Universität des Saarlandes
Lehrstuhl für Softwaretechnik
Prof. Andreas Zeller, Stephan Neuhaus
Design of Secure Software Systems
Handout 1

1 Introduction

This handout contains source code that is relevant for the lecture called "A Day At the Races", which is concerned with race conditions and how to avoid them.

2 Opening and Truncating a File

The following code mimics the standard C library's *fopen*(3) function with the `"w+"` mode. It is an example of how to open a file in that mode in a way that is not susceptibe to race conditions. If you ever need to open a file in this manner, we recommend that you use code like this. Works on Unix and derivatives, but not under Windows.

```c
#include <sys/stat.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <fcntl.h>
#include <unistd.h>
#include <stdio.h>
#include <errno.h>

/* Emulate stdio's "w+" mode. The manual page has this to say:

   w+ Open for reading and writing. The file is created if it does
   not exist, otherwise it is truncated. The stream is positioned at
   the beginning of the file.
*/
FILE *
safe_open_wplus(char *fname) {
  struct stat lstat_info, fstat_info;
  FILE *fp;
  char *mode = "rb+";          /* We perform our own truncation. */
  int fd;

  if (lstat(fname, &lstat_info) == -1) {
    /*
     * If the lstat() failed for reasons other than the file not
     * existing, return 0, specifying error.
     */
    if (errno != ENOENT)
      return 0;

    if ((fd = open(fname, O_CREAT | O_EXCL | O_RDWR, 0600)) == -1)
      return 0;

    mode = "wb";
  } else {

    /* Open an existing file */
    if ((fd = open(fname, O_RDWR)) == -1)
      return 0;

    if (fstat(fd, &fstat_info) == -1
        || lstat_info.st_mode != fstat_info.st_mode
        || lstat_info.st_ino != fstat_info.st_ino
        || lstat_info.st_dev != fstat_info.st_dev) {
      close(fd);
```

```
        return 0;
      }

      /* Turn the file into an empty file, to mimic w+ semantics. */
      ftruncate(fd, 0);
    }

    /* Open an stdio file over the low-level one */
    fp = fdopen(fd, mode);
    if (fp == NULL) {
      close(fd);
      /* unlink(fname); – See exercise */

      return 0;
    }

    return fp;
}
```