CIS 4348-110, CRN 11050, Security Trends and Malware Analysis
CIS 4348-120, CRN 11181, Security Trends and Malware Analysis
Spring 2021
Texas A&M University-Central Texas

Instructor: Dinesh Reddy, Ph.D.
Office: FH 323G
Email: dreddy@tamuct.edu
Office Hours: TR 2 pm - 5 pm virtual (emails, calls, or video desktop sharing) (or by appointment)

Course Dates, Modality, and Location
Jan 19 – May 14. This is a blended course which meets 50% online and 50% face-to-face where section 120 meets on Tuesdays 6 pm - 7:15 pm and section 110 meets on Thursdays 6 pm - 7:15 pm. This course uses the A&M-Central Texas Canvas Learning Management System [https://tamuct.instructure.com]. I use Canvas to post course content, assignments, quizzes, exams, and to communicate any other announcements with the class. So please check Canvas regularly (on a daily basis) for updates.

Student-instructor interaction:
You may use the Canvas "inbox" feature or email me with your questions anytime as you would by attending the class and coming into my office. Your questions will be answered within 24 hours on weekdays and within 48 hours on weekends and holidays.

WARRIOR SHIELD
Emergency Warning System for Texas A&M University-Central Texas
Warrior Shield is an emergency notification service that gives Texas A&M University-Central Texas the ability to communicate health and safety emergency information quickly via email, text message, and social media. All students are automatically enrolled in Warrior Shield through their myCT email account.
Connect to Warrior Shield by 911Cellular [https://portal.publicsafetycloud.net/Account/Login to change where you receive your alerts or to opt out. By staying enrolled in Warrior Shield, university officials can quickly pass on safety-related information, regardless of your location.

COVID-19 SAFETY MEASURES
To promote public safety and protect students, faculty, and staff during the coronavirus pandemic, Texas A&M University-Central Texas has adopted policies and practices to minimize virus transmission. All members of the university community are expected to adhere to these measures to ensure their own safety and the safety of others. Students must observe the following practices while participating in face-to-face courses, course-related activities (office hours, help sessions, transitioning to and between classes, study spaces, academic services, etc.) and co-curricular programs:

- Self-monitoring—Students should follow CDC recommendations for self-monitoring. Students who have a fever or exhibit symptoms of COVID-19 should participate in class remotely and

should not participate in face-to-face instruction. Students required to quarantine must participate in courses and course-related activities remotely and must not attend face-to-face course activities. Students should notify their instructors of the quarantine requirement. Students under quarantine are expected to participate in courses and complete graded work unless they have symptoms that are too severe to participate in course activities.

- Face Coverings— Face coverings must be worn inside of buildings and within 50 feet of building entrances on the A&M-Central Texas Campus. This includes lobbies, restrooms, hallways, elevators, classrooms, laboratories, conference rooms, break rooms, non-private office spaces, and other shared spaces. Face coverings are also required in outdoor spaces where physical distancing is not maintained. The university will evaluate exceptions to this requirement on a case by case basis. Students can request an exception through the Office of Access and Inclusion in Student Affairs.
    - If a student refuses to wear a face covering, the instructor should ask the student to leave and join the class remotely. If the student does not leave the class, the faculty member should report that student to the Office of Student Conduct. Additionally, the faculty member may choose to teach that day's class remotely for all students.
- Physical Distancing—Physical distancing must be maintained between students, instructors, and others in the course and course-related activities.
- Classroom Ingress/Egress—Students must follow marked pathways for entering and exiting classrooms and other teaching spaces. Leave classrooms promptly after course activities have concluded. Do not congregate in hallways and maintain 6-foot physical distancing when waiting to enter classrooms and other instructional spaces.
- The university will notify students in the event that the COVID-19 situation necessitates changes to the course schedule or modality.

COURSE INFORMATION

Course Overview and description: This course analyzes and investigates security threats and ethical hacking methods. It will introduce students to modern malware analysis techniques through a detailed examination of malware, virus, and malicious code operation by examining case studies and hands-on interactive analysis of real world samples. The course will also examine in detail current trends in the threat environment and the most current attack exploits. Student will use a variety of methods to investigate current security threats and their mitigation. Topics include malware morphology, disassembly of malware, ethical hacking methods on systems including penetration, and trends in the threat-scape.

