетевого пакета, во время его обработки маршрутизатором, составляет от 0,64 мкс до 3,2 мс, в зависимости от скорости потока на выходном широкополосном интерфейсе [7] и степени его загруженности.Время оценки возможности наличия сетевого СГК зависит от наличной базы шаблонов поведения соединения при использовании того или иного метода и эффективности системы стегоанализа. Предположительно, для выявления таких стеганографических каналов, необходима выборка перехваченных соединений, в общем, и отдельных сетевых пакетов в частности, а также статистический анализ полученных данных. Таким образом, стегоанализ всех соединений в режиме реального времени, либо с задержками, соизмеримыми с временными характеристиками каналов связи в ИТКС, нецелесообразен для выявления таких СГК.

Основная часть

В основу предлагаемого метода положен механизм генерации начального номера последовательности (ISN - InitialSequenceNumber*)* каждого TCP-соединения и корреляции байтов передаваемых (открытых) данных и стего.

Согласно [3, с. 7, 11], генерация номера основана на текущем (возможно, фиктивном) 32-битовом значении времени, в котором младший бит инкрементируется приблизительно каждые 4 микросекунды. На самом деле, значение ISN вычисляется в разных операционных системах по-разному [7]. Но в общем случае это значение является, своего рода, временным штампом и соответствует значению функции, аргументом которой является текущее значение машинного времени (аппаратных часов конкретной операционной системы), то есть $ISN = F(t_м)$.

Таким образом, значение ISN, для стороннего наблюдателя, при первом наблюдении, является случайным. При анализе достаточной выборки значений F(t), становится возможным вычислить закономерность (аппроксимировать функцию).

В заголовке TCP-фрагмента, значение ISN записывается в поле длинной 32 бита. Данные, переносимые tcp-фрагментом, представляются в виде последо-

вательности байтов, которые. Номер первого передаваемого байта данных соответствует (ISN+1).

На рис. 1 изображён Ethernet-фрейм, перехваченный программой-сниффером. Интервал с нулевого по 54-тый байт включительно занимают заголовки канального, сетевого и транспортного уровней модели OSI. Поле данных протокола транспортного уровня (в данном случае TCP) выделено сплошным серым оттенком и начинается с 55-го байта, если за начало отсчёта брать первый байт фрейма Ethernet. Данные для прикладного приложения (текст в формате txt) передаются в кодировке CP1251. Началу, непосредственно, текста (выделен чёрной линией на рис. 2) соответствует 123 байт от начала фрейма. Ему предшествуют 68 байт служебных данных для прикладного приложения.

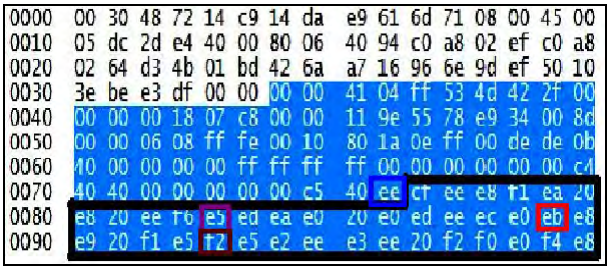

Рис. 1. Ethernet-фрейм

Для скрытной передачи, например, слова «лето», используя в качестве стегоконтейнера поля «номер последовательности» и «данные» tcp-фрагмента необходимо:

1. Пронумеровать байты «поля данных» начиная с нулевого значения;

2. Поставить в соответствие каждую букву слова «лето» с номером байта в поле данных;

3. Согласно следованию букв в секретном слове, заполнить соответствующими значениями номеров 32-разрядное слово;

4. Записать значение полученного слова в поле «номер последовательности»;

5. Предать полученный фрагмент получателю;

6. На приёмной стороне извлечь стего в обратной последовательности.

На рис. 2 чёрным цветом выделен фрагмент текстовых данных, в соответствие порядковым номерам байтов которого, поставлены буквы слова (стего) «лето»: «л» – 87_{10} – 57_{16} – 0001 0100$_2$, «е» – 77_{10} – $4D_{16}$ – 0101 0111$_2$, «т» – 93_{10} – $5D_{16}$ – 0101 1101$_2$, «о» – 67_{10} – 43_{16} – 0100 0011$_2$.

В соответствии с логикой работы описываемого метода, далее необходимо сгенерировать нужный номер ISN. В стеке протоколов TCP/IP заполнение заголовков и полей данных производится в порядке «от старшего к младшему». Нужный начальный номер последовательности имеет вид:

$00010100010101110101110101000011_{16} = 41269827_{10}$.

Отсюда следует, что при объявлении такого ISN, первый байт переносимых TCP данных будет иметь номер $(341269827+1)_{10}$.

