1. Министерство образования и науки Российской Федерации
2. Санкт-Петербургский Политехнический Университет Петра Великого
3. —
4. Институт кибербезопасности и защиты информации

**ЛАБОРАТОРНАЯ РАБОТА № 3**

1. «РАСПРЕДЕЛЕННАЯ СИСТЕМА СБОРА ИНФОРМАЦИИ»
2. по дисциплине «Безопасность современных информационных технологий»
3. Выполнил
4. студент гр. 4851003/00002 Вологдин М.В.

<*подпись*>

1. Преподаватель Дахнович А.Д.

<*подпись*>

1. Санкт-Петербург
2. 2022
3. **Цель работы**

Получить навыки организации параллельной обработки большого количества клиентских соединений при помощи механизма портов завершения Win32. Получить навыки реализации шифрования передаваемых данных при помощи средств CryptoAPI. Получить навыки извлечения информации о системе.

Разработать распределенную систему сбора информации о компьютере, состоящую из сервера и клиента, взаимодействующих через сокеты.

1. **Ход работы**

Была разработана архитектура системы сбора информации. Клиент играет роль центрального компьютера, собирающего информацию с серверов, он же инициирует передачу информации. Сервер же непрерывно работает и ожидает входящие подключения, сервер - stateless, так как для каждого запроса происходит процедура обмена ключами, и после отправки информации соединение закрывается.

Клиент запрашивает у пользователя ip и port для подключения, далее ожидает ввод номера запроса, для 7 и 8 пунктов также требуется ввод пути папки/файла/ключа реестра. Полученная информация записывается в файл log.txt.

Обмен информацией между клиентом и сервером происходит в зашифрованном виде, для этого используется встроенная библиотека <wincrypt.h>.

Схема шифрования с использованием сеансового ключа:

1) Клиент генерирует асимметричный ключ–пару ключей публичный/приватный

2) Клиент посылает публичный ключ серверу

3) Сервер генерирует сеансовый ключ

4) Сервер получает публичный ключ клиента

5) Сервер шифрует сеансовый ключ публичным ключом клиента и отправляет получившееся зашифрованное сообщение клиенту

6) Клиент получает зашифрованное сообщение и расшифровывает его с помощью своего приватного ключа

7) У клиента и сервера есть сеансовый ключ. Теперь можно использовать симметричное шифрование для защищенного обмена сообщениями

Сеансовый ключ использует алгоритм симметричного шифрования RC4, а пара ключей, использующаяся для первоначальной передачи сеансового ключа, использует асимметричное шифрование RSA.

1. **Тестирование**

На рисунке 1 можно увидеть, что пакет, передаваемый от клиента к серверу, содержит 2 байта информации – зашифрованный номер запроса и символ переноса строки, означающий конец сообщения.

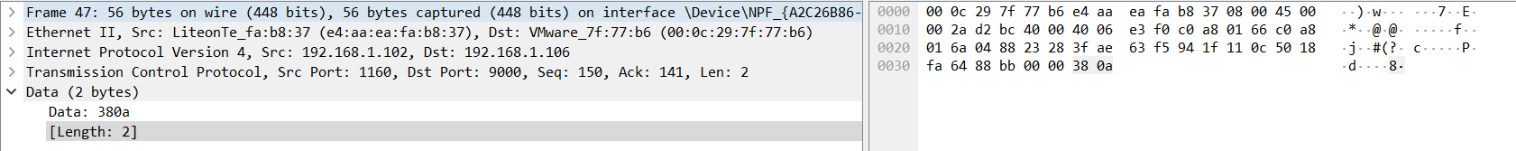


Рисунок 1 – Подтверждение шифрования передаваемых сообщений

Тестирование программ проводилось для каждого типа запроса. Последовательно отправлены запросы с номерами 1-8, в пунктах 7-8 указывался путь C:\Users\Matvey\Desktop\test. В результате в файле log.txt была записана информация, которую можно увидеть на рисунке 2.

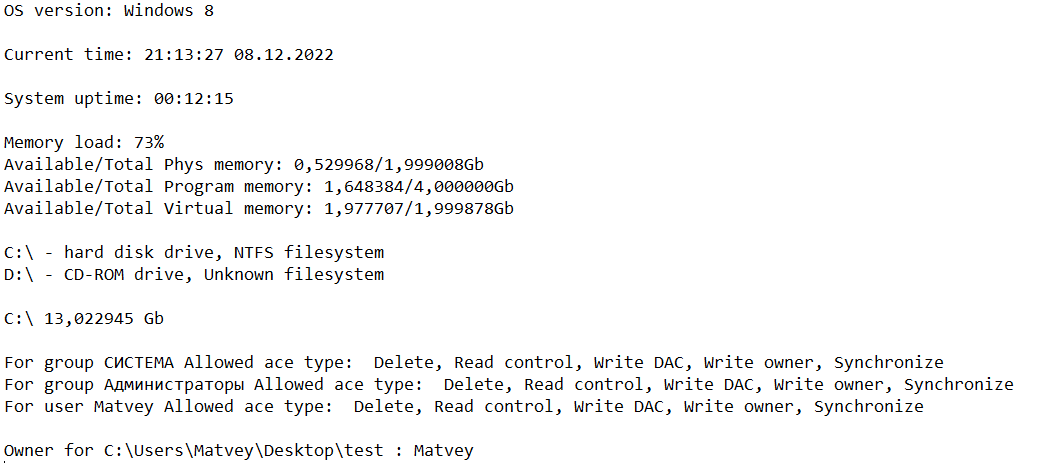


Рисунок 2 – Результаты работы программы

1. **Контрольные вопросы**
2. Какова структура списков контроля доступа в ОС Windows?

typedef struct \_ACL {

**BYTE AclRevision;** Указывает уровень редакции ACL.

**BYTE Sbz1;** Указывает нулевой байт заполнения, который выравнивает член AclRevision по 16-битной границе.

**WORD AclSize;** Определяет размер ACL в байтах.

**WORD AceCount;** Указывает количество записей ACE, хранящихся в ACL.

**WORD Sbz2;** Задает два нулевых байта заполнения, которые выравнивают структуру ACL по 32-битной границе.

} ACL;

1. Что такое наследование прав доступа?

Механизм, при котором права доступа субъекта к объектам настраиваются с учетом прав родительского субъекта

1. Для чего используются well-known SID?

Есть стандартные так называемые well-known SID для пользователей и групп. Они имеют один и тот же SID на любых системах (например, группа Everyone или пользователь System).

1. Как выглядит схема шифрования с использованием сеансового ключа?

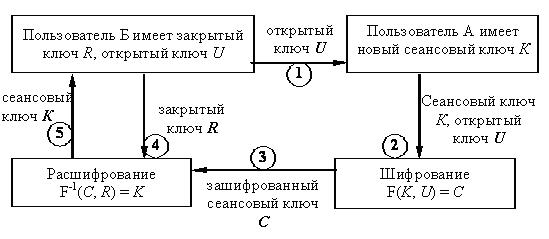


Рисунок 3 – Схема шифрования с использованием сеансового ключа

1. В чем преимущества использования сеансового ключа?

Сеансовый ключ обеспечивает секретность одного диалога: если он попадет под угрозу, будет нарушена конфиденциальность одного сеанса, но не всей системы в целом. Быстро, периодически генерируется.

1. **Выводы**

В ходе работы были получены навыки работы с портами завершения, позволяющими обрабатывать несколько клиентских соединений, были получены навыки реализации шифрования передаваемых данных при помощи средств CryptoAPI, также получены навыки извлечения информации о системе. Была реализована своя система сбора информации.