дукции – научных разработок и результатов инновационной деятельности.

Заключение

На наш взгляд, только формирование виртуальных лабораторий позволит НИИ сориентироваться в современных рыночных условиях, отягощенных глобальным финансовым кризисом, а также уменьшить зависимость российской экономики от экспорта энергоносителей за счет вывода отечественных инновационных разработок на принципиально новый уровень качества и конкурентоспособности.

Литература

1. Вютрих Х.А., Филипп А.Ф. Виртуализация как возможный путь развития управления // Проблемы теории и практики управления. №5, 1999. – С.194-100.
2. Димов Э.М., Маслов О.Н., Скворцов А.Б. Новые информационные технологии: подготовка кадров и обучение персонала. Ч. 1. Реинжиниринг и управление бизнес-процессами в инфокоммуникациях. М.: ИРИАС, 2006. – 386 с.
3. Катаев А.В. Виртуальные предприятия – новая ступень в организации НИОКР // Стратегические аспекты управления НИОКР в условиях глобальной конкуренции: Отчет по НИР № 01.2.00100692. Таганрог: ТРТУ, 2001. – С. 204-211
4. Медынский В.Г., Ильдеменов С.В. Реинжиниринг инновационного предпринимательства. М.: ЮНИТИ, 1999 – 414 с.
5. Стратегия Российской Федерации в области развития науки и инноваций на период до 2010 года [Электронный ресурс]. Режим доступа: http://www.fips.ru/ruptoru/str_rf.htm, свободный. – Загл. с экрана.

УДК 681.327

АКТИВНАЯ СТЕГАНОГРАФИЯ В СЕТЯХ TCP/IP

Орлов В.В., Алексеев А.П.

В статье рассматриваются методы организации стеганографической системы в сети TCP/IP.

Постановка задачи

Защитить информацию при передаче по открытому каналу можно с помощью криптографии (скрыв смысл сообщения), либо с помощью стеганографии (скрыв факт передачи сообщения). Часто оба способа используются совместно. Сети TCP/IP получили широкое распространение, поэтому разработка и исследование новых методов сокрытия данных при передаче по сетям TCP/IP является актуальной задачей.

Стеганографические системы, создающие в сети собственный трафик, будем называть активными. Известны два метода активной скрытой передачи информации в IP-сетях [1].

Первый метод предполагает нестандартное использование опции Internet Timestamp поля «Опции» заголовка IP-дейтаграммы, а также поля «Идентификатор». Второй метод предполагает использование ICMP-пакетов для передачи секретного текста. Оба подхода имеют недостатки.

Первый недостаток заключается в том, что поля заголовка IP-дейтаграммы используются не для целей, определенных протоколом RFC 791 [2]. Это можно рассматривать как демаскирующий признак.

Второй недостаток состоит в том, что вложение и извлечение информации осуществляется без использования ключа. Криптографическая стойкость таких вложений недостаточна.

Разработка метода внедрения секретного текста

Предлагаемый метод скрытой передачи информации заключается в изменении длины TCP-сегмента таким образом, чтобы значение длины данных (число передаваемых символов), переносимых TCP-сегментом, содержало в себе информацию о секретном тексте. В дальнейшем будем называть число символов открытого текста, помещенного в поле данных сегмента, длиной открытого текста (ДОТ).

Выбор TCP-сегментов в качестве контейнеров позволил добиться того, что ни в заголовке TCP-сегмента, ни в заголовке IP-дейтаграммы биты секретного текста не содержатся в явном виде (рис. 1 и 2). Вместе с тем, размер данных, передаваемых в TCP-сегменте, можно вычислить по значениям полей «Общая длина» и ДЗ («Длина заголовка») IP-дейтаграммы, и поля «Смещение данных заголовка» TCP-сегмента.

Отметим важные для реализации метода скрытой передачи информации поля IP-заголовка.

