UNIVERSITY OF CHICAGO
DEPARTMENT OF COMPUTER SCIENCE

PRESENTS:

"Software Side Channels"

Tegan Brennan
University of California, Santa Barbara

Abstract:
Side channels in software are a class of information leaks where non-functional side effects of software systems (such as execution time, memory usage or power consumption) can leak information about sensitive data. In this talk, I present my research on a new class of side-channel vulnerabilities: JIT-induced side channels. In contrast to side channels introduced at the source code level, JIT-induced side channels arise at runtime due to the behavior of just-in-time (JIT) compilation. I show the existence of this class of side channels across multiple runtimes, and I demonstrate JIT-induced timing channels in large, open source projects large enough in magnitude to be detected over the public internet. I also present an automated approach to inducing this type of side channel in programs. In evaluating my automated technique, I show that programs classified as side-channel free by four state-of-the-art side channel analysis tools are, in fact, vulnerable to JIT-induced side channels. Finally, I discuss my contributions towards scalable quantification of side-channel vulnerabilities through a caching framework for model-counting queries.

Bio
Tegan Brennan is a PhD candidate in Computer Science at the University of California, Santa Barbara. Her research is in software engineering, formal verification and computer security. She has worked extensively on side-channel vulnerabilities in software. Tegan is a recipient of an IGERT Fellowship in Network Science, an NCWIT Collegiate Award Honorable Mention in 2018 and an invited participant of the 2019 Rising Stars workshop. She has interned twice with Amazon's Automated Reasoning Group. Tegan is also an aerialist and competitive ballroom dancer.

Monday, February 10, 2020
3:30 pm
Crerar 390
Host: Blase Ur