The University of Texas at El Paso
Department of Computer Science
Syllabus

COURSE INFORMATION

CS 5352/6352: Computer Security
CRN: 21027/ 26958
Term: Spring 2025
Delivery Method: In-person
Meeting Day and Time: Tuesdays and Thursdays, 4:30 pm – 5:50 pm
Location: BUSN 332

INSTRUCTOR INFORMATION

Dr. Sajedul Talukder
Written Communication: Email
Office: CCSB 3.0502
Phone: (915) 747- 8819
Email: stalukder@utep.edu
Website: https://www.cs.utep.edu/stalukder/
Office Hours: F-to-F/Online: TR 5:50-6:50 or by appointment

Teaching Assistant
N/A
TA Office Hours
N/A

COURSE DESCRIPTION

The primary goal of this course is to provide fundamental concepts and applied methods of computer security that addresses various confidentiality, integrity, and availability related challenges associated to data, system, and network assets. Tentative topics include Crosscutting Concepts in Cybersecurity, Risks and Vulnerabilities, Adversarial Attacks, Network Protocols and Internet Security, System and Software Vulnerabilities, System Access and Authentication, Web Security, Human Security, Protection Against External and Internal Threats, Controls and Protection Methods, Applied Cryptography, Issues of Law and Privacy, and Ethical Issues.

Course Prerequisites

Good knowledge of Linux is required.

Course Objectives

On successful completion of the course, students should be able to:

- Analyze security vulnerabilities of a network and develop a set of solutions for specific networking scenarios.
- Explain the various controls available for protection against Internet attacks, including authentication, integrity check, firewalls, and intruder detection systems.
- Exhibit an understanding of the threats posed by various types of malicious codes.
- Describe different ways of providing authentication of a user or program.
- Describe the mechanisms used to provide security in programs, operating systems, databases and networks.
- Find and utilize available online resources as they pertain to developing a secure system.
- Describe the background and properties of widely used encryption algorithms.
- Develop comprehensive plans for network security using a range of available tools.
- Describe legal, privacy and ethical issues in computer security.
- List and explain the typical set of tasks required of an information security professional.

Course Materials

OPTIONAL: 1. Applied Information Security: A Hands-on Approach, by David Basin, Patrick Schaller and Michael Schläpfer. ISBN: 978-3642244735.
2. Computer & Internet Security: A Hands-on Approach, 2nd Edition, by Wenliang Du. ISBN: 978-1733003926.
3. Certified Ethical Hacker (CEH) Cert Guide Network Defense, Michael Gregg. Pearson IT Certification. ISBN: 978-0789751270.
4. Penetration Testing Fundamentals: A Hands-On Guide to Reliable Security Audits, William Easttom. ISBN: 978-0789759375

Edge Advantages

This course is designed to equip students with essential Edge Advantages that contribute to their professional and personal development. Through the completion of course requirements and assignments, such as team projects, presentations, and essays, students will develop the following Edge Advantages:

	Problem-Solving	Assignments will challenge students to identify and address complex issues using innovative and analytical approaches.

	Communication	Class discussions and written assignments will improve students' skills in articulating ideas clearly and persuasively in both oral and written forms.
	Social Responsibility	Through community engagement opportunities and course content that encourages ethical considerations, students will foster a sense of responsibility towards their community and society at large.
	Confidence	By actively participating and successfully completing assignments, students will build self-assurance in their abilities to tackle academic and real-world challenges.
	Critical Thinking	The course's emphasis on analysis and synthesis of information will strengthen students' abilities to think critically and make informed decisions.

COURSE STRUCTURE

Course Policies/ Procedures/Grading

Following is a tentative **rough guide** to how course grades will be established, not a precise formula - we will fine-tune cutoffs and other details as we see fit after the end of the course.

Grades will be based on:

Homework, quizzes/labs/project: 35%
Midterm exam: 30%
Final exam: 30%
Attendance/Class Performance: 5%

Grading Scale:

90 – 100	A
80 – 89	B
70 – 79	C
60 – 69	D
Below 60	F

Course Assignments

Assessment of students' knowledge of computer security will be demonstrated via:

- A combination of homework assignments, quizzes/labs/project and exams.
- Quizzes will be held on random dates.

