CSE 6388-001: Practical Malware Analysis
Fall 2017

Instructor Information:

Instructor:	Jiang Ming	GTA:	John Podolanko
Email:	jiang.ming@uta.edu	Email:	john.podolanko@mavs.uta.edu
Office:	ERB 528	Office:	ERB 316 / 405
Phone:	(817) 272-0906	Office Phone:	N/A
Office Hours:	Tue. 10:00 AM-12:00 PM	Office Hours:	Tue./Thu. 7:00-8:30 PM
Class Website:	https://elearn.uta.edu		
Section Info:	CSE 6388, Section 001	Meeting Times:	Tue./Thu. 5:30 to 6:50 PM
		Location:	SH 105

Course Description:

This is a hands-on advanced course on Practical Malware Analysis that will cover several key topics critical to understanding malware as well as how to reverse engineer and analyze it. These topics include, static analysis, dynamic analysis, sandboxing, binary disassembly, debugging, and malicious Windows programs. This course will also dive into malware functionality and behavior on computers and over the network to include techniques used to evade detection. Students will learn how to analyze, break, and prevent malware by studying live samples up close in a sandbox environment.

Course Objectives:

- Utilize static and dynamic analysis techniques to discover key vulnerabilities in malware.
- Disassemble pre-compiled malware executables and determine its operations without access to source code on Windows and Linux.
- Discover and utilize new tools for debugging malware executables and the Windows kernel.
- Understand and detect malware behavior in different environments including the network.
- Understand and detect malware techniques used to evade detection.
- Apply class knowledge in labs throughout the semester.

Prerequisites:

Information Security 1 (CSE 5380 or equivalent) is required.

Required Textbooks and Other Course Materials:

Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig
ISBN-13: 978-1-59327-290-6 ISBN-10: 1-59327-290-1

Note: The instructor reserves the right to modify course policies, the course calendar, and assignment or project point values and due dates.

Course Grades:

Course grades will be based on the following:

Labs	60%
Quizzes (4 in-class):	40%

Grades for Exams will be curved by the instructor and scaled to a standard A = 90-100, B = 80-89, C = 70-79 scale. Final grades will simply be the weighted average of the scores, based on the percentages shown above. Small amounts of extra credit may be available, but only on a class-wide basis (no individual requests will be granted). No grade bumps will be offered; 89.99 is a B in this class.

Make-ups: Make-ups for graded activities may be arranged if your absence is caused by illness or personal emergency. A written explanation (including supporting documentation) must be submitted to your instructor; if the explanation is acceptable, an alternative to the graded activity will be arranged. Make-up arrangements must be arranged prior to the scheduled due date.

Class Attendance Policy: At the University of Texas at Arlington, taking attendance is not required. Rather, each faculty member is free to develop his or her own methods of evaluating students' academic performance, which includes establishing course-specific policies on attendance. As the instructor of this section, I will be grading attendance based on your participation each lecture. Also, in every class period, you will learn by actively participating in the process of solving problems and working in small groups. Missing class, therefore, means missing out on learning opportunities that cannot be gained from the textbook.

Descriptions of major assignments and examinations with due dates:

- Lab Assignments: Labs will be assigned on a weekly basis (for a total of 14) so that students may apply the knowledge gained from lectures in a practical environment. Students are expected to complete their labs individually. Late submissions will receive a 20% deduction for each day late.
- Quiz 1, in-class, Tue. Feb. 6
  Covers everything discussed up to and including Week 3 (Chapters 1-3)
- Quiz 2, in-class, Tue. Mar. 6
  Covers everything discussed up to and including Week 7 (Chapters 4-7)
- Quiz 3, in-class, Tue. Apr. 3
  Covers everything discussed up to and including Week 11 (Chapters 8-10)
- Quiz 4, in-class, Tue., May 8
  Covers everything discussed up to and including Week 15 (Chapters 11-14)

Course Schedule (Subject to Change):

Week	*Class Dates*	*Topic*	*Activity*	*Due Dates*
1.	Jan. 16/18	Class Intro + Basic Static Analysis	Lab 1	Jan. 28
2.	Jan. 23/25	Basic Static Analysis + Analysis in VMs	Lab 2	Feb. 4
3.	Jan. 30/Feb. 1	Basic Dynamic Analysis	Lab 3	Feb. 11
4.	Feb. 6/8	QUIZ 1 + x86 Disassembly	Lab 4	Feb. 18
5.	Feb. 13/15	Interactive Disassembler (IDA)	Lab 5	Feb. 25
6.	Feb. 20/22	Recognizing C Constructs in Assembly	Lab 6	Mar. 4
7.	Feb. 27/Mar. 1	Analyzing Malicious Windows Programs	Lab 7	Mar. 11
8.	Mar. 6/8	QUIZ 2 + Debugging	Lab 8	Mar. 18
9.	Mar. 13/15	SPRING BREAK		
10.	Mar. 20/22	Debugging with OllyDbg	Lab 9	Apr. 1
11.	Mar. 27/29	Windows Kernel Debugging	Lab 10	Apr. 8
12.	Apr. 3/5	QUIZ 3 + Malware Behavior	Lab 11	Apr. 15
13.	Apr. 10/12	Covert Malware Launching	Lab 12	Apr. 22
14.	Apr. 17/19	Data Encoding	Lab 13	Apr. 29
15.	Apr. 24/26	Malware Network Signatures	Lab 14	May 6
16.	May 1/3	Anti-Reverse Engineering Techniques	Bonus Lab	May 11
17.	May 8	QUIZ 4		

As the instructor for this course, I reserve the right to adjust this schedule in any way that serves the educational needs of the students enrolled in this course. –Jiang Ming

Academic Integrity: Students enrolled all UT Arlington courses are expected to adhere to the UT Arlington Honor Code:

