VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta informačních technologií

ISA 21/22

Secret client/server application
PROJECT DOCUMENTATION

Vladyslav Tverdokhlib

(xtverd01)

Brno, 15.11.2021

TABLE OF CONTENTS

INTRODUCTION TO THE PROBLEMATIC

Networks are transparent these days. The package can get to third parties. It is getting harder and harder to maintain the confidentiality of data. One way to communicate securely and privately on the network is to encrypt data.

The task was to create an application for encrypted communication server-client through the ICMP protocol. It is divided into two parts:

1. Client implementation.
The application must support transferring large files (1500B+).
Transmitted data must be encrypted before sending.

2. Implementation of listening for the server.
The server must listen to the protocols of the ICMP and receive addressed packets.

DESCRIPTION OF IMPLEMENTATION

Sending packets from the **client** side occurs thanks to the *BSD sockets* library:
Producing the resolution of the host to which the data will be sent.
Creating a socket.
Reading a file to send.
Encrypting and sending data by splitting traffic into packets.
The maximum size of one IP packet must not exceed 1500B.

To achieve correct data transfer, the *TRANS* protocol was created.
-tagline - a tag for marking a packet.
-type – for sending various data (metadata and data).

Listening from the **server** side goes thanks to a *pcap*. The implementation was based on ISA examples.