Introducción a seguridad de las aplicaciones

Nos enfocamos en saber sobre vulnerabilidades en software, centralizado en el mundo de las aplicaciones.

Autenticación, autorización y control de acceso

Autenticación

- un usuario tiene que demostrar que es quien dice ser
- En la autenticación mediante usuario y contraseña se encuentran deficiencias que hacen que si las contraseñas no son robustas pueden ser vulnerables a ataques de fuerza bruta. Además las contraseñas deben ser guardadas cifradas. Si se usa un medio no seguro es posible que la contraseña no llegue encriptada.
- En la autenticación mediante tarjetas inteligentes se usa un certificado digital para la autenticación, pero se necesita un medio físico para su uso.
- Un certificado digital es como un pasaporte virtual. Consta de una pareja de claves criptográficas, una pública y una privada, creadas con un algoritmo matemático. El titular del certificado debe tener la clave privada.

Tipos de criptografía

- Simétrica: Clave pública y clave privada
- Asimétrica: Se usa la misma clave para cifrar y descifrar. El tener que distribuir la clave es problemático.

Autorización

Una vez autenticado el usuario entra en juego la política de autorización, que define que puede y que no puede hacer el usuario. Dependiendo del usuario se tendrá acceso a unos elementos u otros.

Control de acceso

Se hace cargo de controlar a que pueden acceder los usuarios.

Aplicaciones y servicios web con estado (stateful)

Aplicaciones y servicios web sin estado (stateless)