Вестник УрФО № 4(22) / 2016, с. 11–14

УДК 004.7.057.4 + 621.391.2 + 621.396.4

Безукладников И. И., Миронова А. А.

МЕТОДЫ СКРЫТОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ НА СЕТЕВОМ УРОВНЕ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

В предложенной статье рассматривается метод несанкционированного доступа известный под названием «скрытые каналы». Определены такие понятия, как «скрытый канал» и «недоиспользованный ресурс». Отражены основные особенности построения «скрытых каналов» на сетевом уровне телекоммуникационных систем. Приведены примеры «скрытых каналов» на сетевом уровне модели OSI. Дано детальное описание канала с использованием модели дискретного канала связи.

Ключевые слова: *телекоммуникационные системы, несанкционированный доступ, сетевой уровень модели OSI, «скрытые каналы», недоиспользованный ресурс, параметр MTU, модель дискретного канала связи.*

Bezukladnikov I. I., Mironova A. A.

THE METHODS OF COVERT DATA TRANSMISSION ON THE NETWORK LAYER OF THE TELECOMMUNICATION SYSTEMS

In the current article such method of unauthorized access as "covert channels" are covered. The notions of "covert channels" and "half used resource" are defined. The basic features of covert channels' construction on the network layer of the telecommunicational systems are also stated in the article. The examples of "covert channels" on the network layer of the OSI model are given. The detailed description of the channel, using the model of the discrete communication channel is suggested.

Keywords: *telecommunicational systems, unauthorized access, network layer of the OSI model, "covert channels", half used resource, MTU setting, model of the discrete communication channel*

В последнее время информационные атаки на телекоммуникационные системы (ТКС) различного назначения становятся все более изощренными. Злоумышленники ищут новые, более эффективные, методы несанкционированного доступа (НСД), характеризующиеся высокой сложностью обнаружения и борьбы с ними. Поэтому, стали возникать угрозы нового поколения, которым раньше не уделялось должного внимания, так как их реализация считалась невозможной. К угрозам такого рода относится осуществление НСД посредством т.н. «скрытых каналов».

«Скрытые каналы» (СК) - методы передачи нелегальной информации незаметно для действующих средств информационной безопасности (ИБ). Принцип их функционирования основан на использовании ресурсов канала, позволяющих в процессе открытой передачи информации внести некоторые изменения, которые не повлекут за собой вред открытой передаче информации пользователя (недоиспользованный ресурс)[1]. Недоиспользованным ресурсом может служить, например, ресурс, выделенный под передачу служебной информации.

В СМИ все чаще стали появляться публикации, связанные с передачей нелегальной информации посредством СК. Однако подавляющее большинство авторов чаще описывают протоколы прикладного и транспортного уровней модели ISO/OSI для реализации СК. В настоящей статье отражены основные особенности построения СК на сетевом уровне ТКС и приведены примеры СК на данном уровне.

В общем виде для создания скрытого канала необходимо выполнить следующие основные задачи:

1. Проанализировать принцип действия и особенности технологии, используемой на соответствующем уровне легальной системы. Предложить принцип, который может быть использован для скрытого переноса информации.

2. Оценить действующую политику ИБ, и выделить ее аспекты, относящиеся к выбранному уровню, а также выделить иные действующие в системе ограничения, препятствующие реализации скрытой передачи информации при помощи предлагаемого принципа.

3. Проанализировать выполнение необходимых условий существования скрытого канала.

4. Предложить конкретную реализацию скрытого канала, использующего предлагаемый принцип передачи информации.

5. Оценить основные технические характеристики полученной реализации скрытого канала[2].

Необходимо отметить, что реализация скрытых каналов на нижних уровнях модели ISO OSI сопряжена с резким ростом числа действий злоумышленника, необходимых для реализации такого канала. Это происходит по причине того, что при реализации СК на произвольном уровне модели OSI злоумышленник пользуется функционалом нижележащих уровней открытого канала. Так, например, реализуя СК на транспортном уровне, злоумышленнику нет необходимости беспокоиться о помехоустойчивости, множественном доступе к среде, генерации маршрутов и т.д. Чем ниже уровень, используемый для СК, тем большее число этих функций должно быть реализовано злоумышленником самостоятельно[1]. По этой причине наиболее выгодным для злоумышленника является реализация СК на уровнях начиная от сетевого и выше. Пример скрытых каналов сетевого уровня в IP-потоке рассмотрен далее.