Рис 1. Формат заголовка IP-дейтаграммы по спецификации RFC 791

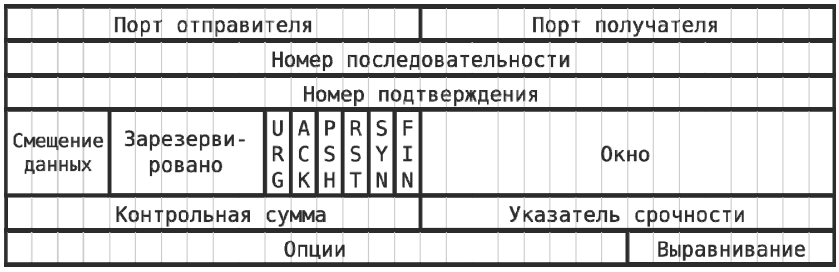

Рис. 2. Формат заголовка TCP-сегмента спецификации RFC 793

Длина Internet-заголовка (Internet Header Length) измеряется в четырехоктетных словах (октет равен восьми битам). Длина заголовка IP-дейтаграммы не может быть меньше 5 четырехоктетных слов.

Общая длина (Total Length) – это длина, измеренная в октетах, включая заголовок Internet и поле данных. Размер поля составляет 16 бит, что позволяет формировать дейтаграмму длиной до 65535 октетов. Однако в большинстве сетей такие большие дейтаграммы не используются. Спецификация RFC 791 устанавливает минимальный размер дейтаграммы, равный 576 октетам. Такая дейтаграмма должна быть принята любым хостом.

Рассмотрим формат заголовка TCP-сегмента (см. рис. 2) и выделим некоторые важные для данного случая поля.

Смещение данных (Data Offset) – длина TCP-заголовка в четырехоктетных словах; PSH – функция проталкивания (PUSH).

Проиллюстрируем предлагаемый метод сокрытия информации с помощью примера.

Предположим, что между сторонами (корреспондентами) уже установлено TCP-соединение. В целях упрощения будем считать, что передаваемые TCP-сегменты и IP-дейтаграммы не содержат полей Options и Padding. Коды символов секретного текста кодируются значением длины данных, передаваемых очередным TCP-сегментом.

Рассмотрим пример скрытой передачи символа «Z», имеющий десятичный код 90 по таблице ASCII.

На передающей стороне формируется TCP-сегмент, который должен перенести пользовательские (открытые, не содержащие секретных сведений) данные. Длина передаваемых открытых данных должна совпадать с кодом скрытно передаваемого символа. Для передачи формируется блок открытых данных длиной 90 октет. К пользовательским данным добавляется TCP-заголовок длиной 20 октет (5 слов по 4 байта). Полученный TCP-сегмент, общая длина которого составляет 110 байт, передается программе IP-протокола, которая, добавив 20-ти байтовый IP-заголовок, формирует IP-дейтаграмму. Общая длина IP-дейтаграммы записывается в поле общей длины (в данном случае длина составляет 130 байт). Сформированная IP-дейтаграмма передается на канальный уровень модели OSI и затем транслируется по открытому каналу.

На приемной стороне для извлечения скрытого символа требуется вычислить длину данных, переносимых TCP-сегментом. Для извлечения информации из общей длины IP-дейтаграммы (поле Total Length) вычитается длина IP-заголовка $130 - 5 \times 4 = 110$ байт. Из полученного значения общей длины TCP-сегмента вычитается значение смещения данных (поле Data Offset) $110 - 5 \times 4 = 90$ байт. Полученное значение длины открытого текста трактуется как код принятого символа секретного текста, то есть на приеме будет зафиксирован символ «Z».

Реальный IP-заголовок принятой из сети дейтаграммы показан на рис. 3 (поля заголовка заполнены двоичными данными в соответствии с рис. 1).

