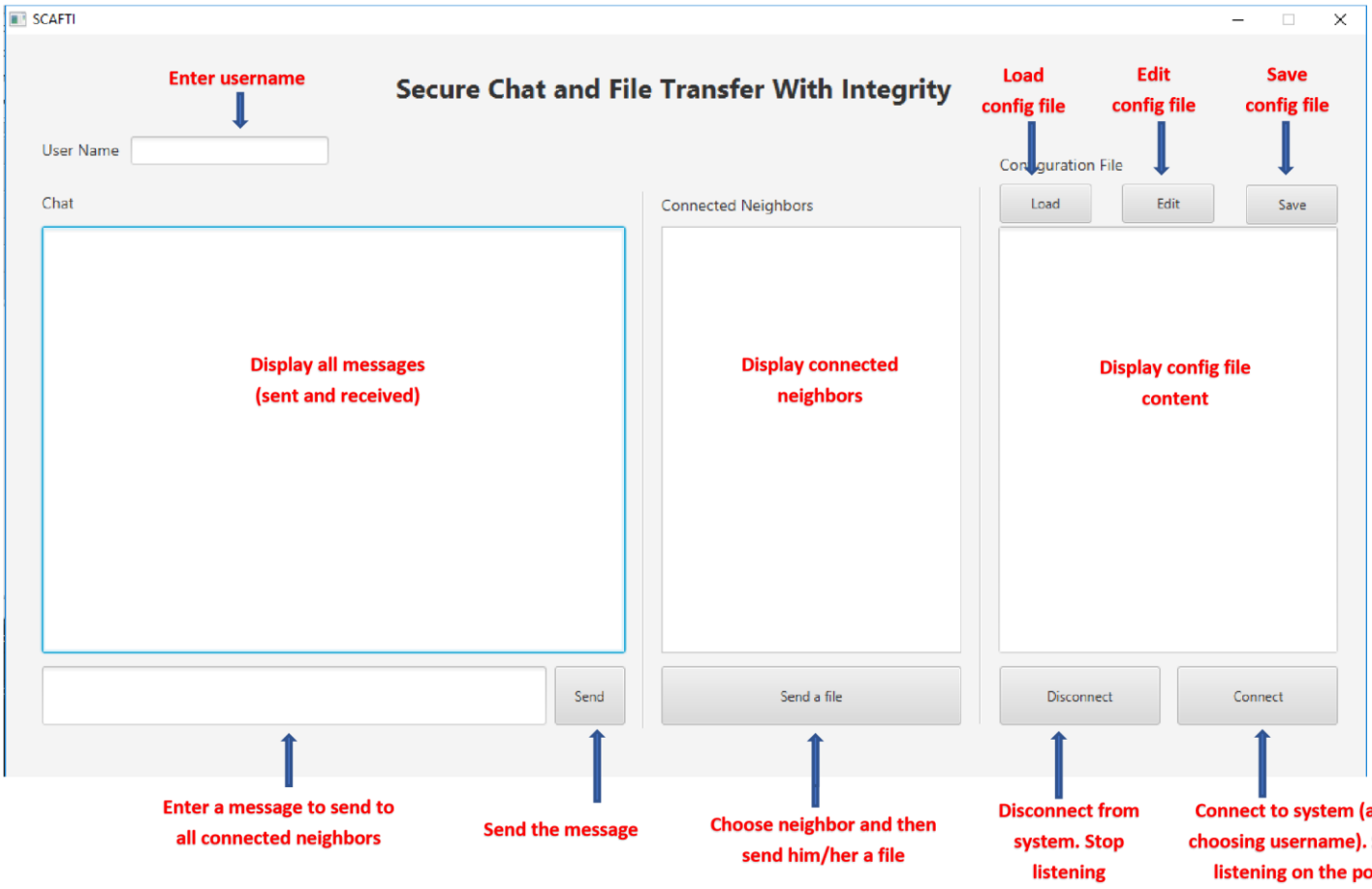
Instructions for compiling the source code for SCAFTI:

1. Open SCAFTI project using IntelliJ.
2. Press on the Run icon (green triangle).

Instructions for running the SCAFTI programs:



Documentation of the communication protocol:

Message formats:

1. HELLO message - HELLO Username IP Port
2. BYE message - BYE Username IP Port
3. OK message - OK Username IP Port MessageContent
4. NO message - NO Username IP Port MessageContent
5. MESSAGE message - MESSAGE Username IP Port MessageContent
6. SENDFILE message - SENDFILE Username IP Port FileName
7. ACK message – ACK Username IP Port Message
8. FAILED message – FAILED Username IP Port Message

Finally: we encrypt the message and send it with the corresponding IV and HMAC-SHA256 digest.

