Relatório - Jogo do Bingo

Universidade de Aveiro(*UA*)

Guilherme Mendonça Claro,
Eduardo Lopes Ferreira,
João Afonso Pereira Ferreira,
Tiago Figueira Mostardinha

VERSAO 1

Project 2 - Secure Game

Segurança Informática e Nas Organizações

João Paulo Barraca & André Zúquete

DETI - Departamento de Electrónica, Telecomunicações e Informática

Mestrado Integrado em Engenharia de Computadores e Telemática (MIECT) &

Licenciatura em Engenharia de Computadores e Informática (LECI)

Guilherme Mendonça Claro,
Eduardo Lopes Ferreira,
João Afonso Pereira Ferreira,
Tiago Figueira Mostardinha

(98432) gui@ua.pt,
(102648) edu.fernandes@ua.pt,
(103037) ferreiraafonsojoao@ua.pt,
(103944) tiago.mostardinhas@ua.pt

01/01/2023

Índice

Lista de Figuras

Capítulo 1

Introdução

A elaboração deste projeto envolveu o desenvolvimento do jogo do Bingo. Bingo é um *"game of chance"*, que usando por base sockets em Python, permite a comunicação em rede entre três entidades: **Users**, **Caller**, **Playing Area**. Este jogo consegue receber um número variável de jogadores. A todos os jogadores é lhes atribuída uma carta com numero M de números, de 1 a N, completamente aleatória. Pelo que, assim que um jogador complete os números da sua carta coincidentes com aqueles ditados pelo *Caller*, apresentados na *Playing Area*, esse jogador será declarado o vencedor pelo **Caller**(inicialmente seria apenas uma coluna de números mas foi decidido usar uma carta para obter uma maior simplicidade). Existe a possibilidade de haver mais do que um vencedor.

Para garantir a segurança, a falta de divergência e evitar fraude dos jogadores no momento da criação e repartição das cartas pelos vários jogadores, considerou-se que cada jogador cria a sua própria carta, baralhando os números disponíveis no baralho disponibilizado pelo **Caller**e, de seguida, é "lançada"a carta para a **Playing Area**.

Os números do baralho não irão ser ditados um a um pelo **Caller** até que um dos jogadores seja declarado um vencedor. Ao invés disso o **Caller** envia os N números disponíveis do baralho, já baralhado, e assim cada jogador é capaz de determinar o(s) vencedor(es) assim que completem a sua carta na menor quantidade de números enviados pelo *Caller*, dependendo da ordem. Deste modo, no final do jogo, todos os jogadores poderão concordar quem é vencedor ou não.

É de notar que nenhuma das entidades tem acesso completo sobre o jogo. Os jogadores conseguem detetar se o *Caller* não enviou com N números baralhados, se receberam um cartão invalido, se um jogador enviou uma mensagem errada ou então se ditou os números errados para um determinado jogador , entre outros ...

Para a realização deste projeto utilizou-se, como recurso, várias fontes, entre elas os slides estudados nas aulas teóricas, o trabalho realizado nas aulas práticas da Unidade Curricular (UC)r de Segurança Informática e Nas Organizações (SIO), bem como dois *WebSites*, também estes fornecidos pelos docentes da

UC, que esclarecem a importância e a utilidade dos *smartcards* ([1], [2]), e o outro contendo receitas de alto nível e interfaces de baixo nível para algoritmos criptográficos comuns, como cifras simétricas, resumos de mensagens e funções de derivação de chaves [3].

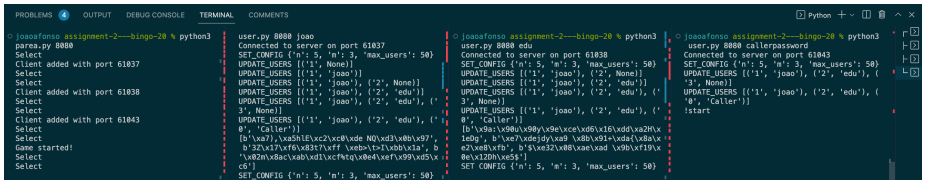

Figura 1.1: Bingo's *User Interface*

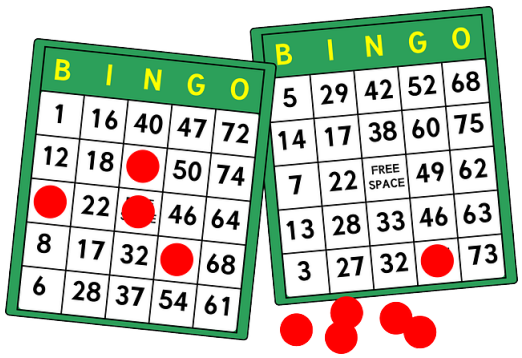

Figura 1.2: Bingo's *Illustration*

Capítulo 2

Aspetos chave a considerar

Neste capítulo ir-se-á abordar alguns dos aspetos chave que se teve em consideração ao longo do desenvolvimento deste projeto, tendo em conta a informação e regras fornecidas pelos docentes da UC.

