MIS 6330/ACCT 6313 — Cybersecurity Fundamentals

Instructor: Professor Alex Ivaschenko

Mobile: Microsoft Teams **Email:** alex.ivaschenko@utdallas.edu

Office Hours: Microsoft Teams (by Appointment) **Classroom:** Room 2.717 JSOM

Textbook - No Textbook required. **Schedule:** Fridays 7pm-9:45 pm

Course Material -

I have prepared an extensive set of course notes that I will use during the class. These notes will be posted on the class website. These lecture notes are intended to function as a summary of topics/issues/concepts discussed in class. These notes are meant to save you the time to take notes in class, so that you can make better use of that time by listening, asking questions, and participating in class. In addition, all homework and solutions will be posted on the class website.

Classroom Expectations –

- “Honesty is the best policy.”. ***Chat GPT is forbidden in this course, all submissions and thoughts should be your own.***
- “Help thy neighbor.” Volunteer to help your peers. This is not only a class, but an experience that all of us want to relish.
- Honor the deadlines.
- Please turn off (or put in silent mode) your cell phone during class time.
- Please restrict your laptop computer use for class-related purposes only. Also, turn off your laptop’s speakers before starting to use it.
- For all communication, please use your @utdallas.edu email and include your UTD ID (e.g., 201/202xxxxx)
- Student is not allowed to take a mid-semester hiatus, skipping any examination, while expecting the Professor / Instructor to coordinate all alternative arrangements.
- Students are responsible for all materials covered in a lecture, irrespective of their attendance. Neither the TA nor the instructor is required to cover lecture content one-on-one for students missing lectures.

Academic Integrity:

The University is committed to academic excellence and expects academic honesty from all members of the University community and believes that it is essential for academic excellence and integrity. Academic honesty includes adherence to guidelines established by the instructor in a particular course for both individual and group work. It prohibits representing the work of others to be one's own (plagiarism); receiving unauthorized aid on an assignment (cheating); and using similar papers or other work products to fulfil the obligations of different classes without the instructor's permission.

Penalties for academic dishonesty may include a grade of "F" on the work in question or for the course. In addition, any student engaged in academic dishonesty will be subject to disciplinary action. Please refer to the General Polices website (see below) for detailed information pertaining to academic dishonesty, including procedures for determining disciplinary action.

https://conduct.utdallas.edu/integrity/

Attendance and Class Participation.

Class Attendance is required for every class. I will take attendance near the end of each lecture. If any student arrives to the class later than 15 minutes, he/she will not get attendance credit for that day. Students can be absent for a maximum of 2 classes per semester with prior approval including sick days and if they do not have a prior approval from Instructor prior to taking time off, this will be treated as absent.

Participation includes engaging in group or other activities during class that solicit your feedback on homework assignments, readings, or materials covered in the lectures (and/or labs). Class participation is documented by faculty. Successful participation is defined as consistently adhering to university requirements, as presented in this syllabus. Failure to comply with these University requirements is a violation of the Student Code of Conduct.

Course Description

This course is intended to prepare students for jobs that require comprehensive understanding of security threats, technical approaches to prevention and countermeasures, and related management issues. Though it does not have pre-requisites, it assumes familiarity with concepts such as DBMS and TCP/IP, topics that I will also briefly revisit for the benefit of those who are not fully familiar.

We will cover the following security-related topics:

1. **Introduction:** challenges, the CIA triad, risk analysis, security assurance, security strategy.

2. **Cryptography**: symmetric encryption, public-key encryption, secure hash functions, message authentication, sender authentication, digital certificates, and signatures.

3. **User Authentication and Identity and Access Management:** password policies, hashing and use of password salts, offline dictionary and rainbow table attacks, remote authentication and replay attacks, challenge-response protocols, biometric systems.

4. **Database Security:** access control basics, role-based security (plus SQL GRANT statement), statistical database security, inference, and tracker attacks (plus query restrictions, perturbation, micro-aggregation, and other common countermeasures).

5. **Software/Application Security**: buffer and stack overflow, SQL and code injection, cross site scripting, software security testing (input fuzzing, output testing)

6. **Intrusion**: review of TCP/IP, firewall types (packet filters, circuit-level gateways, application proxies) and topologies (location of bastions and host firewalls).

