Cybersecurity Project Guidelines

Michele La Manna
Dept. of Information Engineering
University of Pisa
michele.lamanna@phd.unipi.it
Version: 2022-04-13

2022 Guidelines
Scenario: Cloud Storage

The students must implement a Client-Server application that resembles a Cloud Storage.

Each user has a "dedicated storage" on the server, and User A cannot access User B "dedicated storage"

Users can Upload, Download, Rename, or Delete data to/from the Cloud Storage in a safe manner.

Ogni user ha uno storage ed è privato

Pre-Shared Crypto Material

UNIVERSITÀ DI PISA

Users:

- They have already the CA certificate.
- They have each a long-term RSA key-pair.
- The long-term private key is password-protected.

Server:

- It has its own certificate signed by the CA.
- It knows the username of every registered user.
- It knows the RSA public key of every user.
- "Dedicated Storage" already allocated.

Requisites

UNIVERSITÀ DI PISA

- Users are pre-registered on the server.
- When the client application starts, Server and Client must authenticate.
  - Server must authenticate with the public key certified by the certification authority.
  - Client must authenticate with the public key, pre-shared with the server.
- During authentication a symmetric session key must be negotiated.
  - The negotiation must provide Perfect Forward Secrecy.
  - The entire session must be encrypted and authenticated.
  - The entire session must be protected against replay attacks.

Operations

Once connected to the service, the client can:

- **Upload**: Specifies a filename on the client machine and sends it to the server. The server saves the uploaded file with the filename specified by the user. If this is not possible, the file is not uploaded.

The uploaded file size can be **up to 4GB**

Operations

Once connected to the service, the client can:

- **Download**: Specifies a file on the server machine. The server sends the requested file to the user. The filename of any downloaded file must be the filename used to store the file on the server. If this is not possible, the file is not downloaded.

Operations

Once connected to the service, the client can:

- **Delete**: Specifies a file on the server machine. The server asks the user for confirmation. If the user confirms, the file is deleted from the server.

Operations

Once connected to the service, the client can:

- **List**: The client asks to the server the list of the filenames of the available files in his dedicated storage. The client prints to screen the list.

Operations

Once connected to the service, the client can:

- **Rename**: Specifies a file on the server machine. Within the request, the clients sends the new filename. If the renaming operation is not possible, the filename is not changed.

Operations

Once connected to the service, the client can:

- **LogOut**: The client gracefully closes the connection with 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

UNIVERSITÀ DI PISA

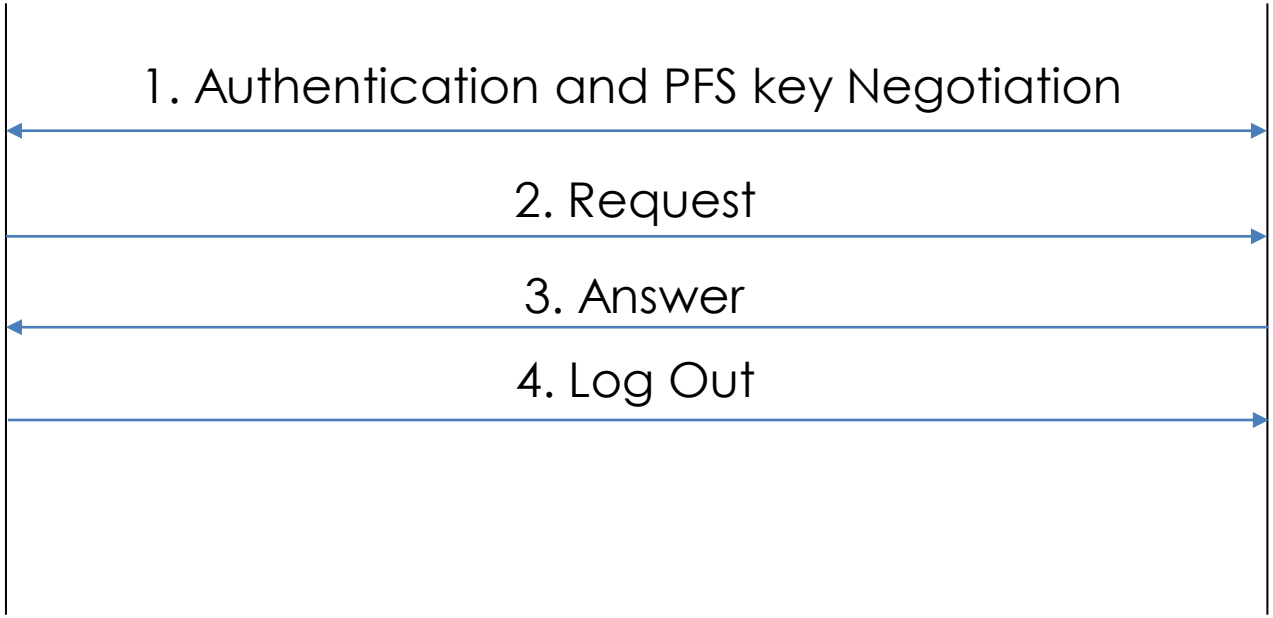
- No coding vulnerabilities (use secure coding principles, in particular CANONICALIZATION/INJECTION)
- Manage malformed messages
- Project report must contain:
  - Project specifications and design choices
  - Format of all the exchanged messages
  - Sequence Diagrams of every used communication protocol (Application Level).

Basic Idea

UNIVERSITÀ DI PISA

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

Alice_public_key
Bob_public_key
Server_certificate



Questions

If you have any question, follow this algorithm:

1. Read Carefully the Project Assignment FAQ
2. Re-read even more carefully the Project assignment FAQ
3. If you did not find an answer to your question(s), send an email to **both**:

michele.lamanna@phd.unipi.it

mariano.basile@ing.unipi.it

Meetings

If you want to review (or submit) your project, send an email to **both**:

michele.lamanna@phd.unipi.it

Mariano.basile@ing.unipi.it

And put in cc your colleague(s), if you are in a group.

Please prepare Sequence Diagrams **before** a review meeting! Don't come with only code!