CSC 471: Modern Malware Analysis

Dr. Si Chen

Spring 2022

E-mail: schen@wcupa.edu
Class Website: [Link]
Class Discord: https://discord.gg/wsg4wCwfdT
Office Hours: MW 12:00PM - 2:00PM, F 10:00AM - 11:00AM

West Chester University's COVID-19 Classroom Protection Requirements

We, as a community of educators and learners, should work together to create a culture that protects our most precious resource: each other. As such, it is the expectation of all members of the University community to continue to do their part to protect the health and safety of others. In our classrooms where the university's primary function is carried out, the following protocols are being implemented:

- Unless otherwise directed by the faculty member, **students must wear a cloth or disposable face mask that covers both the nose and mouth the entire time they are in class**.
- Face shields and gaiters **do not** meet the university's mask requirement.
- Eating and drinking in the classroom are only permitted if they are medically necessary. And please work with the Office of Services for Students with Disabilities to notify the university and your professors of this necessity.

We want you to succeed in this class, but we will have to ask you to leave if you do not follow these guidelines, so please – make the most of this opportunity and help keep our campus safe.

Course Modality (Spring 2022)

In-person class

All class are **in-person** and you **cannot** attend it virtually (except the first two weeks). But I am posting *my slides with (some of) my last year's videos recordings* onto our class website before each lecture. So if you misses a few classes, you can keep up with the content this way.

Virtual (Zoom) Office Hours

My office hours will be Monday/Wednesday from 12:00 PM - 2:00 PM, Friday from 10:00 AM - 11:00 AM, and you can reach me via Zoom. My Zoom URL: **[Link]**. Zoom Meeting ID: **712 131 7214** and Passcode: **cs2020**

Discord Server

We have a class Discord server (https://discord.gg/wsg4wCwfdT). Feel free to join this server to directly talk with me and discuss with the other 471 students. You can ask questions about lectures, homework, etc.

Course Description

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

Enrollment Requirements: CSC 471 requires prerequisites of CSC 231

Because this course is 400-level, it should be designed as advanced. I expect that the class population will be mostly composed of juniors and seniors. My expected demographic for Software Security was students with zero reverse engineering experience. That said, to be able to take this course you will probably need at least the following skills:

- Basic programming concepts
- Knowledge with the C programming language, including pointers, arrays, loops, function calls, etc.
- Familiar with Unix/Linux including the command-line shell and gdb
- Familiar with Intel x86 assembly language and architecture
- Familiar with web programming concepts (HTML, HTTP, TCP, network communications)

Credits: 3

Textbook

Required Textbook

No Textbook

Reference Books

- Monnappa K A, Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware , ISBN 978-1788392501
- Michael Sikorski, Andrew Honig, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, 1st Edition, ISBN 978-1593272906

Course Outcomes

The student outcome of this course includes:

Course Outcomes	Program Outcomes
Student understand how to mitigate certain type of real-world malware attack	(1)*
Student is able to perform static/dynamic analysis using forensics tools (e.g. Volatility) to find system malware and prevent attacks.	(1)*

*(1): Implement secure measurements to protect networks, secure electronic assets, prevent attacks, ensure privacy, and build secure infrastructures that respect ethical principles

Required Hardware

A computer with modern OS (e.g. Windows/ MacOS/ Linux) which can connect to the Internet. We will utilize the Dr. Si Chen's Badger server which hosted in the CS laboratories throughout the semester. You can connect it by using Remote Desktop or Secure Shell (SSH). Credentials / Walkthroughs will be provided to you.

Course Outline

- The legal aspects of malware analysis
- Assembly language for IA-32 compatible processors and how to read compiler-generated assembly language code.
- DLL Injection
- Static Analysis
- PE Format

- Dynamic Analysis
- Hooks
- IAT, IAT Hooks
- Anti-virus Software
- Dynamic Heuristic Analysis
- API Hook
- Rootkit

Programming Language & Tools

The programming language we chose for this course is Python. You'll use Python to create several malware detection programs.

All the assignments (program projects) will be submitted to D2L.

Grading Policy

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

Attendance	**5%**	
Lab	**50%**	5 Malware Analysis Lab
Group Presentation	**15%**	1 Group Presentation
Group Project	**30%**	1 Group project on selected topic

Note: No credit for unexcused late assignments.

