Sistemas Operativos

Departamento de Computación – FCEyN – UBA
Primer cuatrimestre de 2023

Nombre y apellido: Agustín Azzo

Nº orden: 10 L.U.: [redacted] Cant. hojas: 5

1	2	3	4	Nota
18	25	20	25	88

A

Segundo parcial – 01/07 - Primer cuatrimestre de 2023

- Numere las hojas entregadas. Complete en la primera hoja la cantidad total de hojas entregadas.
- Entregue esta hoja junto al examen, la misma no se incluye en la cantidad total de hojas entregadas.
- Cada ejercicio debe realizarse en hojas separadas y numeradas. Debe identificarse cada hoja con nombre, apellido, LU y número de orden.
- **Cada código o pseudocódigo debe estar bien explicado y justificado en castellano. ¡Obligatorio!**
- Toda suposición o decisión que tome deberá justificarla adecuadamente. Si la misma no es correcta o no se condice con el enunciado no será tomada como válida y será corregida acorde.
- La devolución de los exámenes corregidos es personal. Los pedidos de revisión se realizarán por escrito, antes de retirar el examen corregido del aula.
- Los parciales tienen tres notas: I (Insuficiente): 0 a 59 pts, A- (Aprobado condicional): 60 a 64 pts y A (Aprobado): 65 a 100 pts. No se puede aprobar con A- ambos parciales. Los recuperatorios tienen dos notas: I: 0 a 64 pts y A: 65 a 100 pts.

Ejercicio 1. Sistemas de Archivos (25 puntos)

Suponiendo un sistema de archivos `Ext2`, se solicita escribir en pseudocódigo la función `void my_grep(char* palabra, char* path)`. Esta función debe recibir como parámetros una palabra y una ruta a un directorio, y debe imprimir por pantalla las líneas de los archivos regulares (solamente) que contienen esa palabra. La búsqueda debe realizarse también en cada subdirectorio. La salida debe tener el siguiente formato:

`<Nombre_archivo>, línea de texto`

Considerar al caracter `'\0'` como fin de línea, y al caracter `EOF` como fin de archivo. Se cuenta con las siguientes estructuras de `Ext2FS`:

```
struct Ext2FSDirEntry {
    unsigned int inode;
    unsigned short record_length;
    unsigned char name_length;
    unsigned char file_type; // 0x1: regular file, 0x2: directory
    char name[];
};

struct Ext2FSInode {
    unsigned short mode;
    unsigned short uid;
    unsigned int size; // tamaño en bytes
    unsigned int atime;
    unsigned int ctime;
    unsigned int mtime;
    unsigned int dtime;
    unsigned short gid;
    unsigned short links_count;
    unsigned int blocks;
    unsigned int flags;
    unsigned int os_dependant_1;
    unsigned int block[15];
    unsigned int generation;
    unsigned int file_acl;
    unsigned int directory_acl;
    unsigned int faddr;
    unsigned int os_dependant_2[3];
};
```

Se cuenta también con la constante `BLOCK_SIZE` para el tamaño de bloque, y las siguientes funciones:

- `struct Ext2FSInode * Ext2FS::inode_for_path(const char * path)`: que dado un path, devuelve su inodo

- `void Ext2FS::read_block(unsigned int block_address, unsigned char * buffer)`: que lee de disco el bloque de dirección `block_address` y lo coloca en buffer.
- `unsiged int Ext2FS::get_block_address(struct Ext2FSInode * inode, unsigned int block_number)`: que devuelve la dirección del bloque de datos (`block_number`) del inodo (`inode`).
- `struct Ext2FSInode * Ext2FS::load_inode(unsigned int inode_number)`: que devuelve el inodo número `inode_number`.
- `unsigned char * get_line(unsigned char * text)`: que dado un texto, devuelve su contenido desde el inicio hasta el primer caracter de salto de línea inclusive.
- `bool find(unsigned char * line, unsigned char * word)`: que devuelve true si la palabra `word` está en `line`, false en caso contrario.
- `size_t strlen ( const char * str )`: que devuelve la longitud del string `str`.

