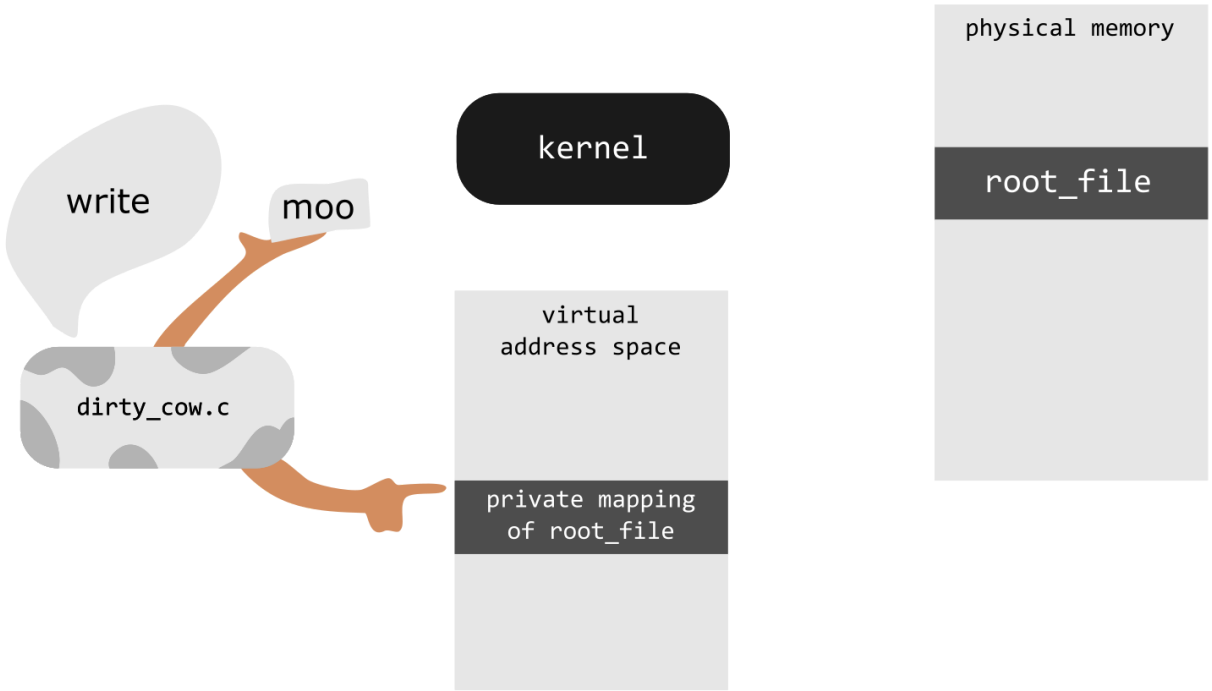
# Dirty COW Demo

by Jake Wilson and Nimesha Jayawardena

The following is a minimalistic demo of the Dirty Cow vulnerability: dirty_cow.c. It will allow you to write to a read-only file. If you want to try it out, download ubuntu-14.04.3-desktop-i386.iso (or any other vulnerable Linux kernel) and run as a virtual machine.

## Visually Explained



Prev Next

The next step is to `write` whatever we want (`moo`) to our private mapping of `root_file`; however, we're not going to write directly to the virtual address that `mmap` gave us. Instead we, write to a very unique file in Linux: `proc/self/mem`.

`proc/self/mem` is a representation of our (`dirty_cow.c`'s) virtual memory. It's part of special filesystem in Linux called `procfs`. You can read more about it on Wikipedia.

The Dirty Cow vulnerability actually requires us to use `proc/self/mem`, because the vulnerability lives insides the Linux kernel's implementation of process-to-process virtual memory access.

Note: You could, alternatively, use other methods that allow process-to-process virtual memory access (e.g., `ptrace`) for Dirty COW.