УДК 004.056.55

Д. М. Маратов
Учреждение образования «Барановичский государственный университет», Барановичи

ЗАШИФРОВАННАЯ СЕТЬ ДЛЯ АНОНИМНОЙ КОММУНИКАЦИИ СЕТЕВЫХ ПРИЛОЖЕНИЙ

Введение. Интернет — инфраструктура, предоставляющая услуги для сетевых приложений, является самой масштабной инженерной системой построенной человеком. По своему строению Интернет-это глобальная сеть, состоящая из иерархически построенных, связанных между собой более мелких сетей, откуда и название Интернет, т.е сеть из сетей. Сегодня Интернет используется во всех сферах деятельности в таких как медицина, банковское дело, в повседневной жизни каждого человека. Данная технология развивается экспоненциально быстро, но существует проблема в данной технологии, которая берёт своё начало еще с предшественника технологии Интернет, прородитель интернета Арпанет, первая компьютерная сеть, основанная на технологии packet — switch [1].

Основная часть. Технология packet — switch была придумана в университете MIT, и первая компьютерная сеть была создана между Стендфордским университетом, и университетом MIT в 1969 году, и данная сеть была названа Arpanet. Проблема заключается в том, что Интернет базируется на идеях первой компьютерной сети Arpanet, та в сваю очередь разрабатывалась как «компьютерная сеть взаимно доверяющих друг другу пользователей», После того как Arpanet начал разрастаться из маленькой сети между двумя университетами в более глобальную сеть состоящую из различных организаций и персональных компьютеров обычных пользователей, Arpanet превратился в сеть из сетей, что и является Интернетом каким мы его знаем. Но сеть Интернет с самого начала не намеревались сделать безопасной. Отсутствие безопасности в Интернет стало причиной многих проблем связанных с утечкой пользовательских данных, с воровством коммерческой тайны организаций. Представьте если бы был способ сделать Интернет немного безопаснее? Например, сделать трафик конфиденциальным. Представьте если бы была зашифрованная сеть в Интернет где все данные пролетают по сетям в зашифрованном виде, и владельцы этих данных неизвестны, почти что полная безопасность. Именно для решения данной проблемы и была разработана зашифрованная сеть, пиринговая сеть в которой трафик перенаправляют сами устройства такие как смартфоны, компьютеры, те они служат как в каком-то смысле роутеры, и трафик, который они передают является полностью зашифрованным. Данная сеть в итоге была названа ratnet.

Основная идея ratnet это использование собственного протокола коммуникации, которая называется ratp. Протокол ratp состоит из последовательности сообщений, и алгоритмов шифрования таких как RSA и AES в режиме GCM [2]. Ниже будут приведены типы сообщений.

Сообщение "/* hell0 fri3nd */\n" — является сообщением для начального рукопожатия между двумя пирами, т.е устройствами такими как смартфоны, ноутбуки, компьютеры и т.д. Данное сообщение может иметь при себе публичный ключ RSA для дальнейшего шифрования коммуникации при помощи этого ключа.

Сообщение "/* I have a gift */\n" — является сообщением для передачи ключа блочного алгоритма шифрования AES, ключ передается в зашифрованном виде. Шифруется ключ алгоритмом RSA публичный ключ которого был передан на этапе начального рукопожатия.

Сообщение "/* I appreciate that */\n" — является сообщением, подтверждающим получение AES ключа.

Сообщение "/* I need fri3nds */\n" — является запросом для создания цепочки соединений между пирами, или узлами сети. Цепь из пиров необходима для того чтобы анонимно перенаправлять трафика через эту сеть.

Сообщение "/* You're welcome */\n" — является подверждением создания цепочки из пиров, и теперь дальнейшая коммуникация будет проходить через эту цепь.

Сообщение "/* Be fri3nds */\n" — является запросом одного пира другому для создания цепь из пиров.

Сообщение "/* We're friends */\n" — является подтверждением одного пира другому что он согласен участвовать в цепи.