Здесь поле общей длины содержит двоичное число 0000000010001110, что эквивалентно десятичному числу 142. Поле длины заголовка

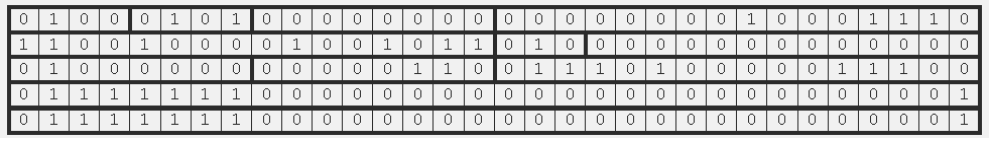

Рис. 3. Пример заголовка реальной IP-дейтаграммы

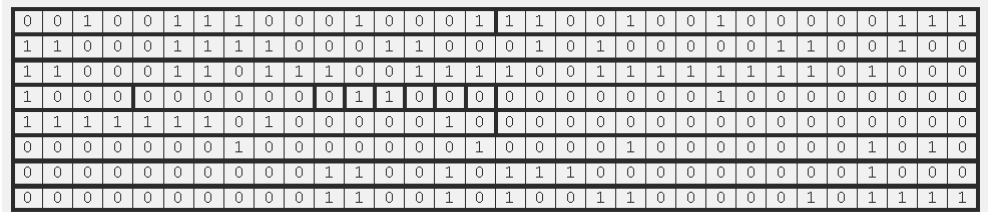

Рис. 4. Пример заголовка реального TCP-сегмента

Internet содержит двоичное число 0101, то есть 5 в десятичной форме. Это означает, что длина IP-заголовка равна пяти четырехбайтным словам (20 байтам). Таким образом, длина TCP-сегмента равна 142 – 20 = 122 байта.

На рис. 3 упомянутые поля выделены серым цветом. На рис. 4 показан дамп заголовка TCP-сегмента.

Здесь в поле смещения данных (Data Offset) записано двоичное число 1000, равное 8 в десятичной системе счисления (на рисунке поле выделено серым цветом). Это означает, что размер заголовка TCP-сегмента равен восьми четырехбайтным словам, то есть 8 × 4 = 32 байтам.

Таким образом, размер данных, содержащихся в TCP-сегменте, составляет 122 – 32 = 90 байт. Согласно кодовой таблице ASCII, десятичный код 90 соответствует символу «Z».

Так как два соседних символа секретного текста передаются в разных TCP-сегментах и IP-дейтаграммах, то можно говорить о сокрытии информации с пространственным распределением секретного текста по контейнерам [4].

Учитывая требования спецификации протокола TCP [3], предложенный метод внедрения секретной информации в TCP-сегмент технически может быть реализован путем управления флагом проталкивания (PUSH). Действительно, в соответствии с RFC 793, данные пользователя, подготовленные для передачи по сети, могут накапливаться в буфере. Отправка данных адресату в этом случае будет производиться при полном заполнении буфера передачи. При этом передача строго заданного объема информации будет невозможна. Однако если в заголовке TCP-сегмента выставлен флаг проталкивания, то программа TCP должна немедленно отправить все имеющиеся в буфере данные. Аналогично на приеме программа-обработчик TCP, встретив флаг проталкивания, должна передать принятые в буфер приема данные программам протоколов верхних уровней.

Для подтверждения возможности реализации описанного метода скрытой передачи информации был проведен эксперимент. На передающей стороне использовался персональный компьютер со следующими характеристиками: процессор E6850 Intel Core2 Duo с тактовой частотой 3 ГГц, и объемом ОЗУ 4 Гбайт. Контроллер жестких дисков Intel 82801 GB/GR/GH (ICH7 Family) Serial ATA Storage Device, жесткий диск WDC WD2500AAJS-00-VTA0. Была использована сетевая плата Realtek RTL8168/8111 PCI-E Gigabit Ethernet NIC (MAC: 00:19:DB:E6:08:8D), ЭВМ работала под управлением операционной системы ОС Microsoft Windows 2003 Service Pack 2. Конфигурация персонального компьютера на приемной стороне была такова: Intel Celeron с тактовой частотой 2,8 ГГц, объем ОЗУ 512 Мбайт, сетевая плата Intel PRO/100 VE (MAC: 00:16:76:1E:EE:89), контроллер жестких дисков Intel 82801EB Ultra ATA Storage Controllers, жесткий диск Samsung SP0401N/P, ОС Microsoft Windows XP Service Pack 2. Взаимодействие отправителя и получателя было организовано через локальную сеть FastEthernet.

Программа отправителя формировала TCP-сегменты, причем длина открытых данных выбиралась равной коду очередного символа секретного текста по таблице CP-1251. Чтобы предотвратить кэширование данных нескольких TCP-сегментов, передача сегментов в сеть осуществлялась с паузой 1 мс.

