CSC 497/583: Topics in Computer Security

M 7:15 PM – 10:00 PM
Anderson Hall 211

Instructor:	Dr. Si Chen
Office:	UNA 142 (25 University Ave.)
Office Hours:	Tuesday 12:00 - 3:30 PM Wednesday 1:15 – 2:45 PM -- or by appointment.
Email:	schen *at* wcupa *dot* edu
Phone: ***(don't** call, email!)*	610-436-6998

Email will get a faster response (usually within 24 hours) for questions, appts, etc. Only use the phone for emergencies when you have no access to email.

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.
Prerequisites: CSC242
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 Malware Analysis 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

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

Required Text:

1. **No Textbook**

Reference book:

- 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:

We will utilize the West Chester University CS laboratories throughout the semester. Credentials will be provided to you.

ABET ACCREDITATION PROGRAMMATIC STUDENT LEARNING OUTCOMES

http://www.cs.wcupa.edu/curriculum/objectives.html
(depends on topic – this is what was used in Spring 2019in CSC497)

(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 Outline: (this topic is the one offered in Spring 2019 in CSC497: Topics in Computer Security)

- The legal aspects of malware analysis.
- 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

- DLL Injection
- Static Analysis
- PE Format
- NT Header, IAT, EAT
- Dynamic Analysis
- Heuristic Analysis
- Hooks
- API Hook
- Stealth process (Rootkit)
- Kernel Mode Rootkit
- Dynamic Heuristic Analysis
- Anti-Virus & Detection Techniques
- Classic Malware Analysis (Stuxnet)
- Introduction to Volatity
- The Future of Malware: IoT Malware, AR Malware

Required Software:
All software will either be free to download or provided to you.

Evaluation Policy:

Attendance	**10%**	**Please check CLASS ATTENDANCE POLICY**
Lab	**50%**	**5 Malware Analysis Lab, 10 Points per assignment**
Reading Questions	**20%**	**4 Reading Questions, 5 Points per assignment**
Presentation	**20%**	**Group Presentation on Selected topic**

Grade Scale:

Number	100-93	92-90	89-87	86-83	82-80	79-77	76-73	72-70	69-67	66-63	62-60	<= 59
Letter	A	A-	B+	B	B-	C+	C	C-	D+	D	D-	F

Lateness Policy:
Assignments that are late are assessed a **10% per day late penalty**. Saturday and Sunday are each days.

Warning to Students!
This is a challenging class. If you do not have the time or energy to dedicate to performing the work for this class, you should not enroll. The requirements for this class will not be reduced no matter how much other work you encounter in other classes that you may be enrolled in.

Phone Policy:
If you let your phone ring during class, you will see your final grade diminish at my discretion. Turn your phone on silent before class begins, not on low or vibrate. It is distracting to your classmates. If you choose to text during class, you will see your grade diminish at my discretion. If you choose to answer your phone during class, you will lose 5% off of your final average. *If you have an emergency situation, please discuss it with me in advance.* Phones are not permitted to be out during exams. If your phone is taken out during an exam, you will receive a 0 for the exam.

Attendance Policy:
You are allocated **two** *unexcused* absences. Each class that you miss thereafter due to an unexcused absence is one point off your final grade. Being late twice is the same as one absence. Sleeping in class is the same as being absent. If you miss a class, you are responsible for getting the notes from one of your classmates.

Absences due to serious illness or family emergencies will be considered *excused*, and will not impact your attendance grade. Be sure to email me and provide documentation. Being in jail, having to go to court to avoid jail, family vacations, etc. are not excusable absences. I reserve the right to determine what is "excused" versus "unexcused".

University Sanctioned Events Policy:
Students participating in participating in University sanctioned events such as, but not limited to, the Marching Band, musical ensembles, theatre group, athletic events, forensics competition, etc., will be granted an excused absence 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. I will designate such times prior to the event and reserve the right to provide a fair alternative to taking the examination or quiz that will be missed. 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:

1. Responsibility for meeting academic requirements rests with the student.
2. Students are expected to notify their professors as soon as they know they will be missing class due to a University sanctioned event.
3. 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 myself.
4. If a scheduled event is postponed or canceled, the student is expected to go to class.
5. Students are not excused from classes for practice on nonevent days.

