Björn Kirschner

Technische Universität München

GetInTUM - Door Access System

Idea Report for Android Practical Course (F13)

May 18, 2015

Contents

---

1 Introduction

2 Selective Symbolic Execution

Symbolic execution is an advanced analysis technique particularly suited for automated software testing and malware analysis . Instead of concrete input (7, "string", ...) symbolic execution uses symbolic values (λ, β, ...) when processing code. Assignments in the program path have impacts on these symbolic values. The integer calculation $x = x - 2$, for instance, would update the symbolic expression representing the input x to $\lambda - 2$. Conditional statements (if <condition> then ... else ...) fork program execution into two new paths. Both paths are then constrained by an additional condition, the 'then' branch with the if-condition and the 'else' branch with the negated if-condition respectively.

cite!

cite

Following this procedure results in a tree-like structure of constrained symbolic expressions. A constraint solver can now take all constraints along one execution path as input and find one concrete input (e.g., $\lambda = 5$) which would lead to the program following exactly this path. Such results greatly alleviate writing reproducible test cases .

cite

On a technical level, symbolic execution engines save state information (program memory, constraint information, ...) in a custom data structure. Each conditional statement involving symbolic values results in a $fork$ of the program state. The two newly created branches are completely independent and can therefore be processed in parallel.

But the exponential growth of conditionals soon reveals scaling problems of this forking strategy. Despite heavy research on optimisations mitigating this path explosion problem only relatively small programs (thousands of lines of code) can be analysed symbolically .

cite

cite

3 bla3

4 Design Alternatives

5 Project Team

6 Action Planning and Scheduling

7 Action Planning and Scheduling

8 Action Planning and Scheduling

9 Action Planning and Scheduling