CIS4361 – Programming Assignment 1
Fuzz Testing (total 100 pts)

Due on 2/24/2012

Group Allowed

You are to implement a mutation based fuzzer, which will used as input a jpg file, and will try to exploit bugs on a binary named jpegconv. The binary is supplied to you, and contains up to 10 exploitable bugs, some easier to find than others. You can work in groups of up to 3 students. The fuzzer may be written in any language of your preference, as long as I am able to run it. **The jpegconv binary is compiled for a Linux machine; hence, any language that can be executed from Eustis' command line (e.g. Java, C/C++, Perl, Python) is appropriate**.

Steps to build your fuzzer:

1. Mutate the sample file.
2. Feed the mutated file to the target program.
3. Record the seed and input file if it fails.

You are to turn in:

- Your fuzzer code (70 pts)
  - README file (10 pts)
  - Comments (10 pts)
  - Compiles/Runs (10 pts)
  - Should at least find 6 bugs (40 pts)
- A 3 page (minimum) report (20 pts)
  - what you learn (5 pts)
  - the fuzzer performance with figures/graphs (5 pts)
  - how would you improve it (5 pts)
  - how could you use it to attack or defend your software/operating system (5 pts)
- Sample files that trigger each bug found (1 per bug, 10 pts)
- Submit your report in pdf format to hector.lugo@knights.ucf.edu