Bezpieczeństwo Systemów Komputerowych
Security of Computer Systems

Project 1

Data encryption with session key transfer - a protocol for sending messages with a session encryption key

Version 1.0, Gdańsk, 2020

Main project tasks:

- the analysis of project assumptions,
- propose and implement the communication protocol,
- project the application GUI,
- perform test of the application,
- prepare the report.

1. The goal of project classes and the rules

The main goal of the 1st project is to familiarize the student with a method of sending the encrypted messages – data files or text messages. During the transmission process a session key must be generated and securely transmitted to the other user. The project is marked regarding the rules:

- Timely and correct realization of the project – 21 points.
- Technical report – 8 points.
- Presentation the project of the GUI interface and partially working application (in a given control term) – 1 point.

The control and submission terms are pointed during the lecture. In a case when the project will not be submitted before the deadline, the final chance of submission will be in September, during the 2nd exam session, 14-18.09.2020.

2. Project tasks

The main task of the project is to design and program an application to cipher text messages and data files and then send them by using the Ethernet network. In general, the application must take a form of a network secure communicational tool. The application must allow sending and receiving the ciphered data and messages on both sides of communication. It means that user A have the application, and so does the user B. They can send each other ciphered text messages and files.

Before the transmission user A and B must exchange their public keys, they will be used for secure session key exchange.

During project realization and submission presentation the application must be executed on two physical computers, or on a physical computer and a virtual machine. In the Fig. 2.1 a sample block diagram of the data flow between the applications was

presented. For the communication purposes the network should be configured as the host-only adapter in the VirtualBox. The IP addresses should be configured by the user manually from a reasonable range, e.g. 192.16.0.1 / 192.168.0.2.

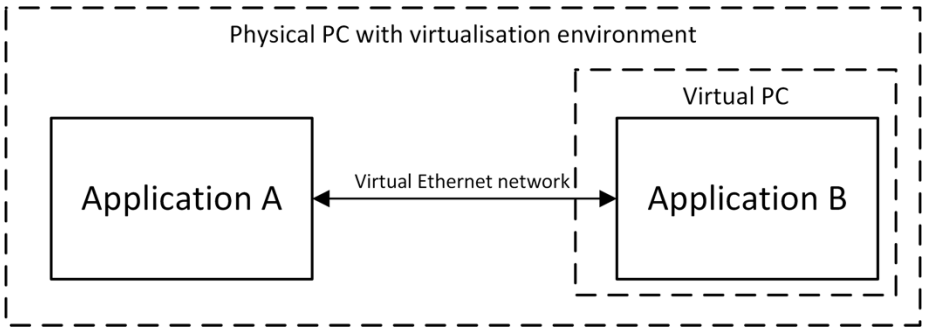

Fig. 2.1 Block diagram of the data flow between the applications.

Requirements:

- The GUI interface must allow to type and send a text message to the other user. Besides the text also an ability of sending any files (e.g. *.txt, *.png, *.mp3, *.avi, itp.), with any size (from 1kB to more that 100 MB) must be implemented. A test files are given by the teacher.
- It is obligatory to implement one of the block ciphers (AES, 3DES).
- It is obligatory to implement all four modes of operation of the block ciphers (ECB, CBC, CFB, OFB), one mode will be selected by the user in the GUI.
- For the CFB and OFB modes the size of the size of the block must be the power of 2.
- It is obligatory to implement a progress bar presenting the progress of sending the large files.
- For large files a method of data division must be implemented before sending them via the Ethernet interface.
- A UDP (*User Datagram Protocol*) or TCP (*Transmission Control Protocol*) communication protocol must be used to send the data between the mashines.
- When the UDP protocol was used a data loss exceptions must be handled.
- A pseudorandom generator must be used to generate the session key. The input data for the generator must be taken “from the environment” (system time, HDD disk sector, mouse position).
- The session key must be encrypted by using the RSA public key of the receiving person and send to the receiving person.

- The public and private keys must be stored separately (e.g. in a different directories). The keys must be encrypted by using the block cipher operating in the CBC mode. The encryption key is the hash (generated by using the SHA-1, SHA-256 function) of the user-friendly password.
- It is allowed to use the available implementations of the block ciphers, RSA encryption.
- In a case of unauthorized decryption (e.g. using an incorrect password) the decryption process should be done with no notification to the user and as a result of the decryption process a pseudorandom data will be obtained.
- In the report the results of performer tests must be included.

Notes:

During realization of the project it is obligatory to generate the following keys:

- session key (used for data encryption),
- private and public keys of the users (used for secure transmission of session keys),
- access key (typed by the user) which hash will be used to encrypt the private RSA key to store it on the hard disk.

The proposed communication protocol must allow the transmission of the encrypted session key (by using the RSA key) besides the transmission of the data (encrypted by the session key). It must be remembered that also the parameters of the cipher (algorithm type, key size, block size, cipher mode, initial vector) must be send (in a secure way) to the 2nd user to allow the correct reception of the encrypted data.

The project report must contain a description of the applications' GUI interface, description of communication protocol and results of performed tests. Additionally, an algorithmic description of the program must be done. The report must be based on a given template.

Only one submission term is planned per project. In a case of obtaining insufficient number of points to obtain a positive mark, a 2nd term to submit the project

is proposed, but in that case totally 60 % of points can be obtained. The second submission is possible only in **14-18.09.2020**.