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

Control de accesos

- JWT: Json Web Token
  - estándar abierto basado en JSON para la creación de tókenes de acceso que permiten la propagación de identidad y privilegios/claims
  - Estructura
    - encabezado o header,
    - contenido o payload
    - firma o signatur
  - www.jwt.io

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

Criptografía: clave pública y privada

- Base64
  - Grupo de esquemas que representa información de binario-a-textos en ASCII traduciéndolo en una raíz de 64 caracteres
  - Diseñado para transportar datos binarios en medios que sólo soportan contenido de texto.
  - Muy usado en la WWW al embeber imágenes/vídeos en texto (HTML o CSS)
  - Java: Base64.encoder()
  - Java: Base64.decoder()

Programación Segura

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

Encriptación

- Funciones hash
  - algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija
  - Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud

Encriptación

- Funciones hash
  - Generación de un valor diferente para cada entrada
    - Evitar colisiones
  - Son irreversibles:
    - Una vez codificada no se puede generar el original
    - Uso: almacenamiento de claves

Encriptación

- SHA (Secure Hash Algorithm)
  - Diferentes versiones evolucionadas del algoritmo
    - SHA-0, la inicial de 1993
    - SHA-1
      - En 2004 se encontraron vulnerabilidades, colisiones
    - SHA-2:
      - Evolución a partir de SHA-1
    - SHA-3
      - Nuevo concepto de “construcción en esponja”

Encriptación

- Java
  - Método hashCode()
    - x.equals(y)
    - Generados por el IDE
  - Tipos de datos:
    - HashMap<K,V>
    - HashSet

Programación Segura

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

Protocolos seguros

- Pensados para mantener la confidencialidad y la privacidad
- Transferencia de archivos
  - TCP → SCTP
- Navegación
  - HTTP → HTTPS
- Terminal
  - TelNet → SSH

HTTPS

- Cifrado basado en la seguridad de textos SSL/TLS para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP.
- consigue que la información sensible (usuario y claves de paso normalmente) no pueda ser usada por un atacante que haya conseguido interceptar la transferencia de datos de la conexión, ya que lo único que obtendrá será un flujo de datos cifrados que le resultará imposible de descifrar