Trustworthy Virtualization of the ARMv7 Memory Subsystem

Hamed Nemati

Abstract

In order to host a general purpose operating system, hypervisors need to virtualize the CPU memory subsystem. This entails dynamically changing MMU resources, in particular the page tables, to allow a hosted OS to reconfigure its own memory. In this talk I present the verification of the isolation properties of a hypervisor design that uses direct paging. This virtualization approach allows to host commodity OSs without requiring either shadow data structures or specialized hardware support. Our verification targets a system consisting of a commodity CPU for embedded devices (ARMv7), a hypervisor and an untrusted guest running Linux.The verification involves three steps: (i) Formalization of an ARMv7 CPU that includes the MMU, (ii) Formalization of a system behavior that includes the hypervisor and the untrusted guest (iii) Verification of the isolation properties. Formalization and proof are done in the HOL4 theorem prover, thus allowing to re-use the existing HOL4 ARMv7 model developed in Cambridge.