Lab 4: Experimenting with Evolutionary Fuzzing

Preparation

Obtain AFL from http://lcamtuf.coredump.cx/afl/

Unzip the tarball and compile the binaries.

Read the documentation to get familiar with it.

Experiment

Download the following two very similar C programs

http://www.cs.ucr.edu/~heng/teaching/cs260-winter2017/afl_strcmp.c

http://www.cs.ucr.edu/~heng/teaching/cs260-winter2017/afl_strcmp2.c

Try to use AFL to fuzz these two programs for at least 10 minutes. For each program: try to answer the following questions:

1. Does AFL crash the program? Explain why do you think AFL can or cannot crash it?

2. Look at the seed files (ending with +cov) in the queue. These inputs increase the branch coverage according to AFL. For each of these seeds, explain what branch coverage it causes. You can use the Line numbers in the source file.

3. Pay attention the file names, they show how these inputs are mutated from their parents. Please explain the evolution of these seed files.