Project 3

Due Thursday, December 2nd, in class

Overview. This project involves buffer overflows. You are to take the program given below and cause an overflow which results in the execution of a command.

Here is the program:

```
void main(int argc, char *argv[]) {
  char buffer[512];

  if (argc > 1)
    strcpy(buffer,argv[1]);
}
```

This program obviously has a vulnerability: the buffer is 512 bytes, but there is no bounds check on the strcpy call. Your job is to create a command-line parameter which causes this program to list the contents of the root directory on your machine. That is, to execute "`ls /`" on your machine.

Please hand in the following:

- The program that you used to create the command line parameter.
- A textual description of the method you used to create the exploit. This write-up should include a picture of the stack during the execution of your exploit, along with an explanation of how you computed the proper offsets for the exploit to change the return pointer.
- An execution of the above program, resulting in the command "`ls /`".

Distance students may email their answers directly to Mazdak.