For assignment submission please include a typed cover sheet with your name, UTEP email address, homework number and undergraduate/graduate level.

Lecture Outline/Schedule (Tentative)

I. Crosscutting Concepts in Cybersecurity
   A. Confidentiality, integrity, availability
   B. Adversarial thinking
   C. Systems thinking
   D. Risk, vulnerability, threat, control
   E. System access and authentication
   F. Authentication methods
   G. Attacks and mitigation measures

II. Network Security
   A. Network fundamentals
      1. Introduction to data communications
      2. Network fundamentals and 7-layer OSI model
      3. Network architectures, network topology
   B. Network protocols and addressing
      1. Network protocols, internet protocol (IP), IP packets
      2. TCP vs. UDP, ICMP, IPv4 vs. IPv6, Ethernet
      3. Network address translation (NAT), ARP, DNS
   C. IP addressing and subnetting
   D. Network hardware and security infrastructure
      1. Hubs, bridges, switches, routers, firewalls
      2. Network interface cards
      3. Virtualization
   E. Connection and transmission attacks
      1. Denial-of-service (DoS) attacks
      2. Buffer overflows
      3. Null sessions, sniffing, spoofing, session hijacking
      4. Man-in-the-middle attacks (MITM)
      5. Replay attacks, redirection attacks
      6. Scanning attacks
      7. Password cracking, client-side attacks
      8. ARP poisoning, cache poisoning

III. Web Security
   A. Browser attacks
      1. Man-in-the-browser
      2. Keystroke logger
      3. Page-in-the-middle
      4. Program download substitution
      5. User-in-the-middle
   B. Web attacks targeting users
      1. False or misleading content
      2. Defaced web site
      3. Fake web site, Fake code
      4. Malicious web content
      5. Substitute content, Drive-by download

C. Obtaining user or website data
    1. Web bug
    2. Clickjacking
    3. Cross-site scripting
    4. SQL injection
    5. Dot-dot-slash
    6. Server-side include

IV. Software Security
    A. Fundamental design principles for secure software
    B. Malicious Code
        1. Viruses, Worms, Trojan horses
        2. Polymorphic malware
        3. Rootkits, Logic bombs
        4. Spyware, Adware, Botnets
        5. Backdoors and trapdoors
        6. Ransomware
    C. Malware defenses

V. System Security
    A. Authentication and access control
    B. User, group, and role management
    C. Identification, authentication, authorization
    D. Password policies
    E. Access control lists
    F. Mandatory Access Control (MAC)
    G. Discretionary Access Control (DAC)
    H. Role-Based Access Control (RBAC)
    I. Rule-Based Access Control
    J. Attribute Based Access Control (ABAC)
    K. Federated Authentication (OAuth)
    L. Vulnerabilities of system components

VI. Human Security
    A. Social engineering
        1. Fake email/spoofing, Spam
        2. Link manipulation
        3. Malicious attachments
        4. Phishing, Spear phishing, Vishing
    B. Email dos and don’ts
    C. Privacy
        1. Social and Behavioral Privacy
        2. Social Media Privacy and Security
    D. Ethical Issues
        1. System misuse and user misbehavior
        2. Cybercrime
        3. Cyber ethics

VII. Cryptography
    A. Introduction

1. Basic Terminology
2. Cryptosystem
3. Classical Cryptography

B. Transposition Techniques
1. Rail Fence Cipher
2. Interleaving Transposition Cipher

C. Substitution Techniques
1. Caesar Cipher
2. Monoalphabetic Cipher
3. Polyalphabetic Cipher
4. Playfair Cipher
5. Vigenere Cipher
6. One time pad (Vernam) Cipher

D. Cryptographic Hash Function
1. One-way Hash Function Properties
2. Hashing Methodologies
3. Birthday Attacks for Hash Collision
4. MD2, MD4, MD5, SHA-1, SHA-2, SHA-3

GENERAL EXPECTATIONS

1. This is a 3-semester hour course where the class meets for 3 hours in a week. Students are expected to have access to an internet-connected computer, and have the required level of computer skills, motivation and a commitment to work on their assignments. Course activities might include attending lectures, completing assignments, exams, participating in discussion forums based on prompts from the instructor, and/or responding to questions that have been designed by the instructor to check the understanding of key concepts.

