UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

DEPARTAMENTO DE
ELECTRONICA

PROTOCOLO SSH

Ignacio Veragua C., Pablo Hernández D.

Redes de Computadores (ELO-322)

13 de Septiembre, 2019

Resumen

Existen protocolos de red que permiten a un host conectarse remotamente a otro vía terminal, permitiendo administrar el sistema, controlar procesos y transferir archivos. Entre ellos SSH (Secure Shell) destaca por su capacidad de encriptación de la sesión de conexión y autenticación de usuario y servidor. Se aborda el estudio del funcionamiento de este protocolo, enfatizando en los servicios de seguridad que ofrece y cómo se establece la conexión. Se estudian las técnicas de cifrado simétrico, asimétrico y hashing, y se expondrá cómo es que SSH las utiliza para ofrecer una transferencia de datos segura. Finalmente se ilustra con una actividad práctica el intercambio de paquetes entre cliente y servidor, desglosando el contenido de cada uno.

Introducción

Desde el advenimiento de Internet, se han desarrollado múltiples protocolos de red que permiten a usuarios acceder remotamente a datos almacenados en distintas partes del mundo. Dentro de esta categoría de protocolos existen aquellos que permiten el acceso a hosts en la red, habilitando la administración de estos dispositivos así como también su mantención de manera simple y rápida sin necesidad de ubicarse físicamente en un mismo lugar. Dado que Internet fue desarrollado pensando en usuarios confiables, los protocolos más populares a fines del siglo XX tales como Telnet, ftp y rsh ofrecían como servicio el acceso remoto en modo terminal, transferencia de archivos y ejecución de comandos en un host remoto respectivamente de manera insegura, comunicándose sin ningún tipo de encriptación o autenticación. Dada la aparición de usuarios maliciosos en la red, se hace necesario crear formas de resguardar la integridad y seguridad de la información.

Un aspecto por mejorar: La seguridad

Estos protocolos antes mencionados, que son de acceso remoto, como mencionamos, carecen de una parte muy importante, que es la seguridad, ya que no poseen un mecanismo que le de protección a los mensajes en la conversación,

ni al canal en general en que estos se transmiten. De ésta problemática nace Secure Shell o SSH, que es un protocolo (capa aplicación) de acceso y administración remota y que permite reemplazar estos protocolos deficientes añadiendo medios para encriptar la sesión de conexión y autenticar tanto al cliente como al servidor

¿Cómo es que SSH soluciona esto? ¿Cómo funciona SSH?, a continuación veremos en qué consiste el protocolo SSH.

Primeramente, SSH funciona con el protocolo TCP en capa transporte en puerto 22, y los elementos que proporcionan la seguridad a éste protocolo, son principalmente sus 3 tecnologías de cifrado: Cifrado simétrico, cifrado asimétrico y hashing. Analizaremos en mayor profundidad estas 3 tecnologías ya que son la parte fundamental y lo que hace que SSH sea tan efectivo.

El **cifrado simétrico** es la tecnología principal, y la que a fin de cuentas, vale para transmitir los datos útiles. Ésta tecnología lo que hace es que se genera una clave privada, o también llamada clave secreta compartida, ya que ésta clave es compartida entre el cliente y el servidor en la conexión ssh, este cifrado es el que se usa durante toda la conexión ssh, ya que durante esta conexión, encriptan y a la misma vez desencriptan los mensajes enviados en el canal. Esta clave nunca es transmitida, si no que es generada por cada parte con un algoritmo de intercambio de claves, el cual se ponen de acuerdo en cual usar, y generan la clave desde los datos públicos de cada parte.

El **cifrado asimétrico**, a diferencia del simétrico, consiste en que las dos partes generan un par de claves pública-privada, donde la pública es compartida abiertamente y la privada nunca es revelada. El hecho es que, los mensajes que se encriptan con la clave pública, solo pueden descifrarse con su respectiva clave privada. Éste mecanismo, el cual es muy seguro, sólo se usa para durante el algoritmo de intercambio de claves (del c.simétrico), vale decir, que se usa sólo para intercambiar los parámetros e información de manera segura, para luego establecer un canal de forma segura, con información que no es compartida a terceros.

El **hashing** es la tecnología que se usa para verificar la autenticidad de cada uno de los mensajes.

Lo importante es entender cómo trabajan estas 3 tecnologías a lo largo del proceso para asegurar el canal y que la conexión ssh sea verdaderamente segura; la figura 1 nos ayuda a ver mejor este proceso el cual describiremos a continuación.

