Versión: Agosto 2012
Autor: Pérez, Juan Pablo

Pasos que se suceden al llamar a una System Call

El siguiente cuadro resume, y ejemplifica, los pasos que se suceden desde el momento en que un proceso de usuario realiza un llamado a una System Call. Los pasos son generales y pueden variar en las implementaciones de cada Sistemas Operativos.

Referencias:

- ***User o Kernel Mode:*** Modo de ejecución en el que se encuentra la CPU
- ***Hard o Soft:*** Si el que realiza la operación es el Hardware o el Software
- ***Stack Utilizado:*** Indica si el stack que se esta utilizando es el de Usuario o de Kernel

User o Kernel Mode	***Hard o Soft***	***Stack Utilizado***	***Descripción***
U	S	U	1. El proceso de Usuario llama a una Syscall por medio de la GlibC
U	S	U	2. La GlibC pone los parámetros para la syscall en el Stack y eleva una interrupción
U	H	U	3. Cambia a Kernel Mode
K	H	U	4. Coloca el PC y PSW en el stack (puede que se coloquen mas registros, dependiente de la arquitectura)
K	H	U	5. Se coloca en el PC la dirección de la rutina de atención de interrupción que se extrae de la IDT y se continua la ejecución
K	S	U	6. Se sacan los parámetros a la syscall del stack
K	S	U	7. De ser necesario se pueden guardar otros mas registros del proceso actual en el Stack o en la PCB, depende de la implementación del SO
K	S	U	8. Se cambia a kernel stack, guardando la dirección del stack en User Mode en la PCB
K	S	K	9. Se colocan los parámetros para la syscall en el Stack
K	S	K	10. Se ejecuta la Syscall
K	S	K	11. Si la Syscall bloquea el Proceso
			11.1. De ser necesario se guarda mas información sobre el proceso bloqueado (registros, estados, etc.)
			11.2. Se ejecuta el Short Term Scheduller para seleccionar un nuevo proceso
			11.3. Se realiza el context switch
			11.3.1. Se cargan los registros del nuevo proceso
			11.3.2. Se acomoda la dirección del Stack, dejando apuntando a la dirección que el HW dejo

			previo a que el proceso seleccionado sea suspendido.
			11.3.3. Se acomodan los datos necesarios en la PCB o estructuras utilizadas
K	S	U	12. Se cambia a User Mode
U	S	U	13. Se ejecuta RET
U	H	U	14. Se sacan de la pila el PSW y PC
U	S	U	15. Continua la ejecución del proceso actual

Mas Información:

+ información sobre HW : http://en.wikipedia.org/wiki/X86_assembly_language#Registers
+ información sobre interrupciones: http://en.wikipedia.org/wiki/INT_%28x86_instruction%29
+ información sobre interrupciones: http://en.wikipedia.org/wiki/Interrupt
+ información sobre SysCalls: http://en.wikipedia.org/wiki/System_call
+ información syscalls en linux; http://www.tldp.org/LDP/khg/HyperNews/get/syscall/syscall86.html
+ información sobre context switch: http://wiki.osdev.org/Context_Switching
+ información sobre context switch: http://en.wikipedia.org/wiki/Context_switch
+ información sobre stack: http://wiki.osdev.org/Stack
+ información syscall en Windows: http://blogs.technet.com/b/ganand/archive/2007/12/23/how-do-transition-from-user-mode-to-kernel-mode-takes-place.aspx