Certificados, firma digital y criptografía

Práctica SL5

Informe de prácticas

1. **Describa los pasos que se deben seguir si se desea enviar un mensaje firmado a una persona empleando certificados.**
   [SUS RESPUESTAS]

2. **Al crea una identidad, debemos introducir una "frase de paso" (keyphrase). Posteriormente, el software nos solicitará dicha frase en determinadas ocasiones. Comente y explique cuándo y para que lo solicita.**
   [SUS RESPUESTAS]

3. **¿Qué diferencias existen entre un password y una keyphrase? Desde su punto de vista, ¿cuál es mejor y por qué?**

   La principal diferencia entre una password y una keyphrase es la longitud de cada una de las mismas. Generalmente esto se debe a que una password no permite introducir caracteres en blanco o espacios. Por el contrario, las keyphrases si que permiten esto, por lo que se pueden utilizar oraciones completas como claves de acceso.

   La principal ventaja que tiene una password frente a la keyphrase es su facilidad para ser recordada en la memoria de una persona. Esto, a su vez lo convierte en una gran vulnerabilidad ya que facilita su descubrimiento mediante fuerza bruta o diccionarios de claves comunes.

   La ventaja principal de una keyphrase es su mayor nivel de seguridad debido al mayor tamaño de la clave que se utiliza, lo cual imposibilita el ataque por fuerza bruta. Por el contrario, el problema de este sistema consiste en la dificultad para recordar dicha clave por parte del usuario que la utilizará.

   Bajo mi punto de vista creo que no existe una alternativa mejor que la otra sino que están orientadas a fines diferentes. Mientras que la keyphrase es una mucho mejor alternativa para ser manejada por una máquina, por su capacidad de almacenamiento "ilimitado", la password tiene sentido cuando debe ser recordada por una persona.

   A pesar de ello, cada vez están ganando más adeptos otros métodos que sustituyen el uso de passwords de usuario como sistemas basados en telemetría (huella dactilar, imagen facial, etc) u otras alternativas que se siguien apoyando en claves de tamaño corto pero utilizan métodos adicionales como verificación en dos pasos que tratan de ser fáciles de usar para las personas.

4. **Al verificar una firma digital se coteja tanto la firma como la identidad del remitente. Capture el mensaje que obtiene al verificar una firma recibida (usando Kleopatra) tanto sobre el fichero recibido como sobre el fichero recibido modificado. Comente los resultados.**
   [SUS RESPUESTAS]