CHAT BASADO EN IRC CON CIFRADO DE CLAVE PÚBLICA

Alejandro Santorum alejandro.santorum@estudiante.uam.es 44090946-S

TEMÁTICA

El trabajo consistirá en desarrollar un servidor que simule un **servicio de mensajería** entre sus clientes. Los mensajes circularán por la red cifrados utilizando el algoritmo de **establecimiento de claves de Diffie-Hellman**.

OBJETIVOS

Implementar un servidor que funcione como **puente de mensajería entre sus clientes**. El objetivo final sería que los clientes pudieran tener **tantas conversaciones como deseen**, es decir, que puedan comunicarse en cualquier momento con cualquier cliente conectado al mismo servidor. No obstante, por simplicidad, al principio nos centraríamos en una conversación única por cliente, es decir, una vez que se establezca una conversación entre dos clientes, estos no podrán comunicarse con otros usuarios hasta la finalización de dicha conversación.

Además, se utilizarían rasgos característicos de un chat **IRC** (o protocolo de aplicación IRC) como la utilización de **comandos** con el fin de distinguir las distintas acciones que un cliente tendría: ver una lista de clientes conectados, enviar un mensaje al cliente X, finalizar conversación, etc.

Por último, se busca implementar un algoritmo de **cifrado de clave pública**, como es el algoritmo **de establecimiento de claves Diffie-Hellman**, con el objetivo de que un tercer individuo que este escuchando la conversación no pueda seguirla.

DESARROLLO

Para cumplir los objetivos comentados, se **programará software** que implementará el servidor, el programa cliente y el algoritmo de establecimiento de claves DH.

La idea inicial es programar un servidor que use un **pool de hilos dinámico**: cuando se agote o este a punto de agotarse el numero de hilos disponible se realiza un nuevo pool de hilos para atender nuevos clientes. Cuando un cliente X mande un mensaje al cliente Y, el hilo que atiende a X **avisará al hilo** que atiende Y del mensaje que tiene que hacer llegar a su usuario.

Además, como existirán **varios comandos (al estilo IRC) disponibles**, el servidor tiene que reconocer, al menos parcialmente, el mensaje que está enviando el cliente, por lo que se plantea que el establecimiento de claves DH se realice entre cada hilo y su cliente, en lugar de entre pares de clientes.