Student Learning Outcomes:

- Students will gain an understanding of hacker tools, techniques, and five stages of ethical hacking methods.
- Students will gain knowledge about penetration tests used to assess vulnerability of systems to current security incident trends including malware attacks.
- Students will learn about footprinting on a targeted website.
- Students will gain an understanding of the following topics related to malware:
    - The malware concepts and technologies
    - The types of malware and how they are categorized
    - How malware protects itself from security products

- The things that malware depends upon to operate
- How to identify and remove malware on a Windows system
- How to collect malware from different sources
- How to perform static analysis of malware sample
- How to perform dynamic analysis of malware sample
- How to disassemble malware using IDA Pro disassembler
- How to use debugging techniques and tools for malware analysis

Required Reading and Textbook(s):

1. eBook on "Security Trends and Malware Analysis"
ISBN: 978-1-284-01407-5
Students will need to purchase an Access Code (by searching above ISBN on jblearning.com) in order to redeem their eBooks on the PUBLISH web site (http://publish.jblearning.com/ebooks).

2. Virtual lab access for "Security Trends and Malware Analysis"
ISBN: 978-1-284-19307-7
More details on purchase options will be provided in class and on Canvas.

3. Practical Malware Analysis - The Hands-On Guide to Dissecting Malicious Software
by Michael Sikorski and Andrew Honig
ISBN-13: 9781593272906

Supplemental Material

Additional required readings and optional readings will be posted on Canvas.

COURSE REQUIREMENTS

Exams

There will be three exams (two mid-terms and one final). Each exam is worth 100 points. Final exam will not be comprehensive. The exams can be conducted either paper-based or on canvas. Exams will be based on the textbook, readings, and class discussions. It is assumed that you will read the assigned chapters and readings in advance. Make up exams are not typically given. The only acceptable excuses for missing an exam are circumstances clearly outside your control, such as illness, death in family, etc. If you miss an exam, notify me as soon as possible. I may require documentation of the circumstances.

Lab Assignments

Labs are designed for students to have hands on experiences on the topics covered in this course. All lab work should be completed via virtual lab environment that accompanies the

required textbook. Instructions on what to submit for each lab will be posted on Canvas. You will be asked to prepare a lab report with your observations and screenshots. All lab reports must be submitted before the end of the day (11:59 PM) on the due date mentioned in the course schedule. Late submissions will not be accepted for full points and will attract 10% deduction for each day that it is late. Each lab assignment is worth 25 points.

Quizzes

There will be ten quizzes (multiple choice, true/false) that are designed to test the general understanding of the topics covered in the course. The quizzes can be conducted either paper-based or on Canvas. Late submissions will not be accepted. Each quiz is worth 20 points.

Project Report

There will be a project based on the concepts learned in this course. The project may be a combination of items such as a malware analysis case, essay questions, lab work, etc. The project deliverables will include a professionally written project report on findings. The project report must be submitted before the end of the day (11:59 PM) on the due date mentioned in the course schedule. Late submissions will not be accepted for full points and will attract 10% deduction for each day that it is late. Project report is worth 150 points.

Project Presentation

Each student will be required to present a topic in class (either individual or in a group). Students will select and explore a current topic/trend in this course. More details on the presentation topics, presentation schedule, and grading rubrics (used for assessing the presentations) will be announced in class and uploaded on Canvas. Late presentations will not be scheduled. Presentation is worth 100 points.

Grading Criteria:

Course Requirement	Points	Weightage
Two Mid-Term Exams (100 points each)	200	20%
Final Exam	100	10%
Ten Lab Assignments (25 points each)	250	25%
Ten Quizzes (20 points each)	200	20%
Project Report	150	15%
Project Presentation	100	10%
Total	**1000**	**100%**

Final letter grade distribution will be as per the following scale:

Letter Grade	Point Range
A	900 and above
B	800-899
C	700-799
D	600-699
F	599 and below

Posting of Grades
All students' grade will be posted on the Canvas Grade book, and students can monitor their progress on Canvas grade book. Students can expect to see their grades within two weeks of the closing of class tests, exams, and assignments. Students are expected to visit Canvas course webpage regularly to get any update regarding this course.

