УДК 004.056

Студ. А.А. Бесман
Науч. рук. ст. преп. Е.А. Блинова
(Кафедра информационных систем и технологий, БГТУ)

ПРОГРАММНОЕ СРЕДСТВО ДЛЯ СКРЫТОГО ОБМЕНА СООБЩЕНИЯМИ ПО ПРОТОКОЛУ ICMP

Многие пользователи сети интернет обеспокоены безопасностью выхода в сеть в связи с участившимися ситуациями, когда сторона, предоставляющая услуги передачи данных или сообщений, использует или продает данные пользователей третьим лицам. В связи с этим у пользователей возникает вопрос о конфиденциальности передаваемых данных. Некоторые инструменты для обеспечения конфиденциальности могут быть платными или сложными, а при использовании криптографии – явно привлекать внимание. В связи с этим актуальной является задача создания программного средства для отправки скрытых сообщений с использованием стеганографического подхода. После изучения инструментов и протоколов, позволяющих передавать данные по сети, нами было предложено передавать скрытые сообщения по протоколу ICMP.

ICMP (InternetControlMessageProtocol) – протокол сообщений об ошибках в сетях, который сетевые устройства, такие как маршрутизаторы, используют для создания (отправки) сообщений об ошибках. Структура сообщений зависит от типа пакета. Для нас наибольший интерес представляют ICMP пакеты типов 8 (эхо-запрос) и 0 (эхо-ответ), которые применяются в программе ping. Современные сетевые оборудования и ОС, использующие стек TCP/IP поддерживают протокол ICMP в обязательном порядке, что позволяет нам быть уверенными в получении получателем отправленных нами пакетов. Помимо этого, ICMP пакеты периодически рассылаются в сетях, что приводит к их большому числу и позволяет нам скрыть пакеты с сообщениями среди пакетов с любой другой информацией.

Немаловажным фактом является то, что мы можем отправлять пакеты только в рамках одной сети. Если же мы хотим отправить данные получателю, который находится в другой сети, то мы должны позаботиться о том, чтобы у нас был установлен и настроен канал для передачи данных. Сделать это можно с использованием VPN, который позволяет создать виртуальную локальную сеть или же чтобы у получателя был специальный «белый» IP адрес, который можно купить у оператора. После этого нужно настроить параметры защиты на компьютерах, чтобы обе стороны смогли видеть друг друга в сети и обмениваться пакетами.

Цель проекта – улучшить безопасность пользователей при передаче сообщений в сети интернет и сократить случаи распространения

данных пользователей третьим лицам. Поставленные задачи: позволить пользователям передавать скрытые сообщения напрямую получателю без участия централизованного узла с использованием протокола ICMP; выделение сформированных пакетов из общего потока трафика принимающей стороной; создать приложение с удобным и интуитивным интерфейсом. Для большей безопасности, а именно подтверждения целостности данных и аутентификации, пользователями могут быть использованы криптографический алгоритм RSA и алгоритм создания цифровой подписи на его основе. Это позволит участникам быть уверенными, что данные пришли в неизмененном варианте и от отправителя. Ближайшими аналогами проекта являются приложенияThunderbirdc пакетом Enigmail, Signal, Telegram, Viber и другие.

Thunderbird позволяет передавать подписанные и зашифрованные сообщения по электронной почте, но он имеет избыточный для нас функционал. Недостатком является отсутствие анонимности, потому что использует аккаунт электронной почты. То же можно сказать и про Signal, Telegramи Viber требующих номер телефона для создания аккаунта. Несмотря на их функционал эти приложения не гарантируют анонимности и регулируются центральным узлом. В нашем же случае не требуется персональных данных о пользователе. Для идентификации в сети будут использоваться криптографические ключи.

Наше приложение будет работать по следующему алгоритму: создается пара RSAключей для всех пользователей, проверяется наличие получателя в сети, сообщение шифруется и подписывается, разбивается на пакеты и отправляется в сеть, получатель проверяет входящие ICMPпакеты и извлекает только необходимые, при получении последнего пакета он собирает зашифрованное сообщение, проверяет подпись и расшифровывает сообщение.Разработка приложения осуществляется на ОС UbuntuLinux в среде PyCharmCommunity, используя ЯПPython, библиотекиScapy, RSA, SOCKETи СУБД SQLite.

ЛИТЕРАТУРА

1. ScapyDocumentation Release 2.5.0 / Philippe Biondi [and the Scapy community.]: 2023. – 221 с.

2. Рябко, Б.Я. Криптографические методы защиты информации: Учебное пособие для вузов. – 2-е издание, стереотип / Б.Я. Рябко, А.Н. Фионов. – М.: Горячая линия-Телеком, 2012. – 229 с.: ил.

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