Resumen #9 - (r9)

Esteban Ignacio Durán Vargas - 2020388144

IC - 7602 - 2023 I Semestre

8.7 PROTOCOLOS DE AUTENTICACIÓN

Autenticación verifica la identidad de un acceso remoto ante la posibilidad presencia de un intruso activo y malicioso. Verifica si se está comunicando con un proceso específico. El servidor de archivos sabe con quién está hablando y para verificar la autorización busca entradas en su base de datos. La mayoría de protocolos tienen una clave de sesión secreta encriptada con clave simétrica (por rendimiento para minimizar tráfico a las claves secretas).

8.7.1 Autenticación basada en una clave secreta compartida

Se comparte una clave secreta. Se envía un número aleatorio que se transforma a una forma y se refresa (desafío respuestas). El receptor elige un desafío, un número aleatorio (marcas aleatorias o nonces) grande y lo envía al emisor en texto llano. El emisor encripta el mensaje con la clave y envía el texto cifrado. El receptor ve el mensaje y sabe que viene del emisor porque otra persona no pudo generarlo. Como es tan grande no es probable que se haya visto en otra sesión. Ya el receptor está seguro de con quién habla. El emisor elige un número al azar y lo envía al receptor con un texto llano y cuando este responde ya sabe con quién habla. Pueden establecer una clave de sesión y encriptarla y enviarla al receptor.

Se pueden eliminar algunos mensajes empezando el desafío respuesta del emisor primero. Pero esto se vence con un ataque de reflexión al abrir múltiples sesiones con el receptor. Pero cuando este ataque afirma que es el emisor y el receptor lo desafía se atora porque no conoce la clave de ambos entonces puede abrir una segunda sesión, proporcionar un nuevo desafío con el mensaje que envió el receptor que lo regresa encriptado que da la información para completar la primera y convence al receptor que es el emisor.

Para diseñar un protocolo de autenticación correcto se siguen estas reglas. Se obliga al iniciador que pruebe ser quien es antes del que contesta, obligar al iniciador como contestador a usar claves diferentes, obligar al iniciador y el contestador a utilizar conjuntos diferentes para elaborar los desafíos y hacer que el protocolo resista ataques con otra sesión paralela. Si en vez de una segunda sesión con el receptor fuera una computadora de propósito general con múltiples sesiones se puede iniciar con el emisor anunciando su identidad, el intruso intercepta el mensaje y comienza otra sesión con afirmando que es el receptor. Al tratar de probarlo se atora pero puede regresar a la primera sesión enviar el desafío que obtuvo para que el emisor se lo responda y obtiene la información para responder el desafío del emisor. El intruso puede esperarse a que el emisor envíe el desafío y envía el mensaje de la sesión 2 para que lo encipte y lo envíe de vuelta cuando lo reciba y así tiene 2 sesiones autenticadas. En el primer ejemplo se tiene una sesión autenticada con el receptor pero se pudo haber detenido con protolos de autenticación, aquí 2.

UInprocolo más simple que tiene altas probabilidades de ser correcto utiliza HMAC (IPsec) que inicia con el emisor enviando una marca aleatoria que el receptor responde con su propia marca y enviándola con HMAC que se forma con una marca aleatoria del emisor, receptor, las identidades y la clave secreta compartida. Se les aplica un hash y cuando el emisor lo recibe tiene una clave que eligió el mismo, una clave como texto llano y dos identidades y la clave secreta que ya sabía. Si corresponde con el HMAC del mensaje ya sabe con quién

habla y responde al receptor con una HMAC de 2 marcas aleatorias. Los intrusos no puedan obligar a una de las 2 partes a encriptar el hash a un valor de su elección.

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

Si no tienen una clave secreta compartida existen protcolos para estabelecer como el intercambiod e claves de Diffie-Hellman. Ambos tienen que tener 2 números grandes, 1 primo n y el otro es el primero menos 1 entre 2 llamado g, con ciertas condiciones. Pueden ser públicos. El emisor escoge un número grande x y mantiene secreto y lo mismo para el receptor pero con y. El emisor inicia el protocolo de intercambio de claves enviando al receptor (n, g^x mod n) un mensaje que este responde (con g^y mod n) el cual eleva a x para obtener (g^y mod n)^x que el receptor le hace una similar pero con los números secretos intercambiados. Ambos dan como resultado g^(xy) mod n y se genera una clave compartida. Un intruso conoce g y n pero solo con g^x mod n no puede encontrar x.

El problema es que cuando el receptor obtiene el triple no sabe de dónde proviene. Mientras los involucrados escogen x y y, el intruso escoge uno aleatorio; el emisor envía el mensaje, el intruso lo intercepta y envía un mensaje al receptor con los valores de g y n pero con su propio valor z en vez de x. Regresa el mensaje al emisor. Luego cuando se envíen más mensajes al emisor el intruso podrá interceptarlo. Los emisores calculan las claves junto con la del intruso y establecen una clave de sesión con este, lo cual permite modificarlo o almacenarlo. Se le conoce como ataque de la brigada de bombero o de hombre en medio.