ABET ACCREDITATION PROGRAMMATIC STUDENT LEARNING OUTCOMES

- (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.
- (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

Course Policies

ATTENDANCE POLICY

Please stay at home and do not go to class if you are feeling ill.

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.

LATE ASSIGNMENTS POLICY

Late assignments will be accepted for **no penalty** if a valid excuse is **communicated to the instructor before the deadline**. No credit for unexcused late assignments.

ACCOMMODATIONS FOR 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 INTEGRITY AND 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

I. Students participating in University-sanctioned events such as, but not limited to, the Marching Band and NCAA athletic events, will be granted an excused absence(s) by the respective faculty members for class periods missed. Students will be granted the privilege of taking, at an alternative time to be determined by the professor, scheduled examinations or quizzes that will be missed. The professor will designate such times prior to the event and the make-up should be as soon as possible following the missed class. Professors can provide a fair alternative to taking the examination or quiz that will be missed. Students must recognize that some activities cannot be directly made up (e.g., a laboratory, group presentation, off-campus experience), and faculty will arrange a fair alternative to the missed work. Students must submit original documentation

on University letterhead signed by the activity director, coach, or adviser detailing the specifics of the event in advance. Specific requirements include the following:

- Responsibility for meeting academic requirements rests with the student.
- Students are expected to notify their professors as soon as they know they will be missing class due to a University-sanctioned event.
- Students are expected to complete the work requirement for each class and turn in assignments due on days of the event prior to their due dates unless other arrangements are made with the professor.
- If a scheduled event is postponed or canceled, the student is expected to go to class.
- Students are not excused from classes for practice on nonevent days.

The following are specifics for the student athlete:

- The student athlete is expected, where possible, to schedule classes on days and at hours that do not conflict with athletic schedules.
- Athletes are not excused from classes for practice or training-room treatment on non-game days.

II. West Chester University recognizes required (non-voluntary) service in the United States military including the Pennsylvania National Guard as a legitimate reason to miss up to the equivalent of 2 weeks during a 15-week semester. Service members must submit a copy of their orders to the Registrar's Office. The Registrar's Office will communicate with respective faculty members and the student will be granted an excused absence(s) for the class periods missed. All points covered in part I of this policy including make-up work and specific requirements 1-4 also apply. Service members required to miss more than the equivalent of 2 weeks during a 15-week semester can withdraw from the term in a non-punitive manner in accordance with Pennsylvania state law. Students are expected to work closely with faculty and the Registrar's Office to ensure their academic success. Students in programs with external accrediting bodies must also be aware that there may be attendance requirements that cannot be made up. III. In the event of a student's unplanned medical emergency, including serious health conditions as outlined in the Family and Medical Leave Act, or the death of a student's immediate family member, faculty members are expected to provide, within reason, an opportunity for students to make up work. Students are responsible for providing proper documentation and will work with respective faculty members to make up course work as described in part I of this policy. Students are encouraged to contact the Assistant Dean of Students and refer to the website on Student Assistance for additional information. IV. Consistent with guidelines set forth by the Family and Medical Leave Act, students who become parents of new children or have children with serious health conditions that require the student-parent to miss up to the equivalent of 2 weeks during a 15-week semester shall be given an excused absence for the courses that are missed. Students will work with respective faculty members to make up course work as described in part I of this policy. Students required to miss more than the equivalent of 2 weeks during a 15-week semester can withdraw from the term up until the term-withdraw deadline. Students required to miss more than one semester should also refer to Admissions policy on consecutive non-enrollment. Students are encouraged to contact the Assistant Dean of Students and refer to the website on

Student Assistance for additional information. V. West Chester University recognizes excused absences in accordance with federal and state legal statutes including but not limited to compliance with jury duty, subpoenas, and notices of deposition. Such excused absences will be dealt with as described in part I of this policy.

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.

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 **http://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.

APSCUF

I am a member of APSCUF, the Association of Pennsylvania State College and University Faculties. We uphold the highest standards of teaching, scholarly inquiry, and service. We are an organization that is committed to promoting excellence in all that we do to ensure that our students receive the highest quality education. For more on our organization, see www.apscuf.org.