

Laboratory on Linux Kernel Haking

OS - Operating System

Simone ROSSI

November 29, 2016

Date Performed: November 29, 2016

Partners: Simone Rossi

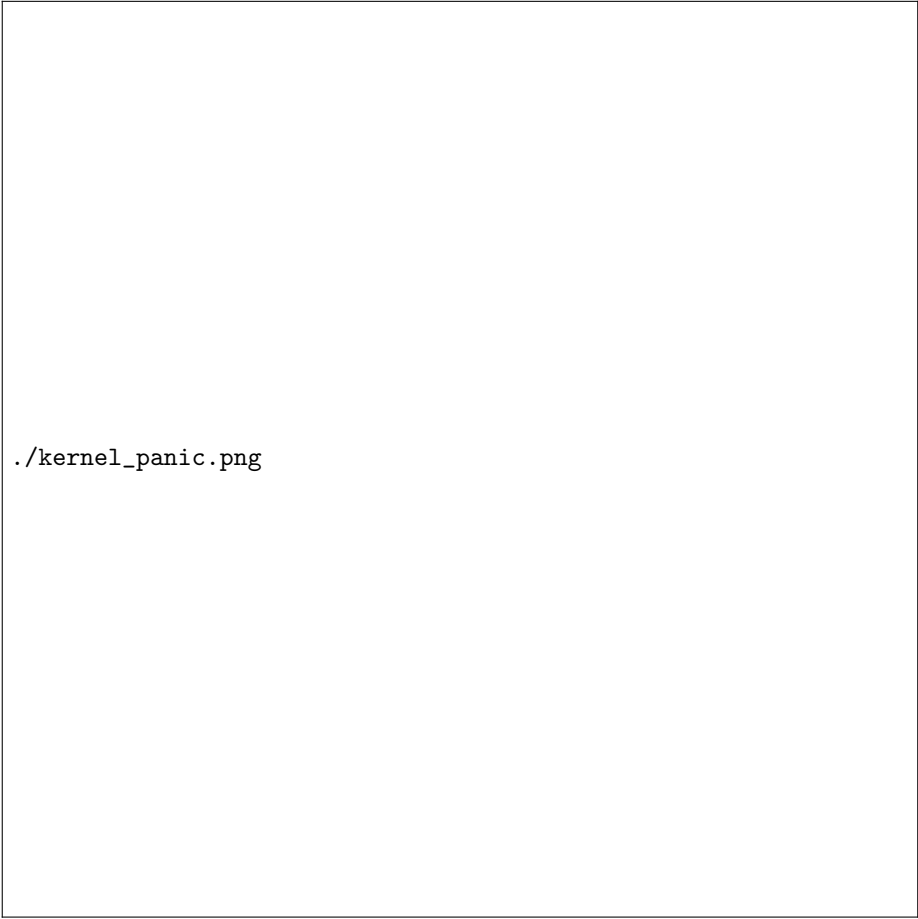
1 Compiling the Linux kernel

To analyze thet version of the kernel currently under execution, the command to be typed is `uname -vr`¹.

From the source code of `linux-2.4`, I tried to remove the support for the Ext3 filesystem. The new kernel has been compiled (computing all the dependencies and compiling all the sources) and mount using `lilo`.

Of course now, without the support for this version of filesystem, the kernel could not correctly load and mount the root filesystem; as consequence, it entered in the kernel panic state (with error 19) with no possibilities to be recovered.

