PRÁCTICA 2018/2019

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, utilizando esencialmente el terminal y 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).

GESTOR DE CONTRASEÑAS

El objetivo consistirá en la creación de un gestor de contraseñas (al estilo de PasswordSafe, Password Gorilla, 1Password, KeePass, etc.) con almacenaje en servidor que permita su acceso desde distintos clientes remotos.

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

- Arquitectura cliente/servidor.
- Cada entrada incluirá, como mínimo, un identificador, un usuario y una contraseña.
- 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).
- Cifrado de la base de datos de contraseñas en el servidor.

Algunos desafíos adicionales (aspectos extra u opcionales para subir nota) para la práctica podrían ser:

- Generación de contraseñas aleatorias y por perfiles (longitud, grupos de caracteres, pronunciabilidad, etc.)
- Incorporación de datos adicionales (notas, números de tarjeta de crédito, etc.) en cada entrada.
- Optimización de la privacidad (conocimiento cero: el servidor sólo recibe datos cifrados por el cliente).
- Compartición de contraseñas con grupos de usuarios usando clave pública.
- Programar una extensión (https://developer.chrome.com/extensions/getstarted) de Google Chrome que se comunique con el servidor para buscar contraseñas guardadas y se puedan usar fácilmente en el navegador.