Ejercicios de clase no entregables

Ejercicio 1

Laboratorio clínico

Ejercicio 1

- Se está diseñando el sistema web de un laboratorio de analíticas para dar servicio tanto a los pacientes como a los distintos laboratorios locales que pertenecen a la misma empresa.

- Diseña los siguientes elementos de seguridad de dicho sistema indicando, parametrizando y justificando las distintas herramientas criptográficas, protocolos de seguridad y otros elementos necesarios:

  - Registro y autentificación de usuarios
  - Transporte seguro y confidencialidad en el almacenamiento de datos
  - Garantía de autenticidad de los resultados

E1: autentificación

Una versión inicial sería hacer una autentificación por contraseñas:

- El usuario introduce <user, passwd> en el cliente.
- El cliente deriva una clave de autentificación a partir de la contraseña (kLogin) y la envía al servidor junto con el usuario:

$$kLogin = SHA\text{-}512(passwd)$$

**podemos concatenar user||passwd si queremos que se derive una clave distinta para usuarios distintos, aunque tengan la misma contraseña.*

- El servidor utiliza un PBKDF + Sal (idealmente Argon2) para comprobar la autentificación:

$$Argon2(kLogin_{user}, Sal_{user}) == Hash_{user} \text{ en BD,}$$

Mientras que en el registro genera una sal aleatoria para el usuario (Sal_{user}) y la guarda junto con el resultado ($Hash_{user}$) de Argon2 en la BD.

Esta autentificación se podría combinar con técnicas más avanzadas (a priori fuera del alcance de la asignatura) como segundos factores de autentificación, biometría, autentificación mediante clave pública, identificación física (ya que los pacientes han de asistir al laboratorio), etc.

E1: transporte y almacenamiento

- Al ser un sistema web, tiene sentido emplear HTTPS (TLS) para asegurar el transporte de datos entre cliente y servidor. Cabe recordar que no se especifican los parámetros criptográficos de TLS, se acuerdan entre cliente y servidor.

- El almacenamiento se puede cifrar a diferentes niveles:
  - Sistema operativo, es transparente para todas las aplicaciones y lo más frecuente en servidores y máquinas virtuales. Suele emplear AES en modo XTS para permitir acceso aleatorio a todas las partes del disco.
  - BD, algunas permiten activar cifrado para la base de datos que resulta transparente a los usuarios de dicha BD.
  - Aplicación, el servidor cifra al almacenar información en el disco y descifra al leer del mismo; aquí se puede utilizar AES (128, 192 o 256bit de clave en modo CTR, por ej.) o ChaCha (256bit de clave).

E1: Autenticidad

La autenticidad se proporciona mediante firma digital, siendo un posible enfoque:

- Los analistas tienen un par de claves pública/privada y firman el análisis (M) al terminarlo:

$$E_{Kpriv}(H(M)),M$$

- Cuando un usuario solicita dicha analítica, el servidor puede comprobar dicha firma mediante la clave pública del analista en cuestión:

$$H(M) == D_{Kpub}(E_{Kpriv}(H(M))$$

- Esta operación de firma requiere que dichas claves públicas estén firmadas a su vez por una autoridad certificadora (el servidor podría actuar como tal), para evitar la suplantación.

- Una buena opción podría ser RSA-3072 o ECDSA-256 (DSA con curvas elípticas) para realizar la firma, y SHA-512 para el resumen en este contexto.

Ejercicio 2

Registro digital

Ejercicio 2

- Se ha decidido modernizar un sistema de registro de solicitudes convirtiéndolo en un servicio online pero que mantenga las mismas garantías de un registro tradicional.

- Diseña conceptualmente dicho protocolo, indicando de forma justificada los pasos a llevar a cabo por ambas partes y las primitivas/herramientas criptográficas elegidas para garantizar:
  - La autoría, integridad y legalidad tanto de las peticiones de los solicitantes como de las respuestas de la entidad registradora.
  - La confidencialidad de los datos tanto en transporte como en descanso.

E2: autoría, integridad, legalidad

Es necesario emplear firma digital en ambas direcciones.

- El solicitante añade una marca temporal (T) a su solicitud (S) y la firma cifrando con su clave privada, y envía ambas cosas (Sf y S+T) a la entidad registradora:

$$S_f = E_{KprivS}(H(S+T))$$

- La entidad recibe dicha solicitud firmada y la comprueba mediante la clave pública del solicitante:

$$H(S+T) == D_{KpubS}(S_f)$$

Para la respuesta de la entidad registradora se realizaría el proceso inverso: se añade una marca temporal a la respuesta y se firma cifrando con la clave privada de la entidad; el solicitante puede comprobar la validez de la firma con la clave pública de la entidad registradora.

Se pueden utilizar los mismos algoritmos de firma y resumen que en el ejercicio anterior.

Además, sería necesario que las claves públicas a su vez estén firmadas por una autoridad certificadora reconocida por todas las partes para evitar la suplantación y garantizar la legalidad del proceso en caso de conflicto. La marca temporal es también un requisito legal y permite evitar la reproducción no autorizada (repetición en el futuro) de solicitudes o respuestas.

E2: confidencialidad

- Para la confidencialidad podemos utilizar la misma estrategia que en el ejercicio anterior: HTTPS (TLS) para el transporte y cifrado de datos al nivel oportuno para el almacenamiento.

- Como capa de confidencialidad adicional, podemos utilizar clave pública para intercambiar claves de cifrado entre solicitante y entidad. De esta forma si queremos cifrar la solicitud:
  - Una vez ha realizado la firma correctamente, el solicitante genera una clave aleatoria simétrica (Ks) y cifra mediante un algoritmo adecuado (AES, por ej.) la información a enviar (S_f y S+T)

$$Sc = E\text{-}AES_{Ks}(Sf \,||\, S+T)$$

  - Para transmitir dicha clave de cifrado de forma segura a la entidad registradora, se puede cifrar con la clave pública de la entidad y el solicitante envía ambas cosas (Kc y Sc)

$$Kc = E_{KpubR}(Ks)$$

  - La entidad registradora puede recuperar Ks descifrando Kc con su clave privada y luego descifrar el resto del mensaje con dicha clave para comprobar la firma con normalidad

$$Ks = D_{KprivR}(Kc)$$
$$Sf||S+T = D\text{-}AES_{Ks}(Sc)$$

  - Se puede realizar el proceso inverso para añadir esta capa de seguridad adicional a la comunicación entre entidad y solicitante.