**

**CECS Seminar Series**

**“Securing Computer Hardware Against Malicious Design and Foundry Attacks”**

**Prof. Siddharth Garg**

Electrical and Computer Engineering

University of Waterloo, Canada

**Abstract:** Digital ICs are the basic building blocks of modern computer hardware. For economic reasons, the design and fabrication of digital ICs is increasingly outsourced. This introduces a security vulnerability — that of a malicious attacker, either a malicious designer or a malicious fab, inserting a hardware Trojan in the IC. A hardware Trojan a piece of digital logic intended to leak secret information from the chip (cryptographic keys for example), or sabotage its functionality (a privilege escalation attack on a microprocessor, for example).

In this talk, I will present some of my recent work on techniques to secure computer hardware against such attacks. In the first part of the talk, I will discuss how 3D integrated circuit (3D IC) technology can be leveraged to defend against Trojan insertion by a malicious fabrication facility (also called “fab”). In particular, by fabricating each tier of the 3D IC in a different fab, the design intent can effectively obfuscated, thus enhancing security.

In the next part of the talk, I will discuss the design of hardware Trojan triggers that cause the maliciously inserted circuitry to activate at a time of the attackers choosing. Although prior work has shown that deterministic time triggers are easily defended against, I will show that by leveraging randomness, attackers can design very precise time triggers that are insusceptible to all existing hardware security mechanisms of which we are aware. I will discuss the security implications of this new vulnerability.

This is joint work with Prof. Mahesh Tripunitara of the University of Waterloo.

**Biography:** Siddharth Garg is an Assistant Professor of ECE at the University of Waterloo. He received a Ph.D. in ECE from Carnegie Mellon University, an M.S. degree in EE from Stanford University and a B.Tech. degree in EE from IIT Madras. He has received best paper awards at the Usenix Security Symposium (2013), SRC TECHCON (2009), and ISQED (2009). He was awarded the A.G. Jordan Award for outstanding thesis contributions and service to the department from the ECE Department at CMU in 2010.

**Friday, March 7, 2014**

2:00-3:00PM

2111 Engineering Hall

 Host: Mohammad Al Faruque at alfaruque@uci.edu

UNIVERSITY OF CALIFORNIA, IRVINE