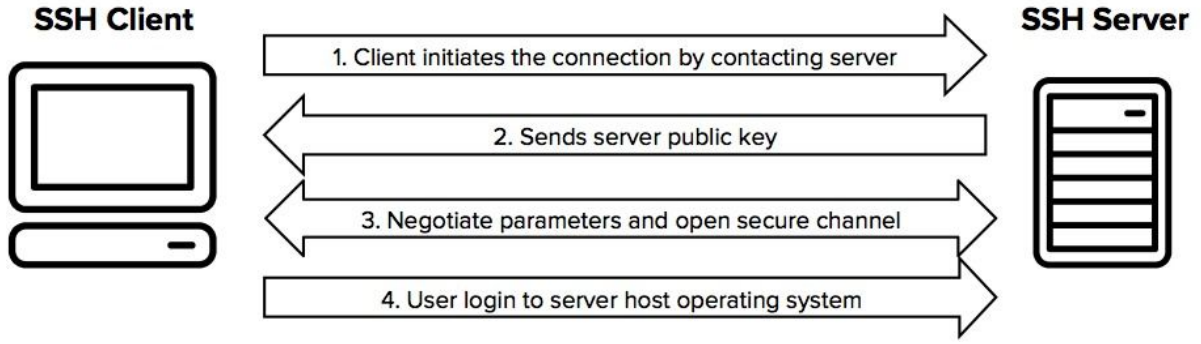

Figura 1 : Diagrama del proceso de la conexión ssh

La conexión se inicia con el cliente contactando al servidor (aquí se comunican la versión del protocolo que soportan), y el servidor responde con su clave pública (y su versión de ssh), obtenida la clave pública del servidor, se transmiten los parámetros que cada uno maneja (esto es, la negociación de parámetros), con los que finalmente acuerdan en utilizar determinado algoritmo de encriptación, lo anterior como vimos antes ocurre usando el cifrado asimétrico.
Con este proceso finalizado, y con el cliente y el servidor ya puestos de acuerdo cómo generarán la clave compartida, generan la clave compartida según el algoritmo que determinaron cada uno y los datos públicos de cada uno, y esto abre paso a la apertura del canal seguro, en donde ya tienen la clave secreta compartida, esto es equivalente a decir, que están usando el cifrado simétrico. Se sigue con la autenticación del usuario, y la conexión ssh es establecida por completo.

Conclusión

Reconocemos por supuesto que la esencia de SSH es su seguridad, por lo que analizamos los métodos y el mecanismo con el que SSH hace segura la transmisión de datos de manera remota. Se mencionó anteriormente, pero cabe destacar el

hecho de que la clave compartida con la que encriptan los mensajes en la conexión ssh ya establecida, nunca es revelada ni transmitida, el cliente y el servidor al final de todo el proceso son capaces de generar la misma clave cada uno por separado.
Éste análisis que se hizo de ssh, es para entender el trasfondo del protocolo, es decir, no nos enfocamos en las muchas aplicaciones a las que ssh da acceso, si no en el estudio más profundo de cómo funciona ssh y ver que efectivamente da seguridad al canal y lo que abre paso a distintas aplicaciones en la red.
Hoy en día SSH es ampliamente utilizado en la mantención y administración de servidores en todo el mundo, contando con versiones libres instaladas por defecto en sistemas UNIX y clientes libres instalables en sistemas Windows.

Resultado actividad práctica

Como actividad se capturan paquetes con Wireshark de una conexión SSH al servidor Aragorn del departamento de Electrónica de la UTFSM. Los paquetes capturados pueden apreciarse en la figura 2. En este caso particular las IPs del cliente y servidor corresponden a 192.168.0.19 y 200.1.17.195 respectivamente. La conexión se inicia con un requerimiento desde el cliente al servidor (paquete No. 29 de la captura) en el que se notifica la versión del protocolo disponible (SSH 2.0). El servidor responde al cliente con un paquete que contiene la versión del protocolo que éste maneja (SSH 2.0), además de especificar el sistema operativo instalado.