1. Considerou-se a **junção** do ficheiro *Caller* com o ficheiro *User*, uma vez que, entendeu-se mais ajustável e flexível trabalhar apenas com dois ficheiros, sempre tendo em consideração a distinção das entidades. Deste modo, o *Caller* tem como entrada no jogo o *nickname:* **callerpassword**, em que irá ser reconhecido como o **Caller** e apenas este tem acesso ás funcionalidades principais do jogo (Ex: Começar o jogo (*!start*). É possível este entrar no jogo fazendo na linha de comandos:

   ```
   $ python3 user 8080 callerpassword
   ```

2. Outro dos aspetos chave é, efetivamente, a **segurança**. Assim, na comunicação estabelecida entre servidores e clientes pretende-se providenciar aos jogadores autenticação, incluindo uma *public key* e um *nickname* não comprometendo a integridade dos dados transmitidos durante esta comunicação.

3. Finalmente, para se considerar um jogo, tem que existir vencedor(es) e perdedor(es), desta forma os jogadores ao preencherem as suas cartas com os números do *deck* e determinar assim o **vencedor** baseado naquele(es) que completaram a carta na menor quantidade de números.

Palavras-Chave:

1. Chave Privada
2. Chave Pública
3. Segurança
4. *Server*
5. *Client/Player*
6. Autenticação
7. Autorização
8. Assinatura Digital
9. Fraude
10. *Log*
11. Cartão de Cidadão
12. *PKI (Public Key Infrastructure)*

Capítulo 3

Objetivos

Para o desenvolvimento deste projeto começou-se por estabelecer objetivos principais, numerados a seguir, de forma a organizar ideias e estabelecer, desde início, os focos cruciais deste trabalho.

1. Garantir que os jogadores possam se autenticar para aceder à área de jogo **(Playing Area)**.
2. Implementar um protocolo seguro de comunicação entre o servidor e os clientes/jogadores no jogo do Bingo.
3. Prevenir e negar a tentativa de falsificação de dados dos jogadores, como a *Public Key* e o *nickname*.
4. Assegurar que a **Playing Area** regists todas as mensagens e ações durante o jogo.
5. Permitir aos jogadores que ao solicitar o *log* tenham acesso aos eventos registados na **Playing Area**.
6. Permitir que os jogadores criem suas próprias cartas com um conjunto de números únicos, de forma mais segura.
7. O *Caller* deve enviar um *deck* baralhado de números para todos os jogadores.
8. Implementar um mecanismo para que os jogadores possam preencher suas cartas com base nos números ditados pelo **Caller** e determinar o(s) vencedor(es) com base na menor quantidade de números usados.
9. Assegurar que qualquer entidade do jogo possa detetar possíveis fraudes durante o jogo.

Capítulo 4

Desafios

Um dos desafios principais deste trabalho foi a implementação de um sistema capaz de estabelecer **comunicação** de clientes autorizados e um servidor. Para tornar isto possível, a solução passou por desenvolver, usando a livraria *json* de forma a permitir esta troca de mensagens.

Outro dos objetivos, foi, efetivamente, assegurar que as cartas dos jogadores seriam enviadas *encrypted* e que pudessem ser *decrypted* pelos jogadores que a recebessem, pelo que foi necessário a implementação no jogo de um sistema de ***encryption and decryption***, utilizado algoritmos de chaves simétricas, neste caso *RSA*.

Ainda, foi indispensável, de forma a interpretar de melhor maneira o que foi pedido, estabelecer, desde início, **objetivos** e tópicos de implementação do jogo. Deste modo, o trabalho começou exatamente pela **execução** e construção do jogo do Bingo, versão simplista do jogo. De seguida, implementou-se o sistema de *encryption and decryption*, previamente referido, e a integração dos **cartões de cidadão** com o jogo utilizando a livraria ***PKCS#11***.

Finalmente, para tornar mais simples e evitar confusão no **código**, tentou-se, ao máximo, a manutenção de um código o menos confuso possível, de forma a ajudar os elementos da equipa a **compreensão** do mesmo e a minimizar possíveis erros que possam ser originados pela má interpretação do mesmo.

Capítulo 5

Conclusão

Concluindo, a implementação do jogo do Bingo apresenta vários pontos chave na realização deste projeto, incluindo garantir a segurança e a imparcialidade do jogo, bem como lidar adequadamente com a comunicação e as interações entre o *Server* e os *Players*, o uso de uma *Playing area* facilita a troca de informações e a implementação da autenticação e autorização ajuda a garantir a integridade dos jogadores e dos dados transferidos ao longo do jogo. Para além destas, foi crucial a execução da geração do cartão, por parte de cada jogador usando uma assinatura digital, e a utilização de um *deck* baralhado a que todos os jogadores têm acesso permite a determinação do vencedor com base na menor quantidade de números usados no seu cartão, ajuda a evitar fraudes. Deste modo, o sucesso do desenvolvimento deste projeto serviu para entender e perceber aprofundadamente a comunicação entre as diferentes entidades, utilizando sockets, bem como todos os protocolos de segurança e encriptação.

Capítulo 6

Distribuição do Trabalho

- Guilherme Claro: 10%
- Eduardo Lopes Fernandes: 40%
- João Afonso Ferreira: 40%
- Tiago Mostardinha: 10%

Bibliografia

[1] THALES, online from https://www.thalesgroup.com/en/markets/digital-identity-and-security/technology/smart-cards-basics, jun. de 2022.

[2] E. Português, online from https://amagovpt.github.io/docs.autenticacao.gov/Manual_de_Utilizacao_v3.pdf, 2010.

[3] Fernet, online from https://cryptography.io/en/latest/, 2022.

Acrónimos

MIECT Mestrado Integrado em Engenharia de Computadores e Telemática

LECI Licenciatura em Engenharia de Computadores e Informática

SIO Segurança Informática e Nas Organizações

UC Unidade Curricular