Trustworthy Verification of Machine Code

Didrik Lundberg
KTH Royal Institute of Technology
didrikl@kth.se

May 10, 2019

In the recent years, cache-based side channel attacks have gained a lot of recognition. These attacks utilize mechanisms like memory aliasing and speculative execution, which are typically not visible in models of high-level languages. Analyzing the code on a machine-code level facilitates including the above in the analysis, as well as components such as the MMU and NIC, for trustworthy proofs of security dealing with low-level mechanisms.

I am working on extending the formal binary analysis tool HolBA (built inside the interactive theorem prover HOL4). HolBA is a toolbox for several methods of verification, for example using Hoare triples with weakest precondition propagation. My main goal currently is to add support for the open RISC-V ISA. The general idea is that the open-design components built for RISC-V will enable more trustworthy verification at the interface between hardware and software, forming a solid foundation for full-stack security.