System calls

Both Linux and Microsoft Windows (and DOS in the past) allowed application programs call on operating system services via a software interrupt. In the case of Linux on the 80x86 platform, applications "call" or generate software interrupt (hex) 80 by executing the following instruction:

```
int $0x80
```

(using the AT&T assembler syntax)

In the case of DOS, the system call was via interrupt (hex) 21 and on Windows NT it was interrupt (hex) 2e. Windows XP and later use a different mechanism (sysenter)

Software interrupts are very similar to hardware ones in that the processor reacts in a similar way. It saves the processor state to the stack, looks up the interrupt vector table entry for interrupt (hex) 80 and jumps to that location.

The operating system can perform a number of different functions for applications so the application needs to specify what it wants. This is done by putting a (function) number into the eax register. Each of the functions that the OS can perform is associated with a particular number. When processing interrupt (hex)80, the value in the eax register is examined and control is transferred to the appropriate part of the kernel.

Usually system calls require additional parameters. For example, if an application wants to read from a file it will have to specify which file and identify a buffer where data can be stored. These parameters are passed via the processor registers. Each of the system calls is written with the expectation that applications will pre-load registers with the correct parameters. A partial list of Linux's system calls is shown below (see /usr/src/linux/arch/i386/kernel/syscall_table.S)

Function	eax	ebx	ecx	edx
sys_exit	1	Program exit code		
sys_fork	2			
sys_read	3	file handle/number	Address of buffer	Length of buffer
sys_write	4	file handle/number	Address of buffer	Length of buffer
sys_open	5	Address of file name string	file mode: 0=read,1=write	
sys_close	6	file handle/number		

As you can see, eax contains the function number. The contents of the other registers depends upon the function in question.