The seL4 Verification Journey: How Have the Challenges and Opportunities Evolved

June Andronick
Proofcraft
Kensington, Australia
june.andronick@proofcraft.systems

***Abstract*—The formal verification journey of the seL4 microkernel is nearing two decades, and still has an busy roadmap for the years ahead. It started as a research project aiming for a highly challenging problem with the potential of significant impact. Today, a whole ecosystem of developers, researchers, adopters and supporters are part of the seL4 community. With increasing uptake and adoption, seL4 is evolving, supporting more platforms, architectures, configurations, and features. This creates both opportunities and challenges: verification is what makes seL4 unique; as the seL4 code evolves, so must its formal proofs. With more than a million lines of formal, machine-checked proofs, seL4 is the most highly assured OS kernel, with proofs of an increasing number of properties (functional correctness, binary correctness, security—integrity and confidentiality—and system initialisation) and for an increasing number of hardware architectures: Arm (32-bit), x86 (64-bit) and RISC-V (64-bit), with proofs now starting for Arm (64-bit). In this talk we will reflect on the evolution of the challenges and opportunities the seL4 verification faced along its long, and continuing, journey.**

https://doi.org/10.34727/2022/isbn.978-3-85448-053-2_1