CSS 576 A Wi 23: Cybersecurity And Artificial Intelligence

Course Overview

The intersection of artificial intelligence (AI) and cybersecurity is emerging as an important field to ensure the integrity of economic and critical infrastructure. Industry and government need more people with training in both AI and cybersecurity.

This course examines the interaction of artificial intelligence and cybersecurity. It covers topics such as data acquisition, model training, applications of AI to cybersecurity, the interaction of AI and humans in security, and securing AI-based systems.

This course is designed to teach content derived from the key concepts for AISec described here.

Prerequisites

Familiarity with applied machine learning or cybersecurity concepts is helpful, but not required. The course will provide a high-level introduction to both.

Learning Objectives

- Demonstrate secure data acquisition and pre-processing.
- Train AI models to perform or augment security tasks.
- Evaluate the computational and classification performance of AI-based security.
- Assess AI-enhanced cybersecurity mechanisms as an attack surface.

Course Materials

- Course reading material will be derived from openly available research papers describing state of the art work at the intersection of cybersecurity and artificial intelligence.
    - S. Siva Kumar *et al.*, "Adversarial Machine Learning-Industry Perspectives," *2020 IEEE Security and Privacy Workshops (SPW)*, 2020, pp. 69-75, doi: 10.1109/SPW50608.2020.00028.
    - Bertino, Elisa, Murat Kantarcioglu, Cuneyt Gurcan Akcora, Sagar Samtani, Sudip Mittal, and Maanak Gupta. "AI for Security and Security for AI." In *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy*, pp. 333-334. 2021.
    - Kevin Wu and Brent Lagesse. *Detecting Hidden Webcams with Delay-Tolerant Similarity of Simultaneous Observation.* Pervasive and Mobile Computing, 2020.
    - Cody Burkard and Brent Lagesse. *Analysis of Causative attacks against SVMs Learning from Data Streams.* International Workshop on Security and Privacy Analytics, 2017.

- Xiao, Liang, Xiaoyue Wan, Xiaozhen Lu, Yanyong Zhang, and Di Wu. "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?." *IEEE Signal Processing Magazine* 35, no. 5 (2018): 41-49.
- Bozic, Josip, and Franz Wotawa. "Planning the attack! or how to use ai in security testing?." In *Iwaise: First international workshop on artificial intelligence in security*, vol. 50. 2017.
- Papernot, Nicolas, Patrick McDaniel, Arunesh Sinha, and Michael Wellman. "Towards the science of security and privacy in machine learning." *arXiv preprint arXiv:1611.03814* (2016).
- Additional papers from top venues such as https://aisec.cc/

Evaluation

In class exercises (10-15) -- 10%

These exercises will be approximately 30 minutes in duration and include both individual and group work. Each one will take a topic that we discuss in class and allow the students to participate in its hands-on application.

Assignments (4) -- 40%

- **Assignment 1:** Introduction to commonly used tools implementing a simple AI-Enhanced security mechanism using existing datasets. Example tasks include training and testing a spam filter, intrusion detection system, or malware classifier from existing sources.
- **Assignment 2:** Design and development of software for data collection, analysis, and preprocessing. Example tasks include reviewing terms of agreement and writing a bot to harvest data from publicly available APIs, analysis of data for bias, and cleaning incomplete data.
- **Assignment 3:** Implementation and assessment of an AI-enhanced cybersecurity mechanism. Examples tasks include utilizing the data from assignment 2 to implement and assess the performance of the security mechanism. Focus on the assessment differentiates this assignment from assignment 1.
- **Assignment 4:** Security analysis of the AI-Enhanced cybersecurity mechanism as a novel attack surface. Example tasks involve conducting red team tests on the security mechanism developed in assignment 3 focusing on adversarial examples, data poisoning, and model extraction.

Final Project (1) -- 20%

A large project spanning the full lifecycle of artificial intelligence and security.

Final Exam (1) -- 30%

A comprehensive exam

Tentative Course Schedule

Week	Topics	Notes	Reading
0	Intro, Cybersecurity Basics and Tools		Cybersecurity AI Survey
1	AI Basics and Tools	Assignment #1 due	AI Overview
2	System Design Requirements		
3	Industry Case Studies	Assignment #2 due	Unbiased Look at Dataset Bias
4	Data Collection, Preprocessing		Poisoning Attacks Survey
5	Model Training and Evaluation (supervised)	Assignment #3 due	
6	Model Training and Evaluation (unsupervised)		ART Documentation
7	System Deployment and Maintenance, Humans in the loop	Assignment #4 due	Adversarial Attacks and Defences: A Survey
8	Incident Response and Lessons Learned		Adversarial Machine Learning -- Industry Perspectives
9	Industry Case Studies		
10	Final Exam	Final Project Due	