CS 4243: Introduction to Computer Security
Fall 2021

Time:  1.30pm – 2.45pm Tuesday
      1.30pm – 2.45pm Thursday

Instructor:
Dr J. P. Thomas
email: jpt@cs.okstate.edu.
Office Hours: Send the instructor an email to set up a time to meet online.

Teaching Assistant:
Rahul Jamalapuram
email: rahul.jamalapuram@okstate.edu
Office Hours: Thursday: 6.00pm-7.00pm
Meeting over teams. A teams link will be sent to students.

Prerequisite:
Prerequisite: CS 3443 or equivalents
Knowledge of Programming

Course Description:
Overview of the components of computer and network security. Discussion of external processes required in secure systems, information assurance, backup, business resumption. Detailed analysis of security encryption, protocols, hashing, certification, and authentication.

Course Objectives:
This course provides an introduction to computer security. The course will cover a broad range of basic topics in security including cryptography, key management, authentication, design of secure systems, digital signatures, software security, web security and network security. Threats and attacks to computer systems will also be discussed. Protective mechanisms such as defensive programming will be presented.

Outcomes:
1. To understand the fundamental concepts of security.
2. To apply secure design principles to design secure systems
3. To implement defensive programming for secure systems
4. To understand and recognize threats and attacks on software, networks and the web
5. To provide countermeasures to threats and attacks
6. To explain the basic concepts of protecting systems using cryptography

Course Outline:
Topics to be covered

1. Introduction to Computer Security
2. Cryptographic Tools
3. User authentication
4. Access control
5. Database and data center security
6. Malicious software
7. Denial of service attacks
8. Intrusion detection
9. Firewalls
10. Software security – writing safe program code, Buffer Overflow attacks
11. Operating systems security
12. Internet security
13. Advanced encryption standard and stream ciphers
14. Public key cryptography
15. Legal and ethical issues

Textbook and other materials:
Material will be taken from a number of sources. These include:

- Computer Security, Matt Bishop, Addison-Wesley, 2019

Grading:

- Homework (*2): 30 marks
- Lab Assignments: 50 marks
- Quizzes (*3): 45 marks (15 marks for each quiz)
Dates - September 16th, October 14th, November 11th. These will be short 20-30 minute quizzes. Class will finish early on quiz dates and the remainder of the class time will be for the quiz

- Finals: 50 marks

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

**Letter Grades:**
Grade A: 90 - 100 %
Grade B: 80 – 89 %
Grade C: 70 – 79 %
Grade D: 60 - 69 %
Fail (Grade F): 0-59 %

**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.

**Late submission penalty:**
1 calendar day late: 50% penalty - date based on submission
2 calendar days late: 70% penalty - date based on submission
3 or more calendar days late: 100% penalty - date based on submission

**Collaboration Policy**

*Examinations/Tests:* No discussion of any kind (except with the instructor) is allowed. No access to any type of written material is allowed unless it is an open book test. 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.

*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 or 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.