Introduction to Formal Methods **Fall 1397**

Assignment 3: Concolic Execution

Hossein Hojjat & Fatemeh Ghassemi *Aban 15*

1 Introduction

The goal of this assignment is to use a concolic execution engine to analyze binary executable programs.

2 Task 1

“angr” (`https://angr.io/`) is a popular concolic analysis framework for analyzing binaries. Your first task is to install angr on your machine. There are two ways to install angr:

- Use the package management system of Python (`pip3`)
- Download the ready Docker image (there might be some limitations on using Docker in Iran)

Check out the documentation (`https://docs.angr.io/`) to get a general idea of how the framework works.

3 Task 2

There is a Windows executable program (`bestteam.exe`) associated with this assignment (you can get it from the webpage). This program is written by a fan of the Esteghlal football team. The program gets an integer as command line input and supposedly prints out “Esteghlal Sarvar Perspolis” on the screen, no matter what input you pass to the program. However, as we all know, the Perspolis football team is superior to Esteghlal. In order to prove to the programmer that Perspolis is better, you need to find at least one input to the program so that it prints out “Perspolis Sarvar Esteghlal” instead of “Esteghlal Sarvar Perspolis”. Instead of trying all the possible integers as inputs to the program, we want to use the smart approach of finding the correct input by concolic execution. Concolic execution basically finds the inputs to the program to reach a certain point of the code. The program `bestteam.exe` can actually output the correct statement (“Perspolis Sarvar Esteghlal”) for some values of the input, but we do not know those input values (even the Esteghlal fan programmer does not know the vulnerability of his code!).

Hints and Suggestions:

- There are many interesting examples with solutions on the angr website. You can read them to familiarize yourself with angr.
- The correct input to `bestteam.exe` is actually a number that can fit in 24 bits, so you can search for a bit-vector of size 24.
- The Python script for angr that finds the correct input to this problem is less than 20 lines of code. This assignment does not require skills such as professional knowledge of Python programming, it is mostly about learning how Concolic execution works in practice.

4 Task 3

Write a report to describe why concolic execution is very popular in the security community and how a hacker may use the approach that you used in this assignment for cracking software.

5 Deadline and Deliverables

The deadline of this project is Aban 30th at 11:59pm. You should submit both your script for angr and your report. Make a zip from your files to make uploading the files easier. Late submissions will get penalty for each day that the submission is late.