CSCI 497.61E AI Robotics Cybersecurity

COURSE SYLLABUS: Fall 2026

INSTRUCTOR INFORMATION

Instructor:	Amy Hays M.S., Computer Science
Office Location:	RELLIS ACB2 210
https://tamuc.zoom.us/j/92711096337?pwd=cS9UZlIXb2xIc2V1dGtoNnArcDZ5UT09	
Office Hours:	Tuesdays and Thursdays, 12 to 2 PM Other times by appointment only via email
University Email Address:	amy.hays@etamu.edu
Preferred Form of Communication:	For all emails, make sure the email the subject line reads: “CSCI 497.61E~~”.
Communication Response Time:	48 hours

COURSE INFORMATION

Lecture: Meets 8/24/2026 through 12/3/2026, Finals week (12/7 – 12/9)
Mondays and Wednesdays, 2:50 p.m. - 4:05 p.m.
Campus: RELLIS Campus Building: ACB2 Room: 218

Class Textbook:

The professor will make supplementary information for the course available online.

Course Description

AI Robotic Cybersecurity is a senior-level, hands-on course on securing AI-enabled robotic and cyber-physical systems. Students learn to map robotic architecture and attack surfaces, develop threat models, perform ethical and safety-aware security assessments, and harden systems across network, firmware, and AI perception/control layers. The NAO6 robot is used as a case-study platform alongside other devices and simulations (e.g., ROS-based stacks) to generalize methods and insights. Emphasis is placed on safety engineering, legal/ethical practice, and alignment with recognized guidance (e.g., NIST, ISO/IEC 62443, OWASP IoT, MITRE ATT&CK for ICS/robotics). Teams culminate the course by delivering a tested, hardened prototype and a professional security report and briefing.

The *syllabus/schedule are subject to change.*

Student Learning Outcomes

Upon completion of this course, students will be able to:

1. Characterize the architecture and attack surface of AI-enabled robotic systems, including compute, network, sensors/actuators, and ML components.
2. Develop and justify a threat model and test plan that aligns with safety, legal/ethical constraints, and recognized standards.
3. Conduct structured, ethical security assessments of robotic systems and document reproducible, evidence-based findings.
4. Design and implement risk-driven mitigations and secure configurations that integrate defense-in-depth and safety mechanisms.
5. Evaluate the robustness of AI perception/control to adversarial conditions and propose practical hardening strategies.
6. Instrument robots for logging/telemetry and outline incident response and recovery to a known-good state.
7. Communicate technical risk and remediation plans effectively through clear reports, metrics, and demonstrations.
8. Collaborate with cross-disciplinary teams to deliver a hardened robotic prototype and reflect on broader societal and compliance implications.

COURSE REQUIREMENTS

Minimal Technical Skills Needed

Prerequisites:

Instructional Methods

During this course, we will using traditional and active learning methods, and work together using:
• In-class lectures: using slides, supplementary materials, and hands-on exercises. The syllabus/schedule are subject to change.
• Assignments and labs that will be released via the D2L Learning Management Systems (LMS).
• Individual / group projects.

Student Responsibilities or Tips for Success in the Course

It is the students' responsibility to keep up with the schedule. Makeup work (exams, quizzes, discussions, or assignments) will only be permitted in cases of emergency with

proper documentation, or prior rescheduling. To reschedule contact me before the due date with a valid reason and suggested make-up dates will be given.

Please feel free to contact me and come to office hours to ask questions and get clarifications or assistance.

GRADING

Final grades in this course will be based on the following scale:

A = 90%-100%
B = 80%-89%
C = 70%-79%
D = 60%-69%
F = 59% or Below

Assessments

Basis for Evaluation:

Assignments & labs	20%
Attendance & Participation	10%
Quizzes	20%
Midterms	25%
Final Exam	25%

TECHNOLOGY REQUIREMENTS

LMS

All course sections offered by East Texas A&M University have a corresponding course shell in the myLeo Online Learning Management System (LMS). Below are technical requirements

LMS Requirements:
https://community.brightspace.com/s/article/Brightspace-Platform-Requirements

LMS Browser Support:
https://documentation.brightspace.com/EN/brightspace/requirements/all/browser_support.htm

