Course Information

Course Number:	CSCE 439/704
Course Title:	Data Analytics for CyberSecurity
Section:	500/602
Time:	Monday, Wednesday, and Friday 11:30 AM-12:20 PM
Location:	ZACH 244
Credit Hours:	3

Instructor Details

Instructor:	Marcus Botacin
Office:	PETR 224
Phone:	(979) 458-6850
E-Mail:	botacin@tamu.edu
Office Hours:	Regular: Mondays and Wednesdays, 1-2 PM (Zoom hours also available) By appointment: Upon email agreement. A calendar link will also be available on Canvas.

Course Description

Students will learn the multiple concepts related to the attack and defense of computing systems in the context of machine learning techniques. Students will be presented with both the attacker's and defender's perspectives to understand the strengths and weaknesses of the defense-in-depth strategy. The intent of this class is to put students in contact with the state-of-the-art literature in machine learning security and to promote their ability to transform this knowledge into practical skills to develop security systems.

Course Prerequisites

There is no strict prerequisite, but students are encouraged to have a background on the topics covered by CSCE 701 (Foundations of Cybersecurity) or CSCE 665 (Advanced Networking and Security) or an undergraduate course in computer and network security, equivalent to CSCE 465, to benefit from this course's discussions fully. Students must be proficient in programming, especially in Python, and to have basic knowledge of Machine Learning, such as how to train a simple ML model. Ask for instructor's advice in case of doubt.

Course Learning Outcomes

With a focus on malicious software but also covering a broad spectrum of other security applications, students successfully completing the course will be able to build their knowledge and abilities in the following fields:

Developing ML models for malware detection, thus understanding how Antivirus and security solutions work.

Developing strategies to keep an ML model functional over time, thus overcoming challenges such as concept evolution and drift.

Understanding the threats of Adversarial Examples to ML models, thus clarifying the context in which ML solutions are suitable.

Using the emerged Large Language Models (LLMs) to automatically generate code and handle malicious constructions, thus understanding the power of automation.

Using LLMs for security tasks such as bug finding and software repair, thus getting in touch with the multiple possibilities brought by the recent technological developments.

Developing practical skills on deploying adversarial attacks and defenses in third-party (pre-trained) models.

Textbook and/or Resource Materials

No textbook required. All materials will be posted on the class website (Canvas). Students should expect to run pre-trained ML models in their own machines. This course follows the minimum device requirements established by the College of Engineering (https://engineering.tamu.edu/academics/byod/devices/index.html).

Grading Policy

Participation and Reflection* (individual): 15%

Seminar Presentations** (Individual or groups of up to 5 students*): 35%

- *Group size might be adjusted to accommodate a large number of students enrolled in the course, at the instructor's discretion. Ask for permission.

Final project/Challenge*** (*Groups of up to 5 students): 50%

- *Group size might be adjusted to accommodate a large number of students enrolled in the course, at the instructor's discretion. Ask for permission.

No written exam, no quiz.

Total: 100%

***Participation and Reflection**

Students are required to keep a series of notes (ideally a blog) about the umbrella topics discussed in each class. Evaluation is as follows:

- Identifying correctly the key concepts of a topic: 40%
- Correctly explaining the concepts: 40%
- Stating own opinions: 10%
- Connection with previous classes/topics: 10%
- The deadline for posting the notes about a previous topic is 1 week after the last seminar presentation about that topic. Later posts will be considered delayed submissions.

****Seminar Presentation grading**

Students should discuss selected/assigned papers (at least one, depending on the number of students enrolled in the course).

- Oral Presentation (Slides should be made available to other students): 50%
- Written Summary (Wikipedia edit): 40%
- Stimulated class discussion quality (Presenters start discussing with the audience): 10%

Extra points: Providing code to reproduce the experiments presented in the paper. (up to 30%, not exceeding 100% of the total)

In case of multiple presentations, grades will be averaged.

