УДК 681.324

И.В. Рубан[1], С.В. Смеляков[2], А.А. Смирнов[2], В.С. Бурковский[1]

[1] *Харьковский национальный университет радиоэлектроники, Харьков*
[2] *Харьковский университет Воздушных Сил им. Ивана Кожедуба, Харьков*

АНАЛИЗ ВОЗМОЖНОСТЕЙ УТЕЧКИ ИНФОРМАЦИИ В ИТКС ПРИ ИСПОЛЬЗОВАНИИ ПРОТОКОЛОВ ТРАНСПОРТНОГО УРОВНЯ МОДЕЛИ OSI В КАЧЕСТВЕ СТЕГОКОНТЕЙНЕРА

В данной статье рассмотрены возможности по использованию особенностей протоколов транспортного уровня модели OSI/ISO в качестве стегоконтейнера. Описаны наиболее распространённые методы tcp – стеганографии. Проведён сравнительный анализ некоторых свойств протоколов TCP иUDP. Обоснована целесообразность использования особенностей протоколов транспортного уровня моделиOSI в качестве стегоконтейнера.

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

Введение

В последнее время приобрели популярность методы, когда скрытая информация передается через информационно-телекоммуникационные сети (ИТКС) с использованием особенностей протоколов базовой модели сетевого взаимодействия OSI (Open System Interconnection).

Такие методы получили название "сетевая стеганография" [1]. Этот термин впервые ввел польский учёный Кристоф Джипъёрски (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].

Одним из требований к стеганографическому каналу (стегоканалу) является надёжность. Это связано с тем, что отправитель должен быть удостоверен в доставке секретного сообщения получателю в исходном виде. Транспортный уровень модели OSI предназначен для соединений типа точка-точка и предоставляет сервисы передачи данных.

В табл. 1 [3, 4] изображена сравнительная таблица наиболее распространённых протоколов транспортного уровня, – TCP и UDP.

Таблица 1

Сравнительная таблица наиболее распространённых протоколов транспортного уровня – TCP и UDP

	TCP	**UDP**
Функции	Устанавливает связь до начала сеанса передачи данных. Определяется начало и конец сеанса передачи данных	Связь устанавливается в одностороннем порядке без обратного ответа. Передаются пакеты данных разных размеров. Сеанс прекращается сразу после отправки пакетов
Применение	Используется для надёжной передачи данных вне зависимости от времени	Используется в играх и приложениях требуемых быструю передачу данных. Передача данных ненадёжная
Порядок пакетов	Перестраивает пакеты данных в определенном порядке	Не имеет никакого определённого порядка, поскольку все пакеты независимы друг от друга. Если требуется порядок, им должен управлять прикладной уровень
Поток данных	Данные считываются как поток байтов, пакеты не имеют определенных границ сегмента	Пакеты посылаются индивидуально и проверяются на целостность только тогда, когда они прибудут. Пакеты имеют определенные границы, которые соблюдаются после получения, то есть данные восстанавливаются в первоначальном виде
Проверка ошибок:	Проверяет на наличие ошибок и исправляет их.	Проверяет на наличие ошибок, но не исправляет их

В отличие от UDP, TCP гарантированно доставляет поток данных получателю, а в случае потери пакета на нижних уровнях модели OSI, осуществляет ретрансмиссию самостоятельно [3]. Одним из недостатков надёжного TCP является его ресурсоёмкость, которая обуславливается процедурами: тройного хэндшейка при соединении; передачи данных и восстановления сессии; постоянного контроля над состоянием виртуального канала передачи данных (ВКПД) и выработки контрмер; закрытие сессии. UDP лишён такой нагрузи, ввиду своего предназначения: передача данных, нетребовательных к надёжности доставки. Такими данными являются: онлайн видео- и аудио-потоки; данные, контроль доставки которых обеспечивают протоколы высших уровней модели OSI.

Исходя из изложенных особенностей протоколов транспортного уровня, подходящим для реализации стегоканала на транспортном уровне модели OSI является протокол TCP.

Основная часть

Под сетевой стеганографией на транспортном уровне модели OSI (далее tcp - стеганография), понимается группа методов сетевой стеганографии, в которых стегоконтейнером являются свойства протоколов транспортного уровня модели OSI.

