

CIS 400 / CIS 600 / CSE 400 / CSE 691**Introduction to AI for Cybersecurity****Syracuse University • Fall 2026**

Class Location: CST 4-201 Class Time: 5:00–6:20 PM, Tu/Th

Class Dates: Aug. 25 – Dec. 8, 2026

Instructor: Kristopher Micinski**E-mail:** kkmicins@syr.edu**Office:** TBD**Phone:** 940-399-8924**Office Hours:** 3 hours per week, TBD**Contact hours:** 3**Course Description**

This course will rigorously study the impact of emerging AI systems on the principles and practices of cybersecurity. Topics include AI-assisted exploit generation and code auditing, autonomous social-engineering attacks, and AI-driven defense strategies such as automated intrusion detection and adaptive threat response. Additional work required for graduate students.

Pre-requisites (that may also be taken as co-requisites)

CIS 351 and CSE 484. The CSE 484 requirement may be waived with instructor permission.

Audience

Students matriculated in the Computer Science BS, Computer Engineering BS, or AI Science BS. The graduate sections (CIS 600 / CSE 691) are open to MS and PhD students in Computer Science, Computer Engineering, AI Science, and Cybersecurity. Senior undergraduates and MS students are the primary audience.

Credits

3

Course Fees and/or Costs

N/A

Learning Objectives

1. Explain how AI systems can be used to both strengthen and undermine cybersecurity defenses.
2. Analyze the capabilities and limitations of AI-based approaches to vulnerability detection and threat analysis.
3. Evaluate the risks that AI poses to existing security models and practices.
4. Apply AI techniques to solve practical cybersecurity problems.
5. Assess the ethical and policy implications of deploying AI in security contexts.
6. Present findings on AI-cybersecurity topics through written analysis and project-based work.

Shared Competencies Course Tags [UNDERGRADUATE ONLY]

<https://effectiveness.syr.edu/shared-competencies/course-tagging/>
Information Literacy and Technological Agility

Required Texts / Supplies

None

Optional Texts / Supplies

- Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd Edition, Wiley, 2020.
- Anthony D. Joseph, Blaine Nelson, Benjamin I. P. Rubinstein, and J. D. Tygar, *Adversarial Machine Learning*, Cambridge University Press, 2019.
- Edward Raff, *Inside Deep Learning: Math, Algorithms, Models*, Manning Publications, 2022.
- Gareth James et al., *An Introduction to Statistical Learning: With Applications in Python*, Springer, 2023.

Course Requirements and Expectations

- **Class Project:** There will be a class project which will be accomplished in the last six weeks of class. Projects can be accomplished either alone or in a group, with higher expectations for groupwork depending on group size (maximum of three participants per group).
- **Presentation:** Students will be divided into groups and assigned a research paper presentation.
- **Weekly Notes and Reflections:** Students are expected to take detailed notes. During each week, students will write a “reflection” on the week’s material, which will be graded by the instructor. These weekly reflections are due by Friday at 11:59 PM (assignment due-date subject to change with notice to students).
- **Homework:** Homework problems will include practice exam questions. Roughly four problem sets will be released throughout the semester. Grading for problem sets will be completion-based, although the instructor will provide solutions well ahead of the exam.
- **Participation:** The instructor will make use of various tools to facilitate and measure in-class engagement with the material. Students are expected to actively contribute by attending lecture and discussing relevant material.
- **Exams:** The semester will include three in-class written exams plus an optional cumulative final. The lowest of these four grades (three written exams and the optional final) is dropped, so three exams count toward the final grade at $13\frac{1}{3}\%$ each, for 40% total. A student satisfied with their three midterm grades may choose not to sit the final. Exam dates will be announced in class and posted on the course site at least two weeks in advance.

Grading

CIS 400 / CSE 400

Class Project	25%
Presentation	10%
Weekly Notes / Reflection	10%
Homework	10%
Participation	5%
Exams	40%

CIS 600 / CSE 691

Class Project [*]	25%
Presentation	10%
Weekly Notes / Reflection	10%
Homework ^{**}	10%
Participation	5%
Exams ^{***}	40%

^{*} Graduate student class projects will be expected to engage at a higher level of intellectual merit; specifically, they will apply concepts from state-of-the-art research publications or similar topics.

^{**} Graduate student homework will also include problems drawn from research papers.

^{***} Graduate students will be given a different exam with a higher bar for theoretical knowledge.

