Validating the Microsoft Hypervisor
(Abstract)

Ernie Cohen

Microsoft Corporation
Redmond, USA

Efforts to validate the Microsoft Hypervisor – a low-level program that partitions a real MP machine into a a number of virtual MP pachines – has led to some interesting formal methods developments. We'll survey some of these, including

- new algorithms for "optimal" stateless search and symbolic stateless search;
- techniques to make stateless search practical for shared memory programs, including efficient shared memory instrumentation and optimal trace replay using breakpoints;
- new techniques for model-based test generation, including the use of symbolic execution to eliminate redundancy and methods to handle invisible internal nondeterminism;
- formal models of the x86/x64 TLB and cache systems;
- verification of algorithms for efficient MP TLB virtualization, which has uncovered subtle design bugs;
- formal analyses of memory sharing between mutually distrustful partitions, which has revealed some surprising cache attacks;
- techniques for eliminating inductive constructs in first-order verification;
- techniques for specifying and reasoning about C code.

J. Misra, T. Nipkow, and E. Sekerinski (Eds.): FM 2006, LNCS 4085, p. 81, 2006.