даже так он всё же остается самой капитализированной и популярной криптовалютой в мире.

ЛИТЕРАТУРА

1. Ethereum Wiki, Ethash. [Электронный ресурс]. – Режим доступа: https://github.com/ethereum/wiki/wiki/Ethash. – Дата доступа: 15.04.2019.

2. Schwartz, D., Youngs, N. and Britto, A. 2014. The Ripple Protocol 2.Consensus Algorithm. White Paper. [Электронный ресурс]. – Режим доступа: https://ripple.com/files/ripple_consensus_whitepaper.pdf. – Дата доступа: 15.04.2019.

3. Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system. [Электронный ресурс]. – Режим доступа: https://bitcoin.org/bitcoin.pdf. – Дата доступа: 15.04.2019.

4. The free encyclopedia Wikipedia. [Электронный ресурс]. – Режим доступа https://en.wikipedia.org/wiki/Bitcoin. — Дата доступа: 15.04.2019.

5. Урбанович, П. П. Компьютерные сети: учебное пособие для студентов высших учебных заведений по техническим специальностям / П. П. Урбанович, Д. М. Романенко, Е. В. Кабак. - Минск: БГТУ, 2011. – 399 с.

УДК 004.056+003.26

Студенты К. В. Клицунова, Е. И. Дубовик
Науч. рук. проф. П. П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

СТЕГАНОГРАФИЧЕСКОЕ ПРЕОБРАЗОВАНИЕ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Некоторые основные понятия из предметной области [1,2], которые будут использованы в докладе.

Стеганография — это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи.

Стеганографическая система – объединение методов и средств, используемых для создания скрытого канала для передачи информации.

Контейнер – любая информация, используемая для сокрытия тайного сообщения.

Стеганографический канал – канал передачи стегоконтейнера.

Ключ – секретная информация для сокрытия стегоконтейнера и излечения информации из него.

Сообщение — контейнер с осажденной тайной информацией.

Цель нашей работы: проанализировать практические аспекты методов сетевой стеганографии.

*Сетевая стеганография*представляет собой группу методов, в которых скрытая информация передается через компьютерные сети с использованием особенностей работы протоколов передачи данных.

Методы сетевой стеганографии включают изменение свойств одного из сетевых протоколов. Так же, может использоваться взаимосвязь между двумя или более различными протоколами с целью более надежного сокрытия передачи секретного сообщения. Под *сетевой стеганографией* на сетевом уровне модели OSI [3] (далее ip-стеганография), понимается группа методов сетевой стеганографии, в которых стегоконтейнером могут являться неиспользуемые места в заголовках и полях данных ip-дейтаграмм.

Метод DF – это метод, основанный на модификации полей «identification» и «fragment-offset» при установленном флаге «DF» (don’t fragment – не фрагментировать).

Если установлен флаг DF, модуль IPне станет фрагментировать дейтаграмму. 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. Несмотря 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 (рис.1).

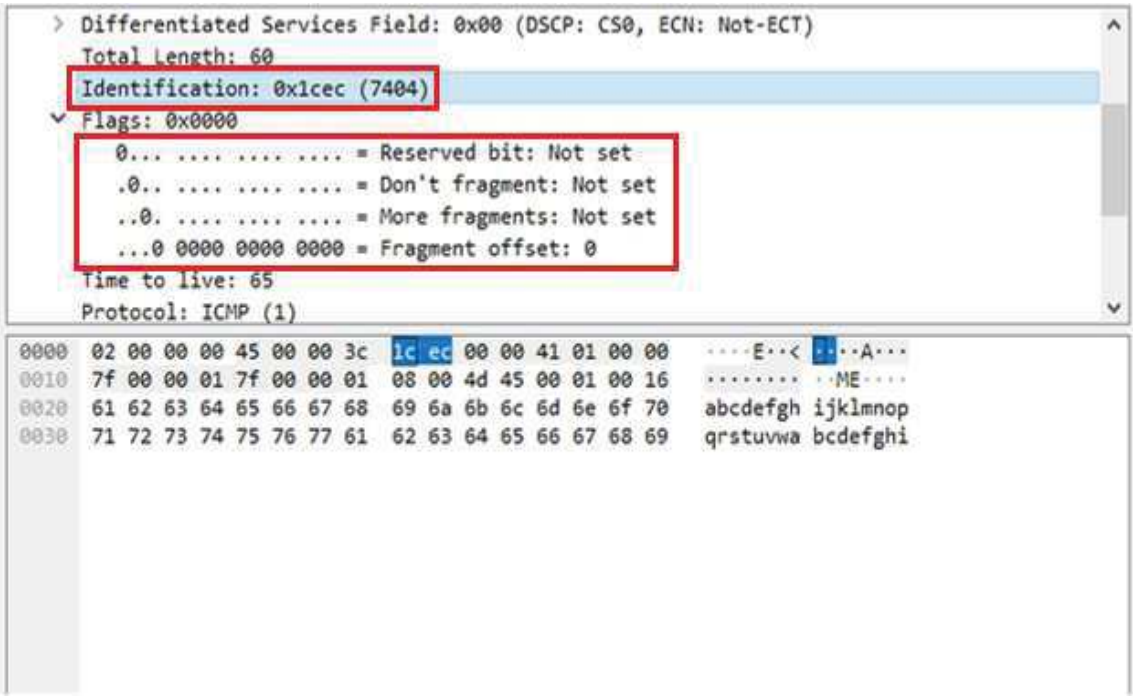

Рисунок 1 – Заголовки IP-дейтаграммы, используемые в качестве контейнера

Важно понимать, что при правильном выборе размера пакета возможно добиться выполнения условия $L \leq PMTU$, где L – длина пакета; *MTU* – maximum transmissionunit (максимальный размер полезного блока данных одного пакета); *PMTU* – MTU трассы от источника до конечного адресата пакета; $PMTU = min\ MTUi$, где *min MTUi* – минимальное значение *MTU* среди интерфейсов маршрута, по которому пройдёт пакет.

