Malware Reverse Engineering

CAP 4136
Class Periods: MWF, Period 4 (10:40-11:30)
Location: E309 CSE
Academic Term: Spring 2023

Instructor:
Joseph N. Wilson
jnw@ufl.edu
E472 CSE
352-514-2191 (This is my cell phone. Call only if it is urgent. Text if it is important.)
Office Hours: to be announced on Canvas

Teaching Assistant/Peer Mentor/Supervised Teaching Student:
Please contact through the Canvas website

- TBA

Course Description
(3 credit hours) Introduction to the theory and practice of software reverse engineering applied to the analysis of malicious software (malware). Students will learn techniques of static and dynamic analysis to help identify the full spectrum of the behavior of code that is presented without documentation or source code and to identify possible remediation and avoidance techniques. The course will use a large number of software tools employed by malware and computer forensic analysts.

Course Pre-Requisites / Co-Requisites
Computer Organization (CDA 3101 or consent of instructor)

Course Objectives
By the end of the course, students will be able to explain how to safely and thoroughly analyze malicious software. Students will be able to describe the behavior and potential security impacts of such code. Students will be able to carry out static and dynamic analysis techniques that help them understand a program's structure and behavior. Students will be able to identify anti-forensic techniques employed by malware and carry out activities to avoid or overcome those techniques. Students will demonstrate familiarity with software tools used for malware analysis. Students will be able to understand and explain the behavior of low-level code such as event handlers and device drivers.

Materials and Supply Fees
A fee of $X is assessed to pay for the cost of virtual machine hosting.

Relation to Program Outcomes (ABET):

Outcome	Coverage
1. An ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics	High
2. An ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors	Low
3. An ability to communicate effectively with a range of audiences	High
4. An ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts	Low
5. An ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives	N/A

6. An ability to develop and conduct appropriate experimentation, analyze and interpret data, and use engineering judgment to draw conclusions	High
7. An ability to acquire and apply new knowledge as needed, using appropriate learning strategies	High

Required Textbooks and Software

Title: Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software
Author: Michael Sikorski and Andrew Honig
Publication date: 2012,
ISBN: 978-1-59327-290-6

Title: Malware Analyst's Cookbook and DVD
Authors: M. Ligh, S. Adair, B. Hartstein, and M. Richard
Publication Date: 2011
ISBN: 978-0-470-61303-0

Recommended Materials

Xeno Kovah's Introductory Intel X86 class
PC Assembly Language, Paul Carter, June 2006.
Practical Reverse Engineering..., B. Dang, A. Gazet, E. Bachaalany, S. Josse
Intel® 64 and IA-32 Architectures Software Developer Manuals, Intel.

Course Schedule (based on proposed UF schedule)

1 Jan 9 Introduction
2 Jan 11 Basic Static Analysis
3 Jan 13 Basic Dynamic Analysis

4 Jan 18 x86 Crash Course I
5 Jan 20 x86 Crash Course II

6 Jan 23 x64 Crash Course
7 Jan 25 Disassembly and Decompilation: Ghidra
8 Jan 27 IDA and Binary Ninja

9 Jan 30 C Code Constructs I
10 Feb 1 C Code Constructs II
11 Feb 3 Analyzing Malicious Windows Programs I

12 Feb 6 Analyzing Malicious Windows Programs II
13 Feb 8 Debugging I
14 Feb 10 Debugging II

15 Feb 13 Data Encoding
16 Feb 15 Malware Behavior I
17 Feb 17 Malware Behavior II

18 Feb 20 Binary Ninja OpenAI Plugin
19 Feb 22 Covert Malware Launching
20 Feb 24 Malware Focused Network Signatures

21 Feb 27 Practical I Debriefing

22 Mar 1 Malware Classification
23 Mar 3 Anti-Disassembly

24 Mar 6 Anti-Debugging
25 Mar 8 Anti-Virtual-Machine Techniques
26 Mar 10 Packers and Unpacking

27 Mar 20 Shellcode Analysis
28 Mar 22 C++ Analysis
29 Mar 24 Kernel Debugging

30 Mar 27 Memory Forensics I
31 Mar 29 Practical 2 Debriefing
32 Mar 31 Memory Forensics II

33 Apr 3 PDF Documents I
34 Apr 5 PDF Documents II
35 Apr 7 PDF Documents III

36 Apr 10 Malicious Office Documents I
37 Apr 12 Malicious Office Documents II
38 Apr 14 Timeless Debugging

39 Apr 18 Practical 3 Debriefing
40 Apr 20 Flailing is Learning
41 Apr 21 Soup to Nuts Reverse Engineering

42 Apr 24 Exam Review 1
43 Apr 26 Exam Review 2

Attendance Policy, Class Expectations, and Make-Up Policy
Attendance is strongly recommended but not mandatory for on-campus students; however. All students are expected to comport themselves in a professional manner. UF policies concerning other classroom issues will be followed. (http://handbook.aa.ufl.edu/teaching/policies/)

Evaluation of Grades
The course grade is based on the following elements: quizzes, practical exercises, and the final examination.

Quizzