Programación Segura

gmq.psp2019@gmail.com

Febrero 2020

Programación Segura

- **Control de accesos**
- Criptografía clave pública y privada
- Encriptación
- Protocolos seguros

Control de accesos

- Una aplicación web puede publicar recursos accesibles por todos y otros privados
  - Control de acceso a los recursos privados
  - La forma habitual es el login mediante usuario/contraseña
    - Identificador por huella
    - Identificador por iris
    - Identificador por morfología

Control de accesos

- Autenticación vs Autorización
  - Autenticación: proceso mediante el cual las credenciales aportadas se validan contra un sistema para verificar la validez de las mismas
    - Error 401 HTTP: UnAuthorized
  - Autorización: proceso mediante el cual, con las credenciales aportadas el usuario no tiene permisos para realizar una acción
    - Error 403 HTTP: Forbidden

Control de accesos

- Usuarios
  - Cada usuario en una aplicación tiene unos permisos determinados.
    - Usuario con permiso de lectura
    - Usuario admin con permiso de lectura y de escritura
  - Los permisos se establecen al dar de alta un usuario
  - Modificables: upgrade/downgrade usuario

Control de accesos

- Usuarios
  - Dada una aplicación, resulta costoso establecer permisos por usuarios
  - Se definen grupos de usuarios y grupos de permisos
  - Concepto de rol: colección de permisos definida para todo el sistema
  - Un usuario puede tener uno o más roles
  - Un rol tiene uno o más permisos

Control de accesos

- Protocolo acceso:
  - Oauth 2.0
    - Utilizado por Google, Facebook, Microsoft, Twitter y Github permitiendo a los usuarios compartir información sobre sus cuentas con aplicaciones de terceros o sitios web
  - OpenId Connect
    - Pensado para sistemas Single Sign-On
    - Define flujos de información para la autenticación

Control de accesos

- Protocolo acceso:
  - Oauth 2.0
    - Utilizado por Google, Facebook, Microsoft, Twitter y Github permitiendo a los usuarios compartir información sobre sus cuentas con aplicaciones de terceros o sitios web
  - OpenId Connect
    - Pensado para sistemas Single Sign-On
    - Define flujos de información para la autenticación

Programación Segura

- Control de accesos
- **Criptografía clave pública y privada**
- Encriptación
- Protocolos seguros

Criptografía: clave pública y privada

- Técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados
- Cifrado es un procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) para transformar un mensaje

Criptografía: clave pública y privada

- Cifrado simético:
  - Las claves de cifrado y descifrado son las mismas
  - Algoritmo DES
- Cifrado asimétrico
  - Las claves de cifrado y descifrado son diferentes
  - Algoritmo: RSA

Programación Segura

- Control de accesos
- Criptografía clave pública y privada
- **Encriptación**
- Protocolos seguros

Encriptación

- Funciones hash

Programación Segura

- Control de accesos
- Criptografía clave pública y privada
- Encriptación
- **Protocolos seguros**