Seminar Topic Selection

- The list of papers (1 to 3, of the same total complexity) for each seminar topic will be available on Canvas.
- A selection formulary will be available on Canvas.
- Groups will be assigned topics on a first-come, first-served basis.
- Topics must be selected at least one week before the presentation date.
- The instructor will remind the next presenters in the classroom in the week before the scheduled presentation date.
- The instructor will assign seminar topics to the students who do not make their topic selections by answering the selection form.

Seminar Preparation:

- The student should make the prepared presentation material (e.g., slides) available to the instructor before the presentation. Hint: Attend the professor's office hours to discuss the material preparation.

*****Final Project/Challenge grading**

Each group should deliver:

- A trained ML model to detect malware samples (defense step): 40%
- Modified malware samples intended to bypass other students' detectors (attack step): 40%
- A presentation explaining their strategies (attack and defense): 20%

Evaluation happens in a tournament. The grade is the greatest score achieved. For the defense part:

- Non-functional models will not receive a positive score.
- Any functional model that achieves FPR<1% and TPR>95% for the non-evasive samples distributed by the professor will receive at least a minimum score: 50.
- Any model that detects at least one Adversarial Example (AE) will receive a 60 score.
- Any model that detects at least one AE from each adversary team will receive a 70 score.
- Any model that detects all AEs from an adversary team but was evaded by the others receives an 80 score.
- Any model that detects at least 90% of all AEs receives a 90 score.
- Any model that detects more than 95% of all AEs receives a 100 score.
- Extra Points: Additional Models.
  - Groups might submit up to 5 additional defensive models.
  - Each additional model might receive a bonus of up to 10% (proportional to the detection performance)
  - Additional models will be evaluated using the same criteria stated above.
  - Additional models must be significantly different (in features) of the primary model.

For the attacking samples:

- If any sample evades at least one adversarial model, the team receives a minimum score of 50.
- If the samples evaded all classifiers of a single model, the team receives a 60 score.

- If the team evades all classifiers with at least one sample, the team receives a score of 70.
- If the samples evaded at least 50% of all classifiers, the team receives an 80 score.
- If the samples evaded at least 90% of all classifiers, the team receives a 90 score.
- If the samples evade all classifiers, the team scores a 100.
- The malware samples should be functional with regard to the execution in a sandbox environment.
- Extra points:
  - Any functional, automatically generated bypass of a model counts as a full bypass for that specific model.
  - Groups that demonstrate bypasses to their own models might earn up to 30% extra points (proportional to the number of bypasses)
- To facilitate the evaluation process and provide early feedback, the professor will establish multiple deadlines and checkpoints throughout the semester for the delivery and presentation of the defense and attack components.

Defenses' and Attacks' deliveries happen in rounds (checkpoints), as follows:

- The first Blackbox delivery counts for 25% of the grade.
- The second WhiteBox delivery counts for 25% of the grade.
- The final delivery counts for 50% of the grade.
- Extra: If the final delivery outperforms the initial checkpoints, this higher grade replaces the previous ones.

Grading Scale

85% <= A
75% <= B < 85%
65% <= C < 75%
60% <= D < 65%
F < 60%

Late Work Policy

Extensions/make-ups can be given 12 hours prior to the deadline upon written/in-person justification request. 20 minutes will be given as a grace period. Otherwise, 50% off from the credit you got for that submission.

Work submitted by a student as makeup work for an excused absence is not considered late work and is exempted from the late work policy (Student Rule 7).

Course Schedule (Tentative)

The course schedule is as follows (course topics are provisional):
All assignments are due at 11:59 PM on the due date, unless specified.

