Secure Game

Security of Information and Organizations Project 2

Rafael Remígio 102435
Bruno Moura 97151
João Correia 104360

January 7, 2023

Departamento de Electrónica, Telecomunicações e Informática
Universidade de Aveiro

Year 2022/2023

Introduction

The proposed assignment focuses on the develpment of a robust protocol for handling a Distributed Game. In this project worked with *Symmetric Cryptography*, *Asymmetric Cryptography*, *SmartCards and Certificates*, *Signature algorithms*.

This document will explain the implementation and the architecture of the Distributed System.

Communication Protocol

To handle communication between nodes in the network we developd a Communication Protocol. Communication is handled by the *Playing Area*. It listens and accepts connections from *Users* (Players, Callers).

Authentication and registration Process

Uses *challenge-response authentication*.

1. A User sends an Authenticate Message. With this message a user authenticates themselves to the playing area.The user sends his *Public Key*.

2. The Playing Area respondes also with an Authenticate Message containing its own *Public Key* and *Challenge* to be validated by the User.

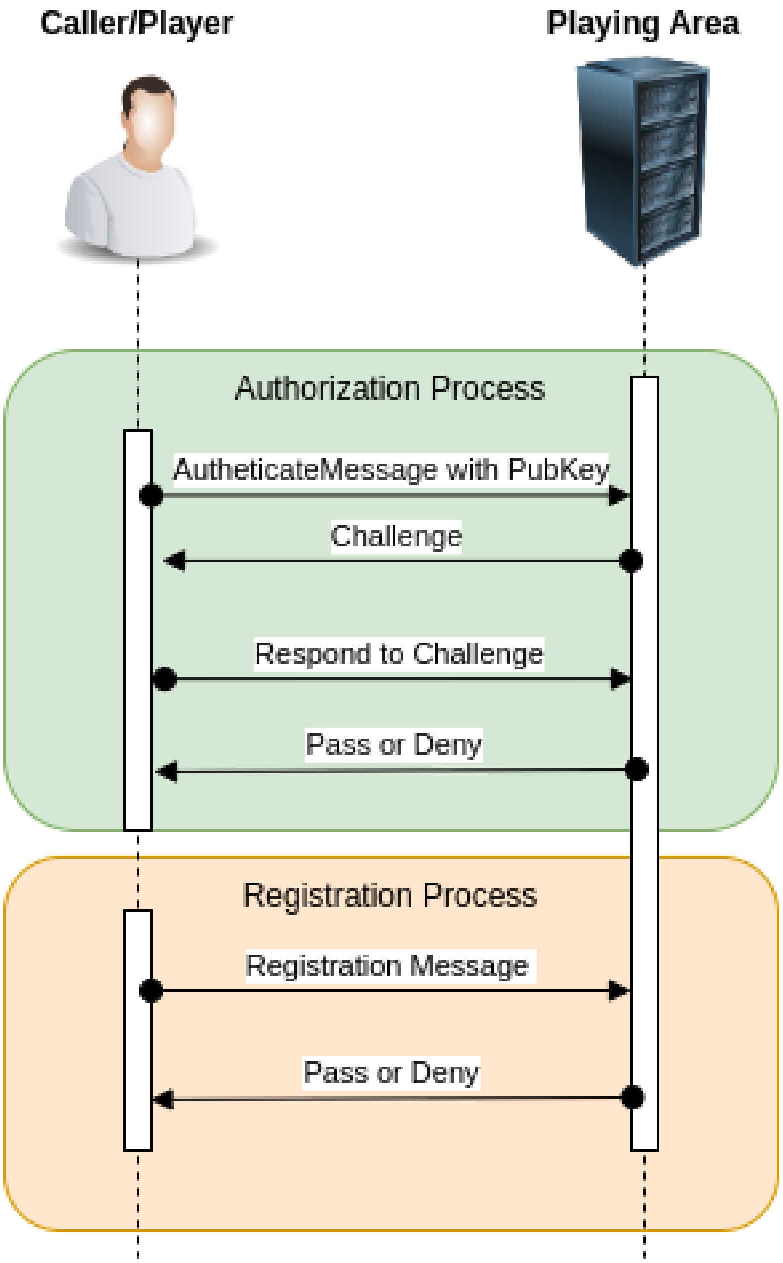
3. The User send an Authenticate Message with a response to the challenge

4. This response is validated by the *Playing Area* and if it successfully authenticates it sends a Authenticate Message with the parameter Success as True. If it does not successfully authenticate the message it **blacklists the connection**.

   With the authentication process completed the user can now register himself.

5. The User then sends a Registration Message. It constains a *nickname*, a *playing key*, an *authorization key* and *signature*.

6. The Playing Area verifies that the nickname is not taken, verifies that the User completed the authentication process, verifies the signature. If the Authorization Key belongs to a known Caller it accepts it as a Caller. Reponds with a Registration Message with the paremeter success as True or False and the sequence number corresponding to that Player.


Caller/Player
Playing Area
Authorization Process
AutheticateMessage with PubKey
Challenge
Respond to Challenge
Pass or Deny
Registration Process
Registration Message
Pass or Deny