Grading Table**CIS 400 / CSE 400**

Grade	Points	Percentage
A	4.000	93.0–100.0
A-	3.667	90.0–92.9
B+	3.333	87.0–89.9
B	3.000	83.0–86.9
B-	2.667	80.0–82.9
C+	2.333	75.0–79.9
C	2.000	70.0–74.9
C-	1.667	60.0–69.9
D	1.000	50.0–59.9
F	0	< 50

CIS 600 / CSE 691

Grade	Points	Percentage
A	4.000	93.0–100.0
A-	3.667	90.0–92.9
B+	3.333	87.0–89.9
B	3.000	83.0–86.9
B-	2.667	80.0–82.9
C+	2.333	75.0–79.9
C	2.000	70.0–74.9
C-	1.667	60.0–69.9
F	0	< 60.0

Course Specific Policies

Course website and communication. Course materials, assignment write-ups, and announcements are posted on the course site. Email (kkmicins@syr.edu) is the official channel for individual questions; please allow up to two business days for a reply, and expect longer response times on weekends.

Late work. Weekly reflections are due Friday at 11:59 PM and are not accepted late, since they are tied to that week's material; the two lowest reflection grades are dropped to accommodate ordinary conflicts. Projects and problem sets may be submitted up to 48 hours late with a 10% penalty. Extensions beyond this require advance arrangement with the instructor, and accommodations arranged through the Center for Disability Resources or Student Outreach and Support are honored without penalty.

Authorized use of security tools and techniques. This course teaches offensive techniques (binary exploitation, automated exploit generation, adversarial machine learning, prompt injection) for defensive and scholarly purposes. All hands-on work must be performed only against the targets, virtual machines, and infrastructure provided for the course, or against systems you own and are explicitly authorized to test. Using these techniques against Syracuse University systems, other students' machines, or any third-party system without written authorization is prohibited, may violate the Syracuse University Information Technology Resources Acceptable Use Policy and state and federal law, and will be referred for disciplinary action.

Relationship to CSE 643. Buffer overflows and related memory-safety attacks are also covered in CSE 643 (Computer Security). The treatment in the two courses is complementary: CSE 643 approaches the topic through the SEED Labs hands-on exercises, while this course focuses on AI-assisted discovery and exploitation of such vulnerabilities. Students may take both courses.

Attendance and electronics. Attendance is expected (see the University Attendance Policy below) and participation is graded. Laptops and tablets are welcome for coursework; please keep them to course-related use during lecture and discussion.

Course Schedule

Key Fall 2026 dates (Syracuse University Academic Calendar)

- First class meeting: Tuesday, Aug. 25
- Labor Day (no classes): Monday, Sept. 7
- Academic/financial deadline to drop: Monday, Sept. 14
- Deadline to withdraw: Friday, Nov. 20
- Thanksgiving break (no classes): Sunday, Nov. 22 – Sunday, Nov. 29
- Last day of classes: Tuesday, Dec. 8
- Final examination period: Thursday, Dec. 10 – Tuesday, Dec. 15

The weekly schedule below is tentative and subject to change with notice to students. Because the semester runs Aug. 25 – Dec. 8 and includes Thanksgiving break, Weeks 14–15 are compressed.

Week	Topic	Required Readings and Assignments	LOs
Week 1	Foundations of Security: Confidentiality, Integrity, Availability. Information flow policies (Bell-LaPadula, noninterference). What it means to “prove” a system secure.	Anderson, <i>Security Engineering</i> , Ch. 1 (“What Is Security Engineering?”). D. E. Bell and L. J. LaPadula, “Secure Computer Systems: Mathematical Foundations,” MITRE Technical Report, 1973.	1
Week 2	Reverse Engineering I: Binary Analysis Basics. Binary formats (ELF/PE), disassembly vs. decompilation, control flow graphs. Introduction to AI-assisted decompilation.	Project 1 assigned: Vulnerability Identification. Hands on with Ghidra: buffer overflow attack. Shoshitaishvili et al., “SoK: (State of) The Art of War: Offensive Techniques in Binary Analysis,” IEEE S&P, 2016. (Sections I–IV)	1, 4
Week 3	Reverse Engineering II: Memory Attacks. Stack layout, calling conventions, buffer overflows, return-oriented programming (ROP).	Aleph One, “Smashing the Stack for Fun and Profit,” <i>Phrack</i> 49, 1996. H. Shacham, “The Geometry of Innocent Flesh on the Bone: Return-into-libc without Function Calls (on the x86),” ACM CCS, 2007.	1, 2, 4

