REDES DE COMUNICACIONES II

PRÁCTICA 3
Seguridad SSL

Jorge Parrilla Llamas
(jorge.parrilla@estudiante.uam.es)
Javier de Marco Tomás
(javier.marco@estudiante.uam.es)

1. INTRODUCCIÓN

La práctica consiste en la implementación de un servidor IRC programado bajo el lenguaje C usando criptografía SSL. Para el desarrollo del servidor se ha seguido la implementación del RFC 2812 y 2813 según se solicitaba como requisito técnico del enunciado de la práctica.

Además, se ha seguido la implementación proporcionada por la librería eps-redes2.

Una vez desarrollada la práctica hemos realizado una serie de pruebas basándonos en los tests proporcionados por el comando de la librería eps-redes2 **c3po**.

```
 5/5 - TestServidorCifrado..................... [CORRECTA] [1.25] [B]


Resultados
----------

Pruebas correctas: 4/5
Puntuación total: 4.750/6  [APROBADA]
```

Además de probar el servidor con el r2d2 hemos accedido al servidor utilizando la tecnología que ofrece XChat para comprobar que el funcionamiento con dicha herramienta también es correcto.

2. DISEÑO

La práctica ha sido desarrollada bajo un diseño fácil e intuitivo, por un lado se utilizan los **servidor/cliente eco** que contiene la base de las funciones de conexión del servidor y cliente SSL: inicialización del socket, aceptación de conexiones, comunicación vía SSL utilizando la librería implementada.

Se utilizan también varios ficheros en los que se encuentran el resto de funciones implementadas para la realización de la práctica:

- **echo/servidor:** Ejecuta las funciones de conexión básicas de SSL para recibir cualquier cadena y devolverla por el mismo canal al cliente.
- **echo/cliente:** Contiene toda la información básica de conexión al servidor echo proporcionado previamente y empleando los diveros métodos implementados en la librería SSL.
- **cliente_servidor/servidor_irc:** En este fichero se encuentran toda la versión de servidor IRC desarrollada en la práctica 1 mediante el uso de SSL.

(Más información en la web de documentación detallada)
G-2313-06-P3/doc/html/index.html

3. FUNCIONALIDAD SSL

Hemos implementado la práctica utilizando la librería básica de SSL y creando un encapsulado propio (que era el objeto de esta práctica) que se proporciona en nuestra librería SSL.

Como resultado de esta práctica hemos conseguido:

- Generación de certificados: Para ello, empleamos las funciones de OpenSSL mediante las cuales generamos 3 certificados básicos (.pem):

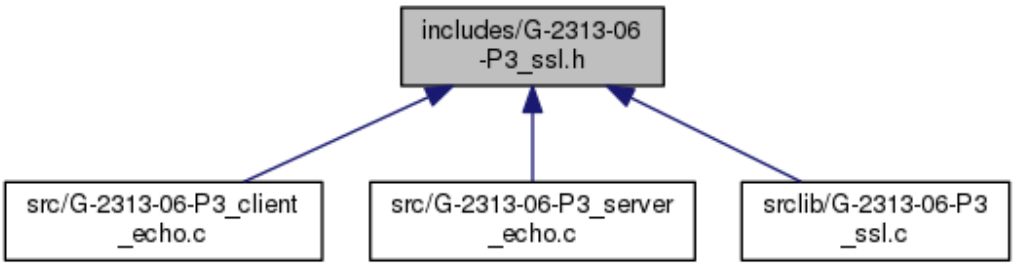
  - ca.pem: Es el certificado que se utilizará para firmar el resto de certificados generados (cliente/servidor).

  - cliente.pem: Es el certificado utilizado para las conexiones del cliente mediante el cuál se conecta al servidor utilizando la firma del ca.pem.

  - servidor.pem: Es el certificado utilizado por el servidor para las conexiones, se utiliza el ca.pem para firmar dicho certificado.

