ECE 7970 – Selected Topics in Electrical Engineering:
MACHINE LEARNING IN CYBER SECURITY

Course Description:

Lec. 3, Credit 3

Advanced topics in securing machine learning models and their applications to solve security/privacy threats.

Prerequisites: (1) ECE 6900: Security and privacy preservation for wireless networks (or other security/cryptography course), (2) CSC 6230: Machine Learning (or other machine learning course), or a consent from the instructor.

Prerequisites by Topic:

1. Knowledge of linear algebra, probability, statistics and calculus.
2. Knowledge of basic programming skills.
3. Knowledge of machine learning concepts.
4. Knowledge of basic security concepts and cryptography primitives.

Textbook(s) and/or Other Required Material(s):

No Required Text Book, Instructor will provide Class notes, tutorials and research papers

Course Coordinator: Dr. Mahmoud Mahmoud

Class Schedule:

Lecture: 3 hrs/week

Course Goal(s):

To address the research streams in securing machine learning models and using machine learning to solve security/privacy problems.

Course Topics:

1. Review to basic machine learning concepts. 15%
2. Review to basic security concepts and cryptography primitives. 10%

3. Attacks on machine learning models and countermeasures. 25%
4. Privacy-preserving evaluation of machine learning models. 15%
5. Using machine learning to launch attacks and counter security threats. 35%

Each topic will be covered via lectures and reading relevant research papers.

Instructional Outcomes for the Course:

Upon completion of this course, the student will be able to:

1. Understand the risks adversaries pose to machine learning models, and how to design secure machine learning models to mitigate those risks.
2. Understand how to protect from stealing machine learning models.
3. Understand how to preserve the privacy of the training datasets used to train machine learning models.
4. Understand how to evaluate machine learning models without leaking sensitive information.
5. Identify security/privacy problems that can be countered using machine learning models.
6. Utilize machine learning models to counter security/privacy threats.