**中国矿业大学计算机学院**

**2015 级本科生课程报告**

课程名称 软件安全

报告时间 2018.6.29

学生姓名 郭晓康

学 号 06152186

专 业 信息安全

任课教师 杨文嘉

### 目录

# 基于angr的符号执行分析

## 一、符号执行

符号执行技术使用符号值代替数字值执行程序，得到的变量的值是由输入变量的符号值和常量组成的表达式。符号执行技术首先由King在1976年提出 ，经过三十多年的发展，现在仍然被广泛研究，它在软件测试和程序验证中发挥着重要作用。符号执行是一种重要的形式化方法和静态分析技术，它使用数学和逻辑首先定义一些基本概念。程序的路径（path）是程序的一个语句序列，这个语句序列包括程序的一些顺序的代码片段，代码片段之间的连接是由于分支语句导致的控制转移。一个路径是可行的（feasible），是指存在程序输入变量的至少一组值，如果以这组值作为输入，程序将沿着这条路径执行。否则，路径就是不可行的（infeasible）。路径条件（path condition,PC）是针对一个路径的，它是一个关于程序输入变量的符号值的约束，一组输入值使得程序沿着这条路径执行当且仅当这组输入值满足这条路径的路径条件。

## 二、angr简介

angr是一个二进制代码分析工具，能够自动化完成二进制文件的分析，并找出漏洞。在二进制代码中寻找并且利用漏洞是一项非常具有挑战性的工作，它的挑战性主要在于人工很难直观的看出二进制代码中的数据结构、控制流信息等。angr是一个基于python的二进制漏洞分析框架，它将以前多种分析技术集成进来，它能够进行动态的符号执行分析（如，KLEE和Mayhem），也能够进行多种静态分析。