CSEC 520/620: Cyber Analytics & ML **Fall 2022**

Instructor Information

Instructor: Nate Mathews
Email: nate.mathews@mail.rit.edu
Zoom:
Office Hours: *On Zoom, Wed. 2-3pm*
Password:
Slack:

Section Information: CSEC 520/620
Class Meeting Times: Tu/Th 3:30-4:45PM **Location**: GOL-1435

Course Description: The course provides students an opportunity to explore methods and applications in cyber analytics with advanced machine learning algorithms including deep learning. Students will learn how to use machine learning methods to solve cybersecurity problems such as network security, anomaly detection, malware analysis, etc. Students will also learn basic concepts and algorithms in machine learning such as clustering, neural networks, adversarial machine learning, etc.

Course Objectives: By the end of the course, students should be able to:

- Understand basic concepts and algorithms of ML and DL
- Apply appropriate ML algorithms to solve computing security problems
- Develop an original solution for computing security problems using ML
- Analyze and evaluate existing ML solutions for computing security problems

Required Textbooks and Other Course Materials:

Clarence Chio and David Freeman, *Machine Learning and Security: Protecting Systems with Data and Algorithms*, 1st Edition, O'Reilly Media. ISBN-13: 978-1491979907 ISBN-10: 1491979909

Prerequisites: Knowledge in Discrete Math, Probability and Statistics, and Linear Algebra, and the ability to program in Python. 4th year standing (520) or Graduate standing (620).

Note: *The instructor reserves the right to modify course policies, the course calendar, and assignment or project point values and due dates.*

Grading: Course grades will be based on the following:

Trends Presentation	2%
Quizzes (9)	10%
Experimentation Assignments (4)	48%
Final Project Report	15%
Final Project Presentation	3%
Exam 1	10%
Exam 2	12%

Final grades will be the weighted average of your scores, based on the percentages above, and not curved (A=93+, A-=90-93, B+=87-90, B=83-87, etc.). Small amounts of extra credit may be available on a class-wide basis (no individual requests will be granted). Grade bumps may be given based on participation in class (max. 1%).

Late Policy: Any assignment may be submitted up to two weeks late, incurring a 2% penalty on the final grade per day beyond deadline. After that time, assignments **will not be accepted**, except for pre-arranged make-ups.

Make-ups: Make-ups for graded activities may be arranged if your absence is caused by illness or personal emergency. A written explanation (including supporting documentation) must be submitted to the instructor; if the explanation is acceptable, an alternative to the graded activity will be arranged. Make-up arrangements must be arranged **prior** to the scheduled due date.

Virtual Adaption: To accommodate students who cannot join in person, we will be using tools for online discussion and remote work. We do not offer any guarantees on how effective this will be for remote students.

Descriptions of major assignments and examinations with due dates:

- *Trends Presentation*: Find a recent article, video, research paper, or blog post about machine learning in cybersecurity and summarize the key points in a 5-minute presentation in class. 10% of presentation grades is for asking good questions following other students' presentations.
- *Quizzes:* Short quizzes will be given to cover each week's videos and readings. Due on Tuesdays before class on weeks 2-6 and 9-12. Team quizzes will be given during Tuesday classes.
- *Experimentation Assignments* (Sep. 15, Oct. 4, Oct. 27, Nov. 14): Work in teams to perform a study using a security-related dataset. Submit your code, a report of your findings, and answers to assigned questions.
- *Final Project* (Dec. 14): Work as a team to investigate a topic of your choice in more depth. It must include an experimental component. Submit your code, a report of your project idea and findings, and present the final results during the course Final period (12/14, 1:30-4:00). 10% of presentation grades is for asking good questions following other students' presentations.
- *Exams* (Oct. 6 and Nov. 17): Exams will be held in class. Exam 2 is comprehensive.

Course Schedule (Subject to Change)

Week	*Class Dates*	*Topic*	*Assignments*	*Due Dates*
1.	Aug. 23/25	Class Intro & Spam Case Study		
2.	Aug. 30/Sep. 1	NLP and Bayesian Classifiers	A1	Sep. 15
3.	Sep. 6/8	ML Basics & Logistic Regression		
4.	Sep. 13/15	HIDS with Clustering	A2	Oct. 4
5.	Sep. 20/22	HIDS with Statistical Analysis		
6.	Sep. 27/29	Malware Analysis with SVM	A3	Oct. 27
7.	Oct. 4/6	Review & Exam	**Exam 1**	**Oct. 6**
8.	Oct. 11/13	**FALL BREAK** & Practical ML in Cybersecurity		
9.	Oct. 18/20	NIDS with Decision Trees		
10.	Oct. 25/27	NIDS with Random Forests	A4	Nov. 15
11.	Nov. 1/3	Neural Networks 1		
12.	Nov. 8/10	Applying Neural Networks	Final Project	Dec. 14
13.	Nov. 15/17	Review & Exam	**Exam 2**	**Nov. 17**
14.	Nov. 22/24	Special Topics & **THANKSGIVING**		
15.	Nov. 29/Dec. 1	Special Topics & Class Wrap-up		
16.	**Finals Week**	**Final Presentations** (TBD)		

Reasonable Accommodations: RIT is committed to providing reasonable accommodations to students with disabilities. If you would like to request accommodations such as special seating or testing modifications due to a disability, please contact the Disability Services Office. It is located in the Student Alumni Union, Room 1150; the Web site is www.rit.edu/dso. After you receive accommodation approval, it is imperative that you see me during office hours so that we can work out whatever arrangement is necessary.

Academic Integrity: As an institution of higher learning, RIT expects students to behave honestly and ethically at all times, especially when submitting work for evaluation in any course or for any degree requirement. CSEC encourages all students to become familiar with the RIT Honor Code and with RIT's Academic Integrity Policy.

Copyright: Certain materials used in this course are protected by copyright and may not be copied or distributed by students. You can find more information at: http://www.rit.edu/academicaffairs/policiesmanual/sectionC/C3_2.html.

Mental Health: Success in this course depends heavily on your personal health and wellbeing. Recognize that stress is an expected part of the college experience, and it often can be compounded by unexpected setbacks or life changes outside the classroom. Moreover, those with marginalized identities may be faced with additional social stressors. Your other instructors and I strongly encourage you to reframe challenges as an unavoidable pathway to success. Reflect on your role in taking care of yourself throughout the term, before the demands of exams and projects reach their peak. Please feel free to reach out to me about any difficulty you may be having that may impact your performance in this course as soon as it occurs and before it becomes unmanageable. In addition to your academic advisor, I strongly encourage you to contact the many other support services on campus that stand ready to assist.