2. All assignments will be given a due date. Students are expected to turn the assignments in by the due date. Late assignments **will not** be graded!!! There will be **no exceptions to this policy**. **Assignments will be submitted to the associated Blackboard Assignments link which once closed will no longer accept any assignments**.

3. All assignments **must be typed**. Handwritten submissions will not be accepted under any circumstances without explicit prior approval.

4. All projects are expected to be done by the individual, unless otherwise directed. Cheating **will not** be tolerated and will result in a ***failing grade for the class AND referral to Judicial Affairs***. **I will entertain NO excuses for cheating!**

5. If you are struggling with the material in the class, please make a point to visit me during my office hours or make an appointment to receive additional help. **It is not wise to wait until after midterms to try and "rescue" your grade**. Establishing a tutoring relationship with anyone during the last week of the semester will be impossible and should not be attempted.

Additionally, please do not ask to submit all missing homework assignments at semester end – they **must be submitted prior to the due date!**

6. If you wish to discuss your grade, please make an appointment or come to see me during office hours. I do not discuss grades over email. **DO NOT REQUEST A GRADE CHANGE ONCE THE FINAL IS OVER.**

7. I will use email to communicate with you about many things outside of the regular class time. It is imperative that you frequently check your email, therefore you **are required** to check your email regularly and I assume that you receive any email message from me within 12 hours of it being sent. Also, please regularly check your spam folder, as sometimes email from me lands there.

8. I reserve the right to modify any part or the entirety of the syllabus as deemed necessary.

TECHNOLOGY REQUIREMENTS

Some course content is delivered via the Internet through the Blackboard learning management system. Ensure your UTEP e-mail account is working and that you have access to the Web and a stable web browser. Google Chrome and Mozilla Firefox are the best browsers for Blackboard; other browsers may cause complications. When having technical difficulties, update your browser, clear your cache, or try switching to another browser.
You will need to have access to a computer/laptop. You will need to download or update the following software: Microsoft Office, Adobe Acrobat Reader, Windows Media Player, QuickTime, and Java. Check that your computer hardware and software are up-to-date and able to access all parts of the course.
If you do not have word-processing software, you can download Word and other Microsoft Office programs (including Excel, PowerPoint, Outlook and more) for free via UTEP's Microsoft Office Portal. Click the following link for more information about Microsoft Office 365 and follow the instructions.
IMPORTANT: If you encounter technical difficulties beyond your scope of troubleshooting, please contact the UTEP Technology Support as they are trained specifically in assisting with technological needs of students. Please do not contact me for this type of assistance. The Help Desk is much better equipped than I am to assist you!

COURSE COMMUNICATION: How we will stay in contact with each other

Here are the ways we can keep the communication channels open:

- Office Hours: I will have office hours for your questions and comments about the course. My office hours are in-person; however, you can request a virtual meeting and I will send you a Zoom link. Please see the days and times at the top of this syllabus.
- Email: UTEP e-mail is the best way to contact me. I will make every attempt to respond to your e-mail within 24 hours of receipt. When e-mailing me, be sure to email from your UTEP student e-mail account and please put the course number in the subject line. In the body of your e-mail, clearly state your question. At the end of your e-mail, be sure to put your first and last name, and your university identification number.

- Announcements: Check the Blackboard announcements frequently for any updates, deadlines, or other important messages.

ATTENDANCE AND PARTICIPATION

Attendance in the course is 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. Participation is determined by the completion of the following activities:

- Reading/Viewing all course materials to ensure understanding of assignment requirements
- Participating in engaging discussions with your peers
- Other activities as indicated in the weekly modules

Because these activities are designed to contribute to your learning each week, they cannot be made up after their due date has passed.

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.

