Jose Daniel Acuña Solano 2018145020

Protocolos de autenticación

Autenticación basada en una clave secreta compartida

Consiste en que ambas partes comparten una llave secreta que usan para desencriptar un mensaje, el proceso es que uno envía un numero aleatorio largo, el receptor encripta el numero y lo devuelve, así se valida que para generar el resultado se uso la llave correcta. Como muchas cosas imperfectas este método es vulnerable a ciertos ataques, por lo que se recomienda usar las siguientes cuatro reglas:

1. Forzar al iniciador a proveer su identidad antes de que la entidad segura lo haga, para evitar brindar información de manera insegura.
2. Que ambas entidades usen llaves diferentes.
3. Que ambas entidades usen retos diferentes, como: uno usa números pares y el otro impares.
4. Asegurarse de manejar correctamente concurrencia para evitar problemas con sesiones paralelas.

Establecimiento de una clave compartida: el intercambio de claves de Diffie-Hellman

Protocolos anteriores implican que se comparta una llave secreta, pero esto ocasiona problemas porque no hay manera global de certificar la autenticidad de toda lleva, por lo que se idean protocolos que pueden compartir una llave de manera segura sin importar de que exista un tercero interceptando.

Se elijen dos números bajo ciertas condiciones que son compartidos entre las entidades de manera pública; adicionalmente crean dos números que mantiene en secreto y no comparten; luego utilizando los numero públicos compartidos y número secreto se genera un mensaje (usando aritmética) que se comparte abiertamente; finalmente en los extremos se hacen operaciones inversas para obtener los números secretos y así se comparten llaves privadas sin enviar la llave explícitamente.

Autenticación que utiliza un centro de distribución de claves

Este método implica un intermediario que regula la veracidad de llaves para certificar la autenticidad de un ente, y así establecer la conexión segura. Esta idea compromete que si el centro de distribución es hackeado compromete la seguridad de todos los participantes.

Jose Daniel Acuña Solano 2018145020

Autenticación utilizando Kerberos

Es un sistema que involucra tres servidores, de ahí el nombre Kerberos:

1. Servidor de autenticación
2. Distribuidor de tiquetes
3. Servidor principal (el que procesa las consultas)

Después de un intercambio de mensajes se garantiza la identidad del usuario a lo largo de los servidores de consultas, dándole acceso sin requerir que comparta su contraseña privada. Es un protocolo muy seguro porque los mensajes tienen un tiempo de vida de milisegundos, por lo que, aunque sean interceptados ya van a haber expirado y cumplido su propósito antes de que sean crakeados.

Autenticación utilizando criptografía de clave pública

Es un mecanismo muy sencillo y extremadamente efectivo, se comparten llaves publicas entre las entidades, estas se usan para encriptar, pero no sirven para desencriptar; por lo que solo el dueño de la llave privada sabe como leer el mensaje.