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

IIC3253 - Criptografía y Seguridad Computacional

Sebasthian von Bergen (15635635)

Tarea 3 – Respuesta Pregunta 1

1. (0) Existen varias consecuencias de guardar el nombre de usuario / correo electronico y la contraseña en texto plano. Si se guarda el correo electronico, es facil asociar a quien le pertenece la sesion con otros servicios. Por ejemplo, si me logueo a facebook y este guarda mi sesion con mi correo electronico y ademas me logueo a twitter, un adversario podria deducir que es la misma persona logueada en ambos servicios. Esto lo puede saber estando en cualquier parte de la red por la que pasen estos paquetes, dentro de la red del router, o en la red del ISP, incluso si esta escuchando fuera de una VPN.

   (1) Guardar la contraseña en texto plano es claramente horrible. Cualquier adversario que este escuchando la transmision seria capaz de extraer la contraseña y guardarla en su base de datos. En principio una pensaria que si solo escucha la contraseña y no el nombre de usuario no tendria mucha importancia. Incluso en ese caso es malo. Por ejemplo, si me logueo a facebook, y el adversario solo escucha una contraseña llegar al servidor y la guarda. El adversario puede despues hacer un ataque de diccionario con esas contraseñas en primer lugar antes de utilizar las generadas automaticamente y aumenta mucho la probabilidad de que tenga exito. Si alguna vez el adversario logra encontrar tu nombre de usuario y aplica este ataque es trivial encontrar el par (cuenta, contraseña).

   (2) Si ambos de estos datos se envian encriptados sigue siendo inseguro autentificar con estos. Asumamos que uno envia el par (usuario, contraseña) a facebook encriptado cosa que ellos puedan autentificarte. Cuando el paquete llega ellos lo desencriptan y buscan en su base de datos el par (usuario, contraseña) que tienen guardado. Si coincide te otorgan la sesion. En caso de que alguien robe la base de datos de facebook, entonces ellos obtendrian tu nombre de usuario y tu contraseña, por ambas razones que vimos arriba esto es malo.

   (3) Incluso si facebook guarda un par (usuario, h(contraseña)) con h una funcion one-way, en caso de que la base de datos sea robada, tendrian tu nombre de usuario (lo que es malo) y un hash de tu contraseña. Si el adversario tiene acceso a otra base de datos robada, por ejemplo twitter, y logro obtener tu contraseña, aunque tu luego la hayas cambiado, el puede hacer h(contraseña_robada) y si corresponde al mismo hash robado de facebook, conoce tu contraseña en el otro servicio.

2. Una posible solucion es implementar una funcion h one-way que reciba n+1 parametros, donde n son los datos de sesion pedidos al usuario (usualmente 2, nombre de usuario + contraseña). El parametro extra es una sal, un string de caracteres sin sentido que es constante en el sistema. Al recibir los datos encriptados, inmediatamente aplicar esta funcion h(nombre de usuario, contraseña, sal). En alguna base de datos tiene que estar guardado este valor, si lo esta se puede entregar la sesion (token) al usuario.

   Una de las caracteristicas necesarias de esta funcion es que sea resistente a pre-imagen, cualquier cambio en cualquiera de estos tres parametros genera un cambio en el resultado que no tiene correlacion con el parametro cambiado.

   La sal generada tiene que no ser utilizada por ningun otro servicio, para evitar el problema que vimos en (3). Esta sesion (token) entregada deberia ser temporal y eliminada frecuentemente. Este sistema

requiere mas poder de procesamiento para cada sesion que entrega, pero no es tanto mas para que no valga la pena mantener la seguridad de los usuarios.