1 (25/Aug)	Lecture	Course Introduction: ML for Security	Seminar Topic/ Group Selection

2 (27Aug) NC (29/Aug) Labor Day (1/Sep) 3 (3/Sep) 4 (5/Sep)	Lecture No Classes No Classes Seminar Seminar	Building ML Models for Security Machine Learning for Security 1.1: Humans vs. Machines classification Machine Learning for Security 1,2: ML vs. DL: Dataset Balances	
5 (8/Sep)	Seminar	Best Practices 2.1: Challenges and Pitfalls 1	Notes for the previous topic.
6 (10/Sep)	Seminar	Best Practices 2.2: Challenges and Pitfalls 2	
7 (12/Sep)	Seminar	Best Practices 2.3: Do's and Don'ts 1	
8 (15/Sep)	Seminar	Best Practices 2.4: Do's and Don'ts 2	BlackBox Defense
9 (17/Sep)	Seminar	Adversarial Attacks 3.1: Droppers	Notes for the previous topic.
10 (19/Sep)	Seminar	Adversarial Attacks 3.2: Obfuscation	
11 (22/Sep)	Seminar	Adversarial Attacks 3.3: Automated Approache	
12 (24/Sep)	Seminar	Adversarial Attacks 3.4: Defenses	WhiteBox Defense + BlackBox Attacks
13 (26/Sep)	Seminar	Concept Drift 4.1: Android Malware 1	Notes for the previous topic.
14 (29/Sep)	Seminar	Concept Drift 4.2: Android Malware 2	
15 (1/Oct)	Seminar	Concept Drift 4.3: Math Modelling	WhiteBox Attacks
16 (6/Oct)	Presentation	Preliminary Project Presentation	Notes for the previous topic.
17 (8/Oct)	Presentation	Preliminary Project Presentation	
18 (10/Oct)	Presentation	Preliminary Project Presentation	
Fall Break (13/Oct)	No Classes		
Fall Break (15/Oct)	No Classes		
Fall Break (17/Oct)	No Classes		
19 (20/Oct)	Seminar	Large Language Models 5.1: Code Generation 1	
20 (22/Oct)	Seminar	Large Language Models 5.2: Code Generation 2	
21 (24/Oct)	Seminar	Large Language Models 5.3: Bug Fixing	
22 (27/Oct)	Seminar	Large Language Models 5.4: Reverse Engineering	
23 (29/Oct)	Seminar	Large Language Models 5.5: Code Poisoning	
24 (31/Oct)	Seminar	Large Language Models 5.6: Malware Generation	
25 (3/Nov)	Seminar	Large Language Models 5.7: Penetration Testing	
26 (5/Nov)	Seminar	ML Applications 6.1: Biometrics	Notes for the previous topic.
27 (7/Nov)	Seminar	ML Applications 6.2: Authentication	
28 (10/Nov)	Seminar	ML Applications 6.3: Rule Generation	

29 (12/Nov)	Seminar	ML Security 7.1: Backdoors	Notes for the previous topic.
30 (14/Nov)	Seminar	ML Security 7.2: Machine Unlearning	Final Project Delivery
31 (17/Nov)	Presentation	Final Project Presentation	Notes for the previous topic.
32 (19/Nov)	Presentation	Final Project Presentation	
33 (21/Nov)	Presentation	Final Project Presentation	
34 (24/Nov)	Presentation	Final Project Presentation	
35 (26/Nov)	Presentation	Final Project Presentation	
36 (28/Nov)	Presentation	Final Project Presentation	
37 (1/Dec)	Presentation	Final Project Presentation	
38 (3/Dec)	Presentation	Final Project Presentation	
39 (5/Dec)	Presentation	Final Project Presentation	
40 (8/Dec)	Presentation	Final Project Presentation	Presentation Notes + Extras

University Policies

Attendance Policy

The university views class attendance and participation as an individual student responsibility. Students are expected to attend class and to complete all assignments.

Please refer to Student Rule 7 in its entirety for information about excused absences, including definitions, and related documentation and timelines.

Makeup Work Policy

Students will be excused from attending class on the day of a graded activity or when attendance contributes to a student’s grade, for the reasons stated in Student Rule 7, or other reason deemed appropriate by the instructor.