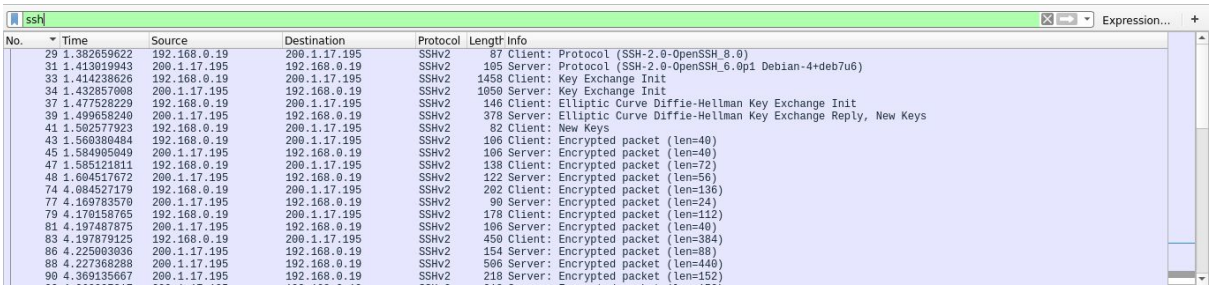

Figura 2 : Paquetes capturados con Wireshark al iniciar sesión SSH

Luego de que el cliente recibe la versión del protocolo de parte del servidor, se procede a la inicialización del intercambio de llaves con los paquetes Key Exchange Init, No. 33 y 34 de la captura. En ellos tanto cliente como servidor envían

información respecto de los algoritmos de intercambio de llaves (para cifrado simétrico), encriptación y hashing que manejan y se encuentran disponibles, tal como se puede apreciar en las figuras 3 y 4. Los algoritmos a utilizar son escogidos buscando el primer algoritmo de la lista del cliente que esté disponible también en el servidor.

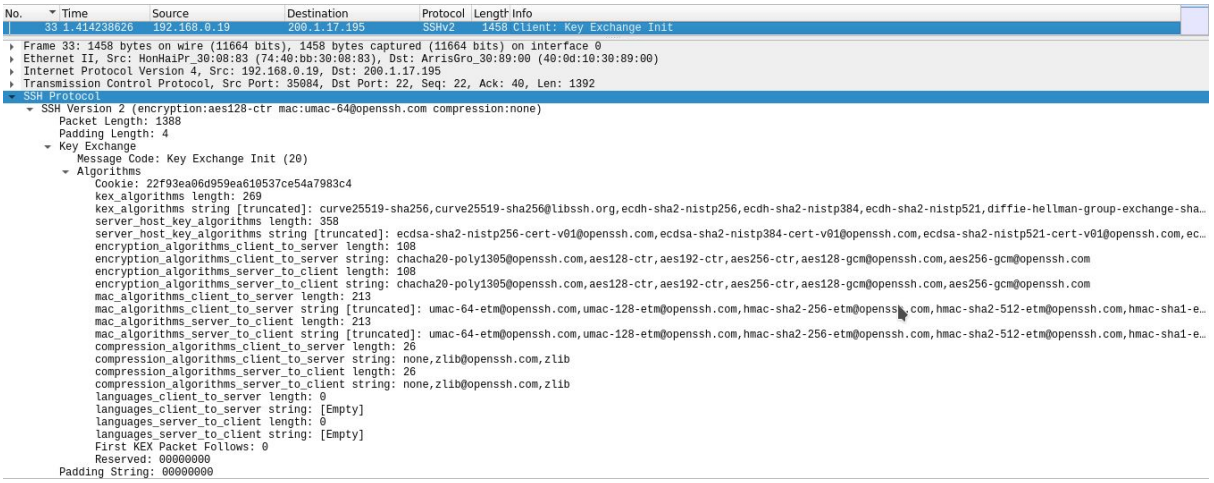

Figura 3 : Paquete inicialización de intercambio de claves cliente.

