CS 5352: Computer Security (Tentative)

Instructor: Dr. Deepak K. Tosh	**Class Hours:** TR, 4:30 - 5:50 PM
Semester: Spring 2019	**Office Hours:** MW, 3:30 PM – 4:30 PM
Office: CCSB 3.1010	**Class Room**: CCSB G.0208

A. Course Description:

General concepts and applied methods of computer security, especially as they relate to confidentiality, integrity, and availability of information assets. Topics include system security analysis, access control and various security models, identification and authentication, protection against external and internal threats, network protocols and Internet security.

B. Course Objectives:

This course provides a broad introduction to a variety of topics in applied computer, network, and system security. These include system/software vulnerabilities, applied cryptography, host-based and network-based security, privacy, anonymity, usability, security economics, risks and vulnerabilities, policy formation, controls and protection methods, and issues of law and privacy.

C. Course Outline (TENTATIVE):

1. **Computer security**
   - Overview of Computer Security Concepts and Foundations
   - Threats, Attacks, and Assets
   - User Identification and Authentication
   - Access Control
2. **Applied Cryptography**
   - Block & Stream Ciphers
   - Symmetric and Asymmetric Cryptosystem
   - Public-Key Cryptography and Message Authentication
   - Message Integrity, Authentication, Digital Signature
   - Public Key Infrastructure
3. **Software Security and Trusted Systems**
   - Buffer Overflow
   - SetUID Program vulnerabilities
   - Trusted Computing and Multilevel Security
4. **Network Security**
   - Internet Security Protocols and Standards
   - TCP Attacks, DNS Vulnerabilities, SSL/TLS, DDoS
5. **Next Generation System Designs and Challenges**
   - Cyber-Physical System Overview and Security
   - Internet-of-Things and Smart Grid Security
   - Data & Infrastructure Security in Cloud/Edge Computing

6. **Blockchain and Decentralized Applications**
    - Hashcash and other Consensus Protocols
    - Blockchain Security
    - Smart Contracts
    - Scalability and Privacy challenges, SNARKS
7. **Security Economics and Risk Modeling**
    - Cyber-Risk Assessment
    - Threat Information Sharing
    - Cyber-insurance

D. Reference Books:

(1) William Stallings, Lawrie Brown, "Computer Security: Principles and Practice", Prentice Hall, 3rd edition
(2) Wenliang Du, “Computer Security, A Hands-on Approach”.

Note: No Single textbook covers all the topics listed here. Necessary handouts/weblinks will be given based on materials covered in the classroom.

E. Grading (Tentative):

Your semester grade will be based on a combination of homework assignments, quizzes, attendance, exam, and a term project. The approximate percentages are as follows:

Grading Policy

- 5% - Attendance
- 15% - In-class Quizzes
- 25% - Homework Assignments
- 30% - Team Research Project
- 25% - Exams

Important Note: You will have one week to appeal for your grades after the graded assignments/tests are returned. So, please keep this in mind if you think that there is a problem/issue with the grading of your work.

F. Standards of Conduct:

Students are expected to conduct themselves in a professional and courteous manner, as prescribed by the Standards of Conduct. Students may discuss work assignments and programming exercises in a general way with other students, but the solutions must be done independently. Similarly, groups may discuss group project assignments with other groups, but the solutions must be done by the group itself. Graded work should be unmistakably your own. You may not transcribe or copy a solution taken from another person, book, or other source, e.g., a web page. Professors are required to -- and will -- report academic dishonesty and any other violation of the Standards of Conduct to the Dean of Students.

G. Academic Dishonesty:

Cheating is defined as submitting work under your name that was not done entirely by you for individual assignments or by your team for team assignments. (This includes taking programs from the web or cutting text from web pages and pasting them into documents, even if the source is cited). Cheating will not be tolerated – those caught cheating will be reported to the Dean of Students. You should be aware of the Standards of Conduct posted at http://www.utep.edu/vpfa/student_affairs/student/studindex/htm.

H. Disabilities:

If you have a disability and need classroom accommodations, please contact The Center for Accommodations and Support Services (CASS) at 747-5148, or by email to **cass@utep.edu**, or visit their office located in UTEP Union East, Room 106. For additional information, please visit the CASS website at **www.sa.utep.edu/cass**.

I. Course Outcomes:

Knowledge and Comprehension

1. Describe the functioning of various types of malicious codes.
2. Enumerate programming techniques that enhance security.
3. Explain the various controls available for protection against internet attacks, including authentication, integrity check, firewalls, intruder detection systems.
4. Describe different ways of providing authentication of a user or program.
5. Describe the mechanisms used to provide security in programs, operating systems, databases and networks.
6. Describe the background, history and properties of widely-used encryption algorithms.
7. Describe legal, privacy and ethical issues in computer security.
8. List and explain the typical set of tasks required of an information security professional.

Application and Analysis

1. Compare different access control, file protection or authentication mechanisms.
2. Set up file protections in a Unix or Windows file system to achieve a given purpose.
3. Incorporate encryption, integrity check and/or authentication into a given program or algorithm.

Synthesis and Evaluation

1. Appraise a given code fragment for vulnerabilities.
2. Appraise a given protocol for security flaws.
3. Assess risk for a given network system using publicly available tools and techniques.