Trustworthy System Design through Gate-Level Information Flow Tracking

Glasgow East 117, 1500-1600, 27 August 2009

Abstract:
Modern processors are a maze of execution units, caches, status bits, exception handling logic, predictors, and other behaviors that modify the state of the machine, where information can leak through a myriad of implicit timing and covert channels. This makes it incredibly hard to provide guarantees on information flow properties (such as complete isolation between programs) that many mission-critical systems require.

In this talk, I will present a novel technique that tracks all information flows through a given hardware design, including timing and covert channels, and makes them explicit. The key to this technique for tracking all information flows precisely is to begin at the lowest level at which information is manipulated in a machine, that of simple logic gates, and observe that all higher-level information flows map down to precise logical functions at the gate level.

From this foundation of Gate-Level Information Flow Tracking, I will then describe how a class of architectures can be constructed, from the gates up, to provide programmers with explicit control over all flows of information. After describing the impact on the hardware implementation, the ISA, and the programmer, I will show that the architecture can support a variety of critical operations such as public-key encryption and authentication, and even enforce policies such as complete isolation.

Biography:
Mohit Tiwari is a PhD student in the Department of Computer Science at UC Santa Barbara, working with Professor Timothy Sherwood. His research is in the area of computer architecture, specifically in the development of novel methods for tracking the flow of information through complex systems. Before joining UCSB in 2005, Mohit received his B.S in Computer Science and Engineering from the Indian Institute of Technology, Guwahati.