EL-GY-9163: Machine Learning for Cyber-security
Instructor: Siddharth Garg (sg175@nyu.edu)

Class Meeting Times: Thu 5 PM - 7.30 PM Rationale: Artificial intelligence (AI) and machine learning (ML) techniques are being increasingly deployed in cyber-security settings. Examples of critical applications include *network anomaly detection*, *biometric authentication*, *spam detection*, and data analytics based *financial fraud detection*. At the same time, advanced ML algorithms also give attacker's an advantage, setting up a complex interplay between attackers and defenders. An important example is in the area of web privacy; it has been shown sophisticated attackers can use advanced inference techniques to compromise the identity of web users. In response, web users can intentionally add ``noise" to their online behaviors to evade advanced recognition attacks, borrowing tools from the literature on differential privacy.

At the same time, as ML techniques become more sophisticated, they themselves are vulnerable to attack. These include stealthy training data poisoning attacks, and so-called ``adversarial input perturbations" which have to been shown to be particularly pernicious for deep neural networks. For these reasons, there is growing interest in techniques to develop and deploy verifiably safe and secure ML systems, adopting and adapting techniques from the software security domain. A final vulnerability involves the fact that modern ML systems and especially deep learning systems are trained and executed in the cloud, raising concerns about the privacy of the user's data. New solutions are being developed to address these privacy concerns.

Anticipated Outcome: The educational outcomes of this class are two-fold: (1) provide solid research foundations for Ph.D. students working in this area, including a number of CCS Ph.D. students; and (2) prepare M.S. students interested in cyber-security for a rapidly growing market segment, especially in New York City, for cyber-security professions with a data-analytics and ML background.

Course Structure and Evaluation: Each lecture will be supplemented with reading material in the form of an in-depth survey or technical paper by a leading expert in the respective discipline. Evaluation will be in the form of:

- 3 take-home programming exercises (individual): 15% each for a total of 45%
- Semester long research project (groups of three): 30%
- Final Programming Examination: 25%

A course outline, along with associated reading material is below.

Pre-requisites: Intro. to Machine Learning (for M.S. students), None for ECE/CS Ph.D. students but will be expected to pick up the required any background they are lacking

TENTATIVE SYLLABUS

Week	Topic	Reading Material	Comments
Sep 2	***Foundations:*** Introduction and Basics I: Point estimation, MLE, linear	The first two lectures are a quick paced introduction to basic topics in ML. More advanced concepts will be	*Will be livestreamed online on Zoom. No on-campus component.*

	regression, bias-variance trade-offs	introduced and applied in the context of specific cyber-security applications	
Sep 9	***Foundations:*** Introduction and Basics II: Linear classification, clustering, feature selection	See Above *LAB 0: Linear Regression*	
Sep 16	***Application:*** Spam Filtering		
Sep 23	***Security Vulnerability:*** Attacks on spam filters	*LAB 1: Spam Filter*	
Sept 30	***Application:*** *Intrusion detection*	Note: Potential change to fake news and fake news detection	
Oct 7	***Foundations:*** *Deep Learning*		
Oct 14	***Application:*** *Biometrics, including face and fingerprint recogntion*	*LAB 2: TBA*	
Oct 21	***Security Vulnerability:*** Training Data-poisoning attacks on deep learning		
Oct 28	***Security Vulnerability:*** Adversarial input attacks on Deep Learning	*Final Project Competition Released*	
Nov 4	***Privacy:*** *Training data and model reconstruction attacks; differential privacy*	*LAB 3: TBA*	
Nov 11	***Application:*** *Social network bot detection and attacks on recommender systems*		
Nov 18	***Societal Implications:*** *Investigating bias and fairness concerns*		
Nov 25	*NO CLASS. Thanksgiving!*	*NO CLASS. Thanksgiving!*	
Dec 2	***Security Vulnerability:*** *Deep fakes and fake news attacks and detection.* Final Project Presentations	*All Project Presentations Due*	
Dec 9	***Conclusions:*** *Conclusions and looking ahead* Final Project Presentations		

	Final Take Home Programming Exam Released		
Dec 16	Final Take-home Programming Exam Due		