Сообщение "/* Your data */\n" — является сообщением к которому прикреплены зашифрованные данные которые мы хотим перенаправить через созданную сеть из пиров.

Сообщение "/* We're done */" — является сообщением об окончании коммуникации.

На основе этого протокола было написано простое приложение, которое скачивает файлы через зашифрованную сеть используя протокол ratp и протокол http. Данное приложение называется bivittatus, и оно просто скачивает файлы из интернета через других пиров.

Как видно при помощи программы bivittatus была скачана часть видеофайла под нвазванием segment-1-v1-a1.ts. Ниже будет приведен скриншот работы сервера, который отвечает за логирование пиров в сети, т.е сервер записывает какие пиры подключились к сети (рисунок 1).

Рисунок 1 — Сообщения сервера о ходе выполнения операции

Заключение. Разработанный протокол, при помощи которого можно создать зашифрованную сеть, в которой узлами являются сами устройства, по-другому известные как пиры служит для зашифрованного соединения пользователей. Эти узлы отвечают за то как будет перенаправлен трафик по сети, и весь трафик является SHA-шифрованным что делают эту сеть конфиденциальной для приложений, которые будут ее использовать.

Список цитируемых источников

1. Packet-switching [Электронный ресурс]. — Режим доступа: https://www.techopedia.com/definition/5603/packet-switching. Дата доступа: 21.02.2019
2. Язык GO [Электронный ресурс]. — Режим доступа: https://www.ibm.com/developerworks/ru/library/l-go_01/index.html. Дата доступа: 21.02.2019

УДК 004.42

Е. А. Миронович
Учреждение образования «Барановичский государственный университет», Барановичи

БАЛЛИСТИЧЕСКАЯ СОСТАВЛЯЮЩАЯ В МИНИ-ПРИЛОЖЕНИЯХ

Введение. Изучая баллистику, учащиеся повторяют основные теоретические положения и законы кинематики, а также исследуют и выводят новые закономерности, которые можно и даже необходимо проверять на опыте.

Баллистика — наука о движении снарядов, мин, пуль, неуправляемых ракет при стрельбе (пуске). Основные разделы баллистики: внутренняя баллистика и внешняя баллистика. Внутренняя баллистика изучает движение снарядов, мин, пуль и др. в канале ствола оружия под действием пороховых газов, а также другие процессы, происходящие при выстреле в канале или камере пороховой ракеты. Основные разделы внутренней баллистики: пиростатика, изучающая закономерности горения пороха и газообразования в постоянном объёме; пиродинамика, исследующая процессы в канале ствола при выстреле и устанавливающая связь между ними, конструктивными характеристиками канала ствола и условиями заряжания; баллистическое проектирование орудий, ракет, стрелкового оружия.

Внешняя баллистика изучает движение неуправляемых объектов (снарядов, мин, пуль, неуправляемых ракет и др.) после прекращения их силового взаимодействия со стволом оружия (пусковой установкой), а также факторы, влияющие на это движение. Основные разделы внешней баллистики: изучение сил и моментов, действующих на снаряд в полёте; изучение движения центра масс снаряда для расчета элементов траектории, а также движение снаряда относительно центра масс с целью определения его устойчивости и характеристик рассеивания. Разделами внешней баллистики являются также теория поправок, разработка методов получения данных для составления таблиц стрельбы и внешне баллистическое проектирование [1].

Основная часть. Цель данного исследования заключается в разработке игры «Катапульта» с использованием баллистики. Данная игра позволяет игрокам ходить по очереди. Игра заканчивается, когда один из игроков попадёт камнем в катапульту противника. Основной задачей является написание простейшего кода, который рассчитывает баллистическую траекторию падения камня.

Для реализации данной работы выбрана интегрированная среда программирования Builder 6.0, как наиболее мощная реализация языка программирования Object C++ с возможностью написания программ как под DOS, так и под операционные системы Windows 95/98/2000 и NT. Для простоты освоения программы необходимо создать удобный интерфейс, который является визитной карточкой приложения.