Operating System Verification for Real Use

Gernot Heiser

School of Computer Science and Engineering, University of New South Wales, and
Embedded, Real-Time and Operating Systems Program, National ICT Australia
Sydney, Australia
gernot@nicta.com.au

Abstract

Software verification remains an academic exercise as long as it focusses on toy problems, such as systems that are too simplified for practical deployment, or perform too poorly. Furthermore, formal verification of software is of limited benefit if the software is deployed in a system where it executes on top of an unverified operating system.

This talk presents an overview of an effort at NICTA which aims to formally verify a complete operating-system kernel, designed for deployment in mainstream embedded systems. It will explain the approach taken to address the conflicting goals of verifiability, general applicability and high performance. The kernel, called seL4, is designed to replace commercially-deployed high-performance L4 microkernels with no more than 10% performance degradation. The project, which has been running since early 2004, is scheduled to complete by the end of this year.