Сетевая стеганография на основе ICMP-инкапсуляции

В.В. Галушка, С.Б. Петренкова, Я.В. Дзюба, В.А. Панченко

Донской государственный технический университет, Ростов-на-Дону

Аннотация: Статья посвящена описанию способа формирования стеганографических сетевых сообщений с использованием служебного протокола ICMP для их скрытой передачи, обхода ограничений межсетевых экранов и других систем защиты компьютерных сетей. В ней приводится описание функций протокола ICMP, его преимуществ при использовании в задачах стеганографии и особенностей обработки ICMP-пакетов операционными системами и промежуточным сетевым оборудованием. Отдельное внимание в статье уделяется вопросам практической реализации и применения предлагаемого метода. В ней приводится описание сетевых утилит для работы с пакетами и пример их использования для передачи скрытого сообщения. Для программной реализации метода сетевой стеганографии предлагается использовать язык программирования C# и библиотеки SharpPCap и Packet.NET, для которых в статье приведены примеры использования и указаны необходимые параметры для формирования пакетов со стеганографическими сообщениями.
Ключевые слова: информационная безопасность, сетевая стеганография, протокол ICMP, стек TCP/IP, инкапсуляция, SharpPCap.

Введение

Проблемам информационной безопасности на сегодняшний день уделяется большое внимание. Это связано с качественными изменениями информационных процессов, в результате которых данные, хранимые на компьютерах и передаваемые по сети, приобретают всё большую ценность. Вместе с этим растёт число угроз и уязвимостей, а параллельно с ними развиваются методы защиты данных. Среди таких технологий отдельного рассмотрения заслуживает стеганография — наука, изучающая методы сокрытия одних данных внутри других.

На сегодняшний день стеганография имеет много применений. На её основе работают, например, технологии так называемых цифровых отпечатков, когда в каждый экземпляр документа, изображения или сообщения внедряется некоторая уникальная метка, не обнаруживаемая стандартными средствами, однако, позволяющая, в случае необходимости, идентифицировать данный экземпляр и однозначно связать его с

пользователем, которому он был передан [1]. Похожим образом работают стенографические «водяные знаки», однако, при их реализации нет необходимости использования различных меток для разных копий информации — используется только одна секретная метка, которая позволяет доказать авторство.

Сетевая стеганография

Однако, если цифровые отпечатки и стеганографические «водяные знаки» представляют практический интерес в области защиты прав интеллектуальной собственности, то с технической точки зрения для информационной безопасности наиболее интересно применения стеганографии для скрытой передачи данных [2].

Сетевой стеганографией называется скрытая передача информации через компьютерную сеть, включая промежуточное оборудование, основанная на модификации данных в заголовках или полях полезной нагрузки сетевых пакетов, а также изменении правил передачи пакетов в том или ином сетевом протоколе [3].

Целью разработки метода сетевой стеганографии, которому посвящена данная статья, является обход фильтров, создаваемых стандартными правилами наиболее распространённых сетевых экранов, а также формирование базы для дальнейшего исследования возможностей выявления стеганографических сообщений.

Модель сетевого взаимодействия

В основе практически всех современных компьютерных сетей лежит стек TCP/IP, который включает в себя набор согласованных протоколов, обеспечивающих передачу данных по сети, а также обмен служебными и управляющими сообщениями для организации взаимодействия между сетевым оборудованием. Одним из важных служебных протоколов является

ICMP (Internet Control Message Protocol — протокол межсетевых управляющих сообщений), предназначенный для рассылки сообщений об ошибках и других исключительных ситуациях, а также проверки связи, трассировки маршрутов и многого другого.

В зависимости от требуемой функции, узел, формирующий ICMP-пакет, указывает в его заголовке соответствующее значение поля «тип», которым определяется формат содержимого пакета. При этом, в соответствии со стандартом, для некоторых типов ICMP-сообщений необходимо заполнение поля данных, например, для получения нужного размера пакета, задание которого является одной из опций команды ping. В результате, несмотря на то, что ICMP относится к служебным протоколам, наличие или отсутствие данных в поле полезной нагрузки пакета само по себе не может быть использовано как признак скрытой передачи информации. Процесс помещения информации в пакет, который затем сам помещается в другой пакет протокола нижележащего уровня, называется инкапсуляцией и представляет собой основу функционирования цифровых сетей передачи данных.

