Cybersecurity
Project Guidelines

Dept. of Information Engineering
University of Pisa

Version: 2020-04-01

2020 Guidelines
Four-in-a-Row Online

- Users are already registered on the server through public keyes. Users authenticate through said public key.
- After the log-in, a user can see other available users logged to the server.
- User can send a challenge to another user.
- The user who receives a challenge can either accept or refuse.
- If the challenge is accepted, the users proceed to play using a peer-to-peer communication.
- The game board must be printed at each move. The board is 6x7 (rows, columns).

2020 Guidelines
Four-in-a-Row Online

- When the client application starts, Server and Client must authenticate.
  - Server must authenticate with a public key certified by a certification authority.
  - Client must authenticate with a public key (pre-installed on server). The corresponding private key is protected with a password on each client.
- After authentication a symmetric session key must be negotiated.
  - The negotiation must provide Perfect Forward Secrecy.
  - All session messages must be encrypted with authenticated encryption mode (e.g., CCM, GCM)
  - Session with server is not interrupted by games.

2020 Guidelines
Four-in-a-Row Online

- After a challenge is accepted, the server sends to both clients the ip address and public key of the adversary.
- Before starting the game a symmetric session key must be negotiated.
  - The negotiation must provide Perfect Forward Secrecy.
  - All session messages must be encrypted with authenticated encryption mode (e.g., CCM, GCM)
- When the game ends, clients disconnect from each other.
- When a client wants to stop playing, it shall log-off from the server.

General Guidelines

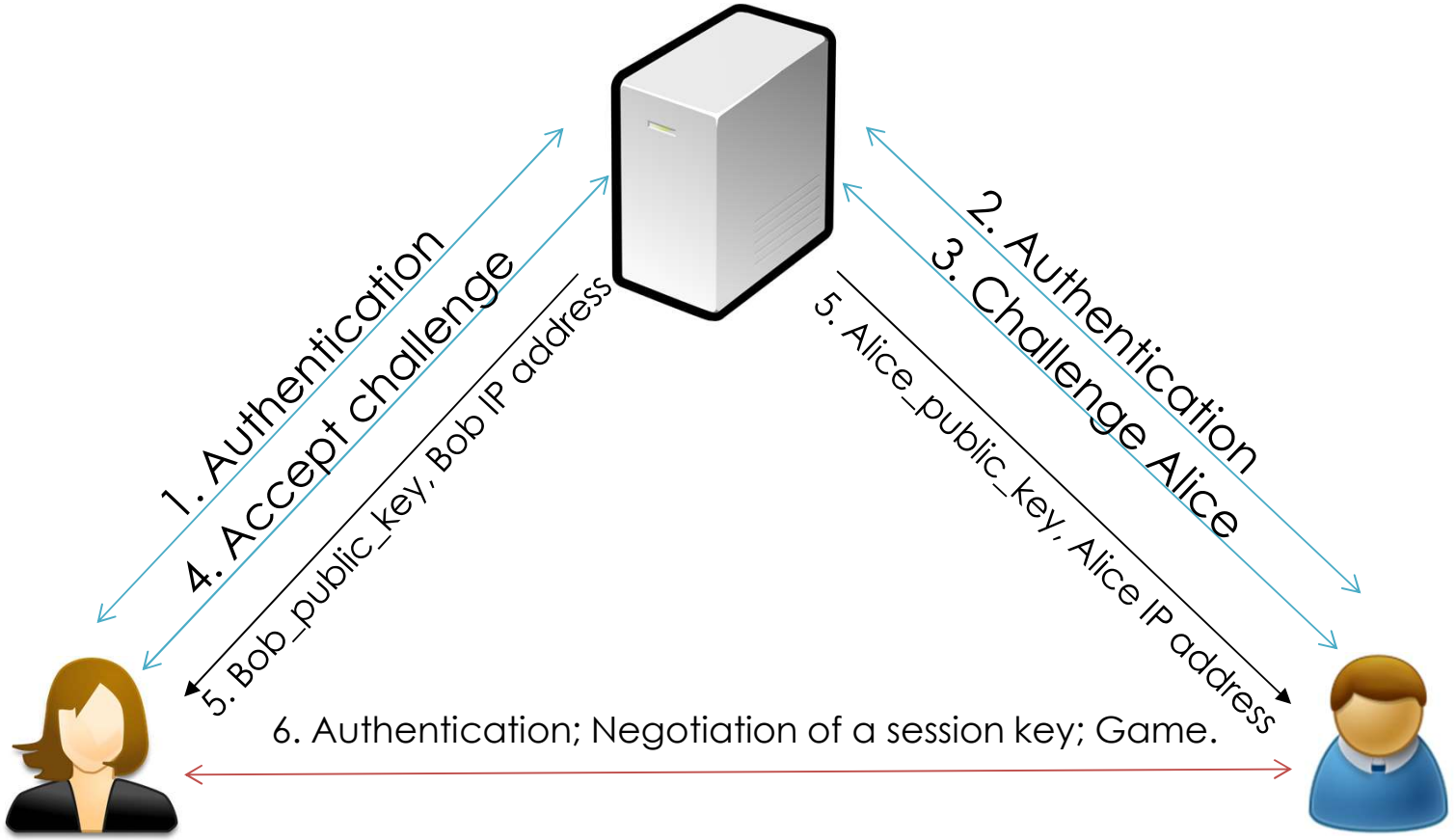
- Use C or C++ language, and OpenSSL library for crypto algorithms.
- Key establishment protocol must establish one (or more) symmetric session key(s) with public-key crypto.
- Then, session protocol must use session key(s) to communicate.
- Communication must be confidential, authenticated, and protected against replay.

General Guidelines

- No coding vulnerabilities (use secure coding principles)
- Manage malformed messages
- Project report must contain:
  - Project specifications and design choices
  - BAN-logic proof of key exchange protocol
  - Format of all the exchanged messages

Basic Idea

Alice_public_key
Bob_public_key
Server_certificate



$\{Alice\_private\_key\}_{pwdA}$
Alice_public_key
Authority_public_key

$\{Bob\_private\_key\}_{pwdB}$
Bob_public_key
Authority_public_key