Plantilla revisión prácticas

Seguridad en el Diseño de Software 2021/2022

Componentes:

Luis Alfonso Jiménez Rodríguez	Juan García Martínez

Descripción breve:

(diseño básico, funcionalidad prevista, etc.)

La aplicación funcionará para el almacenamiento remoto de archivos basado en Cliente-Servidor seguro empleando TLS con Sockets. El cliente se autentificará mediante un sistema de usuario en el que podrá iniciar sesión, o registrarse en caso de no ser cliente, para acceder a su sistema de archivos privado.

La información de los usuarios se almacenará en una base de datos cifrada mediante AES-192 o AES-256 (clave privada) y para la contraseña se realizará una función hash + sal (ARGON2), donde la sal se almacenará en una base de datos.

Los archivos privados de cada usuario se cifrarán con RSA (clave pública) 3072 bits.

Cronología aproximada:

(indicar los hitos esperados y el estado actual de desarrollo del proyecto)

Estado actual: Inicio de sesión y registro de usuarios mediante Cliente-servidor TLS con hash+sal en la contraseña.

Las 2 próximas semanas (18 abril – 1 mayo): Cifraremos por completo los datos del usuario almacenados en la base de datos.

Las 2 siguientes semanas (2 mayo – 15 mayo): Realizar el sistema de archivos con la información cifrada.

Las 2 ultimas semanas (16 mayo – 29 mayo): Realizar la memoria del proyecto y “tener colchón” por futuros contratiempos y dudas que nos puedan surgir.

Observaciones:

(opcional)

No tenemos muy claro donde almacenar las claves privadas (AES) de los usuarios.

En SD lo hicimos en un archivo local, pero tampoco se pedía mucha seguridad.