Artificial Intelligence for Security (AI4Sec): Foundations Syllabus

Department of Computer Science and Software Engineering Samuel Ginn College of Engineering, Auburn University

Spring 2024 (3 credit hours) COMP 5970-005/6970-005/D05

This syllabus is subject to change. Substantive changes will be announced via appropriate communication channels.

Published: November 10, 2023

Course Concept

One of the greatest threats to national security is our adversaries' aggressive pursuit of dominance of cyberspace (e.g., nation states, organized crime, terrorist organizations) through advanced AI. There is thus a critically urgent need to build our nation's workforce and research capacities in the intersection of cybersecurity (security) and artificial intelligence (AI). Unfortunately, efforts to catalyze this union have not kept pace and the disciplines' curricula remain mostly isolated. Fundamental concepts in one discipline (e.g., the notion of an adversary in security and the use of big data in AI) are often seen as novel challenges and new areas to explore in the other. Thus, in addition to learning how to apply techniques across the disciplines, practicing to think from a multidisciplinary perspective by conveying the mindset and "conventional wisdom" of each, makes this course essential to address the threats to national security.

Course Description

This course is built around small highly collaborative teams consisting of a mix of students with AI and/or security backgrounds. These teams will tackle a series of assignments where they learn how to utilize AI to solve various security problems inspired by real-world scenarios. Specifically, this course employs red-vs-blue security interaction as a single, all-encompassing environment. Within this universal learning environment, students are able to not only leverage their existing backgrounds in AI/security but also gain exposure to techniques, perspectives, and application from the lacking discipline (security/AI respectively). The high-fidelity Galaxy emulation platform provides the degree of realism needed to foster a deep understanding of security aspects while simultaneously being designed to allow AI-agent interactions and autonomous operation within a safe setting (i.e., a closed-loop virtual environment).

Instructional Mode

The instructional mode for the on-campus sections (COMP 5970-005 & COMP 6970-005) of this course is *Face-to-Face*. Due to the highly collaborative and group-based nature of this class

which relies on frequent in-class active learning, the instructional mode must be synchronous. Normally distance classes are only offered asynchronously, but to make this unique course offering available to distance students, a *Synchronous Online* section (COMP 6970-D05) is being offered.

Prerequisites

The prerequisite for this course is a minimum grade of C in one of:

- COMP 5130/6130/6136 – Data Mining
- COMP 5370/6370/6376 – Computer and Network Security
- COMP 5600/6600/6606 – Artificial Intelligence
- COMP 5630/6630/6636 – Machine Learning
- COMP 5650/6650/6656 – Deep Learning
- COMP 5660/6660/6666 – Evolutionary Computing
- COMP 5830/6830 – Cybersecurity Threats and Countermeasures

Distance Students

You are expected to have all the equipment and software needed to be successful in this course. You must have a computer and a broadband Internet connection capable of installing and reliably running Zoom to facilitate synchronous interaction during class time and office hours. Zoom is licensed by Auburn University, and you can sign up free of charge for this added-feature version authenticated with your AU credentials at https://auburn.zoom.us/. If you have needs regarding instructional technology, you can contact the AU Bookstore at books@auburn.edu.

Times for all class events will be set in US Central Time, which may not correspond to the time zone in which you will be living and studying. You are responsible for meeting deadlines in Central Time regardless of what your local time zone may be.

Tentative Student Learning Outcomes (SLOs)

This course has two tentative SLOs for all students (COMP 5790-005/6970-005):

- the ability to design, implement, experiment with, and analyze AI approaches in the security domain
- the multidisciplinary perspective melding the mindsets and "conventional wisdom" specific to each of the AI and security disciplines

This course has one additional SLO for graduate and undergraduate honors students (COMP 6970-005):

- equip students with experience leading an interdisciplinary group through multiple series of projects

Justification for Graduate Credit

Graduate credit is justified for the 6000-level section because of additional requirements beyond the 5000-level section which equip students with experience leading and assisting an interdisciplinary group of non-experts through multiple series of projects and assess them on that.

Coding Requirements

This course will make extensive use of Python, but students may also need to utilize CLI tools such as grep, sed, and awk, and in conjunction with whatever scripting/programming language is most appropriate. All code should be properly commented and documented. You are required to consistently employ a high-quality coding style to facilitate collaborative work and artifact review by the instructional team, besides being good practice. For coding style advice and examples of high-quality style guides, see Dr. T's Coding Standards & Tips. If in doubt, contact the TA!

Instructional Team

Instructors

Name	Daniel Tauritz, Ph.D.	Drew Springall, Ph.D.
Office hours	walk-in/by appointment	walk-in/by appointment
E-mail	dtauritz@auburn.edu	aaspring@auburn.edu
WWW	https://bonsai.auburn.edu/dtauritz/	https://aaspring.com/

Teaching Assistant Info

Name	Deacon Seals
E-mail	djs0080@auburn.edu
Lab hours	by appointment

Miscellaneous Class Information

Required textbook	None
Class website	https://bonsai.auburn.edu/dtauritz/courses/ai4sec/fnd/2024spring/
Lecture times	Tuesdays, Thursdays 5:00-6:15 PM
Lecture venue	Shelby Center 2101
Class schedule	Dynamic schedule

Grading Information

Grades will be primarily based on assignment performance; there are no tests in this class.