7. **Malware and DoS:** viruses and other malware, antivirus software evolution, botnets and FFSN, flooding attacks, Denial of Service, reflection and amplification attacks, contingency plans for DoS.

Though our focus is on management of technology and not technology per se, most of the lectures will be technical. It is not possible to implement a security strategy unless you have a good understanding of underlying technologies. I intend to maintain my focus on common security problems and countermeasures. I encourage you to actively participate in every class.

Student Learning Objectives/Outcomes

- Grasp cybersecurity principles, including the CIA triad (Confidentiality, Integrity, and Availability).
- Understand key cybersecurity threats, vulnerabilities, and risk management practices.
- Learn to identify and mitigate security vulnerabilities in IT systems and networks.
- Understand principles of secure system architecture and design.
- Learn methods for implementing access control, authentication, and cryptographic techniques.
- Assess risks in IT systems and propose effective security solutions.
- Analyze and design secure systems to meet specific organizational needs.
- Use cybersecurity tools and techniques to secure IT systems effectively.
- Understand the role of cybersecurity policies, procedures, and frameworks (e.g., NIST, ISO 27001)
- Consider management, security, and business-related issues related to the field.

Technical Tools and Resources

- Students must have a computer for this course and bring their PC to every class.
- Students must have access to Microsoft Office applications – Excel, Word, PowerPoint – for classroom activities.
- Students are responsible for acquiring or using appropriate and usable technology equipment. If your personally owned devices and equipment are

not compatible with the needs of this course, especially for assignments, students should use the computers available in the JSOM computer labs.

Homework

I will post several short individual homework. Keep checking the class website regularly.

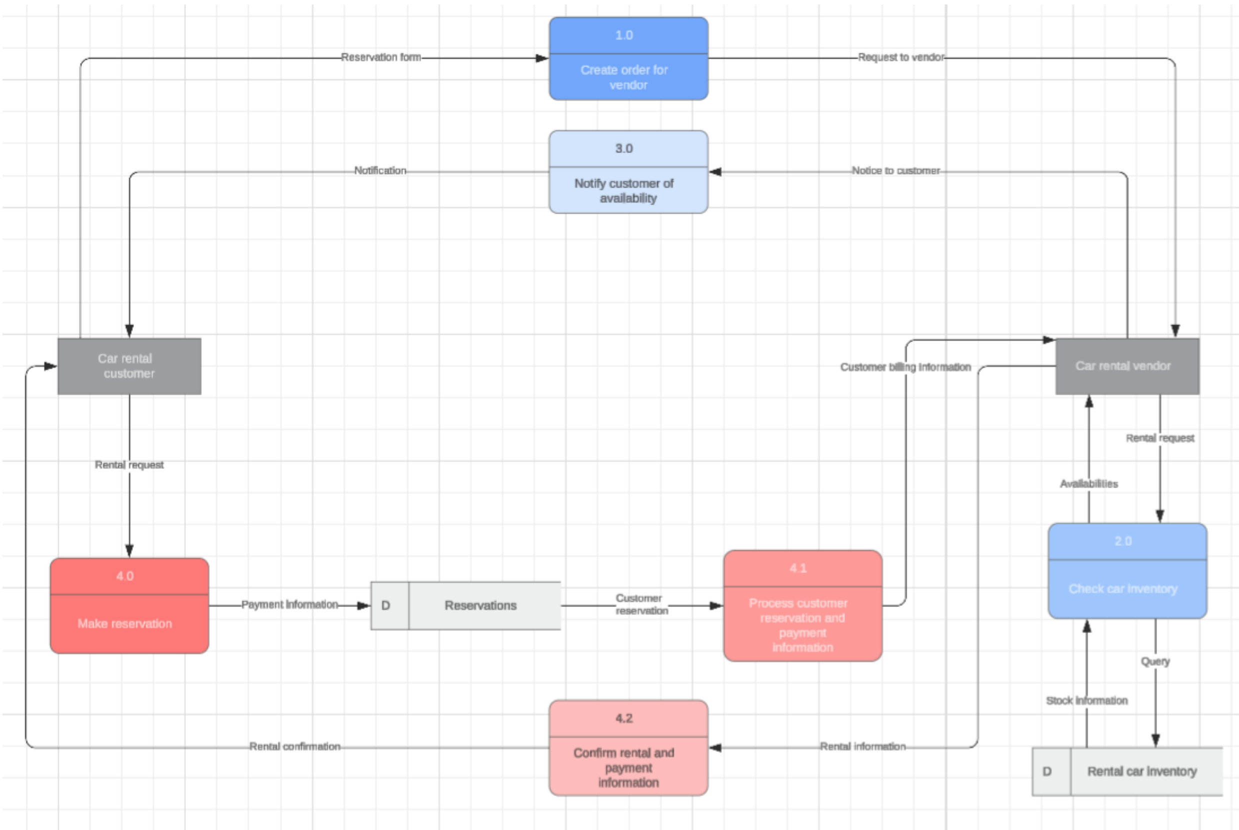
<u>Group Project Assignment (20% of Grade): Secure Application Design & Threat Modeling</u>

