NOMBRE: Felipe Carlos Jiménez Ortega SECCIÓN: 1

Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencia de la Computación

IIC3253 — Criptografía y Seguridad Computacional — 1' 2021

Tarea 3 – Respuesta Pregunta 1

1. En el caso de la autentificación de algún sitio web como Facebook.com, Youtube.com, etc. que solicitan el correo y la contraseña, uno al momento de ingresar dichos datos, entrega los datos al servidor de dichos sitios web, lo que nos deja vulnerable ya que se confía que quién administra el servidor que guarda las autentificaciones de los usuarios lo haga de manera segura y que no realizará alguna acción maliciosa como puede ser utilizar contraseña y correo para hacerse pasar por uno, o incluso si es que el usuario ocupa la misma contraseña en otros sitios, lograr hacer un cruce de datos de autentificación entre dichos sitios y así obtener la clave para ambos sitios, lo que es una clara deficiencia de seguridad.
   En cuanto a la autorización de algún procedimiento bancario por ejemplo, lo que ocurre es que el sitio web genera un Token para dicha sesión y cada vez que el usuario anteriormente *logeado* desea realizar alguna acción, el navegador de este debe enviar su *request* con el Token enviado, el cual por cierto es guardado en el navegador a través de las Cookies. Supongamos que una persona desea comprar por MercadoLibre y al momento de realizar la transferencia esta ingresa a su banco y con su autentificación realiza la transferencia correspondiente. El problema que hay aquí, es que cuando se llega al momento de pago de la compra, MercadoLibre debe realizar una *request* al Banco diciendo que es tal usuario el que desea realizar la transferencia, pero el problema está en que debe mandar el usuario su Token para que el banco identifique que es dicho usuario el que desea realizar la transferencia, pero es en este momento cuando se manda el Token guardado en las Cookies del navegador que perfectamente algún código malicioso de Javascript de parte de Mercado Libre puede hacerse pasar por el usuario y realizar una transferencia bancaria al hacer un cross-site request.

2. Lo que se puede hacer tanto para autentificar como para autorizar es utilizar algún algoritmo de firma digital tal como lo es el protocolo de firma digital de Schnorr. Para el caso de autentificación se crea una clave pública tanto para el usuario como para el servidor para dicho usuario, además de una clave secreta para ambas que no será compartida. Cuando se solicite al usuario autentificarse, lo que se hará es encriptar el correo del usuario con la firma digital de Schnorr y será enviada al servidor el cual con la clave pública y la función de hash asociada, logrará decriptar el mensaje que corresponde al correo y de esta manera el servidor se asegura que dicha persona es efectivamente la del correo puesto que se supone que nadie más tiene la clave secreta de dicho usuario. En el caso que por algún motivo se logre decriptar el mensaje no hay problema, puesto que el correo electrónico es público.
   Para el caso de autorización, el mensaje que se encripta corresponde a la Token que le entrega el servidor al usuario cuando este se *logea*, la cual es encriptada/firmada de acuerdo al protocolo de Schnorr y que sólo ocurre cuando el usuario firme con su clave secreta, no basta con que el sitio web que tenga *JavaScript* malicioso tenga el Token que se guarda en las *cookies*, ya que debe estar firmado por el usuario y su clave secreta.
   El principal problema que se detecta con esta técnica corresponde a la dificultad que conlleva que las personas entendamos y recordemos nuestra clave pública y privada, puesto que ya tenemos problemas "recordando" una clave, imagínense 2 claves por cada sitio web al que tenemos que registrarnos. Lo que se puede hacer es contar con un dispositivo así como el de *Digi Pass* de los bancos que tenga guardadas ambas claves y que simplemente al ingresarle algún input este calcule el mensaje firmado/encriptado listo para enviar. El problema está en que para personas mayores puede resultar demasiado complicado.