A Million Lines of Proof About a Moving Target

June Andronick
CSIRO's Data61, Sydney, Australia
UNSW, Sydney, Australia
June.Andronick@data61.csiro.au

Abstract

In the last ten years, we have been porting, maintaining, and evolving the world's largest proof base, the formal proof in Isabelle/HOL of the seL4 microkernel. But actually, there is no such thing as "the seL4 proof"; there are a number of proofs (functional correctness, binary translation validation, integrity and confidentiality proofs, etc) about a number of instances of seL4 (depending on the hardware platform it runs on, the features it includes, the extensions it supports). We will give an overview of the current state of these proofs, and, importantly, the challenges we face in keeping to maintain, evolve and extend them, and the processes we have put in place to manage their dependence on the evolving implementation.

2012 ACM Subject Classification Software and its engineering → Formal software verification; Software and its engineering → Software evolution; Software and its engineering → Operating systems

Keywords and phrases Proof maintentance, proof evolution, seL4, Isabelle/HOL

Digital Object Identifier 10.4230/LIPIcs.ITP.2019.1

Category Invited Talk