Протокол обмена информацией на стороне отправителя представлен в таблице 1. Протокол об-

Таблица 1. Протокол обмена информацией в ходе эксперимента на стороне отправителя

№ п/п	Символ секретного текста	Длина блока открытых данных, октет	Длина отправляемого TCP-сегмента, октет	Длина отправляемой IP-дейтаграммы, октет
1	С	209	229	249
2	Т	210	231	251
3	Е	197	217	237
4	Г	195	215	235
5	О	206	226	246

Таблица 2. Протокол обмена информацией в ходе эксперимента на стороне получателя

№ п/п	Длина принятой IP-дейтаграммы, октет	Длина принятого TCP-сегмента, октет	Длина блока открытых данных, октет	Символ секретного текста
1	249	229	209	С
2	251	231	210	Т
3	237	217	197	Е
4	235	215	195	Г
5	246	226	206	О

мена информацией на стороне получателя представлен в таблице 2.

Разработка метода скрытой связи с использованием ключа

Рассмотрим метод организации скрытой секретной связи с использованием ключа.

TCP-сегменты, переносящие данные, в значении длины которых закодированы биты секретного текста, условимся называть информационными. Все остальные сегменты, не несущие секретной информации, будем называть маскирующими.

Основная идея предлагаемого метода скрытой передачи информации заключается в том, что секретная двоичная информация скрывается в отдельных битах двоичного числа, равного длине открытого текста.

В отличие от сокрытия информации во всем числе ДОТ, в данном случае используются лишь некоторые отдельные биты ДОТ.

Передаваемая секретная информация представляется в двоичном виде. Поток имеющихся двоичных чисел делится на блоки, состоящие из нескольких бит. Каждый блок двоичных чисел скрытно помещается в информационный сегмент. Сокрытие каждого блока секретной информации осуществляется в значении ДОТ данного сегмента.

На рис. 5 показана общая схема размещения блоков секретного текста в TCP-сегментах. На рисунке использованы следующие обозначения: S – общее число блоков секретного текста; i – номер блока секретного текста (принимает значения от 1 до S); b_i – длина i-го блока секретного текста, принимает значения от 0 до $t = \log_2 d$ бит; d – максимальная длина сегмента для используемой технологии передачи (выражена в числе октетов); B – общая длина секретного текста (1); j – номер очередного TCP-сегмента (принимает значения от 1 до S). Если длина очередного блока секретного текста $b_i > 0$, то соответствующий TCP-сегмент, в котором этот блок скрывается, будет информационным. При $b_i = 0$ соответствующий TCP-сегмент является маскирующим:

