Privacy & Machine Learning

CIS 6930 (Special Topics in CIS) Section 05DH
Class Periods: T 1:55 - 2:45 (Period 7) | R 1:55 - 3:50 (Periods 7-8)
Location: RNK 0225
Academic Term: Fall 2019

Instructor:
Prof. Vincent Bindschaedler
vbindsch (at) cise (dot) ufl (dot) edu

Office Hours: T - 2:45 – 3:45pm or by appointment

Course Description
Machine learning is increasingly integrated into our daily lives and promises advances in many applications domains including autonomous driving, facial recognition, and medical diagnosis. At the same time, machine learning techniques are surprisingly brittle and easy to misuse or abuse which highlights the potential dangers of this technology. Complex models can be fooled by tiny perturbations of their inputs; they can unintentionally memorize their training data; and they make decisions that are often inexplicable.

This course will explore recent academic research at the intersection of machine learning with data privacy. Students will read, analyze, and discuss research papers and undertake a semester-long research project.

Course Pre-Requisites / Co-Requisites
Knowledge of:
- Probability and statistics
- Machine learning

Familiarity with security and/or privacy concepts is a plus but not required.

Note: this course is primarily aimed at graduate students. But highly motivated undergraduates who seek exposure to research in this space are welcomed!

Course Objectives
Students will learn about foundational concepts at the intersection of machine learning with data privacy and acquire a firm grasp on recent developments in this area. By the end of the semester, successful students will be able to critically analyze research papers and will have demonstrated the ability to conduct research in this space.

I expect to cover the following topics:
- Data Privacy & Differential Privacy
- Adversarial Machine Learning & Adversarial Samples
- Membership Inference & Privacy Attacks
- Attacks on ML Models: Inversion, Duplication, Trojan
- Fairness, Transparency & Explainable/Interpretable ML
- DeepFakes & Generative Models

Note: this list is subject to modification based on student interests and time constraints.

Materials and Supply Fees
None.

Required Textbooks and Software
None. PDFs of reading material and academic papers will be provided.

Attendance Policy, Class Expectations, and Make-Up Policy

Attendance is *strongly recommended* but not mandatory. Due to the course format, students who miss many lectures will be at a *significant* disadvantage. To encourage interaction, participation will be assessed and count for 10% of the grade. Students are expected to have done the reading before class and actively participate during lectures and discussions (e.g., by asking questions or by volunteering their opinions). This is important to do well in this course.

Students will be assigned written, hands-on assignments and homework related to course topics and the course research project. Assignments will be announced in class and will be handled through the E-learning platform (elearning.ufl.edu). Assignments turned in late will incur a lateness penalty of 15% per day, up to a maximum of 3 days (after which the grade will be 0). If an extension is required for a legitimate reason (e.g., medical or travel), students should contact the instructor and provide justification a few days ahead of the assignment due date.

Excused absences must in compliance with university policies in the Graduate Catalog (http://gradcatalog.ufl.edu/content.php?catoid=10&navoid=2020#attendance) and require appropriate documentation.

Instruction Format & Evaluation of Grades

Instruction format will be a blend of traditional lecture-style instruction and student-led seminar-style learning through paper reading and discussion. Students will be expected to read several research articles every week and discuss them in class. The research project will require that students execute research alone or in a small group.

Students will be evaluated based on the following breakdown:

Assignment	Total Points	Percentage of Final Grade
Course Research Project	100	40%
Homework & Assignments	100 each	30%
Paper Reviews & Presentation	100 each	20%
Class Participation	100	10%

Grading Policy

Percent	Grade	Grade Points
92.0 - 100.0	A	4.00
85.0 - 91.9	A-	3.67
78.0 - 84.9	B+	3.33
71.0 – 77.9	B	3.00
64.0 - 70.9	B-	2.67
57.0 - 63.9	C+	2.33
50.0 – 56.9	C	2.00
43.0 - 49.9	C-	1.67
36.0 - 42.9	D+	1.33
29.0 - 35.9	D	1.00
22.0 - 28.9	D-	0.67
0 - 21.9	E	0.00

More information on UF grading policy may be found at: http://gradcatalog.ufl.edu/content.php?catoid=10&navoid=2020#grades

Academic Integrity

Students are required to follow the university guidelines on academic conduct and the student honor code (https://sccr.dso.ufl.edu/policies/student-honor-code-student-conduct-code) at all times. Students failing to meet these standards will be reported to the Dean of Students, ***which can result in the student receiving an 'E' for the semester***. In particular, students are explicitly forbidden from copying anything off of the Internet (e.g., source code, text, slides) without proper attribution or citation. Students are also forbidden from copying code/answers from each other for the purposes of completing any assignment or a course project.

Ethics Statement

This course covers topics concerning the security of many systems that are widely deployed and potentially critical. As part of this course, we will investigate methods, tools and techniques whose use may negatively impact the rights, property and lives of others. As security professionals, we rely upon the ethical use of the above technologies to perform research. However, it is easy to use such tools in an unethical manner. Unethical use includes the circumvention of existing security or privacy measurements for any purpose, or the dissemination, promotion, or exploitation of vulnerabilities of these services.

This is **NOT** a class on hacking. Any activity outside of the spirit of these guidelines will be reported to the proper authorities both within and outside of UF and may result in dismissal from the class and the University. Exceptions to these guidelines *may* occur in the process of reporting vulnerabilities through the proper channels; however, students with any doubt should consult Professor Bindschaedler for advice. *DO NOT* conduct any action which could be perceived as technology misuse anywhere or under any circumstances unless you have received explicit permission from Professor Bindschaedler.