Week	Topic	Required Readings and Assignments	LOs
Week 4	Exploit Primitives and Mitigations: ASLR, DEP/NX, stack canaries, CFI.	V. Pappas, M. Polychronakis, and A. D. Keromytis, “Transparent ROP Exploit Mitigation Using Indirect Branch Tracing,” <i>USENIX Security</i> , 2013. Anderson, <i>Security Engineering</i> , Ch. 4 (“Access Control”). Homework 1 assigned.	2, 3
Week 5	Foundations of Automated Exploit Generation. Symbolic execution, path constraints, constraint solving.	Cadar, Dunbar, and Engler, “KLEE: Unassisted and Automatic Generation of High-Coverage Tests for Complex Systems Programs,” <i>OSDI</i> , 2008. Avgerinos et al., “AEG: Automatic Exploit Generation,” <i>NDSS</i> , 2011. Project 2 assigned (LLM vs. symbolic exploit generation).	2, 3
Week 6	AI Agents for Vulnerability Discovery.	Sheng et al., “LLMs in Software Security: A Survey of Vulnerability Detection Techniques and Insights,” <i>ACM Computing Surveys</i> , 2025.	2, 3
Week 7	AI Agents for Code Understanding.	Xu et al., “When LLMs Meet Cybersecurity: A Systematic Literature Review,” <i>Cybersecurity</i> (Springer), 2025. Yang et al., “SWE-agent: Agent-Computer Interfaces Enable Automated Software Engineering,” <i>arXiv 2405.15793</i> , 2024. Homework 2 assigned.	2, 5
Week 8	From Discovery to Exploitation with AI. AI-assisted exploit generation pipelines; combining symbolic execution with LLM-guided heuristics. The gap between bug and working exploit.	Cha et al., “Unleashing Mayhem on Binary Code,” <i>IEEE S&P</i> , 2012. Fang et al., “LLM Agents Can Autonomously Exploit One-Day Vulnerabilities,” <i>arXiv 2404.08144</i> , 2024. Project 3 assigned (AI-assisted vulnerability analysis pipelines).	2, 3, 4
Week 9	AI and Network Security I: Traffic Analysis and Intrusion Detection. Feature engineering from packet captures. ML-based NIDS: classifiers on flow data, anomaly detection. Deep learning versus signature-based methods.	Mirsky et al., “Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection,” <i>NDSS</i> , 2018. Anderson, <i>Security Engineering</i> , Ch. 21 (“Network Attack and Defense”).	1, 4
Week 10	AI and Network Security II. Gradient-based evasion (FGSM, PGD) applied to flow features. Mutation-based evasion of malware classifiers. Defenses: adversarial training, ensemble methods, feature squeezing.	Goodfellow, Shlens, and Szegedy, “Explaining and Harnessing Adversarial Examples,” <i>ICLR</i> , 2015. Carlini and Wagner, “Towards Evaluating the Robustness of Neural Networks,” <i>IEEE S&P</i> , 2017. Project 4 assigned (ML-based intrusion detection, adversarial attacks). Homework 3 assigned.	3, 4

Week	Topic	Required Readings and Assignments	LOs
Week 11	AI-Powered Social Engineering. LLM-generated phishing, voice cloning, and deepfakes. Measuring effectiveness, human detection rates.	Schmitt and Flechais, “Digital Deception: Generative Artificial Intelligence in Social Engineering and Phishing,” <i>Artificial Intelligence Review</i> (Springer), 2024.	1, 3, 5
Week 12	Prompt Injection, Jailbreaking, and LLM Security. Direct vs. indirect prompt injection. Jailbreak taxonomies. Why current defenses fail.	Greshake et al., “Not What You’ve Signed Up For: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection,” AISEC (CCS Workshop), 2023. Zou et al., “Universal and Transferable Adversarial Attacks on Aligned Language Models,” arXiv 2307.15043, 2023. Final Project assigned.	3, 5
Week 13	Security of AI-Integrated Systems. Threat modeling for applications built on LLMs and agents: trust boundaries, tool-use risks, data exfiltration via prompt injection.	OWASP, “Top 10 for LLM Applications,” 2025 Edition. Homework 4 assigned.	3, 5, 6
Weeks 14–15	Advanced Topics (LLM-guided fuzzing, autonomous penetration testing agents, deep learning-assisted side-channel analysis, etc.). Final Project Presentations.	Nasr, Carlini, Sitawarin, Schulhoff, et al., “The Attacker Moves Second: Stronger Adaptive Attacks Bypass Defenses Against LLM Jailbreaks and Prompt Injections,” arXiv 2510.09023, October 2025.	1–6

SU Policies and Services

University Attendance Policy

Attendance in classes is expected in all courses at Syracuse University. It is a federal requirement that faculty promptly notify the university of students who do not attend or cease to attend any class. Faculty will use Early-Semester Progress Reports and Mid-Semester Progress Reports in Orange Success 2.0 to alert the Registrar and Financial Aid Office on non-attendance. For more information visit *Information for Faculty: Non-attendance or Stopped Attending* and *Information for Students: Non-attendance or Stopped Attending*.

