UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA

DEPARTAMENTO DE ELECTRÓNICA

“Encriptación en Redes”

Integrantes: Patricio Rodríguez.

Javier Vergara.

Sergio Vergara.

Profesor: Agustín González.

Fecha: 28 de Julio de 2014.

Resumen

Un tema importante actualmente en la redes de computadores, es el poder cifrar la información, puesto que nadie quiere que un desconocido sepa nuestras contraseñas de acceso, ni los mensajes que le envío a una persona en particular. Debido a esto modelaremos una situación real para poder explicar acerca de la encriptación y utilizar los conocimientos aprendidos de las redes de computadores.

Se buscará en este trabajo que 2 personas en computadores distintos puedan intercambiar información (chat), para esto nos basaremos en un arquitectura de red conocida como P2P centralizada, ya que estos dos clientes además solicitan una lista de los usuarios conectados para poder chatear, a un servidor que contiene la información del cliente, es decir Usuario y contraseña, para poder acceder a chatear.

Se utilizó la API de java para poder crear las aplicaciones Cliente y Servidor, por su fácil uso. A ambas aplicaciones se les agregó la encriptación y desencriptación usando la librería PBEStringEncryptor que cumplía con los requisitos que buscábamos. Uno de esos requisitos era que usara una llave para cifrar la información y que permitiera la manipulación de esta, tanto en el computador donde se corría el servidor como el cliente.

Se buscó primeramente un establecimiento de conexión usando ip's públicas y no dio resultado, por lo que lo intentamos usando IP privadas en una subred y surgieron problemas de conectividad, algunos paquetes no llegaban al destino y puesto que el establecimiento entre cliente y servidor está basado en un protocolo TCP según nuestro diseño, cualquier pérdida botaba el programa.

Se utilizó el comando ping y el programa Wireshark para darnos cuenta de estos detalles y poder solucionarlos. Además con Wireshark se pudo contrastar entre un mensaje cifrado, que se pudo observar claramente en el análisis de los paquetes enviados, y los no cifrados.

Introducción

Se abordará en este proyecto el tema de la encriptación en redes, por lo tanto es necesario que conozcamos cual es su importancia en la actualidad y cuál será su importancia en el futuro. Para ello se espera adquirir conocimientos acerca de cómo funcionan la seguridades de la información en las distintas capas del modelo OSI, acerca de los tipos de encriptación, las firmas digitales y un problema tan importante como lo es Man in the Middle. Se espera encontrar una solución a un problema de una situación particular que es la que escogimos para la parte práctica del proyecto, como lo son el impedir que personas externas tengan conocimiento de nuestras contraseñas de acceso a un chat y de los mensajes que intercambiamos con una persona que nosotros elegimos compartir.

Seguridad en la información

Seguridad a grandes rasgos

En esta área surge el concepto de criptografía, que consiste en el estudio de algoritmos, protocolos y sistemas que se utilizan para aportar seguridad en las comunicaciones, a la misma información y los entes comunicantes. Básicamente nos encontramos en una situación de este estilo: "A" quiere comunicar algo a "B", un mensaje, pero no quiere que nadie más sepa que contiene dicho mensaje. "A" encripta el mensaje utilizando una clave de encriptado, que da como resultado el mensaje encriptado, que le llega a "B" y éste lo desencripta con una clave de desencriptado, pudiendo leer el mensaje escrito por "A". Podría llegar "C", tratar de obtener la clave secreta para recuperar el mensaje y enterarse que se lo que "A" le está diciendo a "B". En un sistema seguro, el mensaje sólo puede ser leído si se tiene la clave de desencriptado. A grandes rasgos la encriptación puede dividirse en 2, simétrica y asimétrica. La simétrica, o de clave privada, consiste en que la llave de encriptación de "A" y la de desencriptación de "B" es la misma. Entonces ambas partes, "A" y "B" deben proteger la clave que utilizan para comunicarse, pues de no ser así alguien externo podría "escuchar su conversación". Por otro lado, la encriptación asimétrica, o de clave pública, existen 2 claves, una pública y una privada que las proporciona el mismo ente. La encriptación asimétrica posee un uso particular con respecto a la autenticación, es decir, el receptor puede comprobar la identidad del emisor del mensaje. Esto corresponde a las firmas digitales, que con el uso de claves públicas y privadas, el receptor verifica que la información es fidedigna. La firma digital tiene un ataque posible, Man in the Middle (hombre en el medio), que consiste en que el atacante se posiciona en el medio de la comunicación entre "A" y "B" y cambia la información, haciéndole llegar a "B" su clave publica del atacante y luego el mensaje con la firma del atacante, en el lado de "B", el resultado de procesar la firma con la clave publica que recibió y el mensaje van a coincidir, y pensará que el mensaje lo envió "A", cuando en realidad lo envió el atacante.

El problema anterior de MITM, es solucionado con los certificados digitales. Un certificado digital básicamente se utiliza para autenticar la clave publica que "A" le envía a "B" en la comunicación, es decir, corresponde a una firma digital cuyo mensaje es la identidad de "A" en este caso y su clave pública, el que genera este certificado digital es una autoridad central, CERTIFYING AUTHORITY (CA) .

Seguridad en niveles del Modelo OSI

El cifrado es un elemento que podemos encontrarlo en capas como:

Enlace de datos: La ventaja del cifrado de enlace es que tanto las cabeceras como los datos se cifran.