Students Requiring Accommodations

Students with disabilities requesting accommodations should first register with the Disability Resource Center (352-392-8565, https://www.dso.ufl.edu/drc) by providing appropriate documentation. Once registered, students will receive an accommodation letter which must be presented to the instructor when requesting accommodation. Students with disabilities should follow this procedure as early as possible in the semester.

Course Evaluation

Students are expected to provide professional and respectful feedback on the quality of instruction in this course by completing course evaluations online via GatorEvals. Guidance on how to give feedback in a professional and respectful manner is available at https://gatorevals.aa.ufl.edu/students/. Students will be notified when the evaluation period opens, and can complete evaluations through the email they receive from GatorEvals, in their Canvas course menu under GatorEvals, or via https://ufl.bluera.com/ufl/. Summaries of course evaluation results are available to students at https://gatorevals.aa.ufl.edu/public-results/.

University Honesty Policy

UF students are bound by The Honor Pledge which states, "We, the members of the University of Florida community, pledge to hold ourselves and our peers to the highest standards of honor and integrity by abiding by the Honor Code. On all work submitted for credit by students at the University of Florida, the following pledge is either required or implied: "On my honor, I have neither given nor received unauthorized aid in doing this assignment." The Honor Code (https://sccr.dso.ufl.edu/policies/student-honor-code-student-conduct-code/) specifies a number of behaviors that are in violation of this code and the possible sanctions. Furthermore, you are obligated to report any condition that facilitates academic misconduct to appropriate personnel. If you have any questions or concerns, please consult with the instructor or TAs in this class.

Commitment to a Safe and Inclusive Learning Environment

The Herbert Wertheim College of Engineering values broad diversity within our community and is committed to individual and group empowerment, inclusion, and the elimination of discrimination. It is expected that every person in this class will treat one another with dignity and respect regardless of gender, sexuality, disability, age, socioeconomic status, ethnicity, race, and culture.

If you feel like your performance in class is being impacted by discrimination or harassment of any kind, please contact your instructor or any of the following:

- Your academic advisor or Graduate Program Coordinator
- Robin Bielling, Director of Human Resources, 352-392-0903, rbielling@eng.ufl.edu
- Curtis Taylor, Associate Dean of Student Affairs, 352-392-2177, taylor@eng.ufl.edu
- Toshikazu Nishida, Associate Dean of Academic Affairs, 352-392-0943, nishida@eng.ufl.edu

Software Use

All faculty, staff, and students of the University are required and expected to obey the laws and legal agreements governing software use. Failure to do so can lead to monetary damages and/or criminal penalties for the

individual violator. Because such violations are also against University policies and rules, disciplinary action will be taken as appropriate. We, the members of the University of Florida community, pledge to uphold ourselves and our peers to the highest standards of honesty and integrity.

Student Privacy

There are federal laws protecting your privacy with regards to grades earned in courses and on individual assignments. For more information, please see: https://registrar.ufl.edu/ferpa.html

Campus Resources:

Health and Wellness

U Matter, We Care:
Your well-being is important to the University of Florida. The U Matter, We Care initiative is committed to creating a culture of care on our campus by encouraging members of our community to look out for one another and to reach out for help if a member of our community is in need. If you or a friend is in distress, please contact umatter@ufl.edu so that the U Matter, We Care Team can reach out to the student in distress. A nighttime and weekend crisis counselor is available by phone at 352-392-1575. The U Matter, We Care Team can help connect students to the many other helping resources available including, but not limited to, Victim Advocates, Housing staff, and the Counseling and Wellness Center. Please remember that asking for help is a sign of strength. In case of emergency, call 9-1-1.

Counseling and Wellness Center: http://www.counseling.ufl.edu/cwc, and 392-1575; and the University Police Department: 392-1111 or 9-1-1 for emergencies.

Sexual Discrimination, Harassment, Assault, or Violence
If you or a friend has been subjected to sexual discrimination, sexual harassment, sexual assault, or violence contact the **Office of Title IX Compliance**, located at Yon Hall Room 427, 1908 Stadium Road, (352) 273-1094, title-ix@ufl.edu

Sexual Assault Recovery Services (SARS)
Student Health Care Center, 392-1161.

University Police Department at 392-1111 (or 9-1-1 for emergencies), or http://www.police.ufl.edu/.

Academic Resources

E-learning technical suppor*t*, 352-392-4357 (select option 2) or e-mail to Learning-support@ufl.edu. https://lss.at.ufl.edu/help.shtml.

Career Resource Center, Reitz Union, 392-1601. Career assistance and counseling. https://www.crc.ufl.edu/.

Library Support, http://cms.uflib.ufl.edu/ask. Various ways to receive assistance with respect to using the libraries or finding resources.

Teaching Center, Broward Hall, 392-2010 or 392-6420. General study skills and tutoring. https://teachingcenter.ufl.edu/.

Writing Studio, 302 Tigert Hall, 846-1138. Help brainstorming, formatting, and writing papers. https://writing.ufl.edu/writing-studio/.

Student Complaints Campus*:* https://www.dso.ufl.edu/documents/UF_Complaints_policy.pdf.

On-Line Students Complaints*:* http://www.distance.ufl.edu/student-complaint-process.