Programación segura. Cosas básicas para tener en cuenta.

No usar contraseñas débiles, ni deducibles. Para tener una contraseña adecuada, la longitud tiene que ser mayor a 12, contener mínimo una letra minúscula, una mayúscula, un número y un carácter especial. No se deben guardar contraseñas en claro, ni en sitios con permisos generales de lectura. Tampoco guardar archivos de datos no encriptados, ni transmitir datos sin encriptar.

Control de acceso a las aplicaciones.

En una organización habrá aplicaciones para todos los usuarios, de las cuales se pueden restringir accesos usando herramientas del sistema. La limitación o concesión de permisos para acceder a aplicaciones se tiene que hacer sobre grupos de usuarios.

Si un servidor SQL se ha configurado con seguridad mixta, podremos crear usuarios en el propio DB.

- Utilización de usuarios del propio DB. Puede ser útil si se conecta remotamente, pero necesitamos el nombre de usuario y la contraseña para conectar, lo que probablemente sea necesario poner en texto claro.
- Utilización de usuarios y grupos del sistema operativo, es muy recomendable para tener mas seguridad, para limitar el acceso haría falta:
    - Definir las funcionalidades diferentes.
    - Definir los grupos de usuarios funcionales que desarrollan estas acciones.
    - Asignar a cada objeto de la base de datos y grupo de usuarios permisos totales.
    - Crear usuarios individuales y asignarlos a los grupos funcionales correspondientes.

Criptografía.

La criptografía estudia formas de convertir información desde su forma original a un código incomprensible sin saber la técnica.

Objetivos de la criptografía.

Cuando se quiere enviar un mensaje, se deben satisfacer los siguientes objetivos:

- Confidencialidad.
- Integridad: El mensaje no debe ser alterado.
- Autentificación de punto a punto: Se debe confirmar la identidad de ambas partes.
- No-repudio: El emisor no puede negar que ha enviado el mensaje, ni el receptor que lo ha recibido.

Conceptos de criptografía.

El texto claro es el mensaje en la forma original, el texto cifrado es el mensaje encriptado. Un cifrado es el proceso con el cual se pasa de texto claro a cifrado, el descifrado es justamente lo contrario. Una clave es un conjunto de caracteres para encriptar o desencriptar.

Algoritmos de reducción criptográfica.

Son algoritmos que permiten transformar un conjunto de datos, en un único valor de longitud fija, el objetivo es controlar la integridad de los datos.

MD5 es un algoritmo de 128 bits muy utilizado, pero que se esta dejando de utilizar porque genera colisiones.

SHA esta desarrollado por la NSA. Bitcoin usa SHA-256 en sus transacciones.

Algoritmos simétricos.

Son algoritmos que permiten ocultar el texto plano, utilizan la misma clave para cifrar i descifrar, por ejemplo, el algoritmo de Julio Cesar.

El cifrado monoalfabético es una evolución del algoritmo de Cesar, donde las letras están desordenadas.

El cifrado polialfabético utiliza múltiples cifrados monoalfabéticos para mejorar la confidencialidad.

Actualmente tenemos dos estrategias, el cifrado por bloques y el cifrado por flujo. Por bloques se utiliza en muchos protocolos de internet (correo electrónico seguro), el cifrado por flujo se utiliza para cifrar flujos de datos combinándolo bit a bit con una clave (conversaciones telefónicas).

Cifrado por bloques.

En un cifrado por bloques, el mensaje se procesa en bloques de k bits, y la medida de la clave puede ser de 128, 192 o 256 bits. El problema es que, en los últimos años, han ido saliendo vulnerabilidades en la mayoría de los métodos.

Algoritmo AES.

AES es un algoritmo de cifrado simétrico por bloques, el bloque es de 128 bits y la medida de la clave puede ser de 128, 192 o 256 bits. El problema es que en los últimos años han ido saliendo vulnerabilidades en la mayoría de los métodos.

