Redes de Comunicaciones II

Práctica 3 - Protocolo SSL

Alfonso Bonilla Trueba
Mónica de la Iglesia Martínez

Pareja 7
Grupo 2313

Introducción

En esta última práctica de Redes de Comunicaciones hemos añadido al cliente y servidor realizados en prácticas anteriores seguridad SSL.

Diseño

Para la realización de la librería que se nos pide hemo seguido las indicaciones del enunciado, y hemos tenido que elegir qué argumentos pasar a cada función y cuál va a ser el retorno de esta, puesto que no se nos indicaban. La elección ha sido la más simple posible, pasando los argumentos justo y necesarios, como puede ser el contexto o la conexión ssl para poder hacer el envío o recepción de datos.

El control de errores que hemos realizado en toda las funciones es exhaustivo, ya que es una librería de seguridad, y en caso de que ocurra cualquier error se libera y se cierra todo lo que se hubiera reservado o abierto hasta el momento.

Conclusiones Técnicas

La creación de los certificados mediante la línea de comandos ha sido relativamente fácil siguiendo el enunciado, el manual en la web y en man. Al crear los certificados se pasan los argumentos para la firma según el enunciado (CN).

Crear esta librería y que funcione no ha sido algo sencillo, ya que no se nos ha proporcionado demasiado información en el enunciado, y cualquier detalle puede causar un error. Además buscar información por internet tampoco ha sido sencillo dada la variedad de versiones y funciones que han quedado desfasadas.

Conclusiones Personales

En esta práctica ha sido de ayuda volver a tener un corrector lo cual ayuda a saber si lo que estamos realizando esta correctamente hecho o no, puesto que en la anterior práctica no tuvimos corrector y fue algo más difícil de testear. Pero como opinión personal que hemos sacado es que este corrector tiene que mejorar puesto que proporciona poca información sobre lo que hace cada test y el formato que tienen que tener los ejecutables. Una dificultad con la que nos hemos encontrado es que el enunciado de la práctica decía alguna cosa contradictoria con lo que dice el enunciado del corrector (carpeta certs o cert, según en qué pdf mires, aunque el corrector quiere que se llame certs)

NOTA: Después de ejecutar c3po el servidor IRC se sigue ejecutando, para detenerlo killall servidor_IRC