Meet with the instructors	1% of total grade
Assignments	99% of total grade
Final Letter Grade	[90-100]: A, [80-90>: B, [70-80>: C, [60-70>: D, <60: F

Class Policies

Attendance
Consistent with AU's policy on class attendance, on-campus students are expected to attend all scheduled class sessions. This is a highly interactive, student-centric course, so attendance for on-campus students is mandatory. Roll will be taken and students with more than two unexcused absences may be dropped. Students with properly authorized excused absences as defined by the Student Policy eHandbook, upon appropriate verification, need to make arrangements with the instructor to make up missed class sessions.

Distance students are highly encouraged to interact with their team mates with both audio and video feeds to maximize interaction quality. Although you may be participating from your domicile, our Zoom meetings are professional interactions. You should behave as you would in a normal F2F classroom. To the extent possible, please minimize distractions in the background. We reserve the right to dismiss anyone from a Zoom meeting whose environment or behavior is distracting or problematic. If you have any issues with sharing your video feed, adhering to this policy, or anything else related to your use of Zoom, you need to notify us via email in the first week of class. We are happy to consider and provide accommodations, but you will need to be in communication with us.

Assignment Deadline Extension Policy
For distance education students, if an assignment deadline is known in advance to pose a hardness, then with sufficient notice the instructor will attempt to accommodate all reasonable requests for extended deadlines (example of a reasonable request: a working professional needing to travel for their job).

For all students, if an assignment deadline cannot be reasonably met due to any of the same circumstances stipulated by the Student Policy eHandbook for properly authorized excused absences, the instructor will attempt to accomodate all reasonable requests for extended deadlines (example of a reasonable request: a student has a documented illness for three days in the period between the due dates for the second and third assignment and requests a three day extension for the third assignment).

Submission Policy
All written documents need to be electronically typeset and submitted in PDF file format. You are encouraged, but not required, to typeset using LaTeX. All assignments are due strictly at 10:00pm central time on their respective due dates and are to be submitted as specified in the assignment write-ups. Students are responsible for submitting their assignments well before the deadline to avoid last minute system-related (or other) issues. The default penalty for late submission is a 5% point deduction for the first 24 hour period and a 10% point deduction for

every additional 24 hour period. So 1 hour late and 23 hours late both result in a 5% point deduction, 25 hours late results in a 15% point deduction, etc.

Re-grading Policy
Any assignment re-grading requests must be made to the instructors within one week of the day the assignment grade and feedback was posted. Even if you believe that you found an error in grading, it will not be re-graded if you request re-grading after this deadline.

Communication Policy
Information related to this class will be communicated during lectures as well as via Discord, E-mail, and the class website. Discord will be the primary online platform for class communication and all enrolled students will be provided an invite to join the class Discord server by the first day of class. Students are expected to monitor all these communication channels daily.

E-mails that you send to the instructors should come from your `@auburn.edu` email address. Sending emails from addresses other than `@auburn.edu` could result in you not receiving a response to your message. All E-mail communications from the instructors to you will be sent to your `@auburn.edu` address.

ADA Policy
The instructors will make all reasonable accomodations to comply with the provisions of the Americans with Disabilities Act. Students who need accommodations need to electronically submit their approved accommodations through AU Access and to make an individual appointment with the instructors as soon as possible during the first week of classes. Students who have not established accommodations through the Office of Accessibility, but need accommodations, need to as soon as possible make an appointment with the Office of Accessibility, 1228 Haley Center, 844-2096 (V/TT).

Academic Honesty
Academic honesty is critical to the entire educational process and is a serious matter in this course. Issues surrounding violations of academic honesty will be handled per the Student Academic Honesty Code. You are encouraged to familiarize yourself with this policy and the academic honesty resources and tips available from: https://www.auburn.edu/academic/provost/academic-honesty/.

Classroom Behavior
The Auburn University Classroom Behavior Policy articulated in the Student Policy eHandbook is strictly followed in this course.

Diversity and Inclusion Statement
It is our intent that students from all diverse backgrounds and perspectives be well served by this course, that students' learning needs be addressed both in and out of class, and that the diversity that students bring to this class be viewed as a resource, strength, and benefit. It is my intent to present materials and activities that are respectful of diversity: gender, religion, sexuality, disability, age, socioeconomic status, veteran status, ethnicity, race, and culture. All students in this course are expected to respect their fellow classmates and actively participate in fostering an

inclusive learning environment. If you experience anything in this class that makes you feel uncomfortable, please bring it to my attention and we will formulate a response. If you would prefer to remain anonymous you may complete a Bias Incident Report which will maintain your confidentiality.

Your suggestions are encouraged and appreciated. Please let me know ways to improve the effectiveness of the course for you personally or for other students or student groups.

Names and Pronouns
Many people might go by a name in daily life that is different from their legal name. In this classroom, we will refer to people by the names that they go by. Pronouns are a way to affirm someone's identity. They are simply a public way in which people are referred to in place of their name (e.g., "he" or "she" or "they" or "ze" or something else). In this classroom, you are invited to share what pronouns you go by, and we will refer to people using the pronouns that they share.

Data Collection and Use Disclosure
Any and all results of graded items in the course are potential data sources for assessment and educational research, and may be used in publications related to educational research and accreditation. All such use will be anonymous. No personal intellectual property (IP) will be infringed.

Extended Student Absence
If illness causes you to be unable to participate for an extended period in the class, please contact the instructors as soon as possible to discuss your options.

Emergency Contingency
If normal class and/or lab activities are disrupted due to illness, emergency, or crisis situations (such as a COVID-19 outbreak), the syllabus and other course plans and assignments may be modified to allow completion of the course. If this occurs, an addendum to the syllabus and/or course assignments will replace the original materials.