8.7.3 Autenticación que utiliza un centro de distribución de claves

Para muchas personas la administración de claves puede ser una carga. Se puede introducir un KDC (centro de distribución de claves confiables) donde cada usuario tiene una clave compartida con este que las administra y autentica. El emisor elige una clave de sesión y le indica al KDC que el receptor; se encripta el mensaje para extraer la identidad de este y envía el mensaje al receptor. La encripción es con la clave del receptor. Cuando se desencripta sabe el emisor y la clave. El KDC sabe que el mensaje es del emisor y el receptor sabe que el mensaje viene del KDC por las claves. El protocolo tiene un defecto importante, si un intruso copia los mensajes de un emisor y los repite con el receptor para que el receptor crea que vinieron otra vez del emisor. Se llama Ataque de repetición. La primera solución es incluir una marca de tiempo para que se descarte, pero los relojes de red no están sincronizados y deben tener un buen rango de tiempo en el que se puede repetir. La segunda es una marca aleatoria en cada mensaje; se deben recordar todas las previas y rechazar reptidas. Debe recordar para siempre y si una máquina falla pierde la lista y es vulnerable. Las marcas aleatorias y de tiempo pueden combinarse para limitar cuánto tiempo deben recordarse.

Otro método es el de Needham-Schroeder. Comienza con el emisor diciendo. Empieza con el emisor pidiendo al KDC hablar con el receptor y se le da una marca aleatoria grande. El KDC regresa el mensaje con el número, clave de sesión y boleto para que regrese al receptor. Con el número aleatorio el emisor está seguro que el mensaje viene actualizado. La identidad del receptor está encerrada para que no pueda ser reemplazada con la de un intruso. El boleto encriptado con la clave del receptor se incluye dentro del mensaje encriptado. El emisor envía el boleto con un nuevo número aleatorio, encriptado con la clave de sesión y el receptor regresa la clave con una marca aleatoria -1 para probar al emisor su identidad. Resta 1 para que no se hayan robado el número del pasado. El emisor está convencido de hablar con el receptor. El último mensaje es para que el receptor asegure la identidad. Ambas partes generaron un desafío y respuesta. Tiene una debilidad si un intruso consigue una sesión de clave antigua en texto llano y puede iniciar una sesión con el receptor y repetir el mensaje con clave comprometid. Se corrige este problema; el emisor genera números aleatorios como identificador y la clave propia para retar al receptor; quien construye un mensaje nuevo de la parte encriptada

del mensaje del emisor y del suyo. Ambas partes identifican sus identificadores comunes y desafíos. El KDC verifica que ambas partes sean igual. genera una clave de sesión y encripta dos veces para ambos. Cada mensaje tiene un número aleatorio del receptor para probar la identidad del KDC. Ambos tienen la misma clave de sesión y se comunican con una copia idéntica de la clave de sesión.

8.7.4 Autenticación utilizando Kerberos

Kerberos se basa en la variante anterior pero supone que todos los relojes están bien sincronizados. Involucra a una Authentication Server que verifica usuarios durante el inicio de sesión, un Ticket Granting Server que emite pruebas de boletos de identidad y un servidor que hace el trabajo del emisor. El AS es como KDC que comparte una contraseña con cada usuario. El TGS emite boletos que puedan convencer a servidores reales de que las identidades son correctas.

Primero el emisor inicia sesión como texto llano, regresa una clave de sesión y boleto para el TGS. Los elementos se empaquetan y encriptan con la clave del emisor. El mensaje llega, la estación de trabajo pide la contraseña del emisor que se usa para generar la clave del emisor para desencriptar el mensaje y obtener la clave de sesión y el boleto TGS. La estación de trabajo sobreescribe la contraseña del emisor para que no esté en la estación de trabajo por mucho tiempo. Al iniciar la sesión el emisor le dice que quiere contactar al receptor (Servidor de archivos); la estación envía un mensjae al TGS preguntando por el boleto de este que se encripta con la clave del TGS para probar el emisor. El TGS responde con la clave de sesión entre las partes y se regresan 2 versiones, una encriptada por la de sesión y otra con la clave del receptor. Un intruso puede copiar el mensaje 3 pero la marca de tiempo no lo permite y no puede reemplazarla porque no conoce la clave de sesión con el TGS. El emisor tiene su sesión. Tiene marcas de tiempo para probar que habla con el receptor. El emisor se comunica con el receptor con la clave, si se necesita otro servidor se repite el mensaje con el TGS pero con el boleto del otro. Ahora el emisor puede acceder a servidores de manera segura. El servidor realiza su propia autorización y determina las acciones que el emisor puede realizar. Existen dominios con AS y TGS propios. Para conseguir un boleto a un servidor distante, el emisor solicita al TGS un boleto para el distante y se lo da si está registrado que le da el boleto valido al emisor y puede realizar negocios con otro domino.

V5 es más elegante y con menos sobrecarga y usa OSI ASN.1 para los tipos de datos y cambia protocolos. Sus boletos duran más y permite que sean renovados. No depende de DES como V4 y soporta dominios porque delega la generación de boletos a múltiples servidores.

8.7.5 Autenticación utilizando criptografía de clave pública

El emisor necesita la clave pública del receptor. Si existe una PIK para certificados el emisor puede pedir la del receptor. Cuando el emisor verifica la firma, envía el mensaje al receptor con la identidad y la marca aleatoria. El receptor no tiene idea de quién lo envió entonces pide al servidor la clave pública del emisor y le envía a al emisor uno con el número aleatorio del emisor y su propia marca y la clave de sesión. El emisor lo desencripta con una clave privada, ve su amrca y sabe de quién. Sabe que es una actualización, no una repetición porquie acaba de enviarle al receptor la marca. El emisor accede a la sesión y envía un mensaje y cuando el receptor ve su marca encriptada con la clave de sesión, verifica la marca del emisor.

Un intruso puede fabricar un mensaje 3 y engañar al receptor para que investigue al emisor, pero el emisor verá una marca que no envió y para.