CSC 495/583: Topics in Computer Security

Professor: Si Chen

Email: schen@wcupa.edu

Office: UNA 142 (25 University Ave.)

Course Website: https://www.cs.wcupa.edu/schen/security/

Office Hours:

Monday/Wednesday 1:00-3:00 PM
Thursday 5:40 – 6:40PM

Note: Office hours may have to be temporarily or permanently changed.
Please email me in advance when you plan to come.
Please also briefly classify the problem or your concern in your email.

Expected Background:

- Basic programming concepts (e.g. complete Java I, II)
- Knowledge with the C programming language, including pointers, arrays, loops, function calls, etc.

Required Textbook: None

Bibliography (not required):

- Randal E. Bryant, Davie Richard O'Hallaron, *Computer Systems: A Programmer's Perspective*, 3rd Edition, ISBN 978-0134092669
- Kris Kaspersky, *Hacker Disassembling Uncovered*, 2nd Edition, ISBN 978-1931769648
- Eldad Eilam, *Reversing: Secrets of Reverse Engineering*, 1st Edition, ISBN 978-0764574818.

Course Description: Topic in computer security to be announced at time of offering.

Grading policy:

1.Attendance	10%	**See CLASS ATTENDANCE POLICY**
2.Reading Questions	30%	Three reading questions, 10 points per assignment
3.Labs	30%	Five Reverse Engineering Lab (6 points each)
4.Final Project	30%	Group Project

Note: No credit for unexcused late assignments.

ABET ACCREDITATION PROGRAMMATIC STUDENT LEARNING OUTCOMES

http://www.cs.wcupa.edu/curriculum/objectives.html

(depends on topic – this is what was used in Fall 2017 in CSC495)

(a) An ability to apply knowledge of computing and mathematics appropriate to the discipline.

(d) An ability to function effectively in teams to accomplish a common goal.

(i) An ability to use current techniques, skills, and tools necessary for computing practices.

(j) An ability to apply mathematical foundations, algorithmic principles, and Computer Science theory in the modeling and design of computer-based systems in a way that demonstrates comprehension of the tradeoffs involved in design choices.

(n) All Computer Science majors will demonstrate proficiency in the latest, cutting-edge technology.

Course Student Learning **Outcomes (SLO's) & Links to Program SLO's (a, d, , i, j, n) & Evaluation Types (1, 2, 3)**

The students will be able to:

- Understand important topics of software security. **Program SLO: a. Evaluation Type: 2**
- Design, implement and evaluate a secure network system. **Program SLO's: i, j. Evaluation Types: 3, 4**
- Apply mathematical foundations, algorithm principles, and computer science theory in topics such as cryptographic operations and security architecture. **Program SLO's: i, j. Evaluation Types: 3, 4**
- Work effectively both independently and in teams through hand-on lab activities and team projects. **Program SLO: d. Evaluation Types: 3, 4**
- Find technical information from the web and other sources when they do assignments and project. **Program SLO's: n. Evaluation Type: 3,4**

Grading Table

- The following table shows how letter grades in the course will be assigned based upon the total number of points earned:

Grade	Points earned	Interpretation
A	93-100	Excellent
A-	90-92	
B+	87-89	Good
B	83-86	
B-	80-82	
C+	77-79	Fair
C	73-76	
C-	70-72	
D+	67-69	Poor
D	63-66	
D-	60-62	
F	<60	Failure

Course Outline: (this topic is the one offered in Fall 2017 in CSC495: Software Security)

This topic is primarily aimed at people interested in software security, reverse engineering and low-level software. Below is a listing of some of the topics discussed throughout this course, with approximately 3 topics presented every 2 weeks, so that a sufficient number of evaluations will be made prior to the withdrawal deadline.

- The legal aspects of reverse engineering.
- Assembly language for IA-32 compatible processors and how to read compiler-generated assembly language code.
- The general principles behind malicious software and how reverse engineering is applied to study such program.
- IA-32 Register, Byte Ordering, x86 ASM, Stack
- Stack Frame, Calling Convention
- System Call

- Stack Overflow
- StackGuard
- Format String Bug
- Return-oriented programming (ROP)
- Web Security: SQL Injection, Upload Hacking, Session Hijacking, XSS, CSRF
- Heap Exploitation
- Internet of Things (IoT) Security
- Mobile Application Security
- Web Browser Security
- Anti-Virus & Detection Techniques
- Secure Systems & Hacking Game Consoles
- Malware
- Side Channel Attack
- Authentication
- Kernel Exploitation
- The Future of Software Security: AR security, Blockchain security

Study Guidelines:

- The topic and paper explained in class are related to your reading question. Please keep it.
- Do assigned reading question. If you have any problems, please first check the examples and methods in your notes. If still cannot solve it, e-mail me or come to UNA 142 during the office hour.
- For the final project, creative solution is always welcome.

