Pontificia Universidad Católica de Chile
Departamento de Ciencia de la computación
IIC325 - Criptografía y Seguridad Computacional

Tarea 1

18 de julio de 2021

1º semestre 2021

José Manuel Domínguez - 17637449

Pregunta 1

a)

La primera consecuencia negativa que vimos en clases es que debemos confiar a ciegas de que el servicio al cual le estamos entregando nuestra clave, que es en este caso nuestro secreto, esté haciendo las cosas "bien". Qué quiere decir que se estén haciendo las cosas bien es básicamente que nuestra clave no se guarde en texto plano, ya que de esa forma cualquier empleado que tenga acceso a la base de datos puede ver cual es nuestra clave lo cual claramente no es bueno ya que este empleado podría tener acceso a nuestra cuenta sin nuestro consentimiento. También nosotros confiamos que nuestra clave esté guardada hasheada y salteada en la base de datos ya que de haber una posible filtración de datos nuestra clave no se pueda comparar con una tabla pre computada para poder descifrarla.

Todas estas alternativas son cosas malas pero el principal problema que se discutió en clases en más fundamental que estos. El problema principal es el de auditabilidad, la auditabilidad es básicamente como me aseguro yo de que efectivamente fui yo el que emitió el mensaje y no la institución o alguien más usando mis credenciales. Imaginémonos que a una institución como por ejemplo un banco un día hace una transferencia a nuestro nombre, esto lo podrían hacer ya que son ellos los que autentifican nuestras credenciales y transacciones. Entonces, nosotros actualmente no tenemos ninguna forma de protegernos contra esto ya que terminaría siendo nuestra palabra (¿o no hice esa transacción") contra la del banco ("tu sí hiciste esa transacción") y no hay ninguna forma de verificar quién tiene la razón. Esto por supuesto que puede traer diversas consecuencias no deseadas y el usuario no tiene absolutamente ninguna protección contra esto.

b)

Como posible solución en clases vimos que se puede usar criptografía asimétrica (llave pública y llave privada). Para autentificarnos lo que haríamos sería, en primer lugar cuando uno se crea una cuenta uno en su computador personal genera un par de llaves una pública y una privada y envía la clave pública al servicio al que uno se está creando un usuario y ellos la guardan en su base de datos junto con el nombre de usuario, mientas que la llave privada uno la guarda en un lugar seguro dentro de su computador, probablemente un archivo encriptado con criptografía simétrica y una clave maestra para que alguien no tenga acceso a estas si es que se pierde el computador.

Luego, si nos queremos autentificar el servicio nos pide que generemos un mensaje estándar y lo firmemos, el mensaje quizás podría tener algún número aleatorio el cual nos ponemos previamente de acuerdo para evitar que se pueda reutilizar ese mensaje siempre. Así la única manera de generar una firma que sea valida para esa llave pública es teniendo acceso a la llave privada lo que demostraría que somos nosotros los que están emitiendo esos mensajes, pagos, etc. También, de esta forma nosotros nunca compartimos nuestro secreto que es la llave privada con nadie, nunca la pasamos por la red (lo cual la pueden interceptar) ni tampoco la escribimos en ningún lugar (podría haber un sitio malicioso para robar nuestras credenciales).

Con esto solucionamos todos los problemas anteriormente descritos, ya no importa si guardan nuestra llave pública en la base de datos con texto plano ya que no importa que alguien pueda ver esa llave pública (por algo se llama pública) ya que no podría hacer nada sin tener acceso a la llave privada y esta está en nuestro computador, pero más importante solucionamos la auditabilidad, osea ahora no existe forma de que el servicio genere mensajes a nuestro nombre ya que ellos no tienen acceso a nuestra llave privada y no podrían firmar esos mensajes sin esta, entonces si es que alguien emitió un mensaje y este no está firmado rápidamente nos damos cuenta de que no fuimos nosotros y lo podemos probar con facilidad.

Dentro de los posibles problemas que tiene esta implementación puede ser que sea más complejo el acceder a sitios desde distintos computadores, esto lo digo ya que es casi imposible aprenderse la llave privada de memoria por lo que siempre la tendríamos que guardar en archivos dentro de nuestro PC, a diferencia de una contraseña normal que nosotros elegimos. Este problema no es tan grave ya de hecho si uno tiene claves seguras ya es muy difícil acordarse de estas, la solución podría ser guardar las llaves en un "key manager"que uno lo podría tener en diferentes lugares como el teléfono o un pendrive y uno lo lleve consigo.

Un segundo problema, un poco más grave es que si una institución o una persona quiere emitir un mensaje a nuestro nombre, lo que podría hacer es en la base de datos cambiar nuestra clave pública por una que generan ellos y de esta forma firmar nuestros mensajes, acá nuevamente recaeríamos en tu palabra contra la mía ya que la institución diría que esa efectivamente era la clave pública que yo envíe mientras que yo diría que no es la que coincide con la que tengo en mi computador y nuevamente no habría forma de probar quien está diciendo la verdad. Una posible solución a este problema es quizás un tercero guarde

todas las llaves públicas en un servidor y de esta forma si la llave privada que tengo guardada en mi computador no coincide con la llave pública del servicio podemos revisar la que está en este servidor y tomar esa como la válida. La otra solución un poco mejor es que tu usuario sea tu clave pública, de esta forma si cambian esa clave se crea un nuevo usuario (se me ocurrió esta solución después y es bastante más lógica y elegante).