NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

C S S E M I N A R

Title: **Towards an Open-Source, Formally-Verified Secure Processor**

Speaker: Professor Srini Devadas
Massachusetts Institute of Technology (MIT)

Date/Time: 26 July 2017, Wednesday, 11:00 AM to 12:30 PM

Venue: SR3, COM1-02-12

Chaired by: Dr Peh Li Shiuan, Provost's Chair Professor, School of Computing (peh@comp.nus.edu.sg)

Abstract:

Architectural isolation can be used to secure computation on a remote secure processor with a private key where the privileged software is potentially malicious as recently deployed by Intel's Software Guard Extensions (SGX). This talk will first describe the Sanctum secure processor architecture, which offers the same promise as SGX, namely strong provable isolation of software modules running concurrently and sharing resources, but protects against an important class of additional software attacks that infer private information by exploiting resource sharing.

The talk will then describe a verification methodology based on a trusted abstract platform (TAP) that formally models idealized enclaves and a parameterized adversary. Machine-checked proofs show that the TAP satisfies the three key security properties needed for secure remote execution: integrity, confidentiality and secure measurement. Machine-checked proofs also show that SGX and Sanctum are refinements of the TAP under certain parameterizations of the adversary, demonstrating these systems implement secure enclaves for the stated adversary models.

Joint work with Victor Costan, Ilia Lebedev, and the Seshia Group at U. C. Berkeley.

Biodata:

Srini Devadas is the Webster Professor of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology (MIT) where he has been on the faculty since 1988. Devadas's research interests span Computer-Aided Design (CAD), computer security and computer architecture. He is a Fellow of the IEEE and ACM. He has received a 2014 IEEE Computer Society Technical Achievement award, the 2015 ACM/IEEE Richard Newton technical impact award, and the 2017 IEEE Wallace McDowell award for his

research. Devadas is a MacVicar Faculty Fellow and an Everett Moore Baker teaching award recipient, considered MIT's two highest undergraduate teaching honors.