CS4390/CS5390: Data-Driven Security and Privacy (ONLINE)

Monday and Wednesday from 1:30 pm to 2:50 pm (MST)

Spring 2021

Dr. Saeid Tizpaz Niari

saeid@utep.edu

COURSE DESCRIPTION

CS4390/5390 is a cross-list special topic course. The primary goal of this course is to study the security and privacy issues in applying data-driven solutions. In previous courses, students have examined computer security, software systems, and machine learning (data mining). In this class, we will explore security of machine learning models as well as the application of machine learning for computer security. After covering the basics of machine learning (ML) models such as linear algebra and stochastic gradient descent, we study the concerns related to safety, security, privacy, and fairness of ML models. In addition, we examine state-of-the-art data-driven techniques to address cybersecurity issues. We also overview paradigms beyond prevalent ML techniques that include probabilistic programming and causal inferences.

COURSE OBJECTIVES

Upon the completion of course:

- Students have a clear understanding of computations in data-driven and ML models,
- Students can evaluate the security, privacy, and fairness of prevalent ML models such as deep neural networks,
- Students can apply data-driven techniques for computer security and aware of the strength and weakness of data-driven solutions.
- Students are familiar with emerging techniques such as probabilistic programming and causal inference to address challenges in prevalent ML applications.

PREREQUISITES

This course requires no prior experience in security and privacy but assumes the willingness to seek out and read background material as needed. Although it is not a requirement, knowledge in core topics of machine learning and familiarity with Python and Numpy would be very helpful.
The first few weeks (estimated to be three weeks) are intended to cover the prerequisites.

Course Outlines

- Overview of machine learning (ML): KNN, linear classification, optimization, and neural networks.
- Attacks against ML: adversarial examples and Data poisoning.
- Challenges in defensing and detecting the ML attacks.
- Certified defenses against adversarial example and data poisoning attacks.
- Attacks against data privacy: reconstruction and membership attacks.
- Differential privacy and its applications (US Census 2020).
- Algorithmic Fairness: definitions, challenges and opportunities.

- Beyond prevalent ML models: probabilistic programming and causal inferences.
- Verification, white-box and gray-box methods for ML security.
- The application of ML for cyber-security: malware analysis and intrusion detection systems.
- The application of ML for security fuzzing and software testing.
- The application of ML for debugging and fault localizations.
- Challenges and opportunities in deploying ML-based software systems.

REQUIRED MATERIALS

The material for this course will be distributed, and there is no requirement to purchase a book. The list of paper is in course calendar.

COURSE ASSIGNMENTS AND GRADING

This is a research-oriented and discussion-based course, which also includes hands-on exercises in the first few weeks. The students are required to write a review for assigned papers prior to the class so that they can participate in class discussions. Every student needs to present one of the paper in class syllabus and lead the class discussion. Students will also work on a major project in group of 1,2, or 3 and deliver in phases. While it is not required, the ideal result of major project is a complete research paper draft, submittable in a well-respected AI/Security/SE venue.

Category	Percentage
Code Assignments	10%
Paper Assignments	20%
Class Presentations	10%
Class Participations	10%
Final Project (Write-up, code, and presentation)	50%

Code Assignment (10% of the grade)

There will be 2 or 3 code assignments in the first few weeks of class.

Paper Assignment (20% of the grade)

After the few first weeks, there will be paper assignments for each class. Students are required to write the paper summary and submit it before the class. The format and deadline for the assignments will be announced in class.

Paper Presentation (10% of the grade)

Students are required to sign-up and present one of major paper from the list of assigned papers.

Class Discussion Participations (10 % of the grade)

Since the course is discussion-based, the participation in class discussion (and online forum) is required.

Final Project (50 % of the grade)

The final project is the most important component for the course. Students need to form a group of 1, 2, or 3 and deliver materials in phases. Deliveries include write-ups, code, and presentations.

ATTENDANCE POLICY

This is a discussion-based senior/grad level class. The participation in class is absolutely required.

TECHNOLOGY REQUIREMENTS

We will use **Zoom** for class meetings. Students are required to install the zoom application and join to the class and office hour sessions via zoom. Other course contents such as submission are delivered via the Blackboard learning management system (LMS). Ensure your UTEP e-mail account is working and that you have access to the Web and a stable web browser. Mozilla Firefox and Google Chrome are the most supported browsers for Blackboard; other browsers may cause complications with the LMS. When having technical difficulties, update your browser, clear your cache, or try switching to another browser. You will need to have or have access to a computer/laptop, a webcam, and a microphone. If you encounter technical difficulties beyond your scope of troubleshooting, please contact the Help Desk as they are trained specifically in assisting with technological needs of students.

STANDARDS of CONDUCT

You are expected to conduct yourself in a professional and courteous manner, as prescribed by the Handbook of Operating Procedures: Student Conduct and Discipline. You are welcome and encouraged to work together in learning the material. However, whatever you submit for individual submissions must be your own.

Please also pay attention to the following netiquettes:

- Always consider audience. Remember that members of the class and the instructor will be reading any postings.
- Respect and courtesy must be provided to classmates and to instructor at all times. No harassment or inappropriate postings will be tolerated.
- Blackboard is not a public internet venue; all postings to it should be considered private and confidential. Whatever is posted on in these online spaces is intended for classmates and professor only. Please do not copy documents and paste them to a publicly accessible website, blog, or other space. If students wish to do so, they have the ethical obligation to first request the permission of the writer(s).

ACCOMMODATIONS POLICY

The University is committed to providing reasonable accommodations and auxiliary services to students, staff, faculty, job applicants, applicants for admissions, and other beneficiaries of University programs, services and activities with documented disabilities in order to provide them with equal opportunities to participate in programs, services, and activities in compliance with sections 503 and 504 of the Rehabilitation Act of 1973, as amended, and the Americans with Disabilities Act (ADA) of 1990 and the Americans with Disabilities Act Amendments Act (ADAAA) of 2008. Reasonable accommodations will be made unless it is determined that doing so would cause undue hardship on the University. Students requesting an accommodation based on a disability must register with the UTEP Center for Accommodations and Support Services.