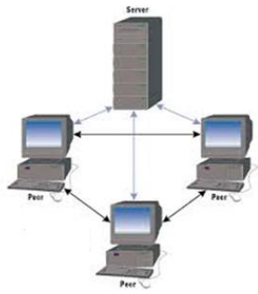
Transporte: TLS (Seguridad de la capa de transporte) es un protocolo que cifra los mensajes y los entrega de un modo seguro.

Red: Las redes Wi-Fi son prácticas y cada vez más habituales. Pero deben protegerse. Lo normal es hacerlo mediante WEP o WPA, que cifran la información de la red inalámbrica.

Aplicación: La API de Java cuenta con paquetes para implementar criptografía en esta capa.

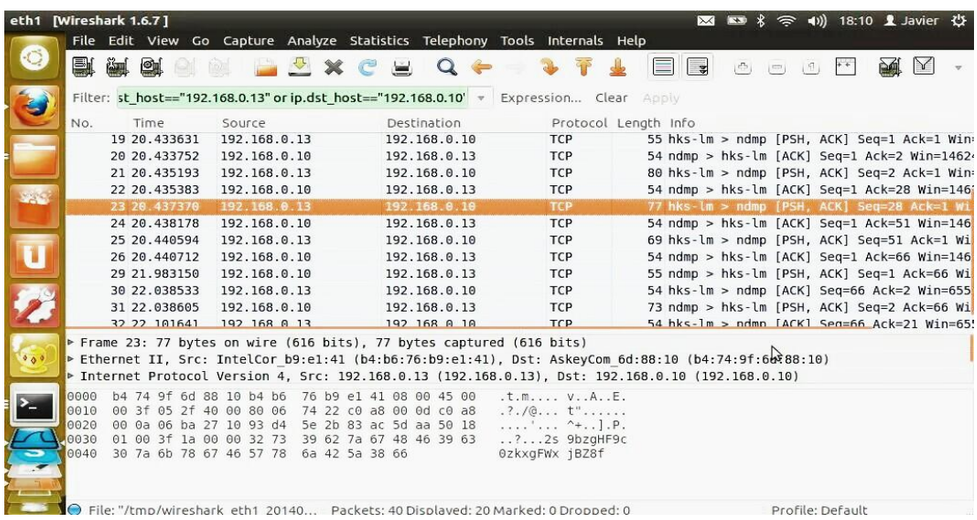
Desarrollo Práctico

Utilizando lo visto en clases decidimos desarrollar un software capaz de presentar un nivel básico de encriptación y desencriptación dentro de una comunicación Cliente-Servidor. Esto con el fin de proteger una hipotética autentificación de los datos de algún cliente. Comenzamos dándole un entorno y un objetivo al programa, éste fue una comunicación (chat) P2P con autentificación en un servidor, quien es el responsable de entregar las direcciones de sus respectivos clientes. La comunicación entre los clientes no es relevante para el tema de seguridad puesto que para nuestros objetivos, si bien es funcional (posee incluso interfaz gráfica) sólo implementamos la encriptación y desencriptación entre Cliente-Servidor (esto con el fin de simplificar el programa). Es importante recalcar que usamos los códigos vistos en clases de conexión TCP en Java junto con una clase creada para encriptar y desencriptar obtenida de internet, la cual usa Codificación Base64,ASCII y Hexadecimal. Las tres anteriores de forma aleatoria para mayor robustez.



Flechas azules: Autentificación, registro de IP y entrega de IP's (otros clientes) encriptado.

Flechas negras: Comunicación (chat) P2P entre clientes.



En la imagen se observa un paquete que va desde 192.168.0.13(cliente) a 192.168.0.10(servidor) en donde parte de su contenido es "2s9bzgHF…", lo cual es parte de la encriptación de un usuario y su IP, se observa una partición en distintos paquetes, la cual luego de ser obtenida por el servidor será ensamblada en orden y desencriptada para su autentificación.

Conclusión

En conclusión la encriptación tiene como fin evitar los llamados (hackers) dotándose cada vez de más tecnología y usando diversos algoritmos, llaves o programas creados para la seguridad de la información de los usuarios.

La solución que usamos en nuestro diseño fue utilizando una encriptación simétrica, ya que la principal información para encriptar y desencriptar en los algoritmos simétricos es la llave KEY, toda la seguridad del sistema depende de donde esta llave, cómo está compuesta y quien tiene acceso.

En el desarrollo de las aplicaciones, surgieron dramas que relentizaban nuestro avance como la conectividad entre los 3 computadores, que se solucionó utilizando ip’s privadas en un pequeña subred de un hogar doméstico, cómo este tema puede cambiar las cosas a futuro (qué otras posibilidades se crean a futuro).

Referencias

http://www.jasypt.org/api/jasypt/1.8/org/jasypt/encryption/pbe/StandardPBEStringEncryptor.html

http://www.textoscientificos.com/redes/firewalls-distribuidos/soluciones-seguridad/encriptacion-paquete

http://tejji.com/ip/my-ip-address.aspx

http://www.informatica-hoy.com.ar/aprender-informatica/Tipos-de-redes-P2P-y-software-utilizado.php

http://notodojava.com/encriptar-cadena-de-texto-con-clave-para-desencriptar-encrypt-string-with-key-to-decrypt/

https://www.owasp.org/index.php/Man-in-the-middle_attack