# Arquitectura de Sistemas de Información

Grado en Ingeniería en Tecnología de Telecomunicación. 3º curso.
Prueba práctica

23 de junio de 2017 Tiempo total: 2,5 h.

El aprobado se establece con la mitad de las claves.

## Descripción de la prueba práctica

En este ejercicio MONITOR propone 16 claves de las cuales las 12 primeras consisten en secretos que se ocultan en diferentes recursos del sistema estudiados en las prácticas del curso. Las cuatro últimas corresponden a una tabla de contadores (de tipo int) que residen en memoria compartida con desplazamiento OFF_KA_COUNTERS (10 bytes). Con respecto a las 12 primeras claves, se han separado en cuatro grupos por establecer un orden. El orden de identificación de los secretos puede ser diferente en función de la estrategia elegida por el alumno.

MONITOR, a petición del alumno, desplegará los secretos por el sistema en diferentes recursos. Para ello se utilizará la opción 1, que iniciará todos los recursos necesarios. El proceso cliente debe iniciarse con posterioridad al MONITOR y quedarse en modo espera. Cualquier cliente iniciado antes no será considerado por MONITOR. La opción 1 se activará posteriormente a la activación del cliente y permitirá desplegar los servicios que debe consultar el programa cliente.

Básicamente se activarán tres servidores por el MONITOR y se espera que el programa cliente sea capaz de establecer una sesión de intercambio de comandos con cada servicio. Los servicios consisten en la comunicación entre cliente y MONITOR (que actuará como servidor) usando tres recursos diferentes y de forma independiente. Estos servicios son: (1) Una comunicación a través de FIFOS con nombre, (2) comunicación con un servidor TCP y (3) comunicación con un servidor UDP.

Los comandos que se intercambiarán serán similares en cada sesión y estarán en formato de texto legible. La diferencia entre un servidor u otro está en los medios que se utilizan para mantener la comunicación. Se presenta a continuación un ejemplo de comunicación que puede producirse en cualquier sesión:

| CLIENTE | MONITOR | Comentario |
|---|---|---|
| “hello 2345” =====> | | Mensaje de solicitud de servicio pid cliente 2345 |
| | <==== “HELLO” | Respuesta de aceptación de MONITOR |
| | <==== “KA” | Mensaje de KEEPALIVE temporizado sin numeración |
| “ka 1” =====> | | Respuesta de cliente indicando la cuenta de KA |
| | <==== “KA” | |
| “ka 2” =====> | | Respuesta de cliente indicando la cuenta de KA |
| | <==== “SECRET 234” | Información de un secreto de la sesión |
| “key 2 234” =====> | | Consulta a MONITOR para comprobar el secreto 2 |
| | <==== “OK” | Confirmación de secreto |
| | <==== “KA” | |
| “ka 3” =====> | | Respuesta de cliente indicando la cuenta de KA |
| | <==== “QUIT” | Solicitud de cierre de MONITOR |
| “quit” =====> | | Confirmación de cierre |

Nota: Los mensajes de cliente están en minúsculas y los de MONITOR en mayúsculas.

En el primer grupo de secretos (del 1 al 3 inclusive) la comunicación se realizará vía FIFOS con nombre. Para hablar del cliente al MONITOR se usará un FIFO con nombre FIFO_WR ("/tmp/fifo_wr"). En sentido contrario se usará un FIFO con nombre FIFO_RD ("/tmp/fifo_rd"). Los FIFOS los construirá MONITOR en la fase de inicialización, pero cada interlocutor debe saber cómo utilizarlos para favorecer la sincronización.

En el segundo grupo (secretos del 4 al 6 inclusive) la comunicación se hará vía TCP, actuando MONITOR como servidor en un puerto que será el 8000 más el pid del proceso padre cliente. (Ej: si el proceso padre cliente es el 1234, el puerto será el 9234). Esto significa que si se necesitara rearrancar el cliente se deberá reiniciar también MONITOR para que el servidor escuche el puerto correcto.

El tercer grupo de secretos (del 7 al 9 inclusive) utilizará una comunicación vía UDP donde MONITOR espera peticiones al mismo puerto usado en el caso anterior, pero con un protocolo diferente.