Анализируемая структурная схема процесса передачи стего по предлагаемому методу изображена на рис. 2, по которой можно сделать вывод о том, что исследование такого СГК, сводится к исследованию «чёрного ящика», так как внешне такое соединение не отличается от любого другого..

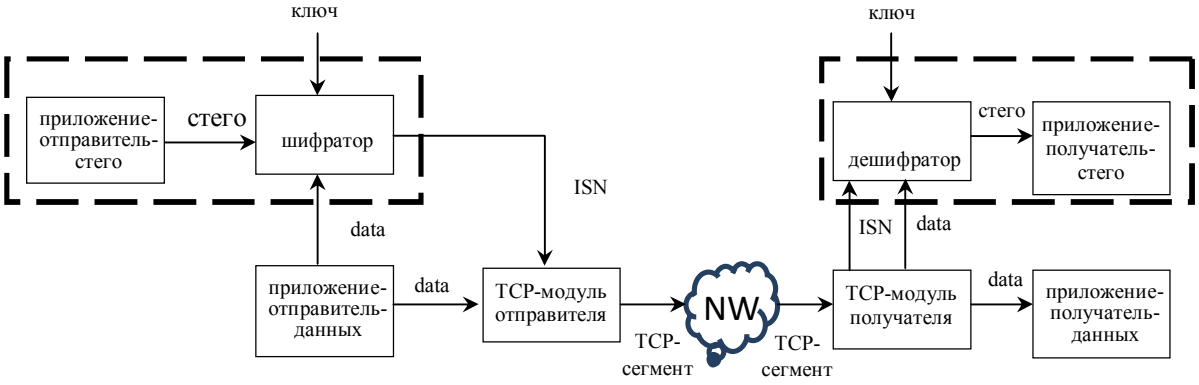

Рис. 2. Структурная схема процесса передачи стего по методу ISN

Выводы

Предлагаемый стеганографический метод, позволяет передавать 4 байта за одно tcp-соединение. Пропускную способность можно повысить, за счёт использования корреляции больших частей стего с фрагментами байтов соответствующей длины.

Список литературы

1. Присяжнюк М. Аналіз засобів ведення інформаційної боротьби з використанням інформаційних технологій, форм і способів їх застосування [Електронний ресурс] / М. Присяжнюк, Я. Жарков. – Центр воєнної політики та політики безпеки. – Режим доступу: http://defpol.org.ua.

2. Тенденции развития компьютерных сетей и интернета Аналіз засобів ведення інформаційної боротьби з використанням інформаційних технологій, форм і способів їх застосування [Електронний ресурс]. – Режим доступу: http://arccn.ru

3. "Internetprotocol – DARPA Internet Program Protocol Specification" RFC-793. TCP. USC/Information Sciences Institute, September 1981.

4. Mazurczyk W. Steganography of VoIP Streams / W. Mazurczyk, K. Szczypiorski. – Warsaw University of Tech-

nology, Faculty of Electronics and Information Technology, Institute of Telecommunications.

5. Szczypiorski K. HICCUPS: Hidden Communication System for Corrupted Networks / K. Szczypiorski – Warsaw University of Technology, Institute of Telecommunications.

6. Орлов В.В. Активная стеганография в сетях TCP/IP / В.В. Орлов, А. П. Алексеев // Инфокоммуникационные технологии. – 2009. – № 2. - С. 73-78.

7. Михайлов С.К. Расчёт вариации задержки (IPDV) для телефонного соединения / С.К. Михайлов, Т.П. Сергеева // T-Comm - Телекоммуникации и Транспорт. – 2013. - № 7. – С. 87-89.

Поступила в редколлегию 30.04.2015

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

МЕТОД СТЕГАНОГРАФІЧНОЇ ПЕРЕДАЧІ ДАНИХ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ НА ОСНОВІ ГЕНЕРАЦІЇ ISN TCP-З'ЄДНАНЬ

І. В. Рубан, А.О. Смірнов

У даній статті запропоновано новий метод мережевої стеганографії, в основі якого лежить використання особливостей протоколу TCP як стегоконтейнера. Описано алгоритм роботи методу і наведено приклад передачі чотирьох байтів даних.

Ключові слова: *мережева стеганографія, стего, початковий номер послідовності.*

METHOD OF STEGANOGRAPHIC DATA TRANSFER IN INFORMATION AND TELECOMMUNICATIONS NETWORKS BASED ON GENERATION OF ISN IN TCP-CONNECTIONS

I.V. Ruban, A.A. Smirnov

In this article proposed a new method of network steganography, which is based on the use of the features of TCP as steganographic container. Described an algorithm of the method operation and shows an example the transfer of four bytes of data.

Keywords: *network steganography, stego, initial sequence number.*