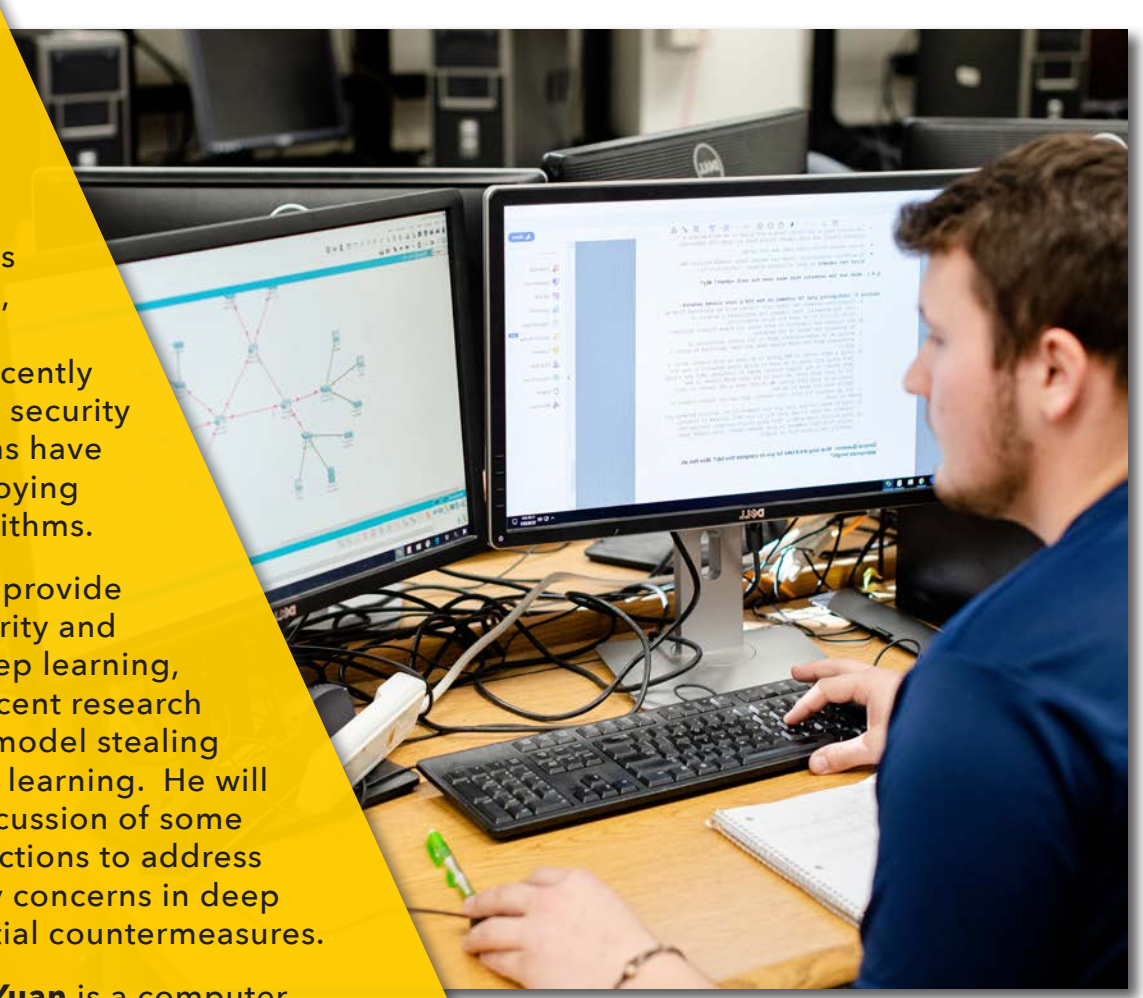
The College of Computing and the College of Engineering are pleased to present a lecture by faculty candidate

Brian Yuan

Wednesday, February 26, 2020

3:00 pm Chem. Sci. 101

Secure and Privacy: Preserving Machine Learning
A Case Study on Model Stealing Attacks Against Deep Learning



Due to recent breakthroughs, machine learning, especially deep learning, is pervasively serving areas such as autonomous driving, game playing, and virtual assistants. Recently however, significant security and privacy concerns have been raised in deploying deep learning algorithms.

In his talk, Yuan will provide an overview of security and privacy issues in deep learning, then focus on his recent research on a data-agnostic model stealing attack against deep learning. He will conclude with a discussion of some future research directions to address security and privacy concerns in deep learning and potential countermeasures.

Xiaoyong "Brian" Yuan is a computer science Ph.D. candidate at the University of Florida. His research interests span the fields of deep learning, machine learning, security and privacy, and cloud computing.

Michigan Tech
College of Engineering

Michigan Tech
College of Computing