Ejercicio 2. Sistema de E/S - Drivers (25 puntos)

Considere un sistema de refrigeración de una sala de reuniones compuesto por dos dispositivos conectados a una computadora que ejecuta un sistema operativo Linux: (i) un ventilador y (ii) un sensor de temperatura ambiente con cronómetro incorporado. Cada dispositivo debe ser manejado por un driver independiente.

Se pide:

a) Proponer un diseño, en donde debe indicar cuántos y qué tipo de registros tendría cada dispositivo, e indicando también para qué se utilizarían. Indicar y justificar el tipo de interacción con cada dispositivo (interrupciones, polling, dma, etc.).

b) Una vez que tenga el diseño, escribir los drivers correspondientes a ventilador y temperatura, de modo tal que cumplan los siguientes objetivos:

   - Al iniciarse, la aplicación de usuario deberá recibir tres parámetros de configuración por entrada estándar: un umbral de temperatura mínima, un umbral de temperatura máxima, y un tiempo T (todos enteros).
   - El sensor de temperatura deberá poder informar con un número entero el promedio de la temperatura de los últimos T segundos.
   - Si la temperatura promedio de los últimos T segundos se encuentra por debajo del valor mínimo, el ventilador deberá apagarse.
   - Si la temperatura promedio de los últimos T segundos se encuentra por arriba del valor máximo, el ventilador deberá encenderse.
   - Cualquier temperatura que se encuentre entre la mínima y la máxima se deberá considerar dentro del rango normal de refrigeración, y no deberá tener ningún impacto en el estado del ventilador.
   - Para reducir el consumo energético del sistema, el ventilador solamente deberá cambiar de estado cuando la temperatura promedio se encuentre fuera del rango normal (menor a la temperatura mínima o mayor a la máxima).
   - No está permitido realizar sleep u otras operaciones similares.
   - Para cada driver se deberá implementar en código C las funciones mínimas necesarias para poder cumplir el objetivo planteado. El código deberá ser sintácticamente válido y respetar las buenas prácticas mencionadas durante las clases. Por simplicidad, siempre que esto no impacte en la solución, se permitirá omitir el chequeo de errores. Todas las decisiones implementativas deberán estar debidamente justificadas.

c) Además, se solicita explicar el funcionamiento de la aplicación de usuario, y su interacción con los drivers utilizando pseudocódigo lo más similar a C posible. Tenga en cuenta que la aplicación de control correrá a nivel de usuario. Indicar con código C cómo interactuará el software de control con los drivers. Cada operación usada debe estar justificada.

Implementar cualquier función o estructura adicional que considere necesaria (tener en cuenta que en el kernel no existe la libc). Se podrán utilizar además las siguientes funciones vistas en la práctica:

```
unsigned long copy_from_user(char *to, char *from, uint size)
unsigned long copy_to_user(char *to, char *from, uint size)
int IN (int regnum)
void OUT(int regnum, int value)
void *kmalloc(uint size)
void kfree(void *buf)
void request_irq(int irqnum, void *handler)
void free_irq(int irqnum)
void sema_init(semaphore *sem, int value)
void sema_wait(semaphore *sem)
void sema_signal(semaphore *sem)
void mem_map(void *source, void *dest, int size)
void mem_unmap(void *source)
```

Ejercicio 3. Sistemas distribuidos: (25 puntos)

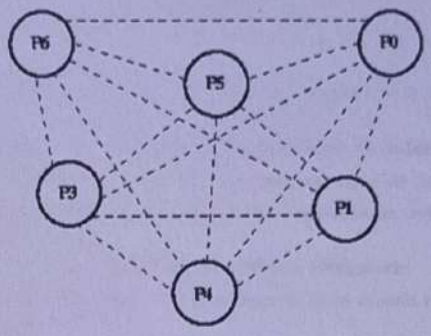

Figura 1: Sistemas distribuidos

Comenzamos con 7 procesos, todos conectados directamente entre sí, con ids del 0 al 6. El Proceso 6 es el líder, ya que tiene el número más alto. Si el Proceso 6 falla y el Proceso 3 se da cuenta de que el Proceso 6 no responde:

a) Explique cómo se utilizará el **algoritmo de Bully** para elegir un nuevo líder. Mencione la cantidad total de mensajes que se envían.
b) Explique brevemente cómo sería la elección de líder usando **Flood Max**. Mencione la cantidad total de mensajes que se envían.

