Chat Cifrado

Integrantes:
Santiago Zúñiga García
Juan Sebastían Palma
Daniel Alejandro Gómez

Enunciado

Chat cifrado. Deben correrse dos instancias del programa en computadores diferentes. Las dos instancias deben conectarse por la red; una vez lograda la conexión, deben negociar una clave de cifrado empleando el algoritmo Diffie-Hellman. Esta clave debe ajustarse a 128 bits, para emplearla con el algoritmo AES. Toda la conversación entre las dos instancias del programa de chat debe ir cifrada a partir de ese momento.

Descripción del problema

Conforme con el enunciado del chat cifrado, se debe realizar un programa capaz de correr en más de un computador. En el caso específico del chat, se habla de un cliente, que a través de una conexión de red (TCP o UDP), pueda realizar una negociación Diffie-Hellman para realizar una comunicación cifrada mediante el algoritmo AES. La clave Diffie-Hellman debe ser de 128 bits, para emplearla con el algoritmo AES en la comunicación cifrada.

Diseño

El lenguaje de programación utilizado en este proyecto es Java, debido a que un requisito de diseño es utilizar la API criptográfica de Java. Ahora bien, para realizar un chat cifrado, se necesita una GUI (Interfaz Gráfica de Usuario) con la cual el usuario pueda interactuar y enviar mensajes,, por lo cual el cliente requiere de la creación de una ventana que se pueda abrir en diferentes computadores con instalación mínima. Ahora bien, para realizar la transmisión de mensajes, es necesario un servidor que permita conectar a todos los clientes, en este sentido, hay dos opciones: Cada cliente es su propio servidor o utilizar un servidor centralizado encargado de gestionar todas las conexiones. En el caso de este proyecto, se decide utilizar un servidor centralizado.

La comunicación se realizará mediante el protocolo TCP/IP debido a su alta resiliencia a los fallos, y la garantía de que los mensajes serán entregados a su destinatario. La negociación con el algoritmo Diffie-Hellman se realiza con transmisiones de texto plano y el cifrado se hace entre cliente y servidor. A partir de ahí, cuando se obtiene la clave compartida, se utiliza el algoritmo AES para la encriptación de los mensajes.

El cliente del chat, se implementa utilizando las librerías de javafx y el modelo se realiza mediante el modelo MVC. Por otro lado, las comunicaciones se gestionan mediante la implementación de un patrón observable.

Dificultades

Una de las principales dificultades presentadas en el proyecto, inicialmente fue la investigación e implementación del algoritmo Diffie-Hellman, debido a que la documentación oficial a menudo resulta confusa, y las clases inherentes y sus descripciones no revelan mucha información. Por otro lado, la sincronización para la negociación del algoritmo Diffie-Hellman, fue inicialmente compleja, sin embargo, adaptando el patrón observer

mencionado, mediante la codificación correcta de la comunicación resolvió este problema. Por otro lado, las claves públicas del algoritmo Diffie-Hellman, inicialmente se transmitían como objeto mediante la conversión directa al formato JSON, sin embargo, la deserialización del objeto de Java resultaba imposible, pues este objeto PublicKey tiene un proceso específico para reconstruir la llave mediante la clase KeyFactory. Esto se resolvió generando un arreglo de bytes con las llave pública codificada y la deserialización en el servidor se realizaba conforme a las especificaciones.

Conclusiones

El desarrollo de este programa nos permitió reforzar conceptos vistos en clase, tales cómo los algoritmos de cifrado y buenas prácticas de programación.

También nos permitió conocer acerca de las negociaciones que se llevan a cabo durante una conexión tcp, y cómo transformar esta conexión en una conexión segura mediante algoritmos de cifrado utilizando la API criptográfica de java.

Entendimos la importancia de tener cifrada la información qué se transmite en un sistema de comunicación, pues hoy en día la información que se comparte entre un dispositivo transmisor y un dispositivo receptor juega un papel importante para diferentes entes interesados, como lo son las empresas de publicidad, los hackers, las redes sociales, y en general a todo tipo de empresas.