If a student is unable to participate in-person or virtually for an extended period of time (48 hours or more), the student may request an absence notification from their home school/college Dean's Office or through the Student Outreach and Support office. Instructors will be notified via the "Absence Notification" flag in Orange Success 2.0.

Barnes Center at the Arch (Health, Counseling, etc.) staff will not provide medical excuse notes for students. When Barnes Center staff determine it is medically necessary to remove a student from classes, they will coordinate with Student Outreach and Support case management staff to provide appropriate notification to faculty through Orange Success. For absences lasting less than 48 hours, students are encouraged to discuss academic arrangements directly with their faculty.

Additional information may be found at Student Outreach and Support: Absence Notifications.

Religious Observances Notification and Policy

Syracuse University's Religious Observances Policy recognizes the diversity of faiths represented in the campus community and protects the rights of students, faculty, and staff to observe religious holy days according to their traditions. Under the policy, students are given an opportunity to make up any examination, study, or work requirements that may be missed due to a religious observance, provided they notify their instructors no later than the academic drop deadline. For observances occurring before the drop deadline, notification is required at least two academic days in advance. Students may enter their observances in MySlice under Student Services / Enrollment / My Religious Observances / Add a Notification.

Orange Success 2.0

Orange Success 2.0 is the platform used to help students succeed by providing timely feedback on academic progress. Timely feedback from faculty members can also enhance advisor efforts. Several opportunities will be provided to offer feedback to students:

Early-semester progress reports (ESPRs). Syracuse University tracks student "Non-Attendance" through Orange Success 2.0 to comply with Title IV regulations. Faculty are expected to indicate students who "Never Attended" a class by the third week of the fall semester. Both the Registrar's Office and the Financial Aid office are notified of the alerts. This allows students to make behavior changes before they fall too far behind. Note that the system provides immediate email notifications to students.

Mid-semester progress reports (MSPRs). Provides an opportunity for early warnings about students' academic progress and success. When you complete your MSPR report, it helps advisors and other student support staff to understand which students may be struggling. MSPRs deployed through Orange Success 2.0 will follow the academic calendar dates. Faculty are expected to provide feedback for all students in their classes. Orange Success 2.0 also supports the entry of midterm grades; midterm grades do not appear on a student's transcript, but are used in this course to

communicate standing before the withdrawal deadline. Note that the system provides immediate email notifications to students.

At any time during the semester, faculty may provide real-time feedback to students by raising early alerts in Orange Success 2.0. As mentioned above, this system provides immediate email notifications to students of alerts. Advisors can review attendance and progress indicators during advising meetings.

Student Mental Health

Mental health and overall well-being are significant predictors of academic success. As such it is essential that during your college experience you develop the skills and resources effectively to navigate stress, anxiety, depression, and other mental health concerns. Please familiarize yourself with the range of resources the Barnes Center provides (<https://ese.syr.edu/bewell/>) and seek out support for mental health concerns as needed. Counseling services are available 24/7, 365 days, at 315-443-8000, and I encourage you to explore the resources available through the Wellness Leadership Institute, <https://ese.syr.edu/bewell/wellness-leadership-institute/>.

Disability-Related Accommodations

Syracuse University values access and inclusion; we are committed to a climate of mutual respect and full participation. There may be aspects of the instruction or design of this course that result in barriers to your inclusion and full participation in this course. I invite any student to contact me to discuss strategies and/or accommodations (academic adjustments) that may be necessary to ensure equitable access, and to collaborate with the Center for Disability Resources (CDR) in this process.

If you would like to discuss disability-related accommodations or register with CDR, please visit the Center for Disability Resources. Please call (315) 443-4498 or email CDRspecialist@syr.edu for more detailed information.

CDR is responsible for coordinating disability-related academic accommodations and will work with the student to develop an access plan. Since academic accommodations are generally not provided retroactively, please contact CDR as soon as possible to initiate this process.

Furniture may be placed in your classrooms for specific use by students with disabilities. This furniture is generally labelled with signs that request that it is not to be moved per the Center for Disability Resources. Students with disabilities rely on this furniture to remain where it is placed within the classrooms.

Note that some students may be accompanied to classes by a service animal. Students are not required to provide prior notice of this to the University. If it is not readily apparent that the student is disabled, students can be asked two questions: do you have this animal due to a disability, and what tasks does it perform for you? Emotional Support Animals are different than service animals and are typically only approved to reside in a student's housing location/room.