Метод DL. Сущность метода DL[5] заключается в том, что секретный текст представляют в виде последовательности бит, которую передают получателю частями. Это связано с тем, ёмкость такого стегоконтейнера ограничена и в случае необходимости передачи большого количества скрываемой информации, её необходимо разбивать на порции. Стегоконтейнером является длина поля данных каждого информационного tcp-сегмента, представленная в двоичной форме исчисления. В [3] сказано, что если при хэндшейке, в начале tcp-сессии, стороны заранее не договариваются о допустимых максимальных значениях MSS (MaximumSegmentSize – максимальный размер сегмента), то его значение принимается по умолчанию равным 536 байтам.

В работе [5] автор предлагает скрытно передавать информацию, представленную в виде текста, где каждой букве соответствует двоичная последовательность из приемлемой таблицы кодировки. Для данного метода это может быть кодировка windows-1251(таблица CP1251). Эта кодировка является 8-разрядной. Длина поля данных tcp-сегмента равна $DL=MSS-L_4=536-20=516$, где L_4-длина заголовка tcp-сегмента без опций.

В этом случае, количество разрядов двоичного значения длины открытого текста (ДОТ) равно $Lot = (Lm - 1)$ разрядов, где $Lm = \log_2(DL) \approx 9{,}07$, при округлении до ближайшего большего соответствует 10 разрядам.

TCP-dump процесса передачи данных, основанном на методе DL, изображён на рис. 1. В методе заложена необходимость получения подтверждений о доставке каждого сегмента до отправки следующего. Для этого используется флаг PUSH(флаг проталкивания данных).

```
TCP: 50240 > scp-config [SYN] Seq=0 Win=32792 Len=0 MSS=16396 TSV=528243 TSER=0 WS=6
TCP: scp-config > 50240 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=16396 TSV=528243 TSER=528243
TCP: 50240 > scp-config [ACK] Seq=1 Ack=1 Win=32832 Len=0 TSV=528243 TSER=528243
TCP: 50240 > scp-config [PSH, ACK] Seq=1 Ack=1 Win=32832 Len=116 TSV=529497 TSER=528243
TCP: scp-config > 50240 [ACK] Seq=1 Ack=117 Win=32768 Len=0 TSV=529497 TSER=529497
TCP: 50240 > scp-config [PSH, ACK] Seq=117 Ack=1 Win=32832 Len=101 TSV=529523 TSER=529497
TCP: scp-config > 50240 [ACK] Seq=1 Ack=218 Win=32768 Len=0 TSV=529523 TSER=529523
TCP: 50240 > scp-config [PSH, ACK] Seq=218 Ack=1 Win=32832 Len=115 TSV=529529 TSER=529523
TCP: scp-config > 50240 [ACK] Seq=1 Ack=333 Win=32768 Len=0 TSV=529529 TSER=529529
TCP: 50240 > scp-config [PSH, ACK] Seq=333 Ack=1 Win=32832 Len=116 TSV=529542 TSER=529529
TCP: scp-config > 50240 [ACK] Seq=1 Ack=449 Win=32768 Len=0 TSV=529542 TSER=529542
TCP: 50240 > scp-config [PSH, ACK] Seq=449 Ack=1 Win=32832 Len=2100 TSV=529543 TSER=529542
TCP: scp-config > 50240 [ACK] Seq=1 Ack=2549 Win=49280 Len=0 TSV=529543 TSER=529543
TCP: 50240 > scp-config [FIN, ACK] Seq=2549 Ack=1 Win=32832 Len=0 TSV=531102 TSER=529543
TCP: scp-config > 50240 [FIN, ACK] Seq=1 Ack=2550 Win=49280 Len=0 TSV=531105 TSER=531102
TCP: 50240 > scp-config [ACK] Seq=2550 Ack=2 Win=32832 Len=0 TSV=531105 TSER=531105
```

Рис. 1. TCP-dump при передаче данных по методу DL

Для достижения большей устойчивости к выделению скрываемой информации автор использует криптографию. А именно, использование шифрования самого скрываемого текста, рассеивание скрываемого текста в двоичных значениях длины полей данных TCP-сегментов, задействование секретной

маски, представляющей собой двоичную последовательность, единичные значения которых соответствуют информационным, а нулевые – камуфлирующим сегментам.

Данный метод располагает возможностью передавать любые данные, которые возможно представить 8 разрядами в двоичной системе исчисления. Это может быть: текст, изображения, аудиозапись, видеозапись.

Метод RSTEG. В [6] предложен метод, который позволяет передавать скрываемые данные внутри пакетов TCP, отправляемых якобы для исправления неудачно переданных данных.

Этот алгоритм получил название RSTEG (Retransmission Steganography – стеганография в повторной передаче).

