CS 1290 (Special Topics) - Fundamentals of Cybersecurity
Spring 2026

CRN: 23598 **Time:** TR 10:30 AM to 11:50 AM. **Location:** EDUC 311 **Textbook:** Check Blackboard	**Instructor:** Monika Akbar (makbar@utep.edu) **Office:** CCSB 3.0422 **Office Hours** Monday (in-person): 9 to 10 AM Thursday (virtual-MS Teams): 4:10 PM to 5:10 PM

Course Objectives:

This course introduces students to the foundational principles of cybersecurity, focusing on the critical knowledge needed to understand the evolving landscape of cyber threats and defenses. The two-credit course is divided into four main components:

1. **Knowledge Foundation**: Students will explore key cybersecurity concepts such as adversarial thinking, attack methods, vulnerabilities, and cybersecurity frameworks. They will also learn about authentication, access control, and best practices. Current events and emerging issues in cybersecurity will be discussed to link theory to real-world applications.
2. **Case Studies**: Students will analyze real cybersecurity incidents to understand how theoretical concepts apply in practice, providing insights into the strategies used by attackers and defenders.
3. **Cybersecurity Research**: Faculty members and industry partners engaged in cutting-edge cybersecurity research will share their work, giving students exposure to current challenges and innovations in the field.
4. **Report Writing and Presentation**: This component focuses on developing students' communication skills. Students may assess the cybersecurity posture of an organization or study a cyber-incident. They are expected to write reports and present their findings in class.

Prerequisite: CS 2302

Course materials: All the course materials will be available through **Blackboard (Bb)**. Please check Bb regularly to stay updated with the class.

Grading and Assessment Methods:

- **Midterms (30%)**: There will be two midterm exams, each assessing the understanding of key cybersecurity concepts. Together, these exams will account for 30% of the final grade.
- **Assignments and quizzes (20%)**: Regular quizzes and homework assignments will make up 20% of the final grade, assessing student's ongoing comprehension of the course material and helping reinforce key concepts.
- **Case Studies and Research Engagement (30%)**: This involves analysis of real-world cybersecurity incidents and engagement with research through reports, discussions, or presentations.

- **Attendance and Class Participation (20%)**: Active participation and attendance in class discussions, particularly during case studies and current events, will make up 20% of the grade. Engaging with peers and instructors is key to success in this course.
- **No Final Exam**: There will be no final exam for this course.

Learning Objectives:

Students will be able to:

1. **Assess Cybersecurity Risks and Recommend Mitigation Strategies:** Through case studies and hands-on activities, students will learn to assess, prioritize, and identify mitigation strategies for cybersecurity risks in organizations by exploring key topics such as access controls, vulnerability assessments, and incident response.
2. **Develop Communication Skills:** Students will enhance their ability to effectively communicate cybersecurity risks and solutions to both technical and non-technical audiences, including business leaders and organizational stakeholders, through written reports and oral presentations.
3. **Engage with Cybersecurity Research and Practical Applications:** By interacting with faculty researchers and exploring real-world cybersecurity incidents, students will bridge the gap between theoretical knowledge and practical application, preparing them for hands-on cybersecurity assessments in real-world environments.

ATTENDANCE AND PARTICIPATION

Attendance in the course is mandatory and determined by participation in the learning activities of the course. Your participation in the course is important not only for your learning and success but also to create a community of learners.

ILLNESS PRECAUTIONS

Please stay home if you have symptoms of a communicable illness. If you are feeling unwell, please let me know as soon as possible, so that we can work on appropriate accommodations.

COURSE DROP POLICY

The instructor will not drop you from the course. However, if you feel that you are unable to complete the course successfully, please inform the instructor and contact the Registration and Records Office to initiate the drop process. If you do not, you are at risk of receiving an "F" for the course.

MAKE-UP WORK

Make-up work will be given *only* in the case of a *documented* emergency. Note that make-up work may be in a different format than the original work, may require more intensive preparation, and may be graded with penalty points.

ACCOMMODATIONS POLICY

The University is committed to providing reasonable accommodations to students with documented disabilities. Students who become pregnant may also request reasonable accommodations, in accordance with state and federal laws and regulations and University policy. Accommodations that constitute undue

hardship are not reasonable. To make a request, please register with the UTEP Center for Accommodations and Support Services (CASS). Contact CASS at 915-747-5148, email them at cass@utep.edu, or apply for accommodations online via the CASS portal.

SCHOLASTIC INTEGRITY

Academic dishonesty is prohibited and is considered a violation of the UTEP Handbook of Operating Procedures. It includes, but is not limited to, cheating, plagiarism, and collusion. Cheating may involve copying from or providing information to another student, possessing unauthorized materials during a test, or falsifying research data on laboratory reports. Plagiarism occurs when someone intentionally or knowingly represents the words or ideas of another as ones' own. Collusion involves collaborating with another person to commit any academically dishonest act. Any act of academic dishonesty attempted by a UTEP student is unacceptable and will not be tolerated. All suspected violations of academic integrity at The University of Texas at El Paso must be reported to the Office of Community Standards for possible disciplinary action. To learn more, please visit HOOP: Student Conduct and Discipline.

GUIDANCE ON ARTIFICIAL INTELLIGENCE

Some AI technologies or automated tools may be beneficial during the early brainstorming stages of an activity, and you are welcome to explore them for that purpose. However, keep in mind that AI-generated ideas are not your own and WILL hinder your ability to think critically and creatively about a problem. It is also important to remember that these technologies often "hallucinate" or produce materials and information that are inaccurate or incomplete—even providing false citations for use.

That said, you are not allowed to submit any AI-generated work in this course as your own. If you use any information or materials created by AI technology, you are required to cite it like you would any other source. Consider how this will affect your credibility as a writer and scholar before doing so. Any direct use of AI-generated materials submitted as your own work will be treated as plagiarism and reported to the Office of Community Standards.