UNIVERSIDAD COMPLUTENSE MADRID

Facultad de Informática

ANUNCIO DE CONFERENCIA

POSGRADO

When You Have a Fuzzer, Everything Looks Like a Reachability Problem

Alastair Donaldson
Imperial College London

Facultad de Informática
Sala de Grados - viernes 3 de octubre de 2025 - 10:00
Entrada libre hasta completar el aforo

Resumen:

I will provide an overview of three projects that explore the idea of using coverage-guided fuzzing, a technique traditionally used for finding bugs in software, in unconventional domains: Efficiently solving SMT formulas that use floating-point constraints; Achieving fast SMT sampling for such formulas; Simulating operational memory models. In each case, the idea is to reduce the problem at hand into a reachability problem: transforming a problem instance into a program equipped with a special error location, such that finding an input that reaches the error location equates to finding a solution to the problem instance. Coverage-guided fuzzing, which excels at mutating a corpus of inputs to achieve increasing statement coverage of a system under test, can then be used to search for an input that reaches the error location—i.e., for a solution to the problem instance. We hope this overview will inspire other researchers to consider recasting search problems into a reachability problem form where coverage-guided fuzzing may prove effective.

Sobre Alastair Donaldson:

Alastair Donaldson is a Professor in the Department of Computing at Imperial College London where he is Director of Research and leads the FastPL Group, investigating novel techniques and tool support for programming, testing and reasoning about high performance systems and their programming languages. He was Founder and Director of GraphicsFuzz Ltd., a start-up company specialising in metamorphic testing of graphics drivers, which was acquired by Google in 2018, after which he spent time working with Google as a software engineer and then as a Visiting Researcher. He was the recipient of the 2017 BCS Roger Needham Award and an EPSRC Early Career Fellowship, and has published more than 100 articles in the fields of programming languages, formal verification, software testing and parallel programming. Alastair was previously a Visiting Researcher at Microsoft Research Redmond, an EPSRC Postdoctoral Research Fellow at the University of Oxford and a Research Engineer at Codeplay Software Ltd. He holds a PhD from the University of Glasgow, and is a Fellow of the British Computer Society.