Ejercicio 4. Seguridad: (25 puntos)

Se cuenta con un código el cual verifica si una clave es válida, permitiendo acceder al sistema con privilegios de administrador en caso afirmativo. Para el siguiente código se pide:

a) Explicar qué vulnerabilidad tiene, y cómo serían los valores exactos de cada byte del input de un *exploit* que permita realizar una ejecución de código arbitrario con escalamiento de privilegios. Aclarar las funciones utilizadas y justificar con un diagrama de las posiciones de memoria afectadas que incluya sus significados y sus valores antes y después de aplicar el *exploit*. ¿Cómo generaría dicho input, y cómo ejecutaría el programa en cuestión? (18p)
b) Proponer una corrección para el código en C que solucione la vulnerabilidad, detallando qué líneas modificaría, y por qué. Proponga además dos formas adicionales de mitigar la vulnerabilidad que no requieran modificar el código, explicando detalladamente su funcionamiento, y mostrando cómo dificultarían el ataque. (7p)

```
extern bool clave_es_valida(const char* clave);
extern void acceder_al_sistema();

void convertir_a_minuscula(char* buffer) {
  do {
    *buffer = tolower(*buffer);
  } while (*(buffer++) != '\0');
}

char* copiar_en_minuscula(const char* str) {
  char buffer[16];
  strcpy(buffer, str);
  convertir_a_minuscula(buffer);
  return strdup(buffer);
}

int main(int argc, const char* argv[]) {
  char* clave = copiar_en_minuscula(argv[1]);
  if (clave_es_valida(clave)) {
    acceder_al_sistema();
  }
  return 0;
}
```

Ayuda 1: Asuma que `clave_es_valida()` y `acceder_al_sistema()` son funciones seguras.

Ayuda 2:

```
Dump of assembler code for function main:
   0x0000555555555080: sub    rsp,0x8
   0x0000555555555084: mov    rdi,QWORD PTR [rsi+0x8]
   0x0000555555555088: call   0x5555555551d0 <copiar_en_minuscula>
   0x000055555555508d: mov    rdi,rax
   0x0000555555555090: call   0x555555555210 <clave_es_valida>
   0x0000555555555095: test   al,al
   0x0000555555555097: jne    0x5555555550a0 <main+32>
   0x0000555555555099: xor    eax,eax
   0x000055555555509b: add    rsp,0x8
   0x000055555555509f: ret
   0x00005555555550a0: xor    eax,eax
   0x00005555555550a2: call   0x555555555220 <acceder_al_sistema>
   0x00005555555550a7: jmp    0x555555555099 <main+25>
```

5 hojas

1)

```
void my_grep (char* palabra, char *path){
    Busqueda_recursiva (inode_for_path(path), palabra);
}

Void Busqueda_recursiva (Ext2FSInode* dir_inode, char* palabra){
  unsigned char* buf_bloque = (unsigned char*) malloc (2*BLOCK_SIZE);
  Unsigned char* sig_bloque = (unsigned char*)(buf_bloque + BLOCK_SIZE);
UINT num_bloque = 0;
UINT offset_dentry = 0;
 UINT recorrido = 0;
 while(recorrido < dir_inode->size){
     int dir_bloque_1 = get_block_addr (dir_inode, num_bloque);
     int dir_bloque_2 = get_block_addr(dir_inode, num_bloque + 1);
     read_block(dir_bloque_1, buf_bloque);
     read_block(dir_bloque_2, sig_bloque);
     while(offset_dentry < BLOCK_SIZE){
       Ext2FSdir_entry* dentry = (Ext2FSdir_entry*)(buf_block + offset_dentry);
       if(dentry->file_type == 0x2){
          Busqueda_recursiva(dentry->inode, palabra);
       } else if(dentry->file_type == 0x1){
         evaluar_archivo(dentry, palabra);
       }
       offset_dentry += dentry->record_length;
       recorrido += dentry->record_length;
     }
     num_bloque ++;
     offset_dentry -= BLOCK_SIZE;
   }
 }
```