Варианты СК на сетевом уровне модели ISO OSI

Вариант 1: При передаче данных на сетевой уровень модели OSI поступает IP пакет. Размер данного пакета должен соответствовать параметру MTU (maximum transmission unit), который задается типом локальной или глобальной сети. Поскольку чаще пакет имеет размер больше максимально допустимого для передачи, он подвергается фрагментации. Так, например, сеть Ethernet имеет параметр MTU равный 1500 байт, это означает, что полезные данные IP пакета необходимо разделить на кадры. При делении пакета часто оставаться остаток (хвост), благодаря которому возникает структурная недоиспользованность информационного потока, которая может быть использована в злоумышленных целях. На рис. 1 показан пример фрагментации IP пакета в условиях сети Ethernet.

Скрытая передача информации в данном случае возможна путем заполнения на передающей стороне недоиспользованного ресурса IP-пакета с помощью определенного алфавита.

Данный пример СК по виду недоиспользованности информационного ресурса мо-

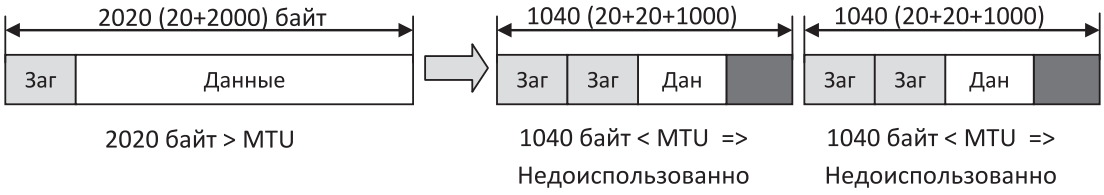

Рис. 1. Пример фрагментации IP пакета

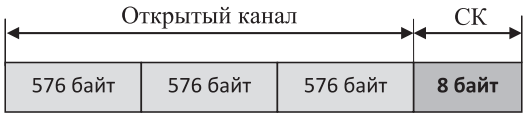

Рис. 2. Пример СК

жет быть классифицирован как недоиспользование логической структуры информационного потока.

Для детального описания канала представим его, используя модель дискретного канала связи[3]:

Участник X передает информацию участнику Y, при этом входной алфавит состоит из M символов y_i, а выходной из N символов x_i. Таким образом, в общем случае матрица канала связи содержит все переходные вероятности $P(x_i/y_i)$ и имеет вид:

$$P_{X/Y} = \begin{pmatrix} P(x_1y_1) & P(x_2y_1) & \cdots & P(x_Ny_1) \\ P(x_1y_2) & P(x_2y_2) & & P(x_Ny_2) \\ \vdots & & \ddots & \vdots \\ P(x_1y_M) & P(x_2y_M) & \cdots & P(x_Ny_M) \end{pmatrix}$$

где $P_{X/Y}$ - вероятность приема символа y_i при передаче символа x_i, от участника X к участнику Y.

В случае двоичного симметричного канала матрица примет следующий вид:

$$P_{X/Y} = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}$$

где p – вероятность успешной передачи, $1\text{-}p$ – вероятность ошибки.

Например, при открытой передаче пакета показанного на рис. 2, возникает недоиспользованность. При этом заданно, что если недоиспользованность менее 8 байт, то СК не может функционировать. Следовательно, в данном случае алфавит будет иметь 2^8 символов. При этом:

$$A = B = \{a_0, a_1, \dots, a_{255}\}$$

где A – выходной алфавит, B – входной алфавит. Мощность СК в данном случае будет равна $|A|$=256 символов.

В общем случае, пропускная способность двоичного симметричного канала может быть найдена по формуле[3]:

$$C = (1-p)\log_2\big(2(1-p)\big) + p\log_2(2p)$$

В приведенном выше примере пропускная способность СК может быть найдена следующим образом:

Если пакеты имеют одинаковый размер, максимальная скорость передачи информации в СК равна: $V_{\text{СК}} = V_{\text{откр.кан.}} * 8$, где $V_{\text{откр.кан.}}$ - пакетная скорость в открытом канале;

Если пакеты имеют разный размер:

$$V_{\text{СК}} = \frac{\sum_{i=1}^{n} K_1 + K_2 + \cdots + K_n}{n}$$

$$K_n = mod\,(\frac{Q_{\text{откр.инф}}}{576})/8$$

где K_n – объем переданной информации по СК, за одно изменение состояния, $Q_{\text{откр.инф}}$ – объем открытой информации.