Протокол ICMP

Для современного сетевого оборудования и операционных систем, использующих стек TCP/IP, поддержка протокола ICMP обязательна, что является его несомненным преимуществом при использовании для передачи скрытых сообщений. Из этого факта следуют ещё несколько преимуществ стеганографии на основе ICMP-инкапсуляции. Одним из них является периодическая рассылка ICMP-сообщений узлами сети, которая происходит при обнаружении ошибок в IP-адресах пакетов, отсутствии маршрутов к запрашиваемым сетям и многих других случаях, что приводит к большому числу ICMP-пакетов, содержащих служебную сетевую информацию, среди которых можно скрыть пакеты с какой-либо другой информацией.

Отключение данного протокола или его блокировка с помощью сетевых экранов, списков контроля доступа и прочих средств безопасности не является хорошим способом защиты от пересылки стеганографических сообщений, так как может нарушить работу сети в следствии невозможности обмена служебной информацией.

Другая особенность протокола ICMP, отличающая его от остальных служебных протоколов, и определяемая долгой историей развития и большим количеством выполняемых функций — сложность внутренней структуры пакетов, которая приводит к наличию большого числа возможных сочетаний полей заголовка и полезной нагрузки.

В соответствии со стандартом [4] ICMP-пакет имеет формат, представленный на рис. 1.

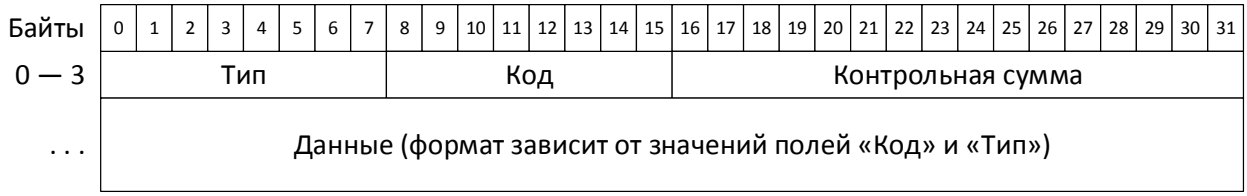

Рис. 1. – Структура заголовка ICMP-пакета.

В стандарте описаны 40 различных типов ICMP-сообщений для каждого из которых могут использоваться разные коды, обозначающие конкретное действие или состояние для пакетов данного типа.

Практическая реализация

Практическая реализация метода сетевой стеганографии с использованием протокола ICMP сводится к двум задачам:

1. Формирование пакета с требуемым содержимым в полях заголовка и полезной нагрузки, отличающегося от стандартных пакетов, генерируемых операционной системой.

2. Выделение сформированного пакета из общего потока трафика принимающей стороной и распознавание помещённых в него стеганографических сообщений.

Решение данных задач возможно с использованием различных программных и инструментальных средств. Формирование пакетов с произвольным содержанием можно осуществлять с помощью соответствующих сетевых утилит. На рис. 2 показан пример формирования ICMP-пакета в одной из таких программ. Помимо непосредственного помещения скрытых сообщений в ICMP-пакет, данная утилита позволяет задавать ему произвольные IP и MAC адреса источника, что может быть полезным для скрытия реального отправителя [5,6].