- Funcionalidad servidor IRC: Utilizando los certificados generados previamente hemos modificado el servidor de la práctica 1 para acomodar las funciones de conexión a la arquitectura basada en SSL. Con ello logramos que las conexiones se realicen de forma segura empleando los algoritmos de RSA.

Árbol de llamadas de la librería SSL



4. CONCLUSIONES TÉCNICAS

Ha sido bastante complicado lidiar con el corrector de esta práctica (C3PO), ya que cuenta con muchos errores que son molestos ya que nos limita a la hora de desarrollar las cosas.

Por ejemplo, el cliente IRC con SSL lo hemos implementado y funciona como debería, pero no pasa la prueba de C3PO por un error que aún no sabemos ya que no detalla para nada el tipo de error.

Ejecución

Para ejecutar la práctica (y el corrector) es necesario realizar varios pasos, realmente es muy simple ya que nuestro Makefile genera todo lo necesario: certificados, ficheros ejecutables, etc.

1) Estando en la carpeta G-2313-06-P3:

make

2) Los resultados obtenidos deberían ser:

```
x0soir@x0soir:~/Documentos/IRCServer/G-2313-06-P3$ make
Generando certificados...
Generating RSA private key, 2048 bit long modulus
.....................................................................................
.....................+++
.............................+++
e is 65537 (0x10001)
        Certificado generado: certs/rootkey.pem
        Certificado generado: certs/rootcert.pem
--> Certificados generados en: certs
Generando claves del cliente...
        Certificado generado: certs/clientcert.pem
        Certificado generado: certs/clientkey.pem
        Certificado generado: certs/cliente.pem
Generando claves del servidor...
        Certificado generado: certs/servercert.pem
        Certificado generado: certs/serverkey.pem
        Certificado generado: certs/servidor.pem
--> Claves generadas en: certs
Compilando servidor echo...
gcc -o ./echo/servidor_echo src/G-2313-06-P3_server_echo.c srclib/G-2313-06-P3_tcp
G-2313-06-P3_ssl.h -Wall -w -pedantic -pthread -rdynamic -lircredes -lirctad -lirc
--> Servidor compilado: ./echo/servidor_echo
Compilando cliente echo...
gcc -o ./echo/cliente_echo src/G-2313-06-P3_client_echo.c srclib/G-2313-06-P3_tcp.
-2313-06-P3_ssl.h -Wall -w -pedantic -pthread -rdynamic -lircredes -lirctad -lirci
--> Cliente compilado: ./echo/cliente_echo
Compilando servidor IRC...
gcc -o ./cliente_servidor/servidor_IRC src/server_irc/G-2313-06-P3_server.c includ
mmon_functions.c includes/server_irc/G-2313-06-P3_common_functions.h src/server_ir
3_function_handlers.h src/server_irc/G-2313-06-P3_thread_pool.c includes/server_ir
.h srclib/G-2313-06-P3_ssl.c includes/G-2313-06-P3_ssl.h srclib/G-2313-06-P3_tcp.c
 -lircredes -lirctad -lircinterface -lsoundredes -lssl -lcrypto
--> Servidor compilado: ./cliente_servidor/servidor_IRC
x0soir@x0soir:~/Documentos/IRCServer/G-2313-06-P3$
```

3) Tras la compilación de los recursos necesarios, es posible ejecutar las pruebas de C3PO de forma sencilla:

c3po

Nota: C3PO ejecuta el servidor_irc generado para tal motivo, por ello (el corrector no cierra el proceso al finalizar) es necesario ejecutar el comando de cierre del proceso:

killall servidor_IRC

5. CONCLUSIONES PERSONALES

Ha sido una práctica sencilla a pesar de las dificultades que nos ha proporcionado el corrector de ella. De todas formas, nos ha gustado ya que hemos puesto en práctica los conocimientos básicos que hemos obtenido en la parte de teoría de la asignatura (relativo a RSA y clave simétrica).

Realmente, las 3 prácticas de la asignatura nos han gustado bastante pero nos han llevado una cantidad de horas desorbitadas para lo que representa en la calificación final de la asignatura.