NOMBRE: Javier Tramon

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

a) Dentro de lo que es el proceso de autenticación con usuario y contraseña, esta la fragilidad de que la información sea interceptada por algún agente externo y pueda usara si es que esta esta enviada en formato plano. Todo esto devido a que le entregamos al servidor nuestra clave privada confiando en que esta no será mal usada por ellos y que no se filtrará en sus bases de datos, algo totalmente fragil e inseguro. Es por ello que se han tomado distintas medidas para que esto no ocurra, una de estas es encriptar la clave de manera que sea indescifrable, pero esto puede ser atacado de distintas maneras, una de esas es usando un diccionario con las distintas claves a computar, lo que deriva a un proceso limitado de pasos para poder encontrar distintas contraseñas, proceso conocido como Reinbows tables, lo cual sigue dejando vulnerable estas. Además , si las contraseñas son reutilizadas en dos o más plataformas distintas, estas podrían encontrarse rápida mente ya que el proceso de encriptación es el mismo. Al final el tema de tener que enviar una contraseña privada y que esta sea almacenada por la plataforma es un gran problema problema.
El segundo gran problema es el proceso de autorización, donde cada comunicación entre el usuario y la entidad tienen que esta autorizada por ambas partes. Esto en pos de cuidar a ambas partes, la entidad, para no recibir operaciones que no estén permitidas para cierto usuario, y para cuidar al usuario, ya que puede haber operaciones fraudulentas supuestamente a nombre del usuario y no son reales. Un ejemplo de esto es que al almacenar las contraseñas el banco, este puede generar transacciones a nombre de de los usuarios sin permiso del usuario.
Estos son los problemas de auditabilidad dentro de las plataformas que manejan autenticación con usuario y contraseña.

b) Según mi forma de verlo, un buena buena forma para lograr sobre pasar las problemáticas mencionadas son manejándolas por separado. Primero esta el solucionar el manejo de autenticación que no sea tan frágil para el usuario, a tal punto de tener que entregar la contraseña privada para autenticarse. Mientras que para la autorización, un sistema que no sea vulnerable y solo utilizable por el usuario que manifieste la ordenes autorizadas.
Para el caso de la autenticación, yo pienso que lo mejor es usar un sistema clave publica y privada, donde se envié el usuario y la firma de este con el algoritmo elGammal de este mensaje y el servidor busca la clave publica de este usuario para corroborar que envía esta autenticación para corroborar que es el usuario el que envía su nombre firmado. Primero, en el proceso de registro para la plataforma se generan dentro de la plataforma web la clave privada para el usuario, y la clave publica que es enviada al servidor. Posteriormente, almacenando esta clave privada, hay dos formas de manejarlo, una es que el usuario al iniciar sección entregue esta calve privada para que la pagina web genere una firma del mensaje del nombre del usuario y sea enviada como clave, o la otra es que el usuario genera la firma dentro de su pc y entregue este dato con el nombre de usuario.
Para el caso de la autorización, el proceso sería usando un hardware distinto al pc para generar el token a enviar. La idea es que el dongle genere el token que autoriza cada una de las solicitudes dentro de la plataforma por un rango de tiempo definido según la sensibilidad de la petición. Esto quiere decir, que para autorizar el manejo dentro de la plataforma para revisar información, solo con la autenticación basta. Tal ves para información sensible se necesite un token que dure unos minutos para poder revisar la información y otras del mismo grado de sensibilidad, y para solicitudes que conlleven alto riesgo, siempre se pida el token

previamente al enviar, con un único uso por petición. El dongle tiene la cualidad de generar los token en base a la clave privada previamente generada por la plataforma cuando se registró, por lo que el proceso de autorización va a ser muy semejante a lo que vimos para la autenticación. Esto se puede hacer más sencillo haciendo un dongle virtual que se maneje dentro de hardware especialidad en las componentes de las CPU para poder virtualizarlo, y así generar las token cuando se le solicite con una clave de autorización que solo sepa el usuario dentro de la misma pc de este.
Ambas medidas tiene el grado de riesgo de que la clave privada pueda ser tomada sin autorización si es que se logra entrar a la computadora, por lo que una buena medida para aminorar los riesgos para este tipo de ataques es encriptar la clave de alguna manera asimétrica con algún pin de corto largo para autorizar su uso