Cybersecurity Project Guidelines

Michele La Manna
Dept. of Information Engineering
University of Pisa
michele.lamanna@phd.unipi.it
Version: 2021-04-14

2021 Guidelines
Online messaging service

- Users are already registered on the server through public keyes. Users authenticate themselves through said public key.
- After the log-in, a user can see other available users logged to the server.
- An user can send a "request to talk" message to another user.
- The user who receives the "request to talk" can either accept or refuse.
- If the request is accepted, the users proceed to chat through the server using an end-to-end encrypted and authenticated communication.

2021 Guidelines
Online messaging service

- 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 and authenticated.
  - Every message in the session must be protected against replay attacks.

2021 Guidelines
Online messaging service

UNIVERSITÀ DI PISA

- After a «request to talk» is accepted, the server sends to both clients the public key of the other client.
- Before starting the chat a symmetric session key must be negotiated.
  - The negotiation must provide Perfect Forward Secrecy.
  - All session messages must be encrypted and authenticated, and they must be protected against a replay attack.
- When a chat starts, the clients cannot start another chat (1 chat active at a time).
- When a client wants to stop chatting, it shall log-off from the server.

Server assumptions

UNIVERSITÀ DI PISA

The server is "honest-but-curious":

- It will not communicate false public keys on purpose. (When the server communicates the public key of the user "Alice", the receiving client trusts that the server has given it the Alice's public key).
- It would try to understand the content of the communications between clients. (Your job is to avoid that this happens)

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.

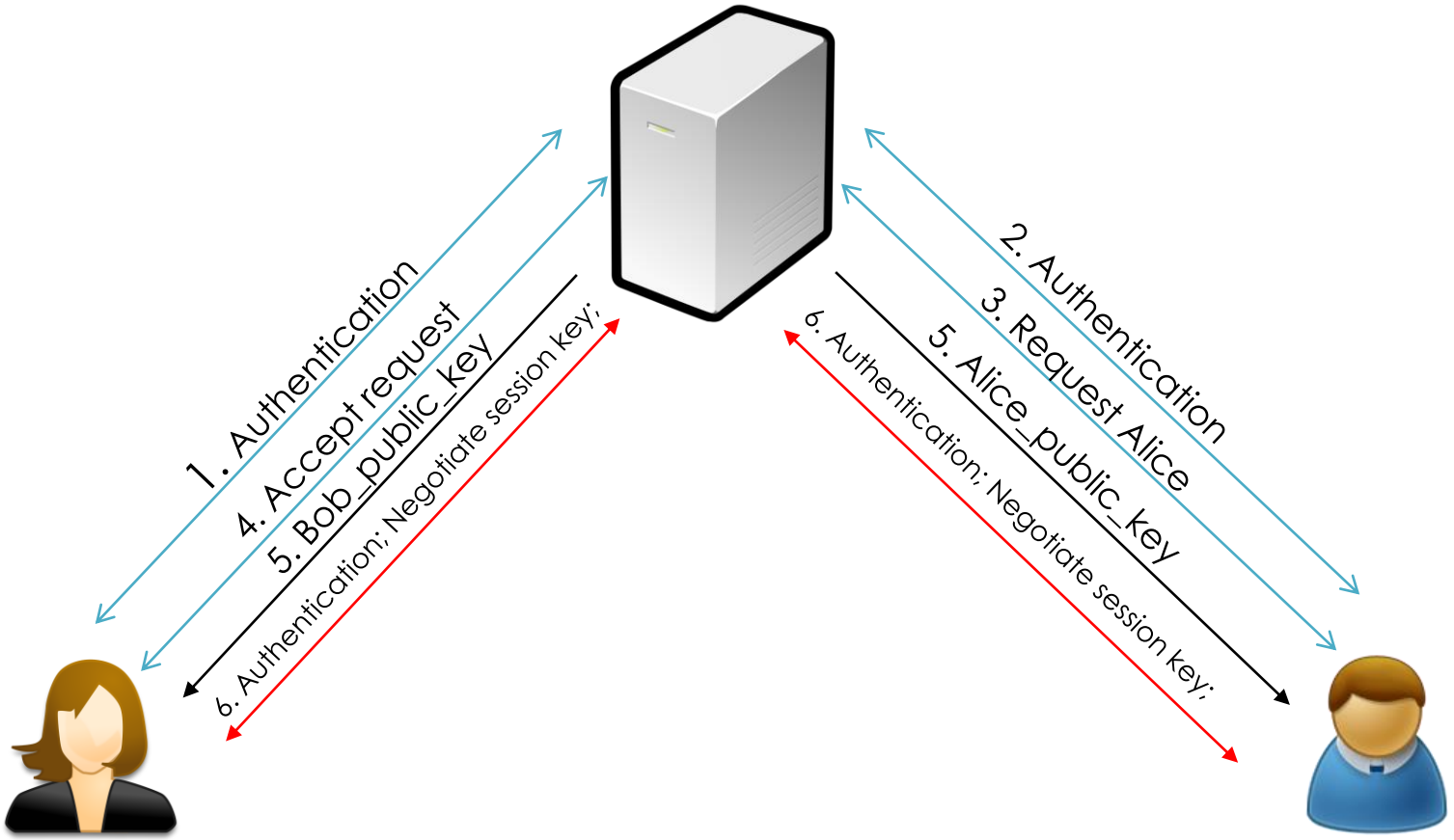
General Guidelines

UNIVERSITÀ DI PISA

- No coding vulnerabilities (use secure coding principles)
- Manage malformed messages
- Project report must contain:
  - Project specifications and design choices
  - 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