Zoom Video Conferencing Tool
https://inside.tamuc.edu/campuslife/CampusServices/CITESupportCenter/Zoom_Account.aspx?source=universalmenu

The *syllabus/schedule are subject to change.*

ACCESS AND NAVIGATION

You will need your campus-wide ID (CWID) and password to log into the course. If you do not know your CWID or have forgotten your password, contact the Center for IT Excellence (CITE) at 903.468.6000 or helpdesk@tamuc.edu**.**

Note: Personal computer and internet connection problems do not excuse the requirement to complete all course work in a timely and satisfactory manner. Each student needs to have a backup method to deal with these inevitable problems. These methods might include the availability of a backup PC at home or work, the temporary use of a computer at a friend's home, the local library, office service companies, Starbucks, a ETAMU campus open computer lab, etc.

COMMUNICATION AND SUPPORT

If you have any questions or are having difficulties with the course material, please contact your Instructor.

Technical Support

If you are having technical difficulty with any part of Brightspace, please contact Brightspace Technical Support at 1-877-325-7778. Other support options can be found here:

https://community.brightspace.com/support/s/contactsupport

COURSE AND UNIVERSITY PROCEDURES/POLICIES

Course Specific Procedures/Policies

Late Policies

Credit will be given for ONLY those exams, quizzes, and assignments turned in no later than the deadline as announced by the instructor of this class unless prior arrangement has been made with the instructor.

Late assignments can gain partial credit upon the following policy. As per University requirements, assignments submitted within 7 days after the deadline can receive up to 20% deduction, assignments submitted between 8-14 days after the deadline can receive up to 50% deduction.

- **No assignments will be accepted two weeks after the assigned due date.**
- **No assignment will be accepted after the term end day.**
- Exceptions to this policy will only be made in extraordinary circumstances. Please let me know your circumstances.

Syllabus Change Policy

The *syllabus/schedule are subject to change.*

The syllabus is a guide. Circumstances and events, such as student progress, may make it necessary for the instructor to modify the syllabus during the semester. Any changes made to the syllabus will be announced in advance.

University Specific Procedures

Student Conduct

All students enrolled at the University shall follow the tenets of common decency and acceptable behavior conducive to a positive learning environment. The Code of Student Conduct is described in detail in the Student Guidebook.
http://www.tamuc.edu/Admissions/oneStopShop/undergraduateAdmissions/studentGuidebook.aspx

Students should also consult the Rules of Netiquette for more information regarding how to interact with students in an online forum:
https://www.britannica.com/topic/netiquette

ETAMU Attendance

For more information about the attendance policy please visit the Attendance webpage and Procedure 13.99.99.R0.01.
http://www.tamuc.edu/admissions/registrar/generalInformation/attendance.aspx

http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/13students/academic/13.99.99.R0.01.pdf

Academic Integrity

Students at East Texas A&M University are expected to maintain high standards of integrity and honesty in all of their scholastic work. For more details and the definition of academic dishonesty see the following procedures:

Undergraduate Academic Dishonesty 13.99.99.R0.03
Undergraduate Student Academic Dishonesty Form

http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/documents/13.99.99.R0.03UndergraduateStudentAcademicDishonestyForm.pdf

Graduate Student Academic Dishonesty Form

http://www.tamuc.edu/academics/graduateschool/faculty/GraduateStudentAcademicDishonestyFormold.pdf

http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/13students/undergraduates/13.99.99.R0.03UndergraduateAcademicDishonesty.pdf

The *syllabus/schedule are subject to change.*

Students with Disabilities-- ADA Statement

The Americans with Disabilities Act (ADA) is a federal anti-discrimination statute that provides comprehensive civil rights protection for persons with disabilities. Among other things, this legislation requires that all students with disabilities be guaranteed a learning environment that provides for reasonable accommodation of their disabilities. If you have a disability requiring an accommodation, please contact:

Office of Student Disability Resources and Services
East Texas A&M University
Velma K. Waters Library Rm 162
Phone (903) 886-5150 or (903) 886-5835
Fax (903) 468-8148
Email: studentdisabilityservices@tamuc.edu
Website: Office of Student Disability Resources and Services
http://www.tamuc.edu/campusLife/campusServices/studentDisabilityResourcesAndServices/

Nondiscrimination Notice

East Texas A&M University will comply in the classroom, and in online courses, with all federal and state laws prohibiting discrimination and related retaliation on the basis of race, color, religion, sex, national origin, disability, age, genetic information or veteran status. Further, an environment free from discrimination on the basis of sexual orientation, gender identity, or gender expression will be maintained.