Class Attendance Policy:

Being present includes your on-time, prepared presence. Being present also means handing in your assignments on time and demonstrating effort and engagement with the class and group work. Absence from class, having computer problems, running out of printer paper, etc., does not excuse a late assignment. Please assume technology, transportation, and your health may get in your way at every turn and plan accordingly.

Unexcused late arrivals / leaving early (15 minutes) are an **unexcused absence**. Notify your professors of **ANY** absence to see if they can be excused.

Each unexcused absence > 1 reduces your course grade by 2 points; non-participation, including not completing non-credit homework, engaging in non-class activities, conversing during lectures, etc., reduces your course grade by 2 points each.

Absences cannot be used as the sole criterion for assigning a final grade in a course. The complete university excused absence policy may be found at: https://www.wcupa.edu/viceProvost/capc/policies.aspx#E

Disabilities:

If you have a disability that requires accommodations under the Americans with Disabilities Act (ADA), please bring me your letter of accommodations and meet with me as soon as possible, so I can support your success in an informed manner. Sufficient notice is needed in order to make the accommodations possible. If you would like to know more about West Chester University's services for students with disabilities, please contact the Office of Services for Students with Disabilities at 610-436-3217. You can find out more information at www.wcupa.edu/ussss/ossd.

Academic Honesty:

The Computer Science Department has adopted the following policies in regard to academic dishonesty in Computer Science classes:

- A student found to be cheating in an assignment will receive zero for that assignment if it is his first offense in that class, but an F for the course if it is for his second offense in that class.
- A student found to be cheating in a test will receive the grade of F in that class.
- For the purposes of this document on cheating, every form or method of evaluation in a class will be considered as being of one of two types: an assignment or a test. Assignments include homework assignments, and short quizzes. Tests include final exams and major exams. An instructor has, subject to these guidelines, the discretion to determine the type of any other form of evaluation, such as a project, in his class.
- The term cheating is used throughout in the sense provided by the rules and regulations of West Chester University. (The following is taken from The Ram's Eye View of 1988-89.)

Cheating includes but not limited to:

- Plagiarism that is copying another's work or portions thereof and/or using ideas and concepts of another and presenting them as one's own without giving proper credit to the source.
- Submitting work that has been prepared by another person.
- Using books or other material without authorization while taking examinations.
- Taking an examination for another person, or allowing another person to take an examination in one's place.
- Copying from another's paper during an examination or allowing another person to copy from one's own.
- Unauthorized access to an examination prior to administration.

A student who has received the grade of F in a course because of cheating and who wants or is required to repeat that course may re-take that course only as a regularly scheduled course that is open to the student community in general. In exceptional circumstances, this condition may be revoked, but only by an explicit action to that effect by the full Computer Science Committee, and only then on a case by case basis.

Excused Absences Policy For University-Sanctioned Events:

Students are advised to carefully read and comply with the excused absences policy for university-sanctioned events contained in the WCU Undergraduate Catalog. In particular, please note that the "responsibility for meeting academic requirements rests with the student," that this policy does not excuse students from completing required academic work, and that professors can require a "fair alternative" to attendance on those days that students must be absent from class in order to participate in a University-Sanctioned Event.

Reporting Incidents Of Sexual Violence:

West Chester University and its faculty are committed to assuring a safe and productive educational environment for all students. In order to meet this commitment and to comply with Title IX of the Education Amendments of 1972 and guidance from the Office for Civil Rights, the University requires faculty members to report incidents of sexual violence shared by students to the University's Title IX Coordinator, Ms. Lynn Klingensmith. The only exceptions to the faculty member's reporting obligation are when incidents of sexual violence are communicated by a student during a classroom discussion, in a writing assignment for a class, or as part of a University-approved research project. Faculty members are obligated to report sexual violence or any other abuse of a student who was, or is, a child (a person under 18 years of age) when the abuse allegedly occurred to the person designated in the University protection of minors policy. Information regarding the reporting of sexual violence and the resources that are available to victims of sexual violence is set forth at the webpage for the Office of Social Equity at http://www.wcupa.edu/_admin/social.equity/.

Emergency Preparedness:

All students are encouraged to sign up for the University's free WCU ALERT service, which delivers official WCU emergency text messages directly to your cell phone. For more information, visit www.wcupa.edu/wcualert. To report an emergency, call the Department of Public Safety at 610-436-3311.

Electronic Mail Policy:

It is expected that faculty, staff, and students activate and maintain regular access to University provided e-mail accounts. Official university communications, including those from your instructor, will be sent through your university e-mail account. You are responsible for accessing that mail to be sure to obtain official University communications. Failure to access will not exempt individuals from the responsibilities associated with this course.