Please refer to Student Rule 7 in its entirety for information about makeup work, including definitions, and related documentation and timelines.

Absences related to Title IX of the Education Amendments of 1972 may necessitate a period of more than 30 days for make-up work, and the timeframe for make-up work should be agreed upon by the student and instructor” (Student Rule 7, Section 7.4.1).

“The instructor is under no obligation to provide an opportunity for the student to make up work missed because of an unexcused absence” (Student Rule 7, Section 7.4.2).

Students who request an excused absence are expected to uphold the Aggie Honor Code and Student Conduct Code. (See Student Rule 24.)

Academic Integrity Statement and Policy

"An Aggie does not lie, cheat or steal, or tolerate those who do."

"Texas A&M University students are responsible for authenticating all work submitted to an instructor. If asked, students must be able to produce proof that the item submitted is indeed the work of that student. Students must keep appropriate records at all times. The inability to authenticate one's work, should the instructor request it, may be sufficient grounds to initiate an academic misconduct case" (Section 20.1.2.3, Student Rule 20).

Texas A&M at College Station
You can learn more about the Aggie Honor System Office Rules and Procedures, academic integrity, and your rights and responsibilities at aggiehonor.tamu.edu.

Texas A&M at Galveston
You can learn more about the Honor Council Rules and Procedures as well as your rights and responsibilities at tamug.edu/HonorSystem.

Texas A&M at Qatar
You can learn more about academic integrity and your rights and responsibilities at Texas A&M University at Qatar by visiting the Aggie Honor System website.

Americans with Disabilities Act (ADA) Policy

Texas A&M University is committed to providing equitable access to learning opportunities for all students. If you experience barriers to your education due to a disability or think you may have a disability, please contact the Disability Resources office on your campus (resources listed below) Disabilities may include, but are not limited to attentional, learning, mental health, sensory, physical, or chronic health conditions. All students are encouraged to discuss their disability related needs with Disability Resources and their instructors as soon as possible.

Texas A&M at College Station
Disability Resources is located in the Student Services Building or at (979) 845-1637 or visit disability.tamu.edu.

Texas A&M at Galveston
Disability Resources is located in the Student Services Building or at (409) 740-4587 or visit tamug.edu/counsel/Disabilities.

Texas A&M at Qatar

Disability Services is located in the Engineering Building, room 318C or at +974.4423.0316 or visit https://www.qatar.tamu.edu/students/student-affairs/disability-services.

Title IX and Statement on Limits to Confidentiality

Texas A&M University is committed to fostering a learning environment that is safe and productive for all. University policies and federal and state laws prohibit gender-based discrimination and sexual harassment, including sexual assault, sexual exploitation, domestic violence, dating violence, and stalking.

With the exception of some medical and mental health providers, all university employees (including full and part-time faculty, staff, paid graduate assistants, student workers, etc.) are Mandatory Reporters and must report to the Title IX Office if the employee experiences, observes, or becomes aware of an incident that meets the following conditions (see University Rule 08.01.01.M1):

> The incident is reasonably believed to be discrimination or harassment.
> The incident is alleged to have been committed by or against a person who, at the time of the incident, was (1) a student enrolled at the University or (2) an employee of the University.

Mandatory Reporters must file a report regardless of how the information comes to their attention – including but not limited to face-to-face conversations, a written class assignment or paper, class discussion, email, text, or social media post. Although Mandatory Reporters must file a report, in most instances, a person who is subjected to the alleged conduct will be able to control how the report is handled, including whether or not to pursue a formal investigation. The University's goal is to make sure you are aware of the range of options available to you and to ensure access to the resources you need.

Texas A&M at College Station

Students wishing to discuss concerns in a confidential setting are encouraged to make an appointment with Counseling and Psychological Services (CAPS).

Students can learn more about filing a report, accessing supportive resources, and navigating the Title IX investigation and resolution process on the University's Title IX webpage.