Falta saber ↑

NOTA

```
Void evaluar_archivo (Ext2FS DirEntry dentry, char* palabra){
  Unsigned char* buf_bloque = (unsigned char*) malloc (2 * BLOCK_SIZE);
  unsigned char * sig_bloque = (unsigned char *)(buf_bloque + BLOCK_SIZE);
  u_int num_bloque = 0;
  u_int offset_bloque = 0;
  u_int recorrido = 0;
  Ext2FS Inode* inodo = load_inode (dentry->Inode);
  while (recorrido < inodo->size){
    int dir_bloque_1 = get_block_addr(inodo, num_bloque);
    int dir_bloque_2 = get_block_addr (inodo, num_bloque + 1);
    read_block (dir_bloque_1, buf_bloque);
    read_block (dir_bloque_2, sig_bloque);
    while (offset_bloque < BLOCK_SIZE){
      unsigned char* inicio_linea = buf_bloque + offset_bloque;
      unsigned char* linea = get_line(inicio_linea);
      if (find (linea, palabra)){
        printf("%s >> %s", dentry->name, linea);
      }
      offset_bloque += strlen (linea);
      recorrido += strlen(linea);
    }
    num_bloque ++;
    offset_bloque -= BLOCK_SIZE;
  }
}
```

Falta leer y escribir el código

NOTA

[redacted] Orden: 10 | Azar Agustín | 25/25 | HOJA Nº 2 | FECHA

Corrigió: Hernán G.

2)

a) Dispositivos:

- Sensor de temperatura:

El sensor tendrá dos registros: TIME, PROM donde el registro TIME se escribe para indicar al controlador el tiempo que debe usar para informar el promedio. Y el registro PROM tiene guardado el último promedio calculado. El dispositivo contará con la interrupción IRQ_TIME que se dispara cada TIME unidades de tiempo. OK

- Ventilador:

El ventilador contará con un registro ON que se escribe con 1 para prender el ventilador y 0 para apagar. OK

b)

Sensor: ¡muy Buena Resolución?

```
Semaphore ready;
void handler(){
    sema_signal(&ready); ✓
}
int driver_init(){
    sem_init(&ready, 0);
    RQuest_IRQ(IRQ_TIME, handler); ✓
    return IO_OK;
}
int driver_remove(){ ✓
    free_IRQ(IRQ_TIME);
    return IO_OK;
}
```

NOTA

open y close van a ser genéricos OK

```
int write (char* data, int cantidad) {
  int time;                                   ✓
  copy_from_user (&time, data, sizeof(INT));
  OUT(TIME, time);
  return sizeof(INT);
}

INT Read (char *data, int cantidad)
  int promedio = IN(PROM);
  copy_to_user (data, &promedio, sizeof(promedio));
  return sizeof(promedio);
```

```
INT Read (char *data, int cantidad) {                ✓
   Sema_wait (&ready);
   int promedio = IN(PROM);
   copy_to_user (data, &promedio, sizeof(promedio));
   return sizeof(promedio);
}
```

Ventilador: drive_init, drive_close, drive_open y drive_remove serán genéricos, solo vamos a implementar write.

```
INT Write (char* data, int cantidad) {
   int valor;                                  ✓
   copy_from_user (&valor, data, sizeof(valor));
   OUT(ON, Valor);
   return sizeof(valor);
}
```

