Software Reversing Lab 1 (10 points)

First read the following papers, and familiarize yourself with the
AFL (http://lcamtuf.coredump.cx/afl/) and
KLEE (https://klee.github.io/)
tools.

KLEE: Unassisted and Automatic Generation of High-Coverage Tests for Complex Systems Programs Cristian Cadar, Daniel Dunbar, Dawson Engler

SAGE: whitebox fuzzing for security testing. Godefroid, Patrice, Michael Y. Levin, and David Molnar.

Driller: Augmenting Fuzzing Through Selective Symbolic Execution. Stephens, Nick and Grosen, John and Salls, Christopher and Dutcher, Andrew and Wang, Ruoyu and Corbetta, Jacopo and Shoshitaishvili, Yan and Kruegel, Christopher and Vigna, Giovanni

Symbolic execution for software testing: three decades later. Cadar, Cristian, and Koushik Sen.

You are asked to write a small report (at most 6 A4 pages, font-size at least 10) on the differences between fuzzing and concolic execution. Your report should be understandable to a fellow student with no knowledge of advanced testing and reversing techniques. It has to contain the following elements:

1. Introduction
2. Explanation of fuzzing – including a small example
3. Explanation of concolic execution – including a small example
4. Descriptions of AFL and KLEE. How do they work? What are they good at?
5. Experiments of both AFL and KLEE on several RERS reachability problems.
6. An analysis of the results.
   a. Explain the produced outputs. What is in what files? What can you accomplish with them?
   b. Find some errors that are found by AFL but not by KLEE, and vice versa, en explain why.
   c. Reflect on the (future) usability of AFL and KLEE

The Driller paper contains good examples of result presentations. Use these for inspiration, although some will be too detailed to include in your 6 pages, be selective! (one large figure in an appendix is allowed)

Bonus task (2 points):

Read the following additional papers on the
ANGR (http://angr.io)
tool.

SoK: (State of) The Art of War: Offensive Techniques in Binary Analysis. Shoshitaishvili, Yan and Wang, Ruoyu and Salls, Christopher and Stephens, Nick and Polino, Mario and Dutcher, Andrew and Grosen, John and Feng, Siji and Hauser, Christophe and Kruegel, Christopher and Vigna, Giovanni.

Add to your paper (still fit it within 6 pages!):

1. A description of ANGR and the differences with AFL and KLEE.
2. Experimental results including analysis for the ANGR tool.

Keep in mind that your paper will be peer reviewed by fellow students!