УДК 004.738:004.42

ПРИЛОЖЕНИЕ ДЛЯ РЕАЛИЗАЦИИ СТЕГАНОГРАФИЧЕСКОЙ СИСТЕМЫ ОБМЕНА СООБЩЕНИЯМИ ПО ПРОТОКОЛУ ICMP

Е. А. Блинова, А. А. Бесман, П. П. Урбанович

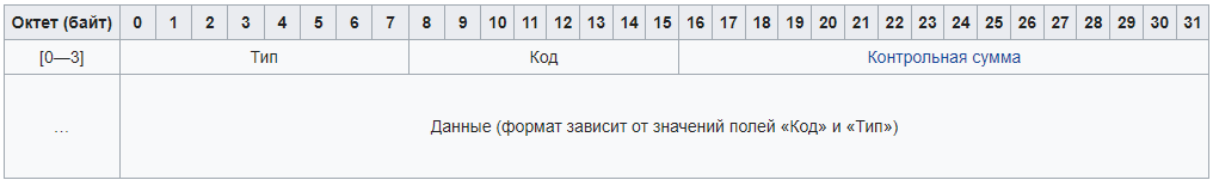
Белорусский государственный технологический университет, Минск
e-mail: evgenia.blinova@belstu.by

Многие пользователи сети Интернет обеспокоены безопасностью обмена сообщениями, когда сторона, предоставляющая услуги передачи данных или сообщений, использует данные пользователей для передачи третьим лицам. Некоторые инструменты для обеспечения конфиденциальности могут быть платными или сложными, а при использовании криптографии – явно привлекать внимание. В связи с этим актуальной является постановка задачи создания стеганографической системы скрытого обмена сообщениями и разработки программного средства для отправки и получения скрытых сообщений с использованием стеганографического подхода. Сетевая стеганография – вид стеганографии, в котором в качестве среды передачи секретных сообщений выступают сетевые протоколы [1]. Одним из перспективных, по мнению авторов, является протокол ICMP.

Протокол ICMP (Internet Control Message Protocol) – протокол сообщений об ошибках в сетях, который сетевые устройства, такие как маршрутизаторы, использует для создания сообщений об ошибках [2, 3]. Поскольку протокол IP (без TCP) не отправляет подтверждения передачи, не проверяет ошибки и не повторяет передачу в случае неуспеха, то протокол ICMP применяется для перенаправления пакетов или уведомления о недоступности узлов. Кроме того, ICMP используется для передачи отклика на пакет или эха на отклик, контроля времени жизни сообщений об ошибках, переадресации пакета, выдачи сообщения о недостижимости адресата, формирования временных меток и др.

Все ICMP пакеты начинаются с 8-битного поля типа ICMP и его кода (15 значений), как показано на рисунке. Код уточняет функцию

ICMP-сообщения, а дальнейшая структура сообщения зависит от типа пакета.



Формат пакета ICMP

Поля «Тип» и «Код» имеют установленные стандартом значения. В таблице приведено описание назначения полей структуры пакета ICMP.

Описание структуры пакета ICMP

Длина	Поле	Описание
1 байт	Тип	Задается тип сообщения ICMP. Значения {0, 3, 4, 5, 8 – 18}: 0, 8 – эхо; 3 – пункт назначения недостижим; 4 – отключение источника; 5 – переадресация; 9, 10 – объявление и запрос маршрутизатора; 11 – время истекло; 12 – некорректные параметры; 13, 14 – временные метки; 15, 16 – устаревание запроса; 17, 18 – адресные маски
1 байт	Код	Дополнительная информация к типу. Значения {0 – 15}, для некоторых типов не указывается
2 байта	Контрольная сумма	Контрольная сумма сообщения ICMP
4 байта	Зависит от типа	Дополнительная информация, зависящая от типа сообщения

Современное сетевое оборудование и операционная система, использующие стек TCP/IP, поддерживают протокол ICMP в обязательном порядке. Это позволяет быть уверенным в получении получателем отправленных пакетов. Вместе с тем пакеты ICMP периодически рассылаются в сетях, что приводит к их большому числу и позволяет скрыть пакеты с сообщениями среди пакетов с любой другой информацией. Наибольший интерес представляют пакеты ICMP типов «8» (эхо-запрос) и «0» (эхо-ответ), которые применяются в программе ping.

Немаловажным фактом является то, что пакеты могут отправляться только в рамках одной сети. Если же предполагается отправить данные получателю, который находится в другой сети, то необходимо позаботиться о том, чтобы был установлен и настроен канал для передачи данных. Сделать это можно с помощью VPN, который позволяет создать виртуальную локальную сеть. Далее нужно настроить параметры защиты на компьютерах, чтобы обе стороны смогли видеть друг друга в сети и обмениваться пакетами.

В работе [4] проанализирована возможность использования протокола ICMP для передачи скрытых сообщений. По мнению авторов, здесь не были обсуждены довольно важные аспекты: контроль целостности и авторства полученного сообщения, вопрос децентрализации приложения. Предлагалось разрабатывать клиент-серверную реализацию, что нецелесообразно, так как противоречит концепции незаметности стеганографической системы. С точки зрения авторов, необходимо позволить отправителю передавать скрытые сообщения напрямую получателю без участия централизованного узла с помощью пакетов типа «0» и «8» протокола ICMP. Что касается контроля авторства сообщений, предлагается ассиметричное шифрование, а для подтверждения получения сообщения можно использовать отправку получателем отправителю хеш-значения полученного пакета. Как только хеш-значения для всех частей сообщения получены отправителем, сообщение считается доставленным.

Для реализации такой стеганографической системы было разработано приложение для ОС Ubuntu Linux в среде PyCharm Community с использованием библиотек Scapy и RSA и СУБД SQLite. Приложение устанавливается и хранит историю сообщений и ключи локально. Обладает простым, удобным и интуитивно понятным интерфейсом, который состоит из двух окон: окна создания подключения, где указываются детали получателя сообщения (адрес, имя, используемые ключи), и окна написания сообщения.

В приложении реализована генерация ключей пользователя для подтверждения целостности данных и аутентификации. Пользователями могут быть использованы ключи, сгенерированные по криптографическому алгоритму RSA, и цифровая подпись на его основе. У отправителя есть возможность проверить наличие получателя в сети и получить его открытый ключ, а затем зашифровать, подписать и отправить сообщение получателю. Приложение со стороны отправителя разделяет сообщение на блоки в соответствии с размером паке-

тов ICMP типа «0» или «8». Приложение со стороны получателя осуществляет выделение пакетов из общего потока трафика, отправляя контрольный ответ отправителю на каждый полученный пакет. Таким образом становится возможным контролировать передачу всех блоков сообщения, повторяя их в случае необходимости.

Список литературы

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

2. Урбанович, П. П. Компьютерные сети и сетевые технологии : учеб. пособие / П. П. Урбанович, Д. М. Романенко. – Минск : БГТУ, 2022. – 608 с.

3. Бабаев, С. И. Компьютерные сети / С. И. Бабаев, Б. В. Костров, М. Б. Никифоров // Стандарты и протоколы : учебник. – Ч. 3. – М. : КУРС, 2018. – 176 с.

4. Сетевая стеганография на основе ICMP-инкапсуляции / В. В. Галушка [и др.] // Инженерный вестник Дона. – 2018. – № 4 (51).