Práctica 3

Comunicación segura con SSL

Enrique Aracil Orduña

Iñaki Cadalso Reymundo

G-2311-03

Introducción

En la practica 3 de Redes II vamos a implementar un tipo de seguridad en lo realizado en las anteriores ,SSL(SecureSocketsLayer).

Con ayudad de certificados y claves se reconocerán las dos partes de una conversación para que sea lo mas privada posible usando el protocolo de criptografía mencionado antes.

Diseño

Creamos lo certificados y claves con la librería openssl , tanto para el servidor/cliente como para un root que es el encargado de firmarlos para dar fe de su autenticidad.

Añadidnos las funciones descritas en el guion de la practica a nuestra biblioteca.

Creamos un servidor/cliente echo mu sencillo a los que aplicamos la funciones ssl creadas en la biblioteca para la inicialización del protocolo y su envío/recepción de información.

Modificamos nuestro servidor de la P1 y cliente de la P2 para que por argumentos acepten la activación de seguridad ssl . Inicialicen el protocolo y a la hora de recibir/enviar lo hagan por el canal SSL habilitado o no en caso de que no se haya activado.

Funcionalidad

Se ha implementado lo pedido por el c3po, creación de certificados, cliente/servidor echo y cliente/servidor IRC.

Han pasado las 4 pruebas correctamente.

Aunque la prueba del cliente ha sido un poco “preparada”. El cliente que debe recibir unos argumentos taless como –ssldata y recoger el mensaje a mandar, solo recogía el primer comando de *NICK yoda*. Por lo que se inicializa la conexión ssl, se conecta la canal con el servidor y se envía el mensaje. Hasta ahí correcto. Pero el corrector espera que mande otro mensaje de *USER* y ese por argumentos no lo vemos por lo que leyendo el fichero entrada.txt que se crea, cogemos el comando que falta y lo mandamos directamente por el canal SSL creado y asi si pasaría la prueba.

Conclusiones técnicas

Ver que un protocolo de seguridad que se usa actualmente sea “fácil” de implementar en lo que hemos hecho y lo bien que funciona haciendo la conexión mucho más segura.

Conclusiones personales

Una practica corta de duración, más de conceptos que de implementación en codigo, se agradece como ultima practica .

Habria estado interesante haber hecho mas tipo de pruebas de ocmo de seguro es y que formas habría de poder interceptar o suplantar a una parte.