A Formal Specification of x86 Memory Management


Abstract:
We are developing a formal and executable x86 ISA specification that includes memory management via paging and segmentation. We regularly use this specification to mechanically verify user-level x86 machine-code programs. Our recent efforts have been devoted to developing a theory for reasoning about system-level programs that are aware of memory management mechanisms like paging. On contemporary x86 implementations, every linear (virtual) address is mapped to a physical address by hierarchical, page-table data structures. We have been analyzing the effect of address mapping on the state of the memory management system. As a part of this effort, we proved that multiple translations of a specific linear address produce the same physical (translated) address. This property is surprisingly complicated because performing a translation may modify the page-table data structures. Establishing properties about the translation mechanism is essential if we are to verify programs such as the memory management code of an operating system.

Biography:
Shilpi Goel is a Ph.D. student and graduate research assistant at the University of Texas at Austin, where she is advised by Prof. Warren A. Hunt, Jr. Her work focuses on mechanical verification of complex properties of programs, including correctness with respect to behavior, security, and resource usage. She received her B.Tech. from Amity University, India in 2010.

Warren A. Hunt, Jr. is Professor at the Department of Computer Sciences of the University of Texas at Austin. Previously, he was a Research Staff Member and Manager at IBM's Austin Research Laboratory. Dr. Hunt holds a BSEE from Rice University and a PhD in computer science from the University of Texas. His research interests include hardware verification, circuit design, and mechanized theorem proving. Hunt's dissertation, published in 1985, was the seminal example of a mechanized microprocessor correctness proof. He extended this verification work, to produce in 1991, the first fully verified microprocessor to be physically realized in hardware, the FM9001. Hunt's continuing refinement of verification technology and methodology continued with his participation on the FM9801 microprocessor verification effort, as well as industrial scale systems such as Motorola's Complex Arithmetic Processor DSP. From 1986 to 1997, Hunt was Vice President of Computational Logic, Inc., in Austin, Texas, where his research was the cornerstone of the "Short Stack," a fully verified tower of systems from the high-level language level down to hardware. This work stands as the most extensive and complete example of a formally correct computing platform. His current research involves the use of formal mathematics to write specifications for computer hardware and software and to use proof techniques to determine the validity of such specifications. He is also interested in computer architecture, low-power computing, garbage collection, and parallel computing. Warren A. Hunt is the Chair of the FMCAD Steering Committee.

License: Creative Commons 2.5