Academic Integrity Policy

As a pre-eminent and inclusive student-focused research institution, Syracuse University considers academic integrity at the forefront of learning, serving as a core value and guiding pillar of education. Syracuse University's Academic Integrity Policy provides students with the necessary guidelines to complete academic work with integrity throughout their studies. Students are required to uphold both course-specific and university-wide academic integrity expectations such as crediting your sources, doing your own work, communicating honestly, and supporting academic integrity. The

full Syracuse University Academic Integrity Policy can be viewed by visiting the Syracuse University Policies website.

Upholding Academic Integrity includes the protection of faculty's intellectual property. Students should not upload, distribute, or share instructors' course materials, including presentations, assignments, exams, or other evaluative materials without permission. Using websites that charge fees or require uploading of course material (e.g., Chegg, Course Hero) to obtain exam solutions or assignments completed by others, which are then presented as your own, violates academic integrity expectations in this course and may be classified as a Level 3 violation. All academic integrity expectations that apply to in-person assignments, quizzes, and exams also apply online.

Students found in violation of the policy are subject to grade sanctions determined by the course instructor and non-grade sanctions determined by the School or College where the course is offered. Students may not drop or withdraw from courses in which they face a suspected violation. Any established violation in this course may result in course failure regardless of violation level.

Student Academic Work Policy

Any work or exams missed due to an excused absence (including University-approved absences, religious observances, and absences documented through Student Outreach and Support) must be made up as soon as possible so that the student does not fall behind in the course. Please email me in advance (if possible) and set up a time to speak with me upon return so that we can discuss timing of turning in missed homework or making up exams. The SU policy on student academic work may be found at <http://coursecatalog.syr.edu/content.php?catoid=3&navoid=270>.

Discrimination

Federal and state law, and University policy prohibit discrimination and harassment based on sex or gender (including sexual harassment, sexual assault, domestic/dating violence, stalking, sexual exploitation, and retaliation). If a student has been harassed or assaulted, they can obtain confidential counseling support, 24 hours a day, 7 days a week, from the Sexual and Relationship Violence Response Team at the Counseling Center (315-443-8000, Barnes Center at The Arch, 150 Sims Drive, Syracuse, New York 13244). Incidents of sexual violence or harassment can be reported non-confidentially to the University's Title IX Officer (Sheila Johnson Willis, 315-443-0211, titleix@syr.edu, 005 Steele Hall). Reports to law enforcement can be made to the University's Department of Public Safety (315-443-2224, 005 Sims Hall), the Syracuse Police Department (511 South State Street, Syracuse, New York; 911 in case of emergency or 315-435-3016 to speak with the Abused Persons Unit), or the State Police (844-845-7269). I will seek to keep information you share with me private to the greatest extent possible, but as a professor I have mandatory reporting responsibilities to share information regarding sexual misconduct, harassment, and crimes I learn about with the University's Title IX Officer to help make our campus a safer place for all.

Email Policy

The instructor will make every effort to respond to emails within 24 business hours. If you do not receive a reply within 24 business hours, the instructor urges you to email again.

Syracuse University has established email as a primary vehicle for official communication with students, faculty, and staff. Emergency notifications, educational dialog, research, and general business correspondence are all consistently enhanced in institutions of higher learning where email policies exist and are supported by procedures, practice, and culture.

An official email address is established and assigned by Information Technology Services (ITS)

for each registered student, as well as for all active faculty and staff members. All University communications sent via email will be sent to this address. Faculty and staff members must use the officially established University email address to communicate with students registered in their classes. Keep in mind that student records sent to a non-syr.edu email address may create a FERPA violation (see the complete policy at the Syracuse University Email Policy).

Use of Artificial Intelligence

Based on the specific learning outcomes and assignments in this course, artificial intelligence is permitted on the following: course project, and homework (with attribution). See each assignment, quiz, or exam instructions for more information about what artificial intelligence tools are permitted and to what extent, as well as citation requirements. If no instructions are provided for a specific assignment, then no use of any artificial intelligence tool is permitted. Any AI use beyond that which is detailed in course assignments is explicitly prohibited except when documented permission is granted.

Statement on Instructor's Usage of Artificial Intelligence

The instructor has used AI to generate portions of the course material. Specifically, the instructor has used AI coding agents to help develop the website, along with interactive teaching-focused applications. The instructor has also used generative AI to help edit portions of class slides and notes. In all cases, the instructor takes full responsibility for the correctness and relevance of all material used in this class.