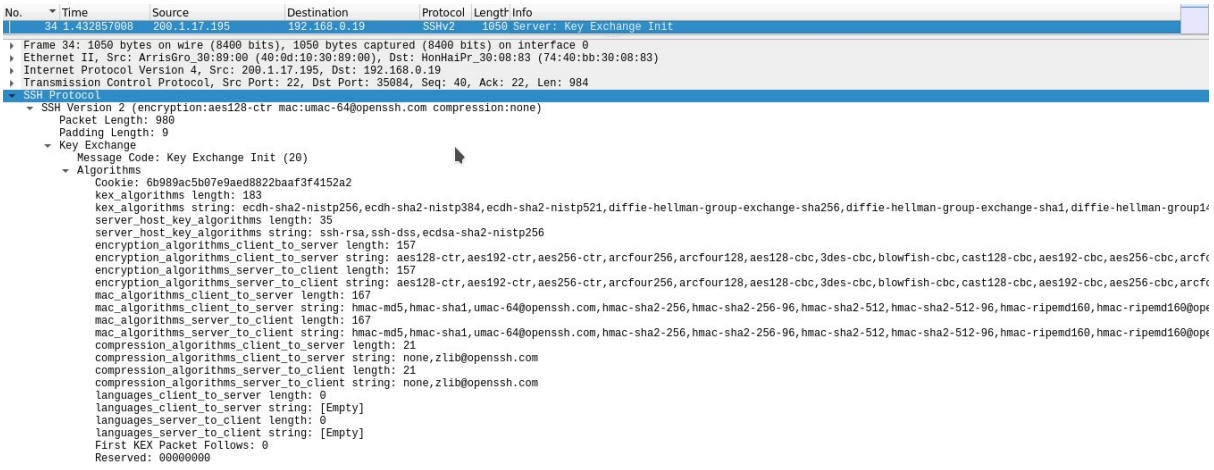

Figura 4 : Paquete inicialización de intercambio de claves servidor.

El algoritmo elegido para realizar el intercambio de claves es Elliptic Curve Diffie-Hellman, y se realiza en los paquetes No. 37 y 39 tal como se puede apreciar en la figura 2. En primer lugar el cliente envía un mensaje al servidor con el algoritmo a utilizar para el intercambio además de su clave pública, con la que el

servidor calcula la clave simétrica a utilizar para cifrar la sesión SSH. Luego, el servidor responde con su clave pública para que el cliente puede calcular la misma clave simétrica, además de enviar un mensaje codificado “New Keys”, que significa que en adelante se comenzará a utilizar los algoritmos de cifrado acordados. Este intercambio se muestra en las figuras 5 y 6. El cliente responde con un mensaje “New Keys”, luego del cual todos los paquetes se encuentran encriptados, tal y como se aprecia en la figura 2.

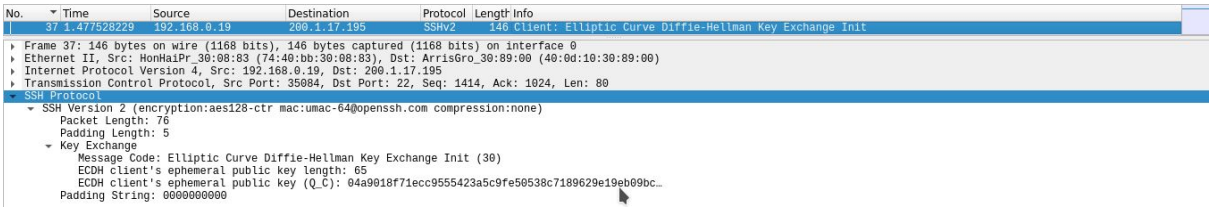

Figura 5 : Paquete intercambio de claves enviado por cliente

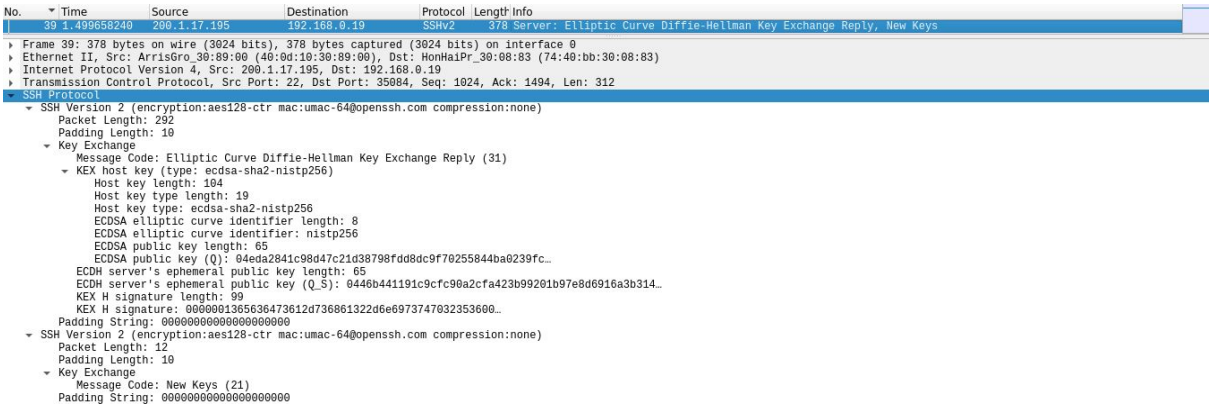

Figura 6 : Paquete intercambio de claves enviado por servidor

Referencias

https://www.hostinger.es/tutoriales/que-es-ssh

https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ssh.html#FTN.AEN20903

https://www.ssh.com/ssh/protocol/