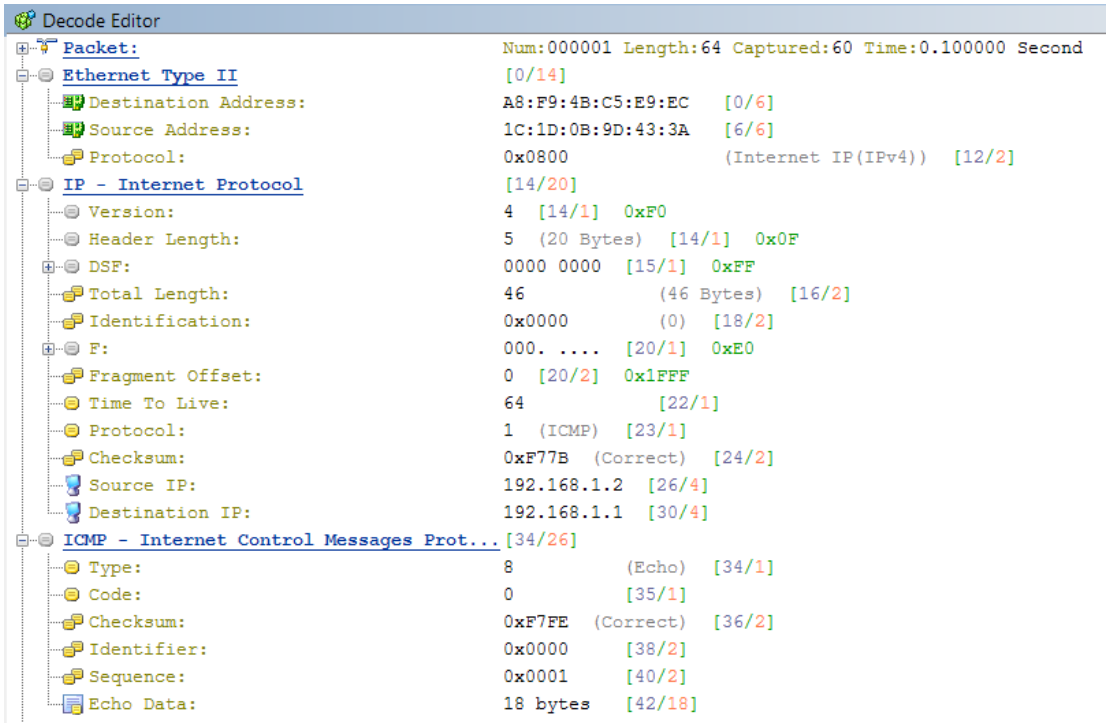

Рис. 2 – Формирование пакета в Colasoft Packet Builder

Приём и распознавание полученных пакетов можно осуществлять с помощью известной утилиты Wireshark, показывающей подробную информацию обо всех проходящих через компьютер сетевых пакетах. Пример её работы показан на рис. 3.

Однако, представленный способ взаимодействия, из-за необходимости вручную заполнять все поля заголовков ICMP-пакта, не может обеспечить эффективной передачи необходимых объёмов данных и больше подходит для тестовых или учебных целей. Для практического применения данного метода

необходимо разработать собственное клиент-серверное приложение, в котором описанные функции по формированию, отправке, приёму и распознаванию пакетов будут выполняться автоматически. Учитывая необходимость отступления от требований протокола, целесообразно при создании такого приложения вместо стандартного механизма сокетов использовать сторонние библиотеки для низкоуровневой работы с сетевыми пакетами [7,8,9]. Применительно к языку программирования C# такими библиотеками являются Packet.NET и SharpPCap, представляющая собой обёртку для платформы .NET над библиотекой PCap, на которой основана работа программы Wireshark, рассмотренной ранее.

