CSCE 3560 – Computer Systems Security

Dual numbered course: Please note that this is a dual numbered course (for both undergraduates and graduates). Unless otherwise mentioned, the syllabus below applies for everybody.

Instructor: Dr. Cihan Tunc

Office: NTDP F230

E-mail Address: cihan.tunc@unt.edu

Class Location/Time: NTDP B140 / MoWe 9:30AM-10:50AM

Office Hours: Mondays at 1PM (NTPD F230)

IA: Poojitha Maridi

E-mail Address: PoojithaMaridi@my.unt.edu

Office Hours: Cubicle D1 in E-247 on Wednesdays 11am to 12pm

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

This course will introduce theoretical and practical aspects of computer systems security and present ways to protect a computer system with an additional focus on the distributed computing systems. Topics include operating system security, hypervisors, virtualization security, storage security, trusted hardware, trusted platform modules, application isolation, hardware security modules, cryptoprocessors, and cloud and IoT security. Students will also explore emerging security challenges facing computer systems based on recent research papers.

PREREQUISITE(S)

CSCE 3560: CSCE 3600 with a grade of C or better.

CSCE 5933: No prerequisites.

Linux, programming, and system knowledge highly needed.

REQUIRED TEXT(S)

There is no required textbook for this course as the material covered are too broad for a single textbook. Instead, the course material will be drawn from a number of books and papers from various sources as well as Internet-based resources.

SUGGESTED OPTIONAL REFERENCE TEXT(S)

- *Computer Security: Principles and Practice (4th Edition),* William Stallings and Lawrie Brown, Prentice Hall, 2018, ISBN-13: 978-0134794105.
- *Principles of Computer Security: CompTIA Security+ and Beyond, Fifth Edition,* Wm Arthur Conklin, Greg White, Chuck Cothren, Roger Davis, and Dwayne Williams, McGraw-Hill Education, 2018, ISBN-13: 978-1260026016.
- *Security in Computing, 5th Edition*, Charles P. Pfleeger, Shari Lawrence Pfleeger, and Jonathan Margulies, Prentice Hall, 2015, ISBN 978-0-13-408504-3.

COURSE OUTCOMES

Upon successful completion of this course, the student will be able to:

1. Examine different layers of the computer system and identify their operations and connections with the other layers.
2. Describe and analyze the vulnerabilities in computer system layers including operating system, applications, hypervisors, storage, etc.
3. Demonstrate how to detect and prevent existing vulnerabilities in a computer system.
4. Analyze and address/mitigate the detected vulnerabilities in hardware modules.
5. Incorporate various defense techniques to protect a computer system.

ACADEMIC INTEGRITY

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. 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.

GRADING POLICY

Course grade will be a weighted average according to the following:

Homework Assignments	20%
Lab Assignments	20%
Group Project	20%
Midterm Exam	20%
Comprehensive Final Exam	20%
Total	100.0%

Homework Assignments: Homework will be assigned based on the lectures and assigned reading. These assignments are meant for you to become familiar with the course material and this practice will aid you in mastering the concepts.

Lab Assignments: We will be having some lab assignments to have some hands-on experience in this domain. You may need to create a virtual machine on your laptop for this case. If you do not have the sufficient computational power, please contact me.

Group Project: Students will complete a group project to apply the material and techniques learned in class such as an application utilizing cloud platforms with the Google app Engine and Amazon Web Services (AWS).

Midterm Exams: There will be one midterm examination given in this course.

Final Exam: There will be a comprehensive final exam given during the scheduled time according to the University. *All students are expected to take the final exam during the scheduled time period.*

TENTATIVE SYLLABUS TOPICS *(subject to change):*

- Introduction to Computer Systems Security
- Operating Systems Security
- Storage and data security
- Application Isolation and Containers
- Hypervisors
- Virtualization Security
- Cloud Computing and Security
- IoT and Security
- Trusted Hardware
- Hardware Security Modules
- Cryptoprocessors
- Trusted Platform Modules (TPM)