7+('(3$570(17 2) &20387(5 6&,(1&(7+(&20387(5 6&,(1&(
*5$'8$7(678'(17 25*$1,=$7,21 *62&6 35(6(17

,19,7(' 63($.(5 6(5,(6

co-sponsored with GSO and partially paid for by student activity fees

3URIHVVRU 6ULQL 'HYDGDV
0DVVDFKXVHWWV ,QVWLWXWH RI 7HFKQ

)ULGD\ 6HSWHPEHU RQ URRP)LQH $UWV

6HFXUH 6SHFXODWLRQ 3(URFHVVRUV

Abstract : Software side channel attacks have become a serious concern with the recent rash of attacks on speculative processor architectures. Most attacks that have been demonstrated exploit the cache tag state as their exfiltration channel. While many existing defense mechanisms that can be implemented solely in software have been proposed, these mechanisms appear to patch specific attacks, and can be circumvented. We propose minimal modifications to hardware to defend against a broad class of attacks, including those based on speculation, with the goal of eliminating the entire attack surface associated with the cache state covert channel. These modifications are layered on top of the Sanctum secure processor architecture that offers strong provable isolation of software modules running concurrently and sharing resources.

Joint work with Ilia Lebedev, Vladimir Kiriansky, Saman Amarasinghe and Joel Emer

Bio: Srini Devadas is the Webster Professor of EECS at MIT where he has been on the faculty since 1988. His current research interests are in computer security, computer architecture and applied cryptography. Devadas received the 2017 IEEE W. Wallace McDowell award and the 2018 IEEE Charles A. Desoer Technical Achievement award for his research in secure hardware. He is the author of "Programming for the Puzzled" (MIT Press, 2017), a book that builds a bridge between the recreational world of algorithmic puzzles and the pragmatic world of computer programming, teaching readers to program while solving puzzles. Devadas is a MacVicar Faculty Fellow, an Everett Moore Baker and a Bose award recipient, considered MIT's highest teaching honors.