UNIVERSITÀ DI PISA

Computer Engineering

Foundations of Cybersecurity

secureCom

Group Project Report

TEAM MEMBERS:
Francesco Iemma
Yuri Mazzuoli
Olgerti Xhanej

Academic Year: 2020/2021

Contents

Chapter 1

How To Handle The Chat Request

1.1 General Part

Client asks the server to chat with someone:

- The standard channel is used to send either the request for chat and for the server's answer
- If the target client accepts then the main process receive the confirmation from the server, then the main process set isChatting to true and it starts to chat.

The tricky part deals with the chat request that comes from another client.

Server asks the client (Alice) if she wants to chat with another client (Bob)

- The request must be done through the request channel
- The daemon process read isChatting, if it is true the daemon process refuses automatically the server request, otherwise it ask (HANDSHAKE) to the main process if he wants to speak with Bob.
- The main process answer to the server through the daemon tools, if the answer is positive then it sets isChatting to true and it waits for the message from Bob

1.2 Server Side

There are two possibilities:

1. Two processes, one for the client main process and another one for the client daemon process. See figure 1.1.
2. One process, it establishes a connection with the main process of the client, then if the server has to sent a chat request to this client it establishes a connection with the daemon process of the client that works as a server process and it is listening on port 4242. See figure 1.2.
3. A third solution can be adding a command to indicate that a client is available to receive chat request. Thus:

   (a) A users is online when it has launched the command "available" (isChatting = false). Notice that in this case the variable isChatting can be called in a more correct way isAvailable.

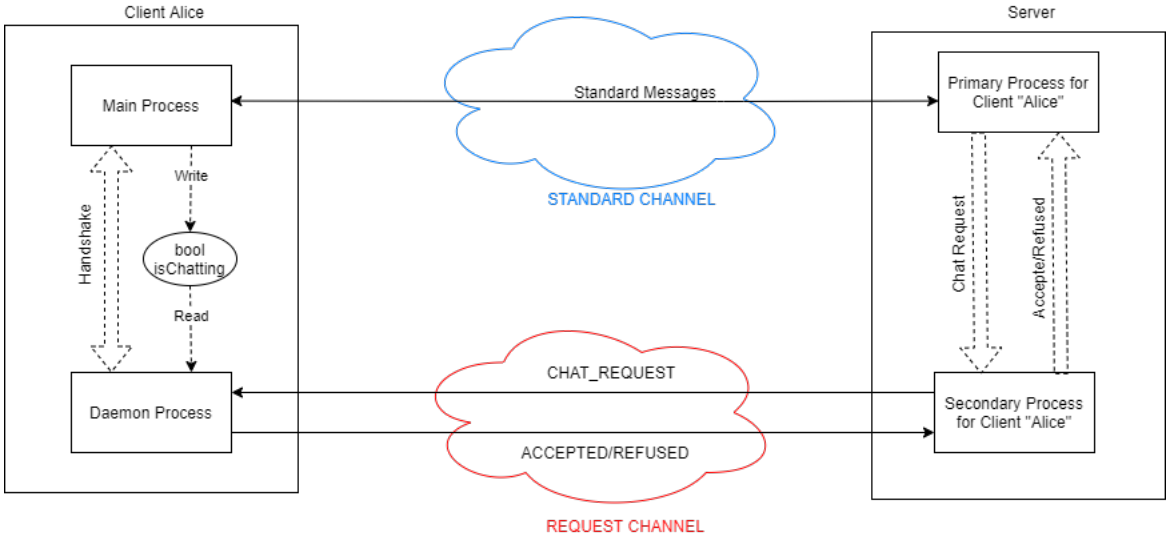

Figure 1.1: Solution with two processes

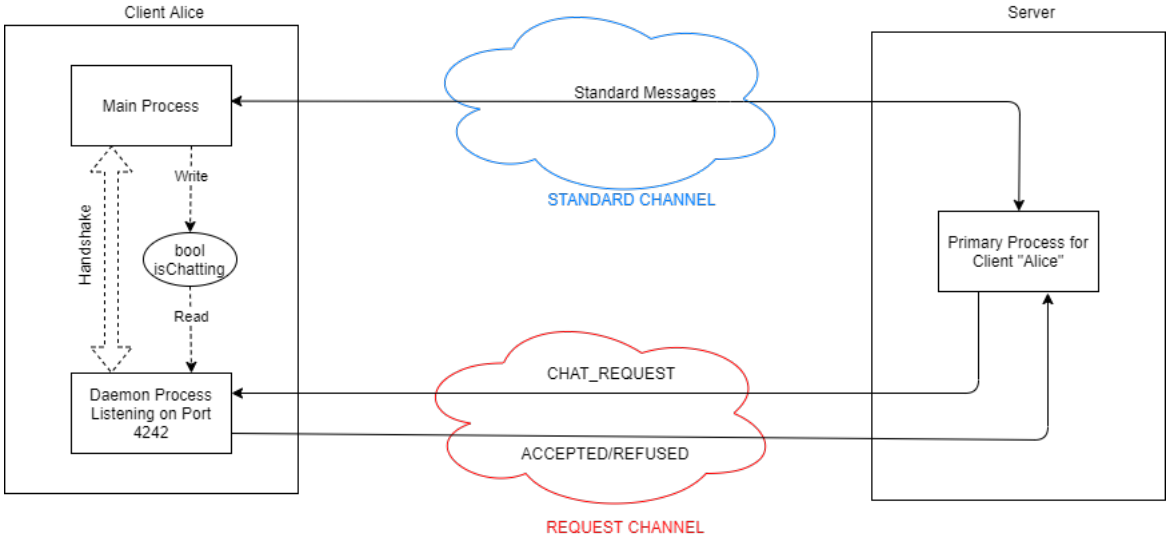

Figure 1.2: Solution with one process

(b) A users is offline (isChatting = false) if it is not available (if he has not launched the command available or if he is chatting with someone else). In that case offline means also busy whereas online means also available.

Notes:

- ASSUMPTION: who request the chat is the first to send messages
- The two processes are connected with the server with two different socket
- Server side for each client two socket must be established, one for the standard channel and another one for the request channel

The authentication problem is not present because in the request channel it is used the session key established during the preliminary phase.