Adversarial Machine Learning Syllabus

Instructor: Bo Li (lxbosky@gmail.com)
TA: Xiaoming Zhao (xz23@illinois.edu)

1 Objectives

After this course, students will be able to understand security and privacy vulnerabilities of machine learning models, as well as how to make the learning tasks robust from various perspectives.

2 Grading

Criteria	Percent of Grade
Project	60%
(Initial Proposal, Due 9.23)	(5%)
(Status Report, Due 10.28)	(15%)
(Final Report & Presentation, Due 12.14)	(40%)
Paper reading and presentation	30%
(Paper reviews)	(10%)
(Presentation)	(15%)
(Peer rating)	(5%)
Class participation	10%

Note: The presentation is evaluated based on both the content of slides and quality of presentation.

3 Prerequisites

1. All enrolled students must have taken machine learning classes.
2. Projects will require training neural networks with standard automatic differentiation packages (TensorFlow, Pytorch).
3. Tentative Goal: Everyone group in the class should have one top-tier conference paper for your project!

4 Reading Materials and Project Topics

Checkout: `http://www.crystal-boli.com/teaching.html`