

The SeaHorn Verification Framework

(Invited Talk)

Arie Gurfinkel

Software Engineering Institute
Carnegie Mellon University
USA

arie@cmu.edu

SeaHorn is a software verification framework developed on top of LLVM compiler infrastructure. Its key distinguishing feature is a modular design that separates the concerns of the syntax of the programming language, its operational semantics, and its verification semantics (semantics used for verification). SeaHorn encompasses several novelties: it (a) encodes verification conditions using an efficient yet precise inter-procedural technique, (b) provides flexibility in the verification semantics to allow different levels of precision, (c) leverages the state-of-the-art in software model checking and abstract interpretation for verification, and (d) uses Horn-clauses as an intermediate language to represent verification conditions. For the users of verification technology, SeaHorn provides a powerful verification tool. For researchers in verification and for tool developers, SeaHorn provides an extensible and customizable framework for experimenting with new state-of-the-art software verification techniques. The effectiveness and scalability of SeaHorn are demonstrated by the results of the 2015 Competition on Software Verification (SV-COMP 2015). SeaHorn is based on joint work with Teme Kashesai, Jorge A. Navas, and Anvesh Komuravelli.