UNIVERSITY OF SOUTH FLORIDA

Major Research Area Paper Presentation

From Hardware to Algorithms: Securing the Next Gen Machine Learning Applications

by

Brooks Olney

For the Ph.D. degree in Computer Science and Engineering

The costs of artificial intelligence (AI) and machine learning (ML) continue to rise. Energy costs of building complex models have driven innovation using alternative hardware platforms like field-programmable gate arrays (FPGAs) and tensor processing units (TPUs). As standard compute paradigms for AI/ML shift away from general purpose fabrics, so too has the discussion on security of these systems. Real-life costs as a result of dangerous security threats have spurred research in adversarial machine learning towards securing these applications and their hardware platforms. In this talk, we discuss the security risks of deploying ML applications in the cloud and at the edge, and present methods for securing ML applications from various cyberattacks, starting from the hardware abstraction layer, up to the ML algorithm itself.

Tuesday, December 7th, 2021
11am-12pm
Online (Microsoft Teams)
THE PUBLIC IS INVITED

Examining Committee
Robert Karam, Ph.D., Major Professor
Srinivas Katkoori, Ph.D.
Mehran Mozaffari Kermani, Ph.D.
Yasin Yilmaz, Ph.D.
Jean-François Biasse, Ph.D.

Xinming Ou, Ph.D.

Disability Accommodations:
If you require a reasonable accommodation to participate, please contact the Office of Diversity & Equal Opportunity at 974-4373 at least five (5) working days prior to the event.