The following are specifics for the student athlete:

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

Email 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.

Please abide by the following email etiquette policies to ensure clear communication:

Subject Line: Please include a descriptive and specific subject heading for all of your emails, including course and section number (e.g. "CSC 050-23: Question about lab 1").

Greeting: Please make a clear and appropriate greeting; I will not answer emails addressed to "hey" or "yo". Please address me as Dr. Chen or simply "Professor".

Tone & Style: Always use a tone and language that is appropriate to an academic setting; I will not respond to emails that are written in short-hand or without proper punctuation and grammar. Your emails should not resemble a text message.

Sign and Proofread: Always sign your full name, especially if you are writing from your smart phone. Always proofread your emails before sending.

Email Account: I do not care which email account you send email from, as long as it is clearly addressed and signed so that I know who you are. But please be advised to appropriately link the email that you wish to use with myWCU and D2L; I will be using those services to send out emails to the entire class. It is your responsibility to make sure this is configured correctly so that you receive my emails.

Computer Science Department Dishonesty Policy:

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

1. A student found to be academically dishonest in an assignment will receive zero for that assignment if it is his/her first offense in that class [the course, not the class period], but an **F** for the course if it is for his/her second offense in that class [the course].
2. A student found to be academically dishonest in a test will receive the grade of **F** in that class [the course].
3. For the purposes of this document on academic dishonesty, 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 [and labs]. 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/her class.

4. A student who has received the grade of F in a course because of academic dishonesty 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.
5. The term academic dishonesty 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 1997-1998: "Academic dishonesty as it applies to students includes but is not limited to academic cheating; plagiarism; the sale, purchase, or exchange of term papers or research papers; falsification of information which includes any form of providing false or misleading information, written, electronic, or oral; or of altering or falsifying official institutional records. Plagiarism is defined as copying another's work or portion thereof and/or using ideas and concepts of another and presenting them as one's own without giving proper credit to the source."

Policies concerning granting of No-Grade, violation of academic integrity, and violation of student code of conduct:
For questions regarding Academic Dishonesty, the No-Grade policy, Sexual Harassment, or the Student Code of Conduct, students are encouraged to refer to their major department's handbook, the Undergraduate Course Catalogue, the Rams Eye View, or the University Web Site. Please understand that improper conduct in any of these areas will not be tolerated and may result in immediate ejections from the class.

ADA Policy:
If you have a disability that requires accommodations under the Americans with Disabilities Act (ADA), please present your letter of accommodations and meet with me as soon as possible so that I can support your success in an informed manner. Accommodations cannot be granted retroactively. If you would like to know more about West Chester University's Services for Students with Disabilities(OSSD), please contact the OSSD which is located at 223 Lawrence Center. The OSSD hours of Operation are Monday – Friday 8:30 a.m. – 4:30 p.m. Their phone number is 610-436-2564, their fax number is 610-436-2600, their email address is ossd@wcupa.edu, and their website is at www.wcupa.edu/ussss/ossd.

Title IX Statement:
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 Contact:
In the event of an emergency during class, the phone number for WCU's Department of Public Safety is 610-436-3311.

EXCUSED ABSENCES POLICY FOR UNIVERSITY-SANCTIONED EVENTS (eff. spring 2017)

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:

1. Responsibility for meeting academic requirements rests with the student.
2. Students are expected to notify their professors as soon as they know they will be missing class due to a University-sanctioned event.
3. 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.
4. If a scheduled event is postponed or canceled, the student is expected to go to class.
5. Students are not excused from classes for practice on nonevent days.

The following are specifics for the student athlete:

1. The student athlete is expected, where possible, to schedule classes on days and at hours that do not conflict with athletic schedules.
2. 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.

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.