PhD Dissertation Defense
Ted Huffmire
Monday, May 14, 2007
10:00am - ECE Conference Room (HFH Room 4164)

Committee: Tim Sherwood (chair), Fred Chong, and Ryan Kastner

Title: Protection Primitives for Reconfigurable Hardware

Abstract:
Blurring the line between software and hardware, reconfigurable devices strike a balance between the raw high speed of custom silicon and the post-fabrication flexibility of general-purpose processors. While this flexibility is a boon for embedded system developers, who can now rapidly prototype and deploy solutions with performance approaching custom designs, this results in a system development methodology where functionality is stitched together from a variety of "soft IP cores," often provided by multiple vendors with different levels of trust. Unlike traditional software where resources are managed by an operating system, soft IP cores necessarily have very fine grain control over the underlying hardware. To address this problem, the embedded systems community requires novel security primitives which address the realities of modern reconfigurable hardware.

This dissertation describes a new approach to reconfigurable system security that relies on both static and runtime techniques to prevent multiple cores on a single device from interfering with each other. While existing security primitives for FPGAs do not provide isolation or protection, mixed trust designs may be supported by exploiting both the spatial nature of computation on reconfigurable devices and the ability to integrate enforcement mechanisms. Key to this strategy is a novel isolation primitive, moats and drawbridges, built around four design properties: logical isolation, interconnect traceability, secure reconfigurable broadcast, and configuration scrubbing. Each of these is a fundamental operation with easily understood formal properties, yet maps cleanly and efficiently to a wide variety of reconfigurable devices. Moats and drawbridges support another important element of our strategy, reconfigurable memory protection, that allows cores to share memory securely. Policies that specify the legal sharing of memory are expressed in a specialized language, and a compiler translates each policy specification to a hardware description of a reference monitor, a runtime enforcement mechanism that can be loaded onto an FPGA.

Everyone Welcome