CS 4243/5243: Introduction of Computer Security  
**Syllabus: Fall 2022**

**Instructor:** Dr. Sharmin Jahan  
**Office:** 208 MSCS  
**Email:** Sharmin.jahan@okstate.edu  
**Class:** 044 Stout Hall in Stillwater Campus, Main Hall 2203 in Tulsa Campus  
**Time:** 1.30pm – 2.45pm Tuesday  
1.30pm – 2.45pm Thursday  
**Office Hours:** Send an email to the instructor to set up a teams meeting or in-person meeting.

**Course Description & Objectives**  
This course provides an introduction to the fundamentals of computer and network security. Topics will include applied cryptography, operating system security, access control measures, secure programming, analysis and defense of malicious software, an introduction to network threats and defenses, and security issues of new technologies. This course will also help you develop the skills to understand security principles and their application. Moreover, this course will give you some hands-on experiences on some basic attacks using isolated VMs and simulated hardware.

By the end of this course, students will be able to:
- State the basic concepts in information security, including security policies, security models, and security mechanisms.
- Explain concepts related to applied cryptography, including plain-text, cipher-text, the four techniques for crypto-analysis, symmetric cryptography, asymmetric cryptography, digital signature, message authentication code, hash functions, and modes of encryption operations.
- Explain the concepts of malicious code, including virus, Trojan horse, and worms.
- Explain common vulnerabilities in computer programs, including buffer overflow vulnerabilities, Return-to-libc attack, Format String vulnerability.
- Outline the requirements and mechanisms for identification and authentication.
- Explain issues about password authentication, including dictionary attacks (password guessing attacks), password management policies, and one-time password mechanisms.
- Describe security requirements for the web.
- Explain common vulnerabilities in websites including XSS and SQL-Injection attacks.
- Describe threats to networks including sniffing and spoofing, and explain techniques for ensuring network security, including encryption, authentication, firewalls, and intrusion detection.
- Explain the requirements and techniques for security management, including security policies, risk analysis, and physical threats and controls.
- Analyze security requirements and vulnerabilities of new systems including deep learning, IoT-based systems, and cyber-physical systems.

**Requirements**  
CS 3443 or ECEN 3213, each with a grade of "C" or better.

**CS 4243/5243 Difference**  
The graduate (CS 5243) course will have additional research presentations.

**CS 5243 Students**  
Graduate students will have to pick one topic to do research
- Secure Microservice-based Application Development
- Self-Protection to Autonomous System
- Machine Learning Application in Cybersecurity Domain

Thorough investigation on the most recent research works on chosen topic
- Existing Challenges, Other’s research approaches, their advantages and limitations.

Propose a research direction and justify your proposal.
Present the research findings in class

**Textbook and Reading Materials**
The primary text for this class is *Introduction to Computer Security*, Matt Bishop.

External reading materials will be made available via Canvas.

**Projected schedule of homework due dates, labs, quizzes, and tests:**
- There will be homework assignments and at least 2 lab projects.
- There will be assigned readings (mostly research papers) for each week and there will be pop up quizzes (or group discussions) about the readings.
- There will be 2 midterms and a final exam.

**Grading**
- 2 Tests .................................................. 30% for CS 4243, 20% for CS 5243
- Homeworks ............................................. 20%
- Quizzes, participation ................................. 10%
- Programs and labs ..................................... 20%
- Research presentation ..............................10% only for CS 5243
- Final exam .............................................. 20%

**Letter Grades**

Grade A (GPA 4.0): 90.0 – 100.0 %
Grade B (GPA 3.5): 80.0 – 89.9 %
Grade C (GPA 3.0): 70.0 – 79.9 %
Grade D (GPA 2.0): 60.0 – 69.9 %
Grade F (GPA 0.0): 0-59.9 %

*Grade will not be rounded up!*

**Attendance Policy**
Attendance is strongly encouraged, but not required. Students are responsible for any material covered in class. Some of the material covered in class will not be in the required textbook. Announcements about tests etc. will be made in class and/or Canvas. Students are also expected to regularly check their e-mails and Canvas.