Our group project provides each student with the opportunity to practice the IT Security principles that we covered in the course. It focuses on many of the student learning objectives and key points under course objectives. The term project is a team effort, and the instructor assigns team members and topics. The term project consists of three major "assignments" (listed below).

Project Plan (Due 04/09 11:59 PM CST) – 5%

1. Each team will select a real-world application scenario from the list below:
    a. University student portal login (Login/Identity)
    b. Two-factor mobile banking login page (Login/Identity)
    c. Online appointment scheduling system (Web/App System)
    d. Job application submission portal (Data Handling)
    e. Campus Wi-Fi authentication portal (Network Connected)
2. Each team will create a Logical Data Flow Diagram (DFD) based upon the real-world scenario chosen from step #1:
    a. Students need to draw out the Actor (User), Application (Web/App/Portal), Database, External Systems (email Server, Payment processor, etc), etc.
    b. Students can use PowerPoint, LucidChart (highly recommend)
    c. Example DFD Elements:
        i. User submits form -> Web App
        ii. Web App queries database
        iii. Database returns results
        iv. App sends email confirmation
    d. Note: Logical Data Flow Diagram (DFD) focuses on what happens information flow, whereas the Physical DFD focuses on how things are happening. Since, we are not programming for this project, we will focus on the Logical aspect.

Example of Logical Data Flow Diagram (DFD):



https://www.lucidchart.com/blog/data-flow-diagram-tutorial

3. Each team will perform a STRIDE Threat Modeling Analysis based upon the real-world scenario chosen from step #1 and end to end diagram from step #2.
    a. Spoofing (Pretending to be someone else)
    b. Tampering (Modifying data, unauthorized modification = integrity)
    c. Repudiation (Denying action)
    d. Information Disclosure (Unauthorized data exposure)
    e. Denial of Service (Making system unavailable)
    f. Elevation of Privilege (Gaining unauthorized access)

   Each team must submit 10-12 threats total across these 6 categories.

   Example of threats:

   a) Spoofing: Attacker uses stolen credentials to log in
   b) Tampering: Manipulated form data before submission
   c) Information Disclosure: Sensitive data leaked due to lack of encryption
   d) Denial of Service: A simple flooding attack on the login endpoint.

4. Each team will provide a Risk Matrix for Impact (Low, Medium, High) and Likelihood (Low, Medium, High) – students will categorize each threat from step #3 into a “risk rank”.

   Example of Matrix:

Risk Level Calculation:

- Low Likelihood * Low Impact = Low Risk
- Medium Likelihood * Low Impact = Low-Medium Risk
- High Likelihood * Low Impact = Medium Risk
- Low Likelihood * Medium Impact = Low-Medium Risk
- Medium Likelihood * Medium Impact = Medium Risk
- High Likelihood * Medium Impact = High Risk
- Low Likelihood * High Impact = Medium Risk
- Medium Likelihood * High Impact = High Risk
- High Likelihood * High Impact = Critical Risk

Threat	**Likelihood (How Likely to happen?)**	**Impact (How bad would it be if it happened?)**	**Risk Level (How urgent is it?)**
Stolen login password	Medium	High	High
SQL Injection	Low	High	Medium

5. Lastly, each team will propose 10-12 security improvements (controls) that address the threats from step #3.
   Example of Controls:
   a. Access Controls (RBAC, least privilege)
   b. Cryptographic Controls (Hashing, Salting)
   c. Input Validation (App / Web Security)
   d. Logging & Monitoring (Audit Logs)
   e. Firewalls / WAF
   f. DoS Mitigation

