INTRODUCTION TO COMPUTER SECURITY
CSCE 4550.002 – FALL 2018

Instructor:	**Professor Mark D. Hoffman**
E-mail Address:	mark.hoffman@unt.ed
Office Hours:	**By Appointment Only**
Class Location/Time:	NTDP B142 (Discovery Park), Wed 5:30 – 8:20 PM
	Every attempt will be made to answer e-mails within 24 hours. Please use your UNT e-mail and include CSCE 4550.002 (or your specific recitation section) in the subject line. Always use your official UNT email address. Messaging via Canvas is NOT recommended.
Textbook:	*Security in Computing, 5th Edition*, Pfleeger, Pfleeger, & Margulies, Prentice Hall, 2015, ISBN 978-0-13-408504-3.
Reference Textbook:	*Introduction to Computer Security*, Matt Bishop, Pearson, 2005, ISBN 0-321-24744-2.
Canvas	This course will use the Canvas learning management system (LMS) to distribute course materials, communicate and collaborate online, post grades, and submit assignments. You are responsible for checking the Canvas course site regularly for class work and announcements.

COURSE DESCRIPTION

The aim of this course is to introduce the concepts and principles of computer security and privacy. It covers theory and practice of computer security and privacy including OS and network security, security threats and countermeasures against them, cryptography, risk analysis and data privacy.

COURSE OUTCOMES

Course outcomes are measurable achievements to be accomplished by the completion of a course. These outcomes are evaluated as part of our ABET accreditation process.

1. Understand common security terminology, threats, vulnerabilities, and security design principles
2. Understand basic cryptography concepts, and specific commonly used algorithms and protocols.
3. Understand common program vulnerabilities, and secure programming techniques.
4. Understand formal security models, including Bell-LaPadula (MLS), Biba, and Chinese Wall security.
5. Understand basic network security issues and controls.
6. Understand administrative issues in security, such as planning, security policies, and risk analysis.
7. Understand privacy concepts and data anonymization
8. Obtain hands-on experience in using common security tools, such as firewalls, intrusion detection systems, and port scanning software.

INTRODUCTION TO COMPUTER SECURITY
CSCE 4550.002 – FALL 2018

ABET STUDENT OUTCOMES

Computer Engineering

1. An ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics.
2. An ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors
4. An ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts
6. An ability to develop and conduct appropriate experimentation, analyze and interpret data, and use engineering judgment to draw conclusions
7. An ability to acquire and apply new knowledge as needed, using appropriate learning strategies

Computer Science

1. Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.
2. Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.
4. Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.
6. Apply computer science theory and software development fundamentals to produce computing-based solutions.

Information Technology

1. Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.
2. Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.
4. Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.
6. Identify and analyze user needs and to take them into account in the selection, creation, integration, evaluation, and administration of computing-based systems.

ADA STATEMENT

The University of North Texas makes reasonable academic accommodation for students with disabilities. Students seeking reasonable accommodation must first register with the Office of Disability Accommodation (ODA) to verify their eligibility. If a disability is verified, the ODA will provide you with a reasonable accommodation letter to be delivered to faculty to begin a private discussion regarding your specific needs in a course. You may request reasonable accommodations at any time, however, ODA notices of reasonable accommodation should be provided as early as possible in the semester to avoid any delay in implementation. Note that students must obtain a new letter of reasonable accommodation for every semester and must meet with each faculty member prior to implementation in each class. Students are strongly encouraged to deliver letters of reasonable accommodation during faculty office hours or by appointment. Faculty members have the authority to ask students to discuss such letters during their designated office hours to protect the privacy of the student. For additional information see the Office of Disability Accommodation website at http://www.unt.edu/oda. You may also contact them by phone at 940.565.4323.

ACCEPTABLE STUDENT BEHAVIOR

Student behavior that interferes with an instructor's ability to conduct a class or other students' opportunity to learn is unacceptable and disruptive and will not be tolerated in any instructional forum at UNT. Students engaging in unacceptable behavior will be directed to leave the classroom and the instructor may refer the student to the Dean of Students to consider whether the student's conduct violated the Code of Student Conduct. The university's expectations for student conduct apply to all instructional forums, including university and electronic classroom, labs, discussion groups, field trips, etc. The Code of Student Conduct can be found at http://deanofstudents.unt.edu.

ATTENDANCE POLICY

Lecture Section: Class attendance is regarded as an obligation as well as a privilege. All students are therefore expected to attend each class meeting. A student who misses class is still responsible to find out what was discussed and to learn the material that was covered and obtain the homework that was assigned on the missed day. The instructor is not responsible for re-teaching material missed by a student who did not attend class. Therefore, each student is accountable for and will be evaluated on all material covered in this course, regardless of attendance. Excessive student absences may have a negative impact on a student's comprehension and learning. If there are extenuating circumstances, please notify your instructor so that you can work together to ensure your success in learning the material.

Recitation Sections: Although attendance at your scheduled recitation is considered to be optional, the recitation classrooms have been especially configured to support working on the laboratory exercises. Students may want to take advantage of attending their recitation section to receive guidance on completing the homework, laboratory exercises, projects, or other course assistance, such as preparing for exams.

ACADEMIC DISHONESTY

This course follows UNT's policy for *Student Academic Integrity* that can be found at https://policy.unt.edu/policy/06-003 as well as the *Cheating Policy* for the Department of Computer Science and Engineering (posted on Canvas). Specifically, the first instance of a student found to have violated the academic integrity (i.e., cheating) policy will result in a grade of "F" for the course and have a report filed into the Academic Integrity Database, which may include additional sanctions.