Algoritmo XChaCha20-Poly1305.

Una alternativa a AES es esta, ChaCha es un algoritmo de cifrado por flujo, con clave de 128 o 256 bits. ChaCha20 son 20 iteraciones de ChaCha. XChaCha20 es ChaCha20 con una clave de 256 bits. Es mas simple y rápido, siendo adoptado por Google.

Algoritmos asimétricos.

En un algoritmo asimétrico la clave que se usa para encriptar es diferente de la que se usa para desencriptar. El objetivo es proporcionar autentificación punto a punto.

Los criptosistemas de clave publica, es donde cada usuario tiene asociada una pareja de claves, la clave publica es accesible para todos los usuarios de la red, son algoritmos que permiten autentificar el origen.

En este tipo de algoritmos el usuario genera dos claves y puede seguir dos estrategias, el emisor encripta el mensaje con su clave privada i deja disponible para todos, la clave publica a una autoridad certificadora.

Otra posibilidad es que el emisor encripte el mensaje con la clave pública del receptor de manera que solo el receptor la desencriptará.

RSA y ECC.

RSA es un algoritmo de encriptación asimétrica utilizado para firmar mensajes, ECC es una buena alternativa de futuro.

ECC es un nuevo método de criptografía que trabaja con la representación matemática de curvas elípticas, es mas seguro que RSA y todavía esta en la fase adaptativa. ECC requiere unas claves mucho más cortas que RSA.

Criptografía hibrida.

Todas las soluciones anteriores, aseguran confidencialidad, integridad o autenticación, pero ninguna de las tres a la vez. Un problema añadido es que los algoritmos asimétricos producen claves muy grandes.

La criptografía hibrida es un método que utiliza tanto un método simétrico como uno asimétrico. Usa la clave compartida y esta se cifra con la clave pública del receptor. Posteriormente se envía el mensaje encriptado y la clave encriptada al destinatario.

Como asegurar todos los objetivos de la criptografía.

El emisor calcula el hash y firma con su clave privada, el resultado se encripta con un algoritmo simétrico, y la clave del algoritmo simétrico, se encripta con la clave pública del receptor, se concatena y se envía.

Autoridades Certificadoras.

Una CA es una entidad que actúa como un notario digital, de forma que nunca se emitirá un certificado con datos incorrectos. Cualquiera puede actuar como una CA pero tiene que ser de confianza, a nivel local, puede ser una empresa y a nivel estatal puede ser el gobierno.

Generación de certificados.

Cuando alguien quiere un certificado tiene que enviar una petición con su clave publica, una vez la recibe, la autoridad comprueba que los datos sean reales y genera el certificado. La clave publica de una CA se distribuye en un certificado digital.

Autoridades certificadoras.

Una vez se ha generado un certificado, quien confíe en la veracidad podrá confiar en que los datos son correctos, nadie puede haberlo falsificado.

Comprobar la validez de un certificado digital.

Para comprobar si realmente ha estado emitido por la autoridad, se tiene que comprobar si la firma digital es correcta, se comprueba la fecha de emisión y de expiración, y la lista de certificados revocados.

Infraestructura de clave pública (PKI).

Las CA son responsables de disponer de una infraestructura que permita generar certificados, intercambiar claves públicas y revocar certificados emitidos.

Almacén de claves.

Un almacén de claves permite guardar diversas claves criptográficas garantizando protección en caso de perdida o robo. Un almacén puede ser un archivo o estar asociado a una maquina (DNI-e).

Formato de un certificado digital.

El formato mas utilizado para hacer un certificado es el formato X-509, tiene que contener como mínimo:

- La firma de la autoridad certificadora.
- El nombre, dirección y domicilio del suscriptor.
- Identificación del suscriptor.
- El nombre, dirección y sitio de la entidad certificadora.
- La clave publica del usuario.
- La metodología para verificar la firma digital.
- Número de serie.
- Fecha de emisión y expiración.