¹The command returns both the kernel version and release

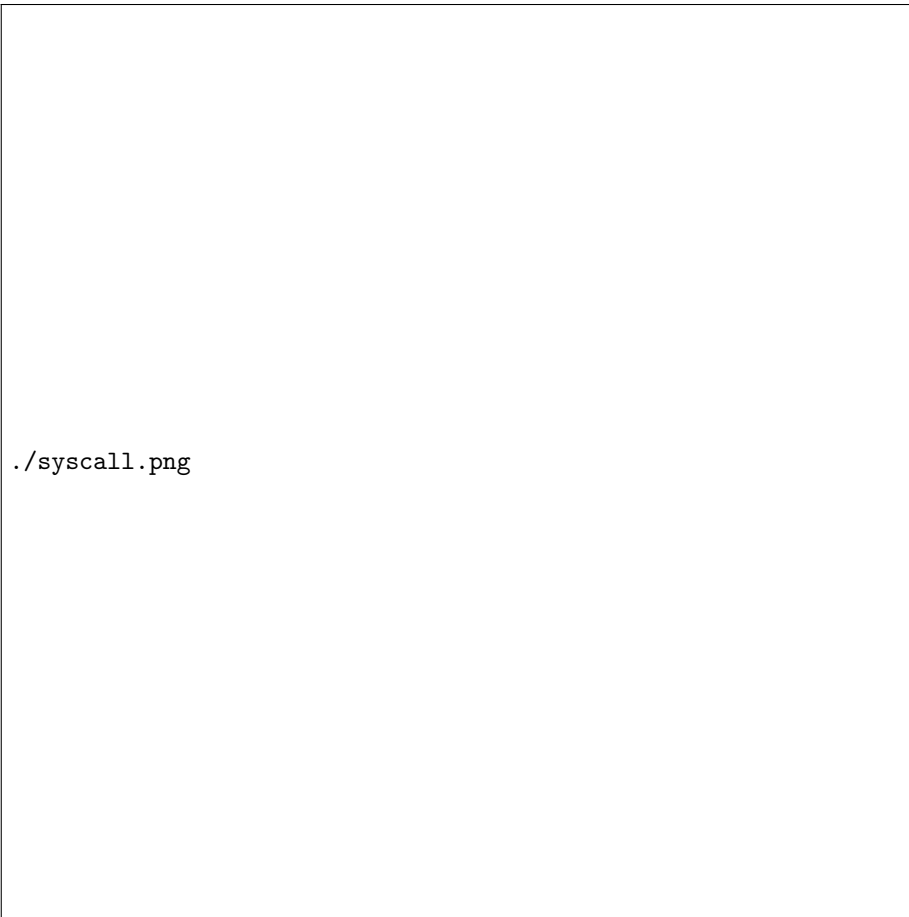


`./kernel_panic.png`

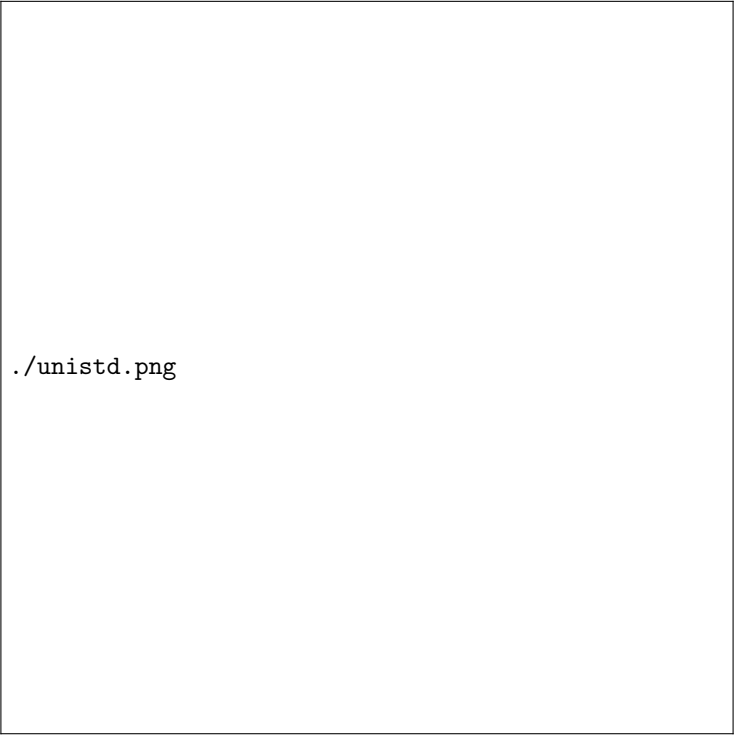
2 Adding new system calls to Linux

The man page of Linux describes the system call as a fundamental interface between an application and the Linux kernel itself. [...] Usually they are not invoked directly but rather via wrapper functions.

The system calls deal with low aspects of the operating systems, while providing high-level Application Programming Interface (API).



`./syscall.png`

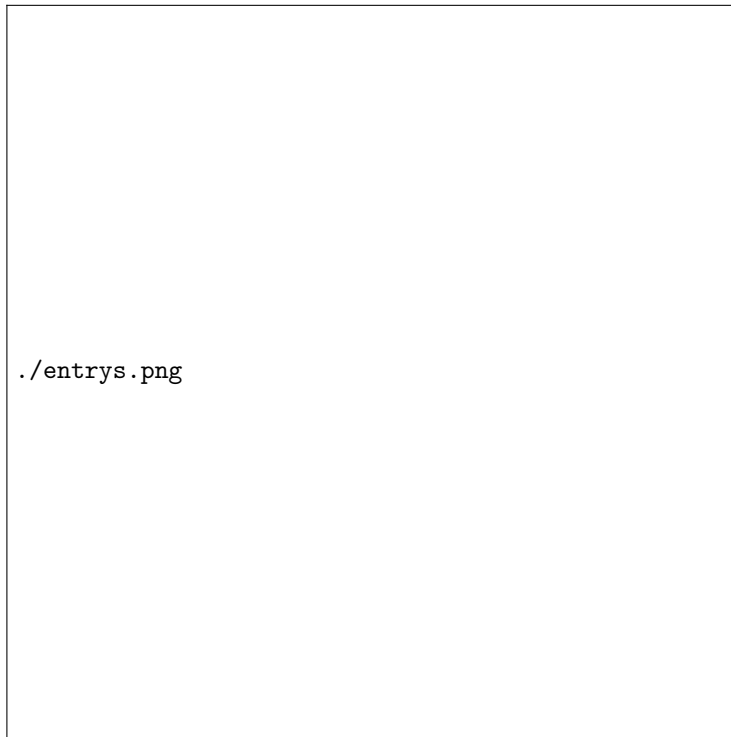


`./unistd.png`

Let's assume the user application calls a library function which actually during its execution makes a system call to the kernel. The name of the system call is used as offset in a system call table and an interrupt is raised.

As explained in the document, to add new system calls to the kernel, two files should be modified in order to let the system know the presence of new syscalls during the compilation:

- `include/asm-i386/unistd.h` contains the system call numbers for the system call table and seven different "template" prototype for the function (with different numbers of parameters).
- `arch/i386/kernel/entry.S` contains the system call low level handling



routines and the link between a system call and an entry of the system call table.