*EXCUSED ABSENCES AND/OR COURSE DROP POLICY

According to UTEP Catalog, "At the discretion of the instructor, a student can be dropped from a course because of excessive absences or lack of effort. A grade of "W" will be assigned before the course drop deadline and a grade of "F" after the course drop deadline." See Policies and Regulations in the UTEP Undergraduate Catalog for a list of excuse absences. Therefore, if I find that, due to non-performance in the course, you are at risk of failing, I will drop you from the course. I will provide 24 hours advance notice via email.

OR

I will not drop you from the course. However, if you feel that you are unable to complete the course successfully, please let me know and then 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.

DEADLINES, LATE WORK, AND ABSENCE POLICY

Assignments

- Writing assignments will be due on posted deadlines at midnight (11:59 PM) via Blackboard. No late work will be accepted if the reason is not considered excusable.

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. If you miss an assignment and the reason is not considered excusable, you will receive a zero. It is therefore important to reach out to me—in advance if at all possible—and explain with proper documentation why you missed a given course requirement. Once a deadline has been established for make-up work, no further extensions or exceptions will be granted.

ALTERNATIVE MEANS OF SUBMITTING WORK IN CASE OF TECHNICAL ISSUES

I strongly suggest that you submit your work with plenty of time to spare in the event that you have a technical issue with the course website, network, and/or your computer. I also suggest you save all your work (answers to discussion points, quizzes, exams, and essays) in a separate Word document as a backup. This way, you will have evidence that you completed the work and will not lose credit. If you are experiencing difficulties submitting your work through Blackboard, please contact the UTEP Help Desk. You can email me your backup document as a last resort.

INCOMPLETE GRADE POLICY

Incomplete grades may be requested only in exceptional circumstances after you have completed at least half of the course requirements. Talk to me immediately if you believe an incomplete is warranted. If granted, we will establish a contract of work to be completed with deadlines.

*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

AI prohibited

Use of AI technologies or automated tools, particularly generative AI such as ChatGPT or DALL-E, is ***not allowed*** for assignments in this class. Each student is expected to use critical and creative thinking skills to complete tasks and not rely on computer-generated ideas. 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.

AI allowed only with prior permission from instructor

Use of AI technologies or automated tools, particularly generative AI such as ChatGPT or DALL-E, is ***only allowed with approval from the instructor BEFORE being used***. Without permission, you will be expected to think creatively and critically to complete assignments without assistance from these tools.

If given permission to use any of these tools, students must properly cite and give full credit to the program used upon submission of every relevant assignment. For example, text generated using ChatGPT must be cited:

> ChatGPT(version). Date of query (year/month/day). "Text of your query." Generated using OpenAI. https://chat.openai.com/

A short paragraph describing how the tool(s) was/were used for the assignment must be included.

AI allowed with proper acknowledgement

Use of AI technologies or automated tools, particularly generative AI such as ChatGPT or DALL-E, is ***only allowed with proper attribution given for its use***.

Students must properly cite and give full credit to the program used upon submission of every relevant assignment. For example, text generated using ChatGPT must be cited:

> ChatGPT(version). Date of query (year/month/day). "Text of your query." Generated using OpenAI. https://chat.openai.com/

A short paragraph describing how the tool(s) was/were used for the assignment must be included.

Using AI for brainstorming

Some AI technologies or automated tools, particularly generative AI such as ChatGPT or DALL-E, can 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 may 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.

Free use of AI without acknowledgement

Use of AI technologies or automated tools, including generative AI such as ChatGPT or DALL-E, is permitted in this class. Students must include a short paragraph, with each relevant assignment, explaining how the tool was used.

PLAGIARISM DETECTING SOFTWARE

Some of your course work and assessments may submitted to SafeAssign, a plagiarism detecting software. SafeAssign is used review assignment submissions for originality and will help you learn how to properly attribute sources rather than paraphrase.

*COURSE RESOURCES: Where you can go for assistance

UTEP provides a variety of student services and support. Please refer to the QR code below for a listing of campus resources or visit https://www.utep.edu/advising/student_resources/student-success-resource-hub.html.