**Collaboration Policy**
I expect you to learn from each other throughout the semester, and I encourage you to work with a diverse set of your classmates. We will complete many ungraded, in-class exercises, including discussing case studies. These exercises are designed to be completed collaboratively, where a small group of students would discuss and creatively analyze the security concerns and requirements for a variety of real and recent cases.

I also expect you to demonstrate your mastery of the material on quizzes, tests, and projects. All tests and quizzes are to be done independently, and they will be completed in class. Projects may be discussed with other students, however the work submitted must be your own work and reflect your understanding of the material. This means:
- you may not share code or assignment with other students (this includes copying-and-pasting, seeing others’ code/assignment, and letting others see your code/assignment).
- you may discuss ideas, syntax, online resources etc. with other students as long as you’re not looking at the same code/assignment.

*Students who do not comply with the described collaboration policy will receive a grade of F in the course. Furthermore, the case will be reported to the University Officials.*
**Communication medium:**

All notes, assignments and class announcements will be on Canvas. Contact the TA or instructor through email with any questions.

**Late submission penalty (without prior permission)**

1 calendar day late: 10% penalty - date based on submission
2 calendar days late: 20% penalty - date based on submission
3 calendar days late: 40% penalty - date based on submission
4 calendar days late: 60% penalty - date based on submission
5 or more calendar days late: 100% penalty - date based on submission

**Drop and Add Policy**

Students will be allowed to drop as long as the University permits them to do so. A grade of W or F will be determined on the basis of the points earned until that time.

**Academic Dishonesty/misconduct**

The Computer Science departmental policy for academic dishonesty and misconduct applies to this class. In addition, a student attempting to gain unfair advantage by keeping an examination paper longer than the time permitted is guilty of academic misconduct. Discussion of homework or lab assignments is encouraged, but students must work independently.

**Computer Usage**

The Computer Science departmental policy for computer usage applies to this class.

**Computer Policy**

Computers and other electronic devices such as cell phones may be used ONLY for legitimate classroom purposes, such as taking notes, downloading course materials, or working on an in class activity. E-mail, instant messaging, surfing the Internet, reading the news, or playing games are not considered legitimate classroom purposes; such inappropriate computer use is distracting to those seated around you and is unprofessional.

**Americans with disabilities act**

The Computer Science departmental policy for students with disabilities applies to this class. Anyone who has a need for examinations by special arrangements should see the instructor as the earliest possible opportunity during scheduled office hours.

**Ethics**

During the course of the semester, you will learn techniques and tools that can be used to compromise the security of computer systems and computer networks. It is very important that you never use these techniques or tools without the permission of the computer or network owner. You should never attempt to attack the computers or networks belonging to the computer science department, the university, a classmate, or the course staff. If a student unethically exploited a vulnerability, the student will fail the class.
Course Schedule (Subject to change if needed)

- Week 1: Computer Security overview
  - Computer security
  - Key security concept
  - Security terminology
  - Vulnerability-attack-threat-countermeasures
  - Importance of computer security
  - Recent cyber attack
- Week 2/3: Cryptography
  - Definition
  - Terminology
  - History and goals
  - Different types of cryptography
  - Encryption algorithms
  - Key management
  - Digital signature
- Week 4/5: Access Control and Authentication
  - Access control principles
  - Access control policies
  - Access control models
  - Authentication basics
  - Password
  - Biometric
  - Multi-factor authentication
- Week 6: Information Flow
- Week 7: Design principles
  - Least privilege
  - Separation of privilege
  - Open design
- Week 8/9/10: Attack
  - Attacks on Software
    - Attacks on privileged programs
    - Attacks through environment variables
    - Buffer overflow attack
    - Attack which does not require the stack (Return-to-libc attack)
    - Exploiting the format string vulnerability
    - Exploiting race condition vulnerability including the Dirty COW race condition
  - Web attacks
    - Cross-site scripting attack
    - SQL injection attack
  - Attacks on Networks
    - Packet sniffing and spoofing
    - Attacks on the TCP protocol
    - Firewall protection
    - Domain Name System attacks
    - Attacks on Public Key Infrastructures
- Week 11: Malicious logic and defense
- Week 12: Vulnerability analysis
- Week 13: Security assurance, auditing, and intrusion detection systems