Individual assignments, including homework, laboratory exercises, and projects, and exams in this course must be the sole work of the individual student. You should not work with other students on shared program solutions or use solutions found on the Internet. Specifically, you should never copy someone else's solution or code, and never let a classmate examine your code. A sophisticated program will be used to compare your work to the work of all other students (including students in past classes). If you are having trouble with an assignment, please consult with your instructor or TA/IA assigned to this course. Failure to adhere to these strict standards may be cause for disciplinary action even leading to expulsion from the University.

In the case that the above description or any in-class discussion of appropriate and inappropriate collaboration do not answer all of your questions, please meet with your instructor and look at the university Student Rights and Responsibilities web page.

INTRODUCTION TO COMPUTER SECURITY
CSCE 4550.001 – FALL 2018

GRADING POLICY

Your course grade will be a weighted average according to the following:

Homework	16.0%
Laboratory Exercises	20.0%
Projects	24.0%
Midterm Exams 1 – 2	25.0% (12.5% each)
Final Exam	15.0%
Total	100.0%

Grades will be posted on Canvas throughout the semester to provide an ongoing assessment of student progress, though final assessment will be measured using the weighted average above. Once a grade is assigned on Canvas, students have two (2) weeks to dispute the grade. The proper channel for grade disputes is to first go to the original grader (i.e., TA/IA) in an attempt to resolve the issue. If, however, a resolution cannot be reached between the student and the grader, the student shall then go to the instructor who will have the final say on the grade.

Projects and laboratory exercises will be due at 11:59 PM on the specified due date to Canvas. All assignments must be completed and submitted according to their specific directives. Projects and laboratory exercises (not homework) will be accepted up to 24 hours late and assessed a 30% grade reduction penalty. Any project or laboratory exercise submitted more than 24 hours late will not be accepted and receive a grade of 0

Homework: Homework will be assigned based on material from the lectures and textbook. These assignments are meant for you to become familiar with the course material and this practice will aid you in mastering the concepts on the labs and exams. No late homework will be accepted, so please make sure that you complete and submit all homework assignments on time.

Laboratory Exercises: Students will complete several in-depth hands-on laboratory projects during the semester intended to give a more thorough view of computer security. These labs may be completed in the Security Lab (F206) during one of the scheduled lab sessions, in the downstairs Student Computer Lab (B129), or on your own laptop/desktop using a Virtual Machine (VM). It is critical that you understand that any OS you install for these labs will be installed on the VM and not your physical machine. Trying to install an OS on your physical machine may result in loss of your data.

Projects: There will be several security-based programming projects assigned in this course. These assignments will be completed outside of class, though some in-class time may be dedicated to answering questions about or working on these projects.

Midterm Exams: There will be two midterm examinations given in this course. The dates of these exams will be posted on Canvas and announced in class at least one week prior to the date of the exams. A make-up exam will be given at the discretion of the instructor when a student misses an exam with an excused absence. Unexcused absences on the date of an exam may result in a grade of 0 for the missed exam, so every effort should be made to attend class on the day of a scheduled exam.

Final Exam: There will be a comprehensive final exam on Wednessday, December 12, 2018, from 5:30 PM to 8:30 PM. All students are expected to take the final exam during the scheduled time period.

INTRODUCTION TO COMPUTER SECURITY
CSCE 4550.002 – FALL 2018

STUDENT RESPONSIBILITY
Students are responsible for submitting the *correct* assignments (i.e., uploading the proper files) for each applicable assignment submission on Canvas. In certain cases, when an assignment is submitted on time, but to an incorrect assignment location (e.g., submitting *Lab 04* to *Lab 05* location on Canvas), the assignment may be assessed a 30% reduction penalty if the due date has passed. If you have any questions or concerns about your submission, please work with your instructor or TA/IA to ensure the correct file(s) is/are submitted.

SYLLABUS REVISIONS
This syllabus may be modified as the course progresses should the instructor deem it necessary. Notice of changes to the syllabus shall be made through Canvas and/or class announcement.

TENTATIVE CLASS SCHEDULE *(subject to change):*

Week	Date	Material Covered	Remarks
1	8/29	First Day, Introduction	Ch 1
2	9/5	Program Security	3.1, 3.2
3	9/12	Program Security	3.2, 3.3
4	9/19	Security Models	Bishop Ch 5 – 7
5	9/26	OS Security	5.1
6	10/3	OS Security, Review	5.2
7	10/10	Network Security	Exam 1, 6.1 – 6.4
8	10/17	Network Security	6.7, 6.8
9	10/24	Internet App Security	2.3
10	10/31	Internet App Security	2.3, 6.6, Ch 9
11	11/7	Internet App Security Review	6.6, Ch 9
12	11/14	Database Security	Exam 2 7.1 – 7.5
13	11/21	Database Security Administering Security	9.4 10.1 – 10.4
14	11/28	Administering Security Legal & Ethical Issues	10.5, 11.1, 11.2 11.4 – 11
15	12/5	Review	
16	12/12		Final Exam

IMPORTANT DATES
Aug 29 First Class Day

Nov 5 Last day to drop a course

Dec 5 Last Class Day

Dec 12 Final Exam