En estos grupos se descubrirá el primer secreto (1,4 y 7) si el alumno resuelve la fase de establecimiento de comunicación y consigue enviar el mensaje de bienvenida adecuado. Los segundos secretos de cada grupo (2,5 y 8) se obtendrán si se identifica en la sesión el mensaje SECRET y se responde adecuadamente con la petición key correspondiente. Los terceros secretos de cada grupo (3,6 y 9) se obtendrán si se supera un límite mínimo de respuestas correctamente sincronizadas sobre los mensajes KA en cada sesión. MONITOR no informa del contador de KA, pero el programa cliente si debe hacerlo para construir la respuesta adecuada. Además, conviene que el alumno haga un control adecuado de los KA recibidos en cada sesión, pues eso le permitirá obtener 3 secretos más (13, 14 y 15) si actualiza cada KA recibido en cada sesión el contador de KA puesto en memoria compartida en la posición OFF_KA_COUNTER (10 bytes) donde habrá una tabla de cuatro enteros. El primero debe tener actualizado el número de KA recibidos en la sesión de FIFOS, el segundo en la sesión de TCP y el tercero en la de UDP. El cuarto contador de esa tabla se reserva como contador de señales para obtener el secreto 16, como se describirá posteriormente.

Para el acceso a la memoria compartida se utilizará como clave el DNI del alumno sin letra codificado en hexadecimal como un long (ej: para el DNI 11234567G la clave sería 0x11234567L).

El alumno debe estructurar el programa cliente de tal forma que exista un proceso padre y que de él deriven tres procesos hijos encargados cada uno de ellos de establecer las comunicaciones con cada servicio. Inicialmente se pueden crear esos hijos y dejarlos dormidos mientras no se escriba el código de esa parte. Esto permitirá resolver secretos del cuarto grupo, sin necesidad de resolver los anteriores.

En el cuarto grupo (secretos 10, 11 y 12) se propone la utilización de señales entre cliente y servidor para descubrir las claves. Cuando el proceso padre complete el despliegue de los procesos de la jerarquía debe enviar la señal SIGUSR1 al proceso MONITOR. Este comprobará que todo está bien y podrá descubrir el secreto 10. Posteriormente a eso, MONITOR enviará al proceso padre de la jerarquía señales SIGUSR1 y SIGUSR2 de forma indiscriminada. El proceso padre debe atenderlas y establecer un contador en memoria compartida (el cuarto contador mencionado anteriormente en la tabla de contadores). Ese contador debe ir actualizando el número de señales SIGUSR2 recibidas entre dos señales SIGUSR1. Es decir, no considerará las señales SIGUSR2 recibidas fuera de ese periodo. Al recibir la segunda señal SIGUSR1, el cliente debe mandar una señal SIGUSR2 en eco al MONITOR. Si se sigue el procedimiento se desvelará el secreto 11. Si se lleva la cuenta de señales SIGUSR2 en el periodo propuesto en el cuarto contador de memoria se podría descubrir la clave 16. La clave 12 se conseguirá si se ha descubierto previamente la 10 (correspondiente al despliegue de la jerarquía) y si se cierra la aplicación cliente correctamente (sin procesos zombies) después de recibir desde MONITOR la señal SIGQUIT. Esto se realizará mediante la opción 2 del menú.

# Arquitectura de Sistemas de Información

Grado en Ingeniería en Tecnología de Telecomunicación. 3º curso.
Prueba práctica

23 de junio de 2017 Tiempo total: 2,5 h.

El aprobado se establece con la mitad de las claves.

Nombre:……
Grupo:……..…… DNI:…….
Aula:……. Fila:…….. Columna:….....

FIRMA:

| | | | |
|---|---|---|---|
| Clave 1: | Clave 2: | Clave 3: | Clave 4: |
| Clave 5: | Clave 6: | Clave 7: | Clave 8: |
| Clave 9: | Clave 10: | Clave 11: | Clave 12: |
| Clave 13: | Clave 14: | Clave 15: | Clave 16: |