PRÁCTICA 2020/2021

SEGURIDAD EN EL DISEÑO DEL SOFTWARE

CONDICIONES GENERALES

- El desarrollo se realizará en Go (www.golang.org).
- Se realizará por parejas (excepcionalmente en tríos).
- Se evitarán interfaces de usuario complejas, concentrando el esfuerzo en el problema y la seguridad.
- El programa irá acompañado de una documentación (en PDF) que explique el diseño, el proceso de desarrollo, así como las decisiones y expectativas de seguridad del proyecto. Se seguirá en la medida de lo posible el modelo explicado en clase (tema 3).

BULLETIN BOARD SYSTEM

Los *Bulletin Board Systems* (o BBS) fueron unos de los primeros sistemas de comunicación online, anteriores incluso a la web. Actualmente, el software más parecido a un BBS, sería un foro como phpBB o vBulletin. El objetivo consistirá en la creación de un sistema de comunicación similar a un BBS o foro, que permita la comunicación e interacción de los distintos usuarios de forma asíncrona y segura.

Las características que se deben incluir en el diseño para aprobar son:

- Arquitectura cliente/servidor.
- Mecanismo de autentificación seguro (gestión de contraseñas e identidades).
- Transporte de red seguro entre cliente y servidor (se puede emplear algún protocolo existente como TLS o HTTPS).
- Sistema de publicación de contenido general (público).
- Sistema de comunicación privado (cifrado) entre usuarios.

Algunos desafíos adicionales (aspectos extra u opcionales para subir nota) podrían ser, entre otros:

- Cifrado con conocimiento cero (el servidor no conoce las claves, todo el cifrado/descifrado se realiza en el cliente). De especial aplicación al sistema de comunicación privado.
- Gestión de subforos (categorización de contenido) o subgrupos (puede incluir seguridad adicional).
- Gestión de diferentes roles de usuarios (administradores, moderadores, etc.).
- Panel de control para los usuarios (la funcionalidad puede depender del rol).
- Sistema de registro de eventos *(logging)*, para mejorar la trazabilidad.
- Otras características interesantes relacionadas con la seguridad, privacidad o funcionalidad del sistema.