MIS 6330/ACCT 6313 — Cybersecurity Fundamentals

Instructor: Professor Alex Ivaschenko

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

Office Hours: 3.604, Fridays 5pm-7pm (by Appointment) **Classroom:** Room 12.206 JSOM

Textbook - No Textbook required. I will provide learning material.

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.

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.

Course motivation

We live in quite a different world today than what our parents lived in. Very recently, CapitalOne has been breached and financial information of thousands of consumers has been stolen. A few years back, large technology companies Sony and Yahoo were hacked, and it has cost them hundreds of millions in shareholder value, if not billions. Curiously, the Pentagon believes that the next 9/11 will not be about planes crashing into buildings; instead, it will be hackers crashing the US stock exchanges, power grids, large telecommunication networks, or nuclear plants.

While the threats have grown, so have technologies that are used to combat them. The security vendors have registered significant growth, even though the economic downturns. Businesses have stepped up their defenses: after the attack on Sony, many businesses have decided to increase their investments in security solutions. There are excellent career opportunities for IT professionals who have a sound understanding of security related threats, technologies, countermeasures, and policies. I recommend that you attend all lectures, as well as leverage readings, assigned review questions, and homework as much as possible.

Homework

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

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)
Midterm Exam – 40%
Final Exam – 40%

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.

Graded work, feedback, and solutions

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	01/24/2025	Introduction	Section 1 PPT	**Post HW1 (S1, S2) – 11:59 PM CST**
Week 2	01/31/2025	Cryptography	Section 2 PPT	
Week 3	02/07/2025	Cryptography	Section 2 PPT	**Submit HW1 (S1, S2); Due 02/09 11:59 PM CST**
Week 4	02/14/2025	User Authentication	Section 3 PPT	**Post HW2 (S3) – 11:59 PM CST**
Week 5	02/21/2025	User Authentication	Section 3 PPT	**Submit HW2 (S3); Due 02/23 11:59 PM CST**
Week 6	02/28/2025	Database Security	Section 4 PPT	**Post HW3 (S4) – 11:59 PM CST**
Week 7	03/07/2025	**Midterm Review**		Review Section 1,2,3,4 to prepare for Midterm **Submit HW3 (S4); Due 03/09 11:59 PM CST**
Week 8	03/14/2025	**Exam 1 Midterm**		**Exam Timeslot: 03/10-03/14**
Week 9	03/21/2025	**Spring Break**		
Week 10	03/28/2025	Software Security	Section 5 PPT	**Post HW4 (S5) – 11:59 PM CST**
Week 11	04/04/2025	Software Security	Section 5 PPT	**Submit HW4 (S5); Due 04/06 11:59 PM CST**
Week 12	04/11/2025	TCP/IP Review, Firewall	Section 6 PPT	**Post HW5 (S6) – 11:59 PM CST**
Week 13	04/18/2025	TCP/IP Review, Firewall	Section 6 PPT	**Submit HW5 (S6); Due 04/20 11:59 PM CST**
Week 14	04/25/2025	Malware & DOS	Section 7 PPT	**Post HW6 (S7) – 11:59 PM CST**
Week 15	05/02/2025	Malware & DOS	Section 7 PPT	**Submit HW6 (S7); Due 05/04 11:59 PM CST**
Week 16	05/09/2025	**Final Exam Review**		Review Section 5, 6, 7 to prepare for Final
Week 17	05/16/2025	**Exam 2 Final (non-comprehensive)**		**Exam Timeslot: 05/12-05/16**

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.