CSC 495/CSC 583: Advanced Topics in Computer Security

Modern Malware Analysis

Instructor: Si Chen

Email: schen@wcupa.edu

Office: UNA 142 (25 University Ave.)

Course Website: **https://www.cs.wcupa.edu/schen/csc497/**

Office Hour:

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.

Class Schedule:

CSC 497 **CSC 583**	TuTh 4:25PM - 5:40PM	Anderson Hall 211

Course Contents:

Malware is a catch-all term for various malicious software, including viruses, adware, spyware, browser hijacking software, and fake security software.
Once installed on your computer, these programs can seriously affect your privacy and your computer's security. For example, malware is known for relaying personal information to advertisers and other third parties without user consent. Some programs are also known for containing worms and viruses that cause a great deal of damage. As a result, the ability to detect, analyze, understand, control, and eradicate malware is an increasingly important issue of economic and national security.

This course will introduce students to modern malware analysis techniques through lectures and hands-on interactive analysis of real-world samples, including explore various recent attacks. These examples and studies will help the students develop a foundation and a well-rounded view of cybersecurity research. Participants in the course will also read and discuss research papers, as well as conduct independent project in a topic related to cyber risk and malware analysis.

After taking this course students will be equipped with **the skills to analyze advanced contemporary malware using both static and dynamic analysis**.

Textbook / Other Materials

No Textbook

Reference book:

1. Michael Sikorski, Andrew Honig, *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*, 1st Edition, ISBN 978-1593272906

GRADING POLICY

A[90-100], B[80-89], C[70-79], D[60-69], F[0-59]

Attendance	10%	**See CLASS ATTENDANCE POLICY**
Lab	40%	5 Malware Analysis Lab, 8 points per assignment
Reading Questions	30%	5 Reading Questions, 6 points per assignment
Presentation	20%	Group Presentation on selected topic

Note: No credit for unexcused late assignments.

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.

Expected Background

No prerequisite for graduate students, although sufficient security background is expected. For undergraduate students, please make sure you **completed CSC 242** or check with the instructor.

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.

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.