$$B = \sum_{i=1}^{S} b_i \ . \qquad (1)$$

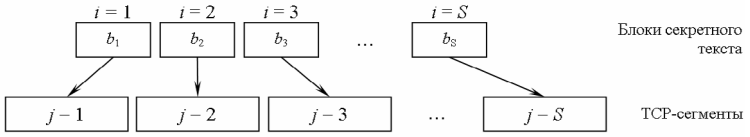

Рис. 5. Общая схема распределения блоков секретного текста между TCP-сегментами

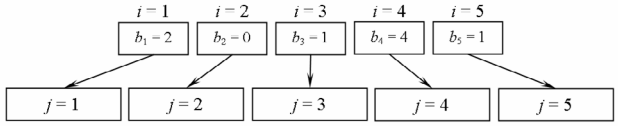

Рис. 6. Пример распределения блоков секретного текста между TCP-сегментами

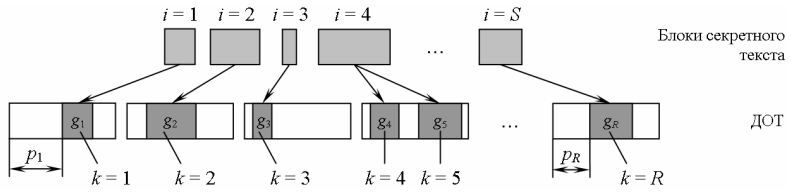

Рис. 7. Общая схема распределения блоков секретной информации по ДОТ

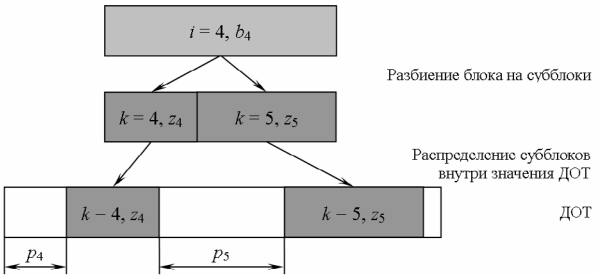

Рис. 8. Распределение субблоков секретных данных по значению ДОТ

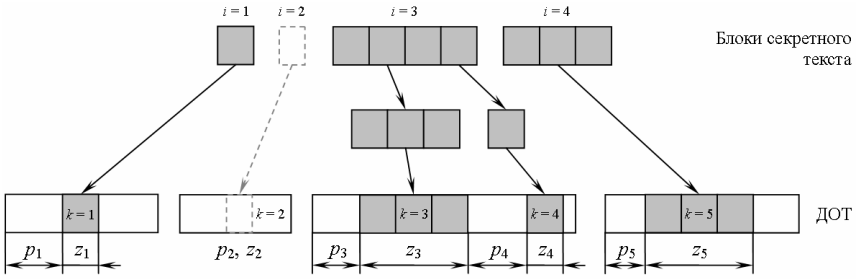

Рис. 9. Пример распределения секретной информации по ДОТ

Поясним сказанное на конкретном примере. Пусть общая длина секретного текста $B = 8$ бит, а общее число блоков секретного текста S = 5. Разбиение секретного текста на блоки выполнено следующим образом: $b_1 = 2$, $b_2 = 0$, $b_3 = 1$, $b_4 = 4$, $b_5 = 1$. Распределение блоков секретного текста по TCP-сегментам показано на рис. 6.

Сегменты с номерами $j = 1$; $j = 3$; $j = 4$ и $j = 5$ в соответствии с принятой терминологией являются информационными, так как длины соответствующих блоков секретного текста b_1, b_3, b_4 и b_5 больше нуля. Сегмент $j = 2$ является маскирующим, так как длина блока секретного текста $b_2 = 0$.

На рис. 7 показана схема распределения блоков секретной информации в двоичном числе, эквивалентном ДОТ.

На рисунке используются следующие обозначения: k – номер субблока секретного текста, внедряемого в очередное значение (ДОТ), принимает значение от 1 до R; R – общее число субблоков секретной информации, $R \geq S$; z_k – длина k-го субблока; p_k – смещение k-го субблока секретного текста внутри значения ДОТ в битах. Очевидно, что суммарная длина всех субблоков секретной информации равна общей длине секретного текста (2):

$$\sum_{k=1}^{R} z_k = \sum_{i=1}^{S} b_i = B. \qquad (2)$$

Схема распределения блоков секретного текста по значениям ДОТ подобна схеме распределения всего секретного текста между TCP-сегментами. Блоки секретной информации могут быть разбиты на субблоки. На рисунке четвертый блок секретного текста при внедрении в значение ДОТ разбивается на два субблока, причем сумма длин этих субблоков равна длине блока секретного текста b_4. Более подробно схема внедрения дробящихся (разделяемых) секретных данных в значение ДОТ показана на рис. 8.

Рассмотрим пример. Пусть секретный текст состоит из одного символа «Z» (двоичный код 01011010), а его длина составляет восемь бит (S = 8). Секретный текст разбивается на блоки следующим образом: 1, 0, 4 и 3 бит. Таким образом, секретный текст будет передан с помощью четырех TCP-сегментов, один из которых (второй) будет маскирующим.

