

UNIVERSIDAD RAFAEL LANDIVAR DE GUATEMALA
Facultad de Ingeniería en Sistemas de Información
Curso de Estructura de Datos II – Jornada Matutina

AUTENTICACIÓN EN UN SISTEMA DE CÓMPUTO CON FUNCIONES HASH

Ensayo Técnico

Max Rubén Cortez Domínguez
1052403
Guatemala, 15 de Febrero del 2007

La seguridad en los sistemas informáticos es de carácter importantísimo, ¿Que sería de un sistema bancario si cualquiera pudiera entrar y modificar el saldo en su cuenta?, ¿Qué pasaría si hoy por la tarde nos atrapa la policía y nos acusa de haber matado a alguien?, ¿Qué pasaría si chocamos nuestro carro hoy en la noche y al llamar a la aseguradora nos dicen que lamentablemente no nos pueden atender porque en el “sistema” aparecemos como usuarios morosos?

Estos casos son un pequeños ejemplos de cosas que pueden pasarle a cualquier persona que tenga su “vida ingresada” en un computador. Es por eso que en un sistema es muy importante estar pendiente de la seguridad y se le debe poner mucha atención a quienes son las personas “confiables” que pueden tener acceso al sistema.

Una forma cuidar la seguridad en un sistema de cómputo es estableciendo ciertas directrices en cuanto a que personas están autorizadas a ingresar a las distintas opciones del sistema de cómputo, por ejemplo en un sistema de caja registradora, solamente el gerente de la tienda puede ver el historial de todas las transacciones que se han realizado en el día, también en una tienda están los supervisores de la tienda que al igual que el gerente tienen autorización para poder hacer devoluciones, pero no para ver el historial de todas las transacciones que se han realizado en el día, dejando al cajero únicamente con la opción de poder vender mercadería. Para que esta discriminación de permisos sea posible debe existir una autenticación por parte de cada usuario ante el sistema de cómputo, esta autenticación en la mayoría de los casos se hace mediante una contraseña y un usuario.

Seguramente al desarrollar un sistema de cómputo con discriminación de usuarios se tiene que pensar en donde se van a guardar estas contraseñas, ya que caeríamos en un error tremendo si las almacenamos de la misma forma que el usuario las ingresa, por poner un ejemplo si mi contraseña es “060484” y el sistema de cómputo lo almacenara en un archivo de texto de la siguiente forma “usuario: maxcortez, contraseña: 060484” cualquier persona con conocimientos básicos sería capaz de entender cual es mi contraseña y ya podría autenticarse ante el sistema de cómputo como si fuera yo. Entonces en este punto es donde surge la inquietud de hacer mas complicado la usurpación de identidades.

Para poder hacer esto nos podemos apoyar en funciones matemáticas, llamadas funciones hash. En su forma básica una función hash realiza una transformación única entre un mensaje de longitud arbitraria a un mensaje de longitud constante. La función hash toma como entrada una cadena de bits de cualquier longitud, y lo introduce en una ecuación matemática previamente definida y el resultado es un valor único e irreplicable (el caso teórico de los algoritmos md5 y sha-0). Otra fortaleza de las funciones hash es que en según la función matemática que utilicemos podemos hacer que solo pueden ser transformadas de la cadena original al resultado, pero nunca pueden ir de regreso; es decir que existe una función F tal que $F(k) = n$, pero no existe ninguna función G tal que $G(n) = k$, donde k es nuestra contraseña original y n es nuestro resultado de aplicarle una función hash a k .

Todo esto quiere decir que al momento de diseñar un sistema de cómputo debemos dedicar especial atención a la autenticación de usuarios, preparándonos para un ataque haciendo que en el momento que se crea un usuario, la contraseña que ingresa sea operada a través de una función hash y luego almacenada. Y en la ejecución de nuestro sistema podemos hacer algo similar y es que cuando un usuario quiera ingresar debemos tomar la contraseña que ingrese, operarla por la función hash y el resultado compararlo con el valor almacenado. Así habremos autenticado a nuestro usuario sin almacenar en ningún momento la contraseña original.