COURSE OUTLINE AND CALENDAR

Course Schedule* ** (* This schedule provides a general plan. Deviations may be necessary) (** Readings for each week will be posted on Canvas)

Week	Date	Readings	Due
1	1/19	Syllabus, eBook Ch 1 – Hacking: The Next Generation	
	1/21	eBook Ch 1 – Continued	Quiz 1
2	1/26	eBook Ch 2 - Footprinting Tools	
	1/28	eBook Ch 2 – Continued	Quiz 2
3	2/2	eBook Ch 3 – Port Scanning	Lab Assignment 1
	2/4	eBook Ch 3 - Continued	Quiz 3
4	2/9	eBook Ch 4 - Enumeration & Computer System Hacking	Lab Assignment 2
	2/11	eBook Ch 4 – Continued	Quiz 4
5	2/16	Exam 1 Review	Lab Assignment 3
	2/18	Exam 1	Exam 1
6	2/23	eBook Ch 5 - Malware	Lab Assignment 4
	2/25	eBook Ch 5 – Continued	Quiz 5
7	3/2	PMA Ch 0 – Malware Analysis Primer	Lab Assignment 5
	3/4	PMA Ch 1 – Basic Static Techniques	Quiz 6
8	3/9	PMA Ch 2 – Malware Analysis in Virtual Machines	Lab Assignment 6
	3/11	PMA Ch 3 – Basic Dynamic Analysis	Quiz 7
9	3/16	SPRING BREAK	
	3/18	SPRING BREAK	
10	3/23	PMA Ch 4 - A Crash Course in x86 Disassembly	Lab Assignment 7
	3/25	PMA Ch 4 – Continued	Quiz 8

11	3/30	Exam 2 Review	
	4/1	Exam 2	Exam 2
12	4/6	PMA Ch 5 – IDA Pro	Lab Assignment 8
	4/8	PMA Ch 5 - Continued	Quiz 9
13	4/13	PMA Ch 6 – Recognizing C Code Constructs in Assembly	Lab Assignment 9
	4/15	PMA Ch 6 - Continued	Quiz 10
14	4/20	PMA Ch 7 – Analyzing Malicious Windows Programs	Lab Assignment 10
	4/22	PMA Ch 7 – Continued	
15	4/27	PMA Ch 8 – Debugging (Intro to OllyDbg & WinDbg)	Project Report
	4/29	Project Presentations	
16	5/4	Project Presentations	
	5/6	Final Exam Review	
17	5/11	Final Exam	Final Exam

Important University Dates:

January 19, 2021 Add, Drop and Late Registration Begins for 16- and First 8-Week Classes $25 Fee assessed for late registrants
January 19, 2021 Classes Begin for Spring Semester
January 21, 2021 Deadline for Add, Drop, and Late Registration for 16-and First 8-Week Classes
January 26, 2021 Deadline to Drop First 8-Week Classes with No Record
February 3, 2021 Deadline to Drop 16-Week Classes with No Record
February 26, 2021 Deadline to Drop First 8-Week Classes with a Quit (Q) or Withdraw (W)
March 1, 2021 Deadline for Teacher Education Program Applications
March 12, 2021 Classes end for 1st 8-Weeks Session
March 15, 2021 Deadline for Clinical Teaching/Practicum Applications
March 16, 2021 Deadline for Faculty Submission of First 8-Week Final Class Grades (due by 3pm)
March 15-19, 2021 Spring Break (No Classes - Administrative Offices Open)
March 22, 2021 Class Schedule Published for Summer Semester
March 22, 2021 Add, Drop, and Late Registration Begins for Second 8-Week Classes $25 Fee assessed for late registrants
March 22, 2021 Classes Begin for Second 8-Week Session
March 24, 2021 Deadline for Add, Drop, and Late Registration for
Second 8-Week Classes
March 26, 2021 Deadline for Spring Graduation Application for Ceremony Participation
March 29, 2021 Deadline to Drop Second 8-Week Classes with No Record
April 1, 2021 Deadline for GRE/GMAT Scores to Graduate School Office
April 5, 2021 Registration Opens for Summer Semester
April 16, 2021 Deadline for Final Committee-Edited Theses with Committee Approval Signatures for Spring Semester to Graduate School Office
April 30, 2021 Deadline to drop Second 8-week Classes with a Quit (Q) or Withdraw (W).
May 14, 2021 Deadline to Withdraw from the University for 16- and Second 8-Week Classes

May 14, 2021 Spring Semester Ends

TECHNOLOGY REQUIREMENTS AND SUPPORT

Technology Requirements
This course will use the A&M-Central Texas Instructure Canvas learning management system. We strongly recommend the latest versions of Chrome or Firefox browsers. Canvas no longer supports any version of Internet Explorer.