Принцип функционирования RSTEG изображён на рис. 2 [5]. Получатель принимает начальный пакет и отправляет сообщение об успешном приеме. Вместо того, чтобы передать следующий пакет, отправитель игнорирует сообщение об успешном приеме и отправляет пакет со скрываемым содержимым, но этот пакет имеет такой же идентификатор, что и предыдущий, а системы анализа сетевого трафика уже не проверяют повторный пакет.

Для всех систем сетевой защиты новый пакет с секретным содержимым неотличим от начального пакета, в котором не содержалось ничего подозрительного.

Когда повторно переданный пакет достигает принимающей стороны, из него извлекается скрытая информация [5].

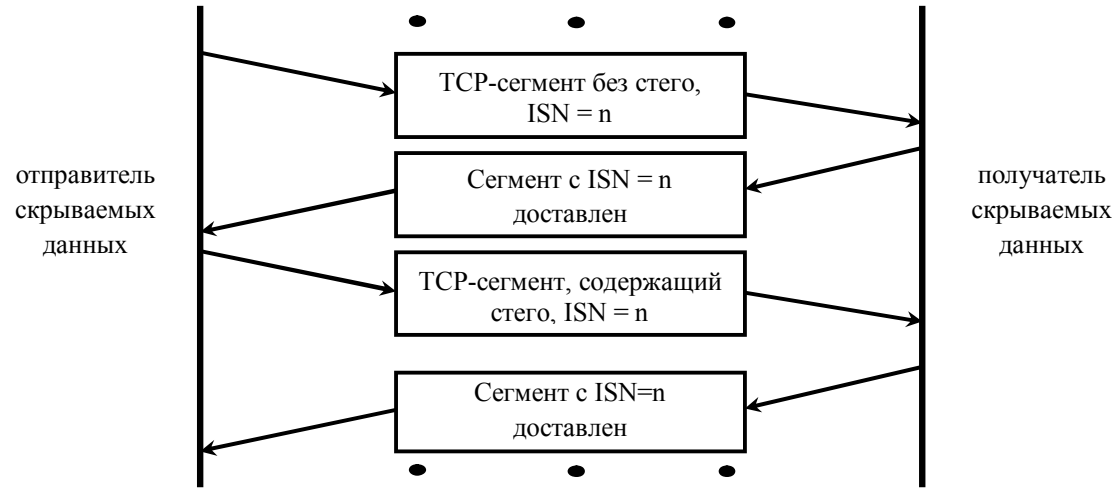

Рис. 2. Принцип функционирования RSTEG

Данный метод характеризуется малой полосой пропускания ввиду того, что количество ретрансляций заметно увеличивается по сравнению со среднестатистическим значением.

Нормальной ситуацией для протокола TCP, является потеря 0,1% переданных сегментов, а при потерях в 1-2%, он перестаёт корректно выполнять свои функции.

Для реализации данного метода необходимо располагать статистическими характеристиками среды, используемой для передачи скрываемых данных.

Метод LACK. LACK – это метод стеганографии для IP-телефонии, который модифицирует пакеты с голосовым потоком. Он использует то, что в типовых мультимедийных коммуникационных протоколах, таких как RTP, чрезмерно задержанные пакеты считаются приемником бесполезными и отбрасываются [6].

Данный метод является гибридным, так как основан на использовании особенностей взаимодействия протоколов транспортного (UDP, RTCP) и прикладного (RTP) уровней. Это связанно с целесообразностью использования UDP в качестве транспортного протокола и необходимостью повторной передачи некоторых из повреждённых пакетов. Контроль над ретрансмиссией возложен на взаимодействие протоколов RTCP и RTP.

Принцип функционирования LACK изображён на рис. 3 [7]. Отправитель выбирает один из пакетов голосового потока с полезной нагрузкой изаменяется битами секретного сообщения – стеганограммой, которая встраивается в пакет N4.

Затем выбранный пакет намеренно задерживается. Каждый раз, когда чрезмерно задержанный пакет достигает получателя, незнакомого с стеганографической процедурой, он отбрасывается. Однако, если получатель знает о скрытой связи, то вместо удаления полученных RTP пакетов извлекает скрытую информацию [7].

Пропускная способность канала, организованного на основе этого метода, позволяет передавать до 1.3Mb информации за один сеанс связи продолжительностью около 9 минут (средняя продолжительность вызовов IP - телефонии в обоих направлениях) [7].

