Communication and Information Security - Assignment 3

תאריך הגשה: 06/07/19

מגישים
דניאל שפר, ת.ז. 301015574, הנדסת תוכנה זוהר קורנבלום, ת.ז. 306267915, הנדסת תוכנה נתנאל גינזבורג, ת.ז. 305091357, הנדסת תוכנה

מעקב שעות

שם הסטודנט	**משימה**	**כמות השעות**
דניאל שפר	תהליך זיהוי בין המשתמשים ושליחת קבצים	16
זוהר קורנבלום	GUI שרת + קוד צד שרת	16
נתנאל גינזבורג	GUI שרת + קוד צד שרת	16
	סה"כ שעות:	48

Instructions for compiling the source code for SCAFTIA:

1. Open IntelliJ IDEA.
2. Load the SCAFTIA project.
3. In the upper bar choose “Run” and from the menu click “Run…” and choose which class to run.

Instructions for compiling the source code for SCAFTIA Server:

1. Open IntelliJ IDEA.
2. Load the SCAFTIA Server project.
3. In the upper bar choose “Run” and from the menu click “Run…” and choose which class to run.

Instructions for running the SCAFTIA program

To run the SCAFTIA program double click on the SCAFTIA.jar.
After the program starts, the first thing to do is to set the settings of the program by clicking on the “Edit Settings” button on the lower-right of the program, the settings section will become editable.
Add / Remove Neighbors: in order to add neighbor there are 2 text fields “Neighbor Name” and “IP:Port”. After typing a neighbor info, click on the “Add Neighbor” button to add the neighbor to our neighbors list. In order to remove a neighbor select a neighbor from the neighbors list and click on the button “Remove Neighbor”.
Shared Password: enter the shared password that was agreed between the users.
My Port: a port that the program will listen to, and that the neighbors will add to your IP in order to communicate with you.
MAC Password: enter the mac password that was agreed between the users.
Added to SCAFTIA:
Private Password: a private password of the current user that is for the file transfer process.
Server Address: the IP:Port of the SCAFTIA authentication server.

After finishing to edit all the settings, click on the “Save Settings” button in order to save the settings.
Before connection a user name must be entered.
Custom Messages: custom messages to the server and neighbor during file transfer authentication.

Instructions for running the SCAFTIA Server program

To run the SCAFTIA program double click on the SCAFTIA_Server.jar.
After the program starts, the first thing to do is to set the settings of the program by clicking on the “Edit Settings” button on the lower-right of the program, the settings section will become editable.
Add / Remove Users: in order to add user to the server there are 2 text fields “Username” and “Password”. Then click on the “Add User” button to add the user to server user list. In order to remove a user select a user from the user list and click on the button “Remove User”.
Shared Password: enter the shared password that was agreed between the users.
MAC Password: enter the mac password that was agreed between the users.
Server Listening IP and Port: an IP and Port that the program will listen to.

After finishing to edit all the settings, click on the “Save Settings” button in order to save the settings.
Before connection a user name must be entered.
Custom Responses: custom responses to the users.

Documentation of how the SCAFTIA tool implements the Needham-Schroeder protocol and uses session keys. If you modified the communication protocol from your assignment 2 submission, you must fully document it here as you did for assignment 2.

Once the sender of the file gets "OK" message from the receiver, the sender sends a message to the server in order to start the authentication process, so the communication protocol has not been modified.

The communication with the server is handled in a dedicated thread, and after that the process continues between the neighbors on a random port that the receiver sent to the sender.

We have added headers to the messages from message 5 to message 9, the headers are:

TOKEN, CHALLENGE, RESPONSE, OK, FILE_TRANSFER

For example the Token message will have this form: <TOKEN_HEADER> <Ks> <sender name>

The header are used to determine which message is received and how to handle it.

Documentation of how the server works, stores user information, and generates session keys.

Once the user decided on an IP and Port to listen to and press "Start Server" the server begin to listen to messages.
The server GUI has a TextArea in which the user can see incoming communication and errors.
The server stores the user information in an INI file, just like SCAFT, SCAFTI and SCAFTIA.
The users section is in the following form: <Username>=<Password>
The password is saved in a format of Byte-to-String, like this:
alice = -115_-106_-98_-17_110_-54_-45_-62_-102_58_98_-110_-128_-26_-122_-49_12_63_93_90_-122_-81_-13_-54_18_2_12_-110_58_-36_108_-110_

We used SecureRandom in order to generate a 32byte session key.

The server has a log file that contains information about the activity of the server, a message in the log has the following form:

[07:33:05] Valid Message::
    Sender: daniel (10.0.212.17)
    Recipient: zohar
    Nonce: 1562257985644
    Error: No Error
    Encryption: No
    Response Sent: Sent
    Fake Response: Not Fake

SCAFTIA Configuration File:

The SCAFTIA program uses an .INI file as configuration file, built as follows:

```
[MyPort]
Port = 444

[MACPassword]
Password = kinneretMAC

[SharedPassword]
Password = kinneret

[Neighbors]
10.9.22.142 = 444
```

SCAFTIA Server Configuration File:

The SCAFTIA Server program uses an .INI file as configuration file, built as follows:

```
[Server IP\:Port]
IPPort = 0.0.0.0\:333

[Passwords]
MacPassword = kinneretMAC
SharedPassword = kinneret

[Users]
alice = -115_-106_-98_-17_110_-54_-45_-62_-102_58_98_-110_-128_-26_-122_-49_12_63_93_90_-
122_-81_-13_-54_18_2_12_-110_58_-36_108_-110_
```