Logon to A&M-Central Texas Canvas [https://tamuct.instructure.com/] or access Canvas through the TAMUCT Online link in myCT [https://tamuct.onecampus.com/]. You will log in through our Microsoft portal.

Username: Your MyCT email address. Password: Your MyCT password

Canvas Support
Use the Canvas Help link, located at the bottom of the left-hand menu, for issues with Canvas. You can select "Chat with Canvas Support," submit a support request through "Report a Problem," or call the Canvas support line: 1-844-757-0953.
For issues related to course content and requirements, contact your instructor.

Online Proctored Testing
A&M-Central Texas uses Proctorio for online identity verification and proctored testing. This service is provided at no direct cost to students. If the course requires identity verification or proctored testing, the technology requirements are: Any computer meeting the minimum computing requirements, plus web camera, speaker, and microphone (or headset). Proctorio also requires the Chrome web browser with their custom plug in.

Other Technology Support
For log-in problems, students should contact Help Desk Central.
24 hours a day, 7 days a week:
Email: helpdesk@tamu.edu
Phone: (254) 519-5466
Web Chat: [http://hdc.tamu.edu]
Please let the support technician know you are an A&M-Central Texas student.

UNIVERSITY RESOURCES, PROCEDURES, AND GUIDELINES

Drop Policy.
If you discover that you need to drop this class, you must complete a Drop Request Form [https://www.tamuct.edu/registrar/docs/Drop_Request_Form.pdf].

Professors cannot drop students; this is always the responsibility of the student. The Registrar's Office will provide a deadline on the Academic Calendar for which the form must be completed, signed and returned. Once you return the signed form to the Registrar's Office, you must go

into Warrior Web and confirm that you are no longer enrolled. If you still show as enrolled, FOLLOW-UP with the Registrar's Office immediately. You are to attend class until the procedure is complete to avoid penalty for absence. Should you miss the drop deadline or fail to follow the procedure, you will receive an F in the course, which may affect your financial aid and/or VA educational benefits.

Academic Integrity.
Texas A&M University -Central Texas values the integrity of the academic enterprise and strives for the highest standards of academic conduct. A&M-Central Texas expects its students, faculty, and staff to support the adherence to high standards of personal and scholarly conduct to preserve the honor and integrity of the creative community. Academic integrity is defined as a commitment to honesty, trust, fairness, respect, and responsibility. Any deviation by students from this expectation may result in a failing grade for the assignment and potentially a failing grade for the course. Academic misconduct is any act that improperly affects a true and honest evaluation of a student's academic performance and includes, but is not limited to, working with others in an unauthorized manner, cheating on an examination or other academic work, plagiarism and improper citation of sources, using another student's work, collusion, and the abuse of resource materials. All academic misconduct concerns will be referred to the university's Office of Student Conduct. Ignorance of the university's standards and expectations is never an excuse to act with a lack of integrity. When in doubt on collaboration, citation, or any issue, please contact your instructor before taking a course of action.

For more information regarding the Student Conduct process,
[https://www.tamuct.edu/student-affairs/student-conduct.html].
If you know of potential honor violations by other students, you may submit a report,
[https://cm.maxient.com/reportingform.php?TAMUCentralTexas&layout_id=0].

Academic Accommodations.
At Texas A&M University-Central Texas, we value an inclusive learning environment where every student has an equal chance to succeed and has the right to a barrier-free education. The Office of Access and Inclusion is responsible for ensuring that students with a disability receive equal access to the university's programs, services and activities. If you believe you have a disability requiring reasonable accommodations please contact the Office of Access and Inclusion, WH-212; or call (254) 501-5836. Any information you provide is private and confidential and will be treated as such.

For more information please visit our Access & Inclusion Canvas page (log-in required)
[https://tamuct.instructure.com/courses/717]

Important information for Pregnant and/or Parenting Students
Texas A&M University-Central Texas supports students who are pregnant and/or parenting. In accordance with requirements of Title IX and related guidance from US Department of Education's Office of Civil Rights, the Dean of Student Affairs' Office can assist students who are pregnant and/or parenting in seeking accommodations related to pregnancy and/or parenting.

Students should seek out assistance as early in the pregnancy as possible. For more information, please visit Student Affairs [https://www.tamuct.edu/student-affairs/index.html]. Students may also contact the institution's Title IX Coordinator. If you would like to read more about these requirements and guidelines online, please visit the website [http://www2.ed.gov/about/offices/list/ocr/docs/pregnancy.pdf].