One member from each team will send me the below (and CC all of their team members on the **email**) by **04/09 11:59 PM CST**:

1. Written Report (10-12 pages double-spaced):
   a. Executive Summary
   b. System Overview (Step 1)
   c. DFD Diagram (Step 2)
   d. STRIDE threat table (Step 3)
   e. Risk Prioritization Matrix (Step 4)
   f. Security Recommendations
   g. Conclusion

Presentation (Due 04/23 11:59 PM CST) – 10%

Same member who sent the written report from each team will send me the below (and CC all of their team members on the **email**) by 04/23 11:59 PM CST:

1. Presentation (10-15 minutes):
   a. System Overview
   b. DFD Diagram

c. Key Threats
d. Most Important Risks
e. Top 5 Recommended Controls (in depth)
f. Expected Business Impact

Peer Evals – 5%

The peer evaluation form allows you to assess the contributions of your group members to the Group Project. Your responses will remain confidential and will be reviewed only by the instructor. Be honest, fair, and constructive. Your evaluation should reflect each member's actual participation, professionalism, and effort. <u>Please do not rate yourself.</u>

Group Member Name	**Attendance & Reliability**	**Quality of Work**	**Timeliness**	**Teamwork & Communication**	**Contribution to Final Deliverables**	**Overall Score**
Name	0-5	0-5	0-5	0-5	0-5	/25

1. **Describe this group member's strengths (e.g., dependable, research oriented, strong communicator, organized, technical, etc.)**
2. **Describe one area (or more) of improvement for this group member.**
3. **If you believe that this team member did not contribute fairly, please explain specifically (write "N/A" if everyone contributed fairly).**

<u>**Each**</u> member from each team will send me <u>**one**</u> word document with the above matrix & questionnaire for <u>**each**</u> member of their group, separating each member by page. (i.e., If there are 3 members in your group. Each member will send me one peer eval (not including themselves) file that is 2 pages long, one page per group member).

Grading Rubric:

Category	**Weight**	**Description**
System Design Clarity	20%	DFD completeness, clarity, understanding
Threat Identification	25%	Broad, accurate STRIDE coverage
Risk Prioritization	15%	Logical, justified reasoning
Security Recommendations	25%	Realistic, aligned with course content
Presentation Quality	15%	Clear, Concise, Visually Organized

Presentation Quality (15%):

1. **Show Up**
2. **Dress Up (No Jeans, T-Shirt, Hats, etc)**
3. **Your presentation must include:**
    a. Title Slide – Group Member names, project title, etc
    b. System overview – What your application/system does
    c. Data Flow Diagram (DFD) explanation
    d. Key Threats (STRIDE)
    e. Risk Prioritization (Top 5 Risks)
    f. Recommended Security Controls
    g. Conclusion & Summary
4. **Your presentation must:**
    a. Use terminology correct (CIA Triad, STRIDE, DoS, encryption, IAM)
    b. Explain diagrams clearly
    c. Provide accurate examples
    d. Avoid unnecessary jargon or overly technical detail
5. **Your presentation must be:**
    a. Readable
    b. Use visuals (LucidChart, DFD, etc)
    c. Use consistent formatting
6. **Your group members should:**
    a. Speak clearly and at an appropriate pace.
    b. Maintain eye contact
    c. Divide speaking roles equitably
    d. Demonstrate preparation and practice
    e. Stay within the 10-15 minute time limit.
7. **Your presentation should demonstrate:**
    a. Understanding of security principles.
    b. Logical reasoning behind threats and controls.
    c. Evidence of critical thinking.
    d. Application of course concepts.

Exams

We will have both a midterm and a final exam. Both are closed books and notes, but one letter-sized 8.5x11 cheat sheet is allowed. **Electronic devices are not allowed.** The final exam is not cumulative. Studying in small groups can help. **Exams will be taken at the Synergy Park Testing Center.**

Grading

Attendance – 10%
Homework – 10% (10%/day for late turn in)
Group Project – 20%
Midterm Exam – 30%
Final Exam – 30%

Extra Credit

Passing one of the "Certifications" (CISSP, CISA, CISM, CCSP, CEH) exams related to the Cybersecurity Profession during course duration will award the student an additional 10 points to their final grade.

