COMP 4/6410 Computer Security Fall 2018

Instructor: Denise Ferebee

Class Schedule: TR (DH 119) **Time: 05:30PM - 06:55PM**

Contact Information:

e-mail: dferebee@memphis.edu

COMP 4/6410: Course Description

Basic issues in computer security; confidentiality, integrity, availability, trust; basic methods and protocols in cryptography, digital signature, authentication, bit commitment; security in computing, programs, databases, operating systems; secure communication, secure channel, public key infrastructure, certification; security policies, digital evidence, forensics tools; monitor and response; legal and ethical issues; risk management, security administration.

PREREQUISITE: COMP 3825, or permission of instructor.

Why this course?

The course is intended to provide basic state-of-the-art knowledge about risks, security and protection issues in computer, data communication, and cyber world. Students will learn the basic notions and importance of computer security. While the foundations of the subject will be thoroughly reviewed, actual practices to cope with increasing concerns about data protection, code execution will be emphasized. These include, in particular, study of some of the standard cryptosystems, protocols, and security strategies in access to devices and shared computing resources. There will also be some discussion on the evolving legal and ethical issues with new information technologies in society.

Textbook:

Principles of Information Security , 6th Edition
Michael E. Whitman; Herbert J. Mattord
ISBN-10: 1-337-10206-7
ISBN-13: 978-1-337-10206-3

Reference Books:

- Erickson, Jon. "Hacking: The Art of Exploitation, 2nd Edition"
- The Web Application Hacker's Handbook: Discovering and Exploiting ... Book by Dafydd Stuttard and Marcus Pinto
- The Shellcoder's Handbook: Discovering and Exploiting Security Holes Book by Chris Anley
- Security Engineering, Ross Anderson, Second Edition, John Wiley & Sons, 2001
- Corporate Computer and Network Security (2nd Edition) by Raymond Panko, 2009 (http://pankosecurity.com/?vbookid=454)

- Introduction to Computer Security by Michael Goodrich and Roberto Tamassia (Oct. 25, 2010)
- Network Security Fundamentals, Mark Ciampa, 2014

Other Resources (hyperlinks checked on 8/18/2017):

- Security, Usenix Security Symposium
- Crypto, International Cryptology Conference
- OWASP Top Ten Project (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)
- Phrack (http://phrack.org/issues/69/1.html)
- https://www.corelan.be/
- https://www.reddit.com/r/netsec/
- https://www.offensive-security.com/community-projects/
- http://www.securitytube.net/
- https://nmap.org/book/nse.html

Evaluation:

Students are expected to participate in class discussions. Participation in class will be viewed as a continuous two-sided feedback process, which (a) allow students to assess themselves on their progress in learning the material/understanding the security issues; and (b) allows the instructor to assess how well he is fostering the communication process with and among students. Good evaluations will thus reflect not only your grasp of the material, but also how well you take advantage of the class time and how well you end up using the knowledge in securing your systems. The evaluation process will include paper presentations, assignments, tests, quizzes, and a term paper/project to make sure that you have integrated the material into your general practice of secure computing.

Your final grade for the course will be based on the grades in the following course-related activities (given in percentages):

Class Participation	10%(15% COMP 4410)
Homework	15%
Quizzes	20%
Midterm	20% (25% COMP 4410)
Final Exam	20% (25% COMP 4410)
Paper/project + proposal	15% (COMP 6410 only)

Graduate students (COMP 6410) have to do some additional works which include paper presentation, project, etc.

Grading Scale:

A+	95.1-100	**B+**	85.1-88	**C+**	76.1-79	**D+**	60.1-66
A	90.1 -95	**B**	82.1-85	**C**	70.1-76	**D**	50 - 60
A-	88.1 -90	**B-**	79.1-82	**C-**	66.1-70	**F**	< 50

Course Policies:

Students are expected to attend all scheduled classes and submit assignments on time. If you miss a class, it is your responsibility to obtain the notes for the missed class from classmates, check course website and catch up on the course content. There will be no make up test for this course.

Any student who anticipates physical or academic barriers based on the impact of a disability is encouraged to speak with me privately. Students with disabilities should also contact Disability Resources for Students (DRS) at 110 Wilder Tower, 901-678-2880. DRS coordinate access and accommodations for students with disabilities.

Ethical behavior is an important part of this course. Since some of the methods, codes and tools that will be discussed and experimented in the course can be very harmful, if abused, it is expected that students will behave in a responsible fashion. In particular, always ask your local site administrator for permission before experimenting with security-related tools. In-class discussions of techniques for exploiting potential security threats and risks **do not** imply to use them! You will be sole responsible for any such violation.

Plagiarism/Cheating Policy:

"Plagiarism or cheating behavior in any form is unethical and detrimental to proper education and will not be tolerated. All work submitted by a student (projects, programming assignments, lab assignments, quizzes, tests, etc.) is expected to be a student's own work. The plagiarism is incurred when any part of anybody else's work is passed as your own (no proper credit is listed to the sources in your own work) so the reader is led to believe it is therefore your own effort. Students are allowed and encouraged to discuss with each other and look up resources in the literature (including the internet) on their assignments, but appropriate references must be included for the materials consulted, and appropriate citations made when the material is taken verbatim.
If plagiarism or cheating occurs, the student will receive a failing grade on the assignment and (at the instructor's discretion) a failing grade in the course. The course instructor may also decide to forward the incident to the Office of Student Conduct for further disciplinary action. For further information on U of M code of student conduct and academic discipline procedures, please refer to: http://www.memphis.edu/studentconduct/misconduct.htm"

"Your written work may be submitted to Turnitin.com, or a similar electronic detection method, for an evaluation of the originality of your ideas and proper use and attribution of sources. As part of

this process, you may be required to submit electronic as well as hard copies of your written work, or be given other instructions to follow. By taking this course, you agree that all assignments may undergo this review process and that the assignment may be included as a source document in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents. Any assignment not submitted according to the procedures given by the instructor may be penalized or may not be accepted at all." (Office of Legal Counsel, October 17, 2005).

Tentative schedule *(topics to be covered and other course-related activities during the semester)*:

Weeks	*Chapters/Topics*	*Quizzes or Tests*
1	1: Introduction to Information Security	
2	2: The Need for Security	
3	3: Legal, Ethical, and Professional Issues in Information Security	
4	4: Planning for Security	Quiz 1: Topics 1 - 3
5	5: Risk Management	
6	6: Security Technology: Firewalls, VPNs, and Wireless	Quiz 2: Topics 4 - 5
7	7: Security Technology: Intrusion Detection and Prevention Systems and Other Security Tools	
8	Review	Mid-term Exam
9	8: Cryptography	
10	9: Physical Security	Quiz 3: Topics 7 - 8
11	10: Implementing Information Security	
12	11: Security and Personnel	Quiz 4: Topics 9 - 10
13	12: Information Security Maintenance and eDiscovery	
14	Review	
15	Final Comprehensive Written Exam	

Project/Presentation Tentative Notes:

NOTE 1: Each paper presentation will be of 15 minutes long. Students have to submit the presentation material (put in elearn ***dropbox****) one day before their presentation date.*
NOTE 2: Each project is due on the next assignment date (i.e. project 1 is due on October 12th and so on).
NOTE 3: There will be a term paper/project, individual student or a group consisting of two members (both members need to actively participate in Project Demo).
NOTE 4: We will be using eCourseware for lecture notes, grades and all submissions. If I need to communicate with the class as a group, I'll be using elearn. You may need to check your email regularly.