CSC 471: Modern Malware Analysis

Dr. Si Chen

Spring 2024

E-mail:	schen@wcupa.edu
Class Website:	[Link]
Office Hours:	Monday 10:00 AM - 12:00 PM
	Wednesday 10:00 AM - 12:00 PM
	Thursday 12:15 PM - 1:15 PM

Course Description

Malware, a term used to describe various types of malicious software, poses a significant threat to both personal privacy and computer security. This can include viruses, adware, spyware, browser hijacking software, and fake security software. When installed on a computer, these programs can relay personal information to third parties without user consent, and may also contain worms and viruses that cause significant damage. As a result, the ability to detect, analyze, understand, control, and eradicate malware is becoming a crucial issue in both economic and national security.

This course aims to provide students with a comprehensive understanding of modern malware analysis techniques through lectures and hands-on interactive analysis of real-world samples. This includes exploring various recent attacks to develop a foundation and well-rounded view of cybersecurity research. Participants will also read and discuss research papers, and conduct an independent project on a topic related to cyber risk and malware analysis.

Upon completion of the course, students will be equipped with the skills to analyze advanced contemporary malware using both static and dynamic analysis methods. This knowledge will enable them to effectively detect, understand, and mitigate the impact of malware threats.

Enrollment Requirements: CSC 471 requires prerequisites of 1. (CSC 302) and 2. (CSC 231 or CSC 242)

As a 400-level course, this offering is intended for advanced students. The class is expected to primarily consist of juniors and seniors. In terms of prerequisites, it is assumed that students enrolled in Malware Analysis have no prior experience with reverse engineering. However, in order to be successful in this course, it is recommended that students possess 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

Required Hardware

In order to fully participate in this course, students will need to have access to a computer with a modern operating system (such as Windows, MacOS, or Linux) that is capable of running VirtualBox software. Additionally, students will be required to use Dr. Si Chen's Badger server, which is hosted in the CS laboratories, later in the semester. Connections to the server can be made through Remote Desktop or Secure Shell (SSH), and credentials and instructions will be provided to students.

Topics Outline and Tentative Schedule

The weekly schedule will be posted on our class website.

#	Topic	Homework
Week 1	Introduction	
Week 2	Basic Concepts, DLL Injection (1)	
Week 3	DLL Injection (2), Static Analysis, PE Format	Lab1: "Hello World" – DLL Injection
Week 4	PE Format, Static Analysis: Real-world Case Study	Lab2: Build a heuristic malware detection system
Week 5	Assembly and disassembly primer, IAT, EAT	
Week 6	Stack	
Week 7	Stack Frames	Lab3: Stack and Stack Frame in Linux
Week 8	Dynamic Analysis	
Week 9	Hooks	Lab 4: Build a Dynamic Heuristic Analysis Tool for Detection of Unknown Malware
Week 10	IAT, IAT Hooks	
Week 11	Anti-virus Software, Dynamic Heuristic Analysis	
Week 12	API Hook, Stealth process (Rootkit)	
Week 13	Kernel Mode Rootkit	Lab 5: Stuxnet
Week 14	Kernel Forensics	Final Project
Week 15	Group Presentation	

- 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 selected for this course is Python. Students will utilize Python to develop a variety of malware detection programs. All assignments and program projects will be submitted through the course's D2L site.

Grading Policy

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

Attendance	**10%**	
Lab	**50%**	5 Malware Analysis Lab
Group Presentation	**15%**	1 Group Presentation on selected paper
Group Project	**25%**	1 Group project on selected topic

Note: No credit for unexcused late assignments.

Course Policies

EXCUSED ABSENCES POLICY

Students are advised to carefully read and comply with the excused absences policy, including absences 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.

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.

Program Learning Outcome (PLO)

- (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.

Computer Science Program (ABET) Outcome

- ABET-1: Analyze a complex computing program and to apply principles of computing and other relevant disciplines to identify solutions
- ABET-2: Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline
- ABET-5: Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline

Course Outcomes (CO)

Students will be able to perform the following after completing this course:

- Student is able to perform static/dynamic analysis system malware. (Lab 1, Lab 3, Lab 5) (PLO-a, i, n) (ABET-1)
- Student is able to build anti-malware system. (Lab 2, Lab 4) (PLO-a,i,n) (ABET-2)
- Student is able to work as team and use forensics tools (e.g.,Volatility) to analysis kernel-level rootkit. (Final Project) (PLO-a,d,i,n) (ABET-5)
- Student understand how to mitigate certain type of real-world malware attack. (Lab 1, Lab 2, Lab 4) (PLO-a,i,n) (ABET-2)

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.

ABOUT CHATGPT AND OTHER LLM TOOLS

At present (2024), the use of ChatGPT and other LLM AI tools are permitted in this course for the purpose of enhancing lab/project reports and presentation slides. However, it should be noted that malware analysis requires specialized tools and techniques such as the use of sandboxes, disassembly, and reverse engineering. ChatGPT is not designed to perform these types of tasks and should not be considered a replacement for specialized malware analysis tools. Additionally, ChatGPT is a model that is trained on a large corpus of text data, and does not possess the capability to analyze code or execute it.

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.