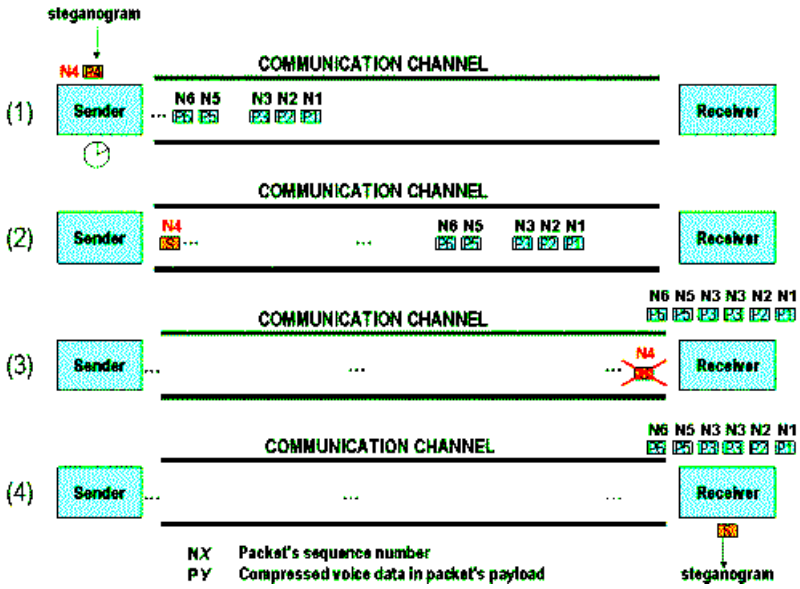

Рис. 3. Принцип функционирования LACK

Выводы

Основой для принятия решения о выборе метода сетевой стеганографии на транспортном уровне модели OSI является тип трафика, преимущественно используемого в сетях контрагентов скрытого канала связи. Если таковым является TCP-трафик (данные чувствительные к потерям пакетов), то предпочтением должны пользоваться методы DL и RSTEG. Если в сети преобладает трафик с потоковыми данными (нечувствительными к потерям пакетов), то подходящим методом может быть LACK.

Надёжность и скрытность методов сетевой стеганографии на транспортном уровне обуславливает целесообразность их использования в противовес методам сетевого уровня модели OSI.

Список литературы

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

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

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

4. "Internet protocol – DARPA Internet Program Protocol Specification" RFC-768. UDP. USC/Information Sciences Institute, 28 August 1980.

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

6. Mazurczyk Wojciech. Retransmission Steganography Applied (RSTEG) / Wojciech Mazurczyk, Krzysztof Szczypiorski. – Warsaw University of Technology, Faculty of Electronics and Information Technology, Institute of Telecommunications, 15/19 Nowowiejska Str., 00-665 Warsaw, Poland.

7. Mazurczyk Wojciech. LACK—a VoIP steganographic method / Wojciech Mazurczyk, Józef Lubacz. – «TelecommunSyst». DOI 10.1007/s11235-009-9245-y.

Поступила в редколлегию 5.05.2015

Рецензент: д-р техн. наук, проф. Ю.В. Стасев, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

АНАЛІЗ МОЖЛИВОСТЕЙ ВИТОКУ ІНФОРМАЦІЇ В ІТКМ ПРИ ВИКОРИСТАННІ ПРОТОКОЛІВ ТРАНСПОРТНОГО РІВНЯ МОДЕЛІ OSI У ЯКОСТІ СТЕГОКОНТЕЙНЕРА

І. В. Рубан, С.В. Смеляков, А.О. Смірнов, В.С. Бурковський

У даній статті розглянуті можливості з використання особливостей протоколів транспортного рівня моделі OSI/ISO у якості стегоконтейнера. Описано найбільш поширені методи tcp-стеганографії. Проведено порівняльний аналіз деяких властивостей протоколів TCP та UDP. Обґрунтовано доцільність використання особливостей протоколів транспортного рівня моделі OSI/ISOу якості стегоконтейнера.

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

ANALYSIS OF INFORMATION DISCLOSURE IN ITCN USING THE PROTOCOLS OF THE TRANSPORT LAYER OF OSI MODEL AS STEGANOGRAPHIC CONTAINER

I.V. Ruban, S.V. Smelyakov, A.A. Smirnov, V.S. Burkovskij

This article describes the ability to use the features of the transport layer protocols of OSI / ISO model as steganographic container. Describes the most common methods of tcp - steganography.The comparative analysis of some properties of the protocols TCP and UDP. The expediency of using the features of transport layer protocols in the OSI model as steganographic container.

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