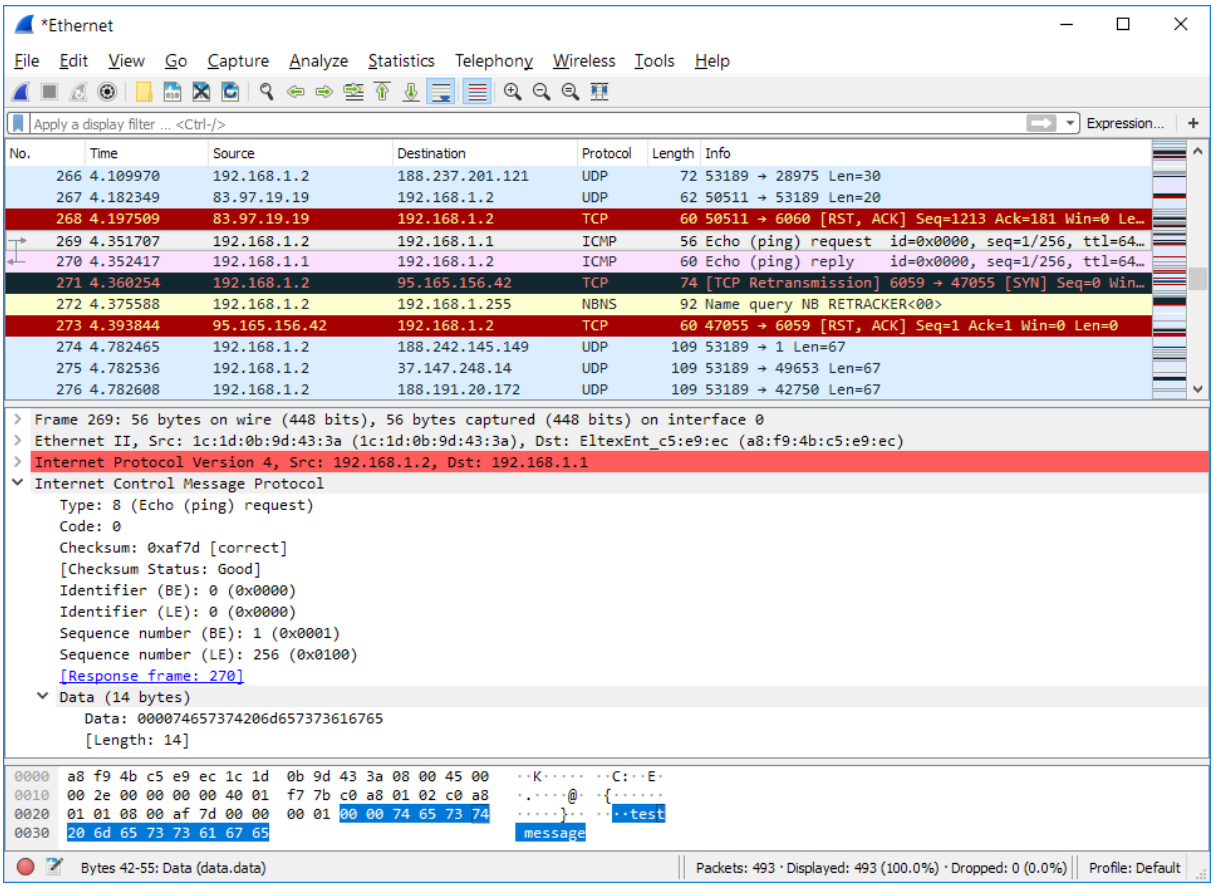

Рис. 3. – Получение пакета в Wireshark

Использование Packet.NET заключается в написании алгоритма последовательного формирования пакетов разных уровней модели TCP/IP, от верхнего (прикладного) к нижнему (уровню доступа к среде).

Соответственно программная реализация рассматриваемого метода сетевой стеганографии включает в себя несколько этапов инкапсуляции [10].

На начальном этапе создаётся ICMP-пакет, который в соответствии с парадигмой объектно-ориентированного программирования представлен объектом класса ICMPv4Packet, описанным в библиотеке Packet.NET. Для него необходимо задать значения полей заголовка, описанных ниже.

TypeCode — числовой идентификатор типа сообщения. В библиотеке Packet.NET значения для данного поля хранятся в перечислении ICMPv4TypeCodes и позволяют вместо чисел использовать их более понятные текстовые эквиваленты. При выборе какого-либо значения автоматически заполняются поля «тип» и, при необходимости, «код» (рис. 1) в заголовке пакета. Правильное заполнение этих полей требуется только в случае использования протокола ICMP по назначению, а для скрытой передачи данных они не имеют никакого значения, потому могут быть установлены, например, в EchoRequest (тип 8, код 0) и EchoResponce (тип 0, код 0).

Sequence — номер пакета в последовательности, который необходим для его идентификации в задачах, для которых требуется отправка нескольких пакетов. Данное поле необходимо использовать при отправке длинного сообщения, которое разбивается на несколько более коротких, каждое из которых помещается в отдельный ICMP-пакет со своим номером в последовательности, задаваемым целым числом от 0 до $2^{16} – 1$.

Data — поле для записи служебных данных, которое при реализации стеганографической системы будет содержать в себе информацию, передаваемую скрыто.

После заполнения всех необходимых полей ICMP-пакета, вычисляется контрольная сумма, которая также записывается в его поле Checksum. Затем полученный пакет передаётся нижележащему протоколу сетевого уровня, на

котором требуется заполнение полей SourceAddress и DestinationAddress, предназначенных для записи IP-адресов источника и назначения. Адрес источника может быть получен из свойств сетевого интерфейса, а адрес получателя должен быть задан пользователем.

Для данного IP-пакета также потребуется вычисление контрольной суммы с помощью имеющегося в классе IPv4Packet метода UpdateIpChecksum, после чего пакет передаётся следующему, канальному, уровню.

На канальном уровне, по аналогии с предыдущим, требуется добавить в заголовок пакета MAC-адреса источника и назначения. При этом MAC-адрес источника, как и его IP-адрес, может быть получен из свойств сетевого интерфейса, а для определения MAC-адреса назначения необходимо воспользоваться либо ARP-таблицей, либо послать предварительный ARP-запрос, который определит MAC-адрес по IP-адресу назначения. После успешного завершения всех описанных действия Ethernet-пакет, сформированный на канальном уровне, может быть передан в сеть.

Принимающая сторона должна выполнить такие же действия, но в обратном порядке, то есть сначала получить Ethernet-пакет, извлечь из него IP-пакет, затем из IP-пакета извлечь ICMP-пакет и прочитать записанные в нём данные.

