CS 4243: Introduction to Computer Security
Fall 2019

Location: 317 Classroom Building

Time: 12.30pm – 1.45pm Tuesday
12.30pm – 1.45pm Thursday

Instructor*:*
Dr J. P. Thomas
email: jpt@cs.okstate.edu.
Office Hours: Tuesday: 11.00am-12.15pm
Office: 201 MSCS

Instructor has an "open-door" policy. If his door is open, you may stop by for a quick chat without making an appointment.

Teaching Assistant:
Likhitha Ramisetty
email: lramisetty04@gmail.com
Office Hours: Tuesday: 10.30am-11.00am, Thursday: 11.00am-12.00noon
Office: MSCS 227

Contact the TA by email to meet at an alternative time.

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, symmetric/public key encryption, authentication, design of secure systems, hash functions, digital signatures, software security, web security and network security.

Course Outline:

Topics to be covered

A. Overview of Computer Security

<u>Part I: Introduction to security protection mechanisms (4 weeks)</u>

B. Protection using Access Control Matrix
C. Introduction to Cryptography. Topics to be covered in outline include Data Encryption Standard and Advanced Encryption Standard, Public key cryptography, Cryptographic checksums such as HMAC and Digital signatures
D. Introduction to Key Management. Topics will include Key generation and exchange, Cryptographic key infrastructures, storing and revoking keys
E. Authentication mechanisms. This section will briefly describe password selection, Attacking passwords, Biometrics, Location based authentication and Multifactor authentication
F. Design of secure systems

<u>Part II – Vulnerabilities and attacks (11 weeks)</u>

G. Attacks on Software
    a. Attacks on privileged programs
    b. Attacks through environment variables
    c. Buffer overflow attack
    d. Attack which does not require the stack (Return-to-libc attack)
    e. Exploiting the format string vulnerability
    f. Exploiting race condition vulnerability including the Dirty COW race condition
H. Web attacks
    a. Cross-site scripting attack
    b. SQL injection attack
I. Attacks on Networks
    a. Packet sniffing and spoofing
    b. Attacks on the TCP protocol
    c. Firewall protection
    d. Domain Name System attacks
    e. Attacks on Public Key Infrastructures

Textbook:

Computer & Internet Security: A Hands-on Approach 2nd Edition, Wenliang Du, 2019
ISBN-13: 978-1733003926
ISBN-10: 1733003924

References (optional):

Computer Security: Art and Science, 2nd Edition by Matt Bishop, Addison Wesley, 2019
ISBN-13: 978-0-321-71233-2
ISBN-10: 0-321-71233-12

Grading:

- Homework = 20%
- Lab Assignments = 40%
- Quizzes (*4) = 20% (September 17th, October 8th, October 29th, November 19th)
- Finals = 20%

Communication medium:
All notes, assignments and class announcements will be on Canvas

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: 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

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.

[Acknowledgment: Course syllabus, lectures, and homework assignments inspired by Professor Eric Chan-Tin]