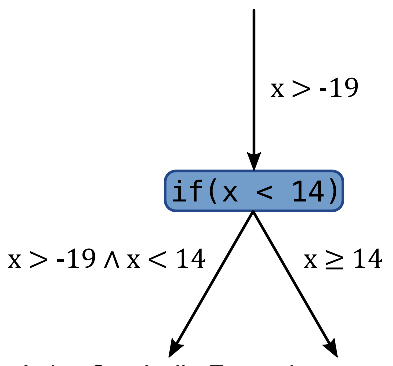
HiWi

COM SYS Research

Symbolic Execution

Introduction

To assist with our research in the SYMBIOSYS project we are looking for a motivated student assistant.



A tiny Symbolic Execution tree

Our - and possibly soon your - work revolves around a program analysis technique called *Symbolic Analysis*. The most important property of this technique is that it allows us to efficiently enumerate all possible program behaviors. This is achieved by making variables *symbolic*, which really means that it is not assigned a specific value, like e.g. 7, but rather is left unspecified.

Upon encountering a conditional like `if(x < 14)`, execution is forked and continues along both paths. For each of these execution paths, we remember all conditions that we encountered, which allows us to ensure that only possible program paths are taken. When encountering `if(x < 14)` a second time, we can ensure that only legal paths are taken by testing the following expressions for satisfiability: $x < 14 \land x < 14$ and $x < 14 \land \neg(x < 14)$. Obviously, only one path is taken.

Your Task

Our student assistants are actively involved in our ongoing research and have contributed by implementing new features for our symbolic execution engine of choice (*KLEE*) and working on diverse and interesting topics like: Packet filtering inside the Linux kernel or the difference between IEEE754 and x87 floating point formats.

Other technologies you may encounter as one of our student assistants include: Containerization via Docker, the C standard, the LLVM compiler framework and convoluted build systems.

The unofficial eBPF ponycorn

Useful Skills

You will be working on a somewhat large and nontrivial C++ project (`klee.llvm.org`). You should therefore be confident in your ability to program software in C++ and have a firm grasp of memory management.

Prior knowledge of Symbolic Execution is explicitly *not* required, although we encourage interested students to check out `klee.github.io/publications` beforehand.

Contact

Daniel Schemmel   daniel.schemmel@comsys.rwth-aachen.de

follow us on
http://comsys.rwth-aachen.de