Title IX of the Education Amendments Act of 1972 prohibits discrimination on the basis of sex and gender–including pregnancy, parenting, and all related conditions. A&M-Central Texas is able to provide flexible and individualized reasonable accommodation to pregnant and parenting students. All pregnant and parenting students should contact the Associate Dean in the Division of Student Affairs at (254) 501-5909 to seek out assistance. Students may also contact the University's Title IX Coordinator.

Tutoring

Tutoring is available to all A&M-Central Texas students, on a remote online basis. Visit the Academic Support Community in Canvas to view schedules and contact information. Subjects tutored on campus include Accounting, Advanced Math, Biology, Finance, Statistics, Mathematics, and Study Skills. Tutors will return at the Tutoring Center in Warrior Hall, Suite 111 in the current semester. Student success coaching is available online upon request.

If you have a question regarding tutor schedules, need to schedule a tutoring session, are interested in becoming a tutor, success coaching, or have any other question, contact Academic Support Programs at (254) 501-5836, visit the Office of Student Success at 212F Warrior Hall, or by emailing studentsuccess@tamuct.edu .

Chat live with a tutor 24/7 for almost any subject from on your computer! Tutor.com is an online tutoring platform that enables A&M-Central Texas students to log in and receive online tutoring support at no additional cost. This tool provides tutoring in over 40 subject areas except writing support. Access Tutor.com through Canvas.

University Writing Center

The University Writing Center (UWC) at Texas A&M University–Central Texas (TAMUCT) is a free service open to all TAMUCT students. For the current semester, all services will be online as a result of the COVID-19 pandemic. The hours of operation are from 10:00 a.m.-5:00 p.m. Monday thru Thursday with satellite hours online Monday thru Thursday from 6:00-9:00 p.m. The UWC is also offering hours from 12:00-3:00 p.m. on Saturdays.

Tutors are prepared to help writers of all levels and abilities at any stage of the writing process. By providing a practice audience for students' ideas and writing, our tutors highlight the ways in which they read and interpret students' texts, offering guidance and support throughout the various stages of the writing process. While tutors will not write, edit, or grade papers, they will assist students in developing more effective composing practices. Whether you need help brainstorming ideas, organizing an essay, proofreading, understanding proper citation

practices, or just want a quiet place to work, the UWC is here to help!

Students may arrange a one-to-one session with a trained and experienced writing tutor by making an appointment via WCOnline [https://tamuct.mywconline.com/]. In addition, you can email Dr. Bruce Bowles Jr. at bruce.bowles@tamuct.edu if you have any questions about the UWC and/or need any assistance with scheduling.

University Library

The University Library provides many services in support of research across campus and at a distance. We offer over 200 electronic databases containing approximately 250,000 eBooks and 82,000 journals, in addition to the 85,000 items in our print collection, which can be mailed to students who live more than 50 miles from campus. Research guides for each subject taught at A&M-Central Texas are available through our website to help students navigate these resources. On campus, the library offers technology including cameras, laptops, microphones, webcams, and digital sound recorders.

Research assistance from a librarian is also available 24 hours a day through our online chat service, and at the reference desk when the library is open. Research sessions can be scheduled for more comprehensive assistance, and may take place on Skype or in-person at the library. Assistance may cover many topics, including how to find articles in peer-reviewed journals, how to cite resources, and how to piece together research for written assignments.

Our 27,000-square-foot facility on the A&M-Central Texas main campus includes student lounges, private study rooms, group work spaces, computer labs, family areas suitable for all ages, and many other features. Services such as interlibrary loan, TexShare, binding, and laminating are available. The library frequently offers workshops, tours, readings, and other events. For more information, please visit our Library website [http://tamuct.libguides.com/index].

All reference service will be conducted virtually. Please go to our Library website [http://tamuct.libguides.com/index] to access our virtual reference help and our current hours.

Behavioral Intervention

Texas A&M University-Central Texas cares about the safety, health, and well-being of its students, faculty, staff, and community. If you are aware of individuals for whom you have a concern, please make a referral to the Behavioral Intervention Team. Referring your concern shows you care. You can complete the referral online [https://cm.maxient.com/reportingform.php?TAMUCentralTexas&layout_id=2].

Anonymous referrals are accepted. Please see the Behavioral Intervention Team website for more information [https://www.tamuct.edu/student-affairs/bat.html]. If a person's behavior poses an imminent threat to you or another, contact 911 or A&M-Central Texas University

Police at 254-501-5800.