> *I pledge, on my honor, to uphold UT Arlington's tradition of academic integrity, a tradition that values hard work and honest effort in the pursuit of academic excellence.*
>
> *I promise that I will submit only work that I personally create or contribute to group collaborations, and I will appropriately reference any work from other sources. I will follow the highest standards of integrity and uphold the spirit of the Honor Code.*

UT Arlington faculty members may employ the Honor Code as they see fit in their courses, including (but not limited to) having students acknowledge the honor code as part of an examination or requiring students to incorporate the honor code into any work submitted. Per UT System Regents' Rule 50101, §2.2, suspected violations of university's standards for academic integrity (including the Honor Code) will be referred to the Office of Student Conduct. Violators will be disciplined in accordance with University policy, which may result in the student's suspension or expulsion from the University.
Additionally, there is a special ethics form for this course about malware distribution that you must sign and uphold.

Title IX: *The University of Texas at Arlington does not discriminate on the basis of race, color, national origin, religion, age, gender, sexual orientation, disabilities, genetic information, and/or veteran status in its educational programs or activities it operates. For more information, visit www.uta.edu/eos. or information regarding Title IX, visit www.uta.edu/titleIX.*

Drop Policy: Students may drop or swap (adding and dropping a class concurrently) classes through self-service in MyMav from the beginning of the registration period through the late registration period. After the late registration period, students must see their academic advisor to drop a class or withdraw. Undeclared students must see an advisor in the University Advising Center. Drops can continue through a point two-thirds of the way through the term or session. It is the student's responsibility to officially withdraw if they do not plan to attend after registering. **Students will not be automatically dropped for non-attendance.** Repayment of certain types of financial aid administered through the University may be required as the result of dropping classes or withdrawing. For more information, contact the Office of Financial Aid and Scholarships (http://wweb.uta.edu/aao/fao/).

Disability Accommodations: UT Arlington is on record as being committed to both the spirit and letter of all federal equal opportunity legislation, including *The Americans with Disabilities Act (ADA), The Americans with Disabilities Amendments Act (ADAAA), and Section 504 of the Rehabilitation Act*. All instructors at UT Arlington are required by law to provide "reasonable accommodations" to students with disabilities, so as not to discriminate on the basis of disability. Students are responsible for providing the instructor with official notification in the form of a letter certified by the **Office for Students with Disabilities (OSD)**. Students experiencing a range of conditions (Physical, Learning, Chronic Health, Mental Health, and Sensory) that may cause diminished academic performance or other barriers to learning may seek services and/or accommodations by contacting:

The Office for Students with Disabilities, (OSD) www.uta.edu/disability or calling 817-272-3364.
Counseling and Psychological Services, (CAPS) www.uta.edu/caps/ or calling 817-272-3671.

Only those students who have officially documented a need for an accommodation will have their request honored. Information regarding diagnostic criteria and policies for obtaining disability-based academic accommodations can be found at www.uta.edu/disability or by calling the Office for Students with Disabilities at (817) 272-3364.

Electronic Communication: UT Arlington has adopted MavMail as its official means to communicate with students about important deadlines and events, as well as to transact university-related business regarding financial aid, tuition, grades, graduation, etc. All students are assigned a MavMail account and are responsible for checking the inbox regularly. There is no additional charge to students for using this account, which remains active even after graduation. Information about activating and using MavMail is available at: http://www.uta.edu/oit/cs/email/mavmail.php.

Student Support Services: UT Arlington provides a variety of resources and programs designed to help students develop academic skills, deal with personal situations, and better understand concepts and information related to their courses. Resources include tutoring, major-based learning centers, developmental education, advising and mentoring, personal counseling, and federally funded programs. For individualized referrals, students may visit the reception desk at University College (Ransom Hall), call the Maverick Resource Hotline at 817-272-6107, send a message to resources@uta.edu, or view the information at: http://www.uta.edu/universitycollege/resources/index.php

Student Feedback Survey: At the end of each term, students enrolled in classes categorized as "lecture," "seminar," or "laboratory" shall be directed to complete an online Student Feedback Survey (SFS). Instructions on how to access the SFS for this course will be sent directly to each student through MavMail approximately 10 days before the end of the term. Each student's feedback enters the SFS database anonymously and is aggregated with that of other students enrolled in the course. UT Arlington's effort to solicit, gather, tabulate, and publish student feedback is required by state law; students are strongly urged to participate. For more information, visit http://www.uta.edu/sfs.

Final Review Week: A period of five class days prior to the first day of final examinations in the long sessions shall be designated as Final Review Week. The purpose of this week is to allow students sufficient time to prepare for final examinations. During this week, there shall be no scheduled activities such as required field trips or performances; and no instructor shall assign any themes, research problems or exercises of similar scope that have a completion date during or following this week *unless specified in the class syllabus*. During Final Review Week, an instructor shall not give any examinations constituting 10% or more of the final grade, except makeup tests and laboratory examinations. In addition, no instructor shall give any portion of the final examination during Final Review Week. During this week, classes are held as scheduled. In addition, instructors are not required to limit content to topics that have been previously covered; they may introduce new concepts as appropriate.

Emergency Exit Procedures: Should we experience an emergency event that requires us to vacate the building, students should exit the room and move toward the nearest exit, which is right in front of you when you exit the classroom. When exiting the building during an emergency, one should never take an elevator but should use the stairwells. Faculty members and instructional staff will assist students in selecting the safest route for evacuation and will make arrangements to assist individuals with disabilities.

Emergency Phone Numbers: In case of an on-campus emergency, call the UT Arlington Police Department at **817-272-3003** (non-campus phone), **2-3003** (campus phone). You may also dial **911**. Non-emergency number 817-272-3381.