Additional certifications may be considered at Professor's discretion.

It is the student's responsibility to provide a written (e-mail) proposal regarding an additional certification that is not listed above for approval by Professor.

Grading Scale

Scaled Score	Letter Equivalent
>= 93.3	A
>= 90.0 and < 93.3	A-
>= 87.7 and < 90.0	B+
>= 83.3 and < 87.7	B
>= 80.0 and < 83.3	B-
>= 77.7 and < 80.0	C+
>= 73.3 and < 77.7	C
>= 73.3	P
Less than 73.3	F

Letter grading will be in line with UTD grading criteria.

<u>Graded work, feedback, and solutions</u>

Solutions will be posted on the class website. If you want anything regraded, please write a separate memo (not an email) describing your concerns and hand it to me along with the exam or homework that you want regraded. Please do not write anything on the graded exam or homework, if you want it regraded.

Week	**Date**	**Topics**	**Readings**	**Deliverables**
Week 1	01/23/2026	Introduction	Section 1 PPT	**Post HW1 (S1, S2) – 11:59 PM CST**
Week 2	01/30/2026	Cryptography	Section 2 PPT	
Week 3	02/06/2026	Cryptography	Section 2 PPT	**Submit HW1 (S1, S2); Due 02/08 11:59 PM CST** **Assign Group Project Team Members 02/08 11:59 PM CST**
Week 4	02/13/2026	User Authentication	Section 3 PPT	**Post HW2 (S3) – 11:59 PM CST** **Group Project Team Members Provide their real-world application scenario of choice by 02/15 11:59 PM CST**
Week 5	02/20/2026	User Authentication	Section 3 PPT	**Submit HW2 (S3); Due 02/22 11:59 PM CST**
Week 6	02/27/2026	Database Security	Section 4 PPT	**Post HW3 (S4) – 11:59 PM CST** **Group Project Team Members Provide their Data Flow Diagram by 03/01 11:59 PM CST**
Week 7	03/06/2026	**Midterm Review**		Review Section 1,2,3,4 to prepare for Midterm **Submit HW3 (S4); Due 03/08 11:59 PM CST**
Week 8	03/13/2026	**Exam 1 Midterm – No Class**		**<u>Exam Timeslot: 03/09-03/13</u>** **Group Project Team Members Provide their STRIDE Threats by 03/15 11:59 PM CST**
Week 9	03/20/2026	**Spring Break – No Class**		
Week 10	03/27/2026	**Exam 1 post-review**	Section 5 PPT	**Post HW4 (S5) – 11:59 PM CST** **Group Project Team Members Provide their RISK Matrix and Security Improvements (Controls)**

				by 03/29 11:59 PM CST
Week 11	04/03/2026	Software Security	Section 5 PPT	**Submit HW4 (S5); Due 04/05 11:59 PM CST**
Week 12	04/10/2026	TCP/IP Review, Firewall	Section 6 PPT	**Post HW5 (S6) – 11:59 PM CST** **Project Plan Deliverables Due 04/09 11:59 PM CST**
Week 13	04/17/2026	TCP/IP Review, Firewall	Section 6 PPT	**Submit HW5 (S6); Due 04/19 11:59 PM CST**
Week 14	04/24/2026	Malware & DOS	Section 7 PPT	**Post HW6 (S7) – 11:59 PM CST** **Group Project Presentation Due 04/23 11:59 PM CST**
Week 15	05/01/2026	**Group Project Presentation**	Section 7 PPT	**Submit HW6 (S7); Due 05/03 11:59 PM CST**
Week 16	05/08/2026	**Final Exam Review**		Review Section 5, 6, 7 to prepare for Final **Group Project Peer Evaluations Due 05/07 11:59 PM**
Week 17	05/15/2026	**Exam 2 Final (non-comprehensive) – No Class**		**<u>Exam Timeslot: 05/11-05/15</u>**

UT Dallas Syllabus Policies and Procedures

The information contained in the following link constitutes the University's policies and procedures segment of the course syllabus.

Please go to http://go.utdallas.edu/syllabus-policies for these policies.

The descriptions and timelines contained in this syllabus are subject to change at the discretion of the Professor.