NOTA

c)

```
int main () {
int T, min_t, max_t;
scanf("%d", t);
scanf("%d", min_t);
scanf("%d", max_t);
int sensor = open("/dev/sensor"); //permisos r+w
int ventilador = open("/dev/ventilador"); //permisos w
write(sensor, &T, sizeof(T));
[tachado] (Read(sensor
int temp
while(Read(sensor, temp, sizeof(temp)) != -1)
    if (temp < min_t) {
        int data = 0;
        write(ventilador, &data, sizeof(data));
    } else if (temp > max_t) {
        [tachado] ventilador
        int data = 1
        write(ventilador, &data, sizeof(data));
    }
}
return 0;
}
```

¿Da -1 en algún momento? Igual OK

El programa de usuario recibe por Std_in los valores de T, min_t y max_t. Luego abre los dispositivos de sensor y ventilador.
Al sensor le escribe el tiempo que debe tener en cuenta para calcular el promedio.
Luego hace read al sensor, como esta operación es bloqueante recién tendrá la respuesta una vez el sensor haya calculado el promedio (una vez cada T unidades de tiempo) OK

NOTA

luego, si la temperatura está fuera del rango normal escribe al ventilador para que este se prenda o apague.

NOTA

3)

a) a) El nodo 3 envía a los otros nodos con id mayor a el (4,5) su numero de id para postularse como lider. (2 mensajes)

b) El nodo 4 y 5 responden que no a 3 (2 mensajes)

c) El nodo 4 envía a los nodos con id mayor (5) su numero de id para postularse como lider (1 mensaje) P4 no sabe que Pallo P6 tambien (nadie mas)

d) El nodo 5 responde que no a 4 (1 mensaje)

e) El nodo 5 envia a los nodos con id mayor su id (ninguno) Será P6, tampoco sabe qué falló al no recibir respuesta se declara lider. Falta que P5 avise al resto que será el nuevo lider

total 7 mensajes

b)

a) El nodo 3 avisa que ~~el~~ el nodo 6 falló para mejorar el algoritmo (5 mensajes)

b) Todos los nodos envían a todos su id (6*5 mensajes)

c) Todos los nodos envían a todos el id más alto recibido (6*5 mensajes)

d) El nodo 5 recibio de todos los nodos su propio id no lo que se proclama lider.

total 35 mensajes. ✓

NOTA

c)

a)

El código presenta una vulnerabilidad del tipo stack overflow. ✓
En la función copiar_en_mayuscula no se valida el largo de str y se intenta guardar en un buffer de 16 bytes. ✓ Esto permite modificar el valor del ret addr del stack ya que STRCPY no trunca el input. ✓

Stack:

8B	ret-addr	+
8B	old rbp	✓
8B	buffer[8:15]	
8B	buffer[0:7]	↓ -

Sabiendo la estructura del stack podemos ver que con un input de 32 B sobreescribimos el ret-addr.
En concreto queremos que ret-addr vea la linea a la llamada de acceder_al_sistema().

sabemos que la dirección de acceder_al_sistema es: 0x00005555555550a2 pero para usarlo en nuestro exploit necesitamos que esté en little endian:
0xa2505555555550000 y luego, como en el código se llama a convertir mayúscula este input debemos "pasarlo a mayúsculas" en clase aplicamos codo carácter que corresponde a este valor de input toupper().
Esto lo podemos hacer con un script de pyton. ✓
La entrada que generara el script sera un array de 32 B donde los primeros 8B serán el resultado de la operación anterior y el resto basura.
⇒ LOS ÚLTIMOS 8 SON LA DIRECCIÓN!

b)

- forma de mitigar la vulnerabilidad en el código:
  Cambiar la función STRCPY por STRNCPY que trunca el largo de la entrada. ✓

- forma de mitigar la vulnerabilidad en tiempo de código:
  - Canarios de stack: luego de pushear el ret-addr se pushea un valor aleatorio al stack, si en el momento del ret el canario tiene un valor diferente significa que la pila fue manipulada por lo que se aborta el programa. ✓

NOTA

- randomizar las direcciones de salto: Cada vez que se carga el programa en memoria las direcciones de las instrucciones son diferentes, por lo que no se puede predecir que dirección debe estar en el ret. addr para ~~ex~~ saltar a la función que debe tomar ✓

ITEM A: - Perfecto!	ITEM B - Perfecto!

NOTA