Campus Concealed Carry Statement

Texas Senate Bill - 11 (Government Code 411.2031, et al.) authorizes the carrying of a concealed handgun in East Texas A&M University buildings only by persons who have been issued and are in possession of a Texas License to Carry a Handgun. Qualified law enforcement officers or those who are otherwise authorized to carry a concealed handgun in the State of Texas are also permitted to do so. Pursuant to Penal Code (PC) 46.035 and East Texas A&M Rule 34.06.02.R1, license holders may not carry a concealed handgun in restricted locations.

For a list of locations, please refer to the Carrying Concealed Handguns On Campus document and/or consult your event organizer.

Web url:
http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/34SafetyOfEmployeesAndStudents/34.06.02.R1.pdf

Pursuant to PC 46.035, the open carrying of handguns is prohibited on all East Texas A&M campuses. Report violations to the University Police Department at 903-886-5868 or 9-1-1.

The *syllabus/schedule are subject to change.*

East Texas A&M Supports Students' Mental Health

The Counseling Center at East Texas A&M, located in the Halladay Building, Room 203, offers counseling services, educational programming, and connection to community resources for students. Students have 24/7 access to the Counseling Center's crisis assessment services by calling 903-886-5145. For more information regarding Counseling Center events and confidential services, please visit www.tamuc.edu/counsel

AI use policy [Draft 2, May 25, 2023]

East Texas A&M University acknowledges that there are legitimate uses of Artificial Intelligence, ChatBots, or other software that has the capacity to generate text, or suggest replacements for text beyond individual words, as determined by the instructor of the course.

Any use of such software must be documented. Any undocumented use of such software constitutes an instance of academic dishonesty (plagiarism).

Individual instructors may disallow entirely the use of such software for individual assignments or for the entire course. Students should be aware of such requirements and follow their instructors 'guidelines. If no instructions are provided the student should assume that the use of such software is disallowed.

In any case, students are fully responsible for the content of any assignment they submit, regardless of whether they used an AI, in any way. This specifically includes cases in which the AI plagiarized another text or misrepresented sources.

The *syllabus/schedule are subject to change.*

COURSE OUTLINE / CALENDAR

WEEK	CONTENT	Events
Unit 1: Foundations of Robotic Systems & Security		
8/24	Course Introduction & Robotic Architecture	
8/31	ROS & Attack Surface	
9/7	Threat Modeling I	**9/7 – Labor Day**
9/14	Threat Modeling II & Test Plan	**Quiz 1**
Unit 2: Assessing and Exploiting Robotic Systems		
9/21	Network, Wireless Security, & Exploitation	
9/28	Firmware & System-Level Security	
10/5	Application-Layer Security & Documenting Findings	
10/12	Project Workshop and Milestone Review	**Midterm**
Unit 3: Security the Stack & The AI Layer		
10/19	Hardening Network & Systems	
10/26	Adversarial ML: Attacks on Perception	
11/2	Emerging Threat: Agentic AI Attackers	**Quiz 2**
11/9	Defensive AI Agents, Logging, Telemetry & Recovery	
Unit 4: Project Integration, Reporting, and Final Delivery		
11/16	Final Project Work Sessions	
11/23	Communication Workshop	**Nov 25th – 27th- Reading Day & Thanksgiving**
11/30	Final Project Presentations and Demos	
12/7	Final Exam **Due 12/7 at 11:59 pm**	

Note: The right to modify the presentation order of materials is reserved. Course progress will be based on feedback and suggestions from students. We would cover the course materials, so if we slow in some topics, we must accelerate elsewhere.

HAVE A HAPPY AND SUCCESSFUL SESSION

The *syllabus/schedule are subject to change.*