For example: Encrypt(HELLO Username IP Port)-IV-digest

4a28b97db2e4-fa45d46bafad4cd46e5b4a28b97db2e4

Encrypt/Decrypt messages and integrity explanation:

Encryption:

1. Generate key – get password from config file, encode it using UTF8 encoding and then hash it with SHA256 algorithm.
2. Generate random IV – each sending we create new random IV (128 bits).
3. Encryption using AES/CTR.

Decryption:

1. Parse the encrypted incoming message by splitting it by "-" character. First section is the message and the second is the IV.
2. Generate key – get password from config file, encode it using UTF8 encoding and then hash it with SHA256 algorithm.
3. Decryption using AES/CTR.

Integrity:

1. Generate key – get password from config file, encode it using UTF8 encoding and then hash it with SHA256 algorithm.
2. Calculate digest using HMAC-SHA256 algorithm.

How SCAFTI parses the messages:

The SCAFTI tool listens to incoming messages on the port from the config file. When received a new message, SCAFTI calculate the digest of the IV concatenated to the encrypted message, and finally decrypt the message. SCAFTI compare the calculated digest to the received digest -> if the comparison is false, i.e. the message is corrupted or the key is wrong, SCAFTI does not show the incoming message, displays an error message about the corrupted message and writes it to the log.
SCAFTI parse the decrypted output by splitting it by " "(space) character.
SCAFTI takes the information from the parsed message according to the formats we described above.

How the SCAFTI tool reacts to the different messages:

1. HELLO message – if the sender of the message isn't in the connected neighbors list add the sender to the connected neighbors list, and send HELLO message back. Displays an appropriate message
2. BYE message – delete the sender of the message from the connected neighbors list. Displays an appropriate message.
3. OK message - displays a message that the receiver accepted the file.
4. NO message - displays a message that the receiver refused to accept the file.
5. MESSAGE message – display the message content in the chat.
6. SENDFILE message – display a message to the user that someone wants to send a file to him, and wait for the user to answer. According to the user answer – send back OK or NO message.
7. ACK message – displays a message that the receiver received the file successfully.
8. FAILED message – displays a message that the receiver did not receive the file because the file is corrupted.

File Transfer Explanation:

After sending a SENDFILE message and receive OK message back:

- Encrypt the file:
    - Generate key and random IV (see Encrypt/Decrypt messages explanation). ○ Encode the file name using UTF8 encoding and encrypt it.
    - Read all file bytes, encode the bytes using BASE64 encoding and encrypt them.
- Calculate the digest of the IV concatenated to the encrypted file.
- Encrypted file looks something like this:
  Encrypted(ip:port)-Encrypted(file name)- Encrypted(file content)-IV-digest
- After encrypting, we set up a new socket with another port and sending the encrypted file.
- The receiver listens to the same port, receive the encrypted file, calculate the file's digest, compare the calculated digest to the received digest -> if the comparison is false, i.e. the file is corrupted or the key is wrong, SCAFTI does not save the incoming file, displays an error message about the corrupted file and writes to the log. Finally, SCAFTI decrypt the file in a similar way.
- If the file is corrupted SCAFTI displays an error message, and the receiver does not receive the file.
- SCAFTI ask the user to choose location to save the file – with the original name.

- If a file with the same name already exists, SCAFTI ask the user if he/she wants to overwrite:
    - If the user says yes – overwrite, and save the new file in the selected location.
    - If the user says no – abort.

Log File:

- The name of the log file is *SCAFTI-Logger.log.*
- The location of the log file is the same as the location you open the SCAFTI tool.
- The format of the log file, all in one line:
  [2019-05-28 09:13:51]
  INFO - Received Message –
  ip: 10.0.201.22, port: 4200,
  name: Alice, type:
  MESSAGE, message: new
  message,
  iv: EB4328BE1F44E7FA1187B30B50CA7559,
  hmac: F61AE9B5C4D61D4C30CB40CCBFD3DAECDD323C127C861F95B634EFE1FA6BDF6A,
  valid: TRUE