При выполнении условия ($L \leq PMTU$) 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.

Для исследования метода DF выбрана программная реализация утилиты *ping* (утилита отправляет запросы (ICMP Echo-Request) протокола ICMP указанному узлу сети и фиксирует поступающие ответы (ICMP Echo-Reply)). Так как частой практикой является непрерывная

отправка запросов для проверки соединения, большое количество ICMP-пакетов не вызовут подозрения.

В программной реализации утилиты имеются переменные, соответствующие всем полям заголовка. При помощи данных переменных можно модифицировать значения полей.

В качестве стеганоконтейнера было выбрано поле «identification».

Стеганосообщением является текстовый документ с тайной информацией.

Для реализации данного метода требуется:

- изменить значение поля «fragment-offset» на 0x00 (don't fragment),
- считывать информацию из документа,
- помещать значение считавшегося символа в поле «identification»,
- производить отправку запроса (см. рис.2).

```
const char text[20] = "Tqwepasdfghjsdfghbk"; // сообщение

for (int i = 0; i < 20; ++i)
{
    IpHead.id = (int)text[i]; // заносим символ в поле идентификатора
    memcpy(FullPack, &IpHead, sizeof(IpHeader));
    memcpy(FullPack + sizeof(IpHeader), Packet, icmp_size);

    int bytes = sendto(listn, (char*)PACKET_, size, 0, (sockaddr*)&list_adr, sizeof(list_adr)); // отправляем пакет
```

Рисунок 2 – Фрагмент кода, отвечающий за занесение информации и отправку пакета

На рис. 3 можно видеть пример пакета с осажденным символом.

Два последних пункта выполняются до тех пор, пока вся считанная информация не будет отправлена.

Для получения секретной информации стороне получателя потребуется специализированный софт для «отлова» пакетов.

Исследуя метод DF, была использована программа *Wireshark*, которая позволяет «отловить» полученные пакеты и считать в полях заголовков нужную информацию.

Выводы: в ходе исследовательской работы мы освоили технологию сетевой стеганографии, а также на практике реализовали один из методов скрытной передачи информации в сети.

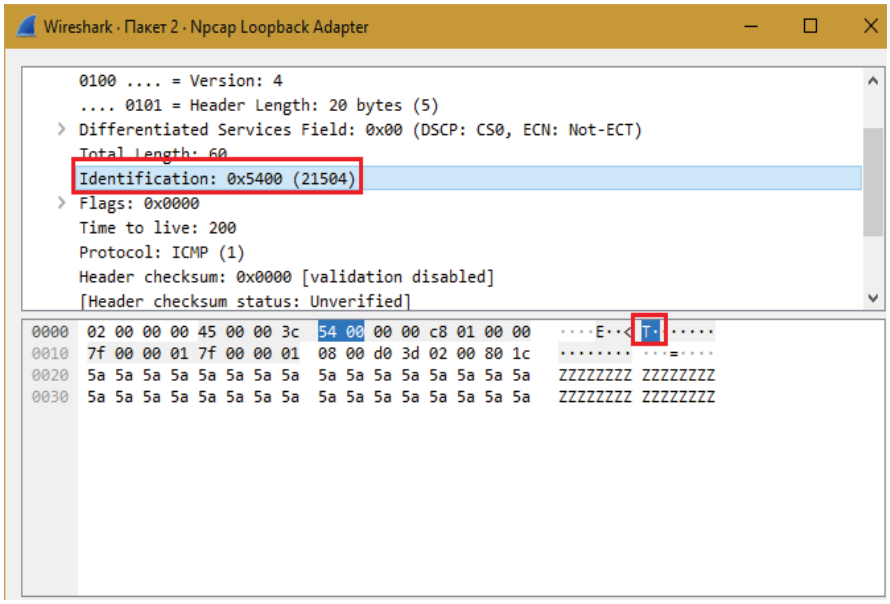

Рисунок 3 – Пакет с осажденным символом “T”

Стеганографические методы могут применяться для решения других задач [5-6].

ЛИТЕРАТУРА

1. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие для студ./ Урбанович П.П. – Минск: БГТУ, 2016. – 220 с.

2. Урбанович, П. П. Информационная безопасность и надежность систем: учебно-методическое пособие по одноименному курсу для студентов специальности 1-40 01 02-03 "Информационные системы и технологии" / П. П. Урбанович, Д. М. Романенко, Е. В. Романцевич. – Минск: БГТУ, 2007. – 87 с.

3. Урбанович, П. П. Компьютерные сети: учебное пособие для студентов высших учебных заведений по техническим специальностям / П. П. Урбанович, Д. М. Романенко, Е. В. Кабак. – Минск: БГТУ, 2011. – 399 с.

4. Internet protocol – DARPA Internet Program Protocol Specification/ RFC-791 USC/Information Sciences Institute, September 1981. [Электронный ресурс]. – Режим доступа: https://tools.ietf.org/html/rfc791. – Дата доступа: 13.04.2019.

5. Urbanovich, P. Theoretical Model of a Multi-Key Steganography System / P. Urbanovich, N. Shutko // Recent Developments in Mathematics and Informatics. Contemporary Mathematics and Computer Science. Vol. 2, Chapter 11. – Lublin : KUL, 2016. – P. 181-202.

6. Text steganography application for protection and transfer of the information / Pavel Urbanovich, Konstantin Chourikov, Andrey Rimorev, Nadzeya Urbanovich // Przegląd elektrotechniczny. – 2010. – R. 86.– № 7.– P. 95-97.