Заключение

Программная реализация описанного метода сетевой стеганографии на основе ICMP-инкапсуляции позволяет осуществлять передачу данных по сети, скрывая их в общем потоке трафика под видом служебных пакетов. При этом особенности протокола ICMP не позволяют блокировать его пакеты без нарушения работоспособности сети, а глубокий анализ содержимого каждого пакета с целью выявления стеганографических сообщений требует больших вычислительных затрат и может вносить задержки в передачу пакетов.

Практическое применение данного метода стеганографии может быть полезным при построении ICMP-туннелей, используемых для обхода различного рода ограничений, накладываемых интернет-провайдерами, межсетевыми экранами или системами фильтрации трафика.

Литература

1. Frank Y.Sh. Digital Watermarking and Steganography. Fundamentals and Techniques, Second Edition // Boca Raton: CRC Press. 2017. 292 p.

2. Wojciech Frączek, Krzysztof Szczypiorski Perfect undetectability of network steganography Perfect undetectability of network steganography. Security Comm. Networks, 2016, 9: pp.2998–3010.

3. Белкина Т.А. Аналитический обзор применения сетевой стеганографии для решения задач информационной безопасности // Молодой ученый, 2018, №11 URL: moluch.ru/archive/197/48821/.

4. RFC 792 — Internet Control Message Protocol. URL: tools.ietf.org/html/rfc792 (date of access: 21.09.2018).

5. Пескова О.Ю., Халабурда Г.Ю. Применение сетевой стеганографии для скрытия данных, передаваемых по каналам связи // Известия южного федерального университета. Технические науки. 2012. №12(137). С. 167-176.

6. Голубев Е.А., Емельянов Г.В. Стеганография как одно из направлений обеспечения информационной безопасности // T-Comm - Телекоммуникации и транспорт. 2009. №S3. С. 185-186.

7. Земцов А.Н., Аль-Макреби И.М. Исследование устойчивости цифровых водяных знаков-логотипов, внедряемых в статические изображения // Инженерный вестник Дона, 2015, №2-2. URL: ivdon.ru/ru/magazine/archive/n2p2y2015/2963.

8. Земцов А.Н., Аль-Макреби И.М. Об оценке вносимых искажений методом маркирования в низкочастотной области вейвлет-спектра

изображения // Инженерный вестник Дона, 2015, №2-2. URL: ivdon.ru/ru/magazine/archive/n2p2y2015/2962.

9. Павлин Д.В., Макосий А.И., Жданов О.Н. О сетевой стеганографии. Реализация алгоритма RSTEG // Решетневские чтения. 2014. №18 (2). С. 322-324.

10. Бойченко М.К., Иванов И.П., Кондратьев А.Ю., Лохтуров В.А. Обеспечение потребных нагрузок сетевых интерфейсов утилитой ping программного обеспечения протокола ICMP // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия «Приборостроение». 2016. №4(109). С. 74-84.

References

1. Frank Y.Sh. Boca Raton: CRC Press. 2017. 292 p.

2. Wojciech Frączek, Krzysztof Szczypiorski Perfect undetectability of network steganography Perfect undetectability of network steganography. Security Comm. Networks, 2016, 9: pp. 2998–3010.

3. Belkina T.A. Molodoy uchenyy (Rus), 2018, №11. URL: moluch.ru/archive/197/48821/.

4. RFC 792 — Internet Control Message Protocol. URL: tools.ietf.org/html/rfc792.

5. Peskova O.Yu., Khalaburda G.Yu. Izvestiya yuzhnogo federal'nogo universiteta. Tekhnicheskie nauki. 2012. №12(137). pp. 167-176.

6. Golubev E.A., Emel'yanov G.V. T-Comm - Telekommunikatsii i transport. 2009. №S3. pp. 185-186.

7. Zemtsov A.N., Al'-Makrebi I.M. Inzhenernyy vestnik Dona (Rus), 2015, №2-2. URL: ivdon.ru/ru/magazine/archive/n2p2y2015/2963.

8. Zemtsov A.N., Al'-Makrebi I.M. Inzhenernyy vestnik Dona (Rus), 2015, №2-2. URL: ivdon.ru/ru/magazine/archive/n2p2y2015/2962.

9. Pavlin D.V., Makosiy A.I., Zhdanov O.N. Reshetnevskie chteniya. 2014. №18(2). pp. 322-324.

10. Boychenko M.K., Ivanov I.P., Kondrat'ev A.Yu., Lokhturov V.A. Vestnik Moskovskogo gosudarstvennogo tekhnicheskogo universiteta im. N.E. Baumana. Seriya «Priborostroenie». 2016. №4(109). pp. 74-84.