Texas A&M at Galveston

Students wishing to discuss concerns in a confidential setting are encouraged to make an appointment with the Counseling Office in the Seibel Student Center, or call (409)740-4587. For additional information, visit tamug.edu/counsel.

Students can learn more about filing a report, accessing supportive resources, and navigating the Title IX investigation and resolution process on the Galveston Campus' Title IX webpage.

Texas A&M at Qatar

Texas A&M University at Qatar students wishing to discuss concerns in a confidential setting are encouraged to visit the Health and Wellness website for more information.

Students can learn more about filing a report, accessing supportive resources, and navigating the Title IX investigation and resolution process on the University's Title IX webpage.

Statement on Mental Health and Wellness

Texas A&M University recognizes that mental health and wellness are critical factors that influence a student's academic success and overall wellbeing. Students are encouraged to engage in healthy self-care by utilizing available resources and services on your campus

Texas A&M College Station
Students who need someone to talk to can contact Counseling & Psychological Services (CAPS) or call the TAMU Helpline (979-845-2700) from 4:00 p.m. to 8:00 a.m. weekdays and 24 hours on weekends. 24-hour emergency help is also available through the National Suicide Prevention Hotline (800-273-8255) or at suicidepreventionlifeline.org.

Texas A&M at Galveston
Students who need someone to talk to can call (409) 740-4736 from 8:00 a.m. to 5:00 p.m. weekdays or visit tamug.edu/counsel for more information. For 24-hour emergency assistance during nights and weekends, contact the TAMUG Police Dept at (409) 740-4545. 24-hour emergency help is also available through the National Suicide Prevention Hotline (800-273-8255) or at suicidepreventionlifeline.org.

Texas A&M at Qatar
Texas A&M University at Qatar students wishing to discuss concerns in a confidential setting are encouraged to visit the Health and Wellness website for more information.

Campus-Specific Policies

Texas A&M at Galveston

Classroom Access and Inclusion Statement

Texas A&M University is committed to engaged student participation in all of its programs and courses and provides an accessible academic environment for all students. This means that our classrooms, our virtual spaces, our practices and our interactions are as inclusive as possible and we work to provide a welcoming instructional climate and equal learning opportunities for everyone. If you have an instructional need, please notify me as soon as possible.

The Aggie Core values of respect, excellence, leadership, loyalty, integrity and selfless service in addition to civility, and the ability to listen and to observe others are the foundation of a welcoming instructional climate. Active, thoughtful and respectful participation in all aspects of the course supports a more inclusive classroom environment as well as our mutual responsibilities to the campus community.

The following statements below are optional. Leave as is to include, or delete if preferred. Either way, delete this note.

Statement on the Family Educational Rights and Privacy Act (FERPA)

FERPA is a federal law designed to protect the privacy of educational records by limiting access to these records, to establish the right of students to inspect and review their educational records and to provide guidelines for the correction of inaccurate and misleading data through informal and formal hearings. Currently enrolled students wishing to withhold any or all directory information items may do so by going to howdy.tamu.edu and clicking on the "Directory Hold Information" link in the Student Records channel on the MyRecord tab. The complete FERPA Notice to Students and the student records policy is available on the Office of the Registrar webpage.

Items that can never be identified as public information are a student's social security number, citizenship, gender, grades, GPR or class schedule. All efforts will be made in this class to protect your privacy and to ensure confidential treatment of information associated with or generated by your participation in the class.

Directory items include name, UIN, local address, permanent address, email address, local telephone number, permanent telephone number, dates of attendance, program of study (college, major, campus), classification, previous institutions attended, degrees honors and awards received, participation in officially recognized activities and sports, medical residence location and medical residence specialization.

College and Department Policies

College and departmental units may establish their own policies and minimum syllabus requirements. As long as these policies and requirements do not contradict the university level requirements, colleges and departments can add them in this section. Please remove this section if not needed.