Разбиение на субблоки осуществлено следующим образом. Первый блок не может быть разбит на субблоки, так как его длина $z_1 = 1$ бит. Второй блок является маскирующим, его длина $z_2 = 0$. Третий блок разбивается на два субблока дли-

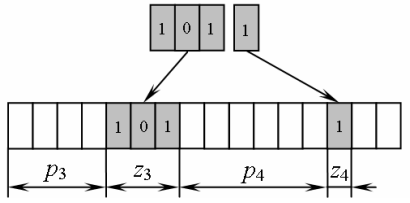

Рис. 10. Распределение бит субблоков секретных данных по двоичному значению ДОТ

ной $z_3 = 3$ и $z_4 = 1$ бит, соответственно. Четвертый блок внедряется без разбиения, образуя пятый субблок, длина которого составляет $z_5 = 3$ бита. Таким образом, общее количество субблоков равно пяти ($k = 5$), а их общая длина $1 + 0 + 3 + 1 + 3 = 8$ бит $= S$.

Первый субблок внедряется со смещением $p_1 =$ 5 бит, второй со смещением $p_2 = 0$ бит, третий – $p_3 = 2$ бит, четвертый – $p_4 = 4$ бит, пятый – $p_5 = 3$ бит. Распределение секретной информации по ДОТ показано на рис. 9.

На приеме априори известная информация о количестве субблоков, переносимых данным сегментом, их смещении внутри двоичного значения ДОТ и длины субблоков, позволяет однозначно восстановить скрытый текст.

Рис. 10 поясняет распределение субблоков секретных данных, внедряемых в биты двоичного значения ДОТ.

Двоичное значение ДОТ состоит из нескольких бит, количество которых зависит от значения максимальной длины блока (MTU) IP-дейтаграммы для используемой технологии передачи. Формирование этого значения на передаче (при шифровании) производится следующим образом. Первоначально все разряды двоичного числа ДОТ заполняются случайно. Затем в соответствии со значениями p_3, z_3, p_4, z_4 производится размещение бит субблоков секретных данных в двоичном значении ДОТ. Пусть первоначальное двоичное значение ДОТ выбрано таким: 10110110100. Такое значение ДОТ выбрано для использования в сетях Ethernet, где максимальная длина сегмента (MSS) составляет 1460 октет. Затем производится размещение третьего субблока длиной три бита. Для этого первые два разряда ДОТ пропускаются (так как $p_3 = 2$), а следующие три разряда заменяются субблоком z_3. Двоичное значение ДОТ приобретает вид: 10**101**110100 (биты секретного текста выделены жирным шрифтом). Аналогично производится внедрение следующего субблока. Для этого следующие четыре разряда ДОТ оставляют без изменений (так как $p_4 = 4$), а следующий разряд заменяется субблоком z_4. Окончательное значение ДОТ в двоичном виде получает следующий вид: 10**101**1101**1**0. Таким образом, в сеть должен быть отправлен TCP-сегмент, переносящий открытые данные длиной 1398 октет. Эти данные будут переносить часть информации о секретной букве «Z» (точнее – 4 бита). Аналогично скрываются остальные четыре разряда буквы «Z».

Нетрудно заметить, что как для внедрения, так и для извлечения секретных данных необходимо обладать некоторой информацией о порядке обработки двоичного значения ДОТ, а именно надо знать количество субблоков секретного текста, смещение каждого субблока внутри двоичного значения ДОТ и длину каждого субблока. Совокупность этих данных дает ключ, используемый для сокрытия или извлечения информации. Отсутствие ключевой информации не позволит отделить информационные сегменты от маскирующих и выделить биты скрытых данные в правильном порядке.

Выводы

Таким образом, разработаны оригинальные методы скрытой передачи информации по открытым сетям TCP/IP. Реализуемость разработанного метода стеганографической передачи с использованием длины открытого текста подтверждена экспериментально.

Литература

1. Savateev E. O. Design of Steganography System Based on the Version 4 Internet Protocol // IEEE International Siberian Conference on Control and Communications (SIBCON-2005). Tomsk, 2005. – P. 36-49.
2. Postel J. RFC 791. Internet Protocol. USC/ Information Sciences Institute. September, 1981.
3. Postel J. RFC 793. Transmission Control Protocol. USC/Information Sciences Institute. September, 1981.
4. Алексеев А.П., Орлов В.В. Сокрытие сообщений путем их распыления в пространстве // ИКТ, Т.6, №3, 2008. – С.52-56.