Вариант 2: Для структурированного информационного потока существуют случаи, когда модуляция временных интервалов между различными событиями в информационном потоке не оказывает влияния на передаваемые открытые данные[1]. Таким образом, изменение временного интервала, так же может повлечь за собой скрытую передачу данных (рис. 3).

В простейшем случае возможна передача информации по СК с использованием входного и выходного алфавита состоящего из двух символов (например, «0» и «1»):

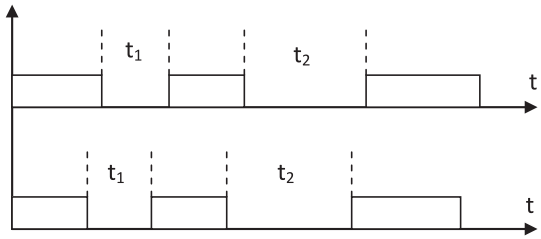

Рис. 3. Пример СК

1. передача «0», возможна при условии $0 < t_{\text{пак}} < t_1$;

2. передача «1», при условии $t_1 < t_{\text{пак}} < t_2$.

Данный вариант СК, так же может быть описан с помощью модели дискретного канала связи. Пропускная способность может быть найдена аналогично варианту 1.

Стандартные политики ИБ, составленные на основе действующего законодательства, не могут помешать работе, приведенных выше СК. Например, использование таких средств, как межсетевые экраны, антивирусные программы, датчики атак и. др. не могут создать препятствие для скрытой передачи информации данными методами.

Таким образом, проведенный анализ СК, которые могут беспрепятственно функционировать на сетевом уровне ТКС, позволяет охарактеризовать особенности отдельного класса угроз информационной безопасности. В связи с тем, что используемые в рамках функционирования СК принципы скрытой передачи информации не учитываются в большинстве политик информационной безопасности, данная проблема может считаться достаточно актуальной. Дальнейшее исследование проблемы СК предполагает нахождение способов их выявления и уничтожения, внесения соответствующих изменений в действующие требования в системе политик ИБ для совершенствования систем защиты информации ТКС.

Примечания

1. Безукладников И.И. Особенности синтеза скрытых каналов в многоуровневых системах / И. И. Безукладников, Е. Л. Кон // Системы мониторинга и управления: сборник научных трудов / Академия электротехнических наук Российской Федерации; Пермский государственный технический университет; Под ред. Е. Л. Кона .— Пермь, 2010 .— С. 230-238.

2. Безукладников И.И. Скрытые каналы в распределенных автоматизированных системах / И.И.Безукладников, Е.Л.Кон // Вестник УГАТУ, 2010, Т.14 №2. С. 245-250.

3. Гладких А. А. Основы теории мягкого декодирования избыточных кодов в стирающем канале связи / А. А. Гладких. – Ульяновск : УлГТУ, 2010. – С. 149-151.

БЕЗУКЛАДНИКОВ Игорь Игоревич, кандидат технических наук, доцент кафедры Автоматика и телемеханика Пермского национального исследовательского политехнического университета; 614990, Пермь, Комсомольский пр., 29. E-mail: fantomtk@yandex.ru.

МИРОНОВА Анна Алексеевна, студент кафедры Автоматика и телемеханика Пермского национального исследовательского политехнического университета; 614990, Пермь, Комсомольский пр., 29. E-mail: mir550@yandex.ru.

BEZUKLADNIKOV Igor' Igorevich, PhD of Technical Sciences at the Department of Automation and Telemechanics, Perm National Research Polytechnic University; 614990, 29, Komsomolsky prospect, Perm. E-mail: fantomtk@yandex.ru.

MIRONOVA Anna Alekseevna, student at the Department of Automation and Telemechanics, Perm National Research Polytechnic University, 614990, 29, Komsomolsky prospect, Perm. E-mail: mir550@yandex.ru.