

**THURSDAY  
OCTOBER 11, 2007**

**Scaife Hall Auditorium  
Room 125**

**4:30 p.m.  
Refreshments—4:00 p.m.**

**Sri Parameswaran**  
ASSOCIATE PROFESSOR



Sri Parameswaran is an Associate Professor in the School of Computer Science and Engineering. He also serves as the Program Director for Computer Engineering at the University of New South Wales. Sri has received the Faculty of Engineering Teaching Staff Excellence Award in 2005. His research interests are in System Level Synthesis, Low power systems, High Level Systems and Network on Chips. He has served on the Program Committees of numerous International Conferences, such as Design and Test in Europe (DATE) and the International Conference on Computer Aided Design (ICCAD). He has received best paper nominations from the International Conference on VLSI Design and the Asia South Pacific Design Automation Conference.

ECE Seminar Hosts:  
Radu Marculescu,  
[radum@ece.cmu.edu](mailto:radum@ece.cmu.edu)  
Yi Luo,  
[y1827@andrew.cmu.edu](mailto:y1827@andrew.cmu.edu)  
Bruno Sinopoli,  
[brunos@andrew.cmu.edu](mailto:brunos@andrew.cmu.edu)

## Micro-architectural Answers to Questions of Security

Secure computation on reliable machinery is a must to safeguard the integrity of data and the computation associated with the data. Improving capabilities of embedded processors enable larger, complex applications, making systems increasingly vulnerable to reliability and security concerns. Typical attacks include stack / heap based buffer overflows, dangling pointer references, integer error vulnerabilities, format string vulnerabilities and side channel attacks. Reliability is often compromised by soft errors. Numerous methods are used to address security and reliability, ranging from reliable and secure software / operating systems to hardware assisted runtime monitors. Traditionally the use of software / operating systems solutions was prevalent, which incur huge performance overheads and lack generality. Hardware support for monitoring proper runtime behavior has recently emerged as a promising alternative, where additional hardware monitors perform reliability and security monitoring. While such monitors outperform 'software only' techniques, the monitoring hardware itself becomes open to reliability issues and security vulnerabilities, requiring additional interfaces to the processor to interact with monitors at runtime. To overcome difficulties of the "software only" and "hardware only" approaches, we propose a novel hardware assisted runtime monitoring technique that can share the hardware used for regular processing. We achieve this via embedded micro monitoring, where micro instruction routines or small hardware blocks are embedded into machine instructions to perform monitoring. Thus, the monitoring procedure is incorporated into the data path of the processor and performed by instruction execution. Our experiments with real embedded application benchmarks show very minimal overheads with our monitoring mechanism, and show equal or better performance than all previous methods. Additionally, a dual-core method will be illustrated which is resilient to side channel attacks.