University of Maryland
CMSC414 — Computer and Network Security
Professor Jonathan Katz

Homework 3

Please turn in a hard-copy in class on Nov 16
This homework is to be done individually

In this homework you will exploit buffer overflow attacks in three password authentication programs. The goal in each case is to get the program to print out an "Authorization successful" message *even though you do not know the password*. The compiled programs and their source code can be found on grace in the following directory:

```
/afs/glue.umd.edu/class/fall2009/cmsc/414/0101/public
```

The permissions are set so that you can execute the compiled programs and read the source code. (Note that the passwords hardcoded into the source code were changed before compilation.) If you want to use gdb to analyze the programs, you will need to re-compile the source code using the following command (which is the same command I used to compile):

```
gcc -g -Wall file.c -m32 -fno-stack-protector
```

I have only tested the programs/attacks on the linux cluster; therefore, I recommend that you log into `linux.grace.umd.edu` for this assignment.

For each of the three programs, you should turn in the following:

1. A 1- or 2-paragraph summary of how your attack works/what your attack does. If it helps, you can draw a picture of the memory layout.
2. A 1-line command that executes the attack from the command line. E.g., your attack on `pwd1` might look like this:

```
perl -e 'print ''abc'' ' | pwd1
```

The goal of the assignment is to learn about buffer overflow attacks. Thus, even though there may be other ways to "attack" the programs (e.g., brute-force password guessing), these will not be given credit for this homework.

Collaboration. This homework is to be done *without assistance from other students in the class*. There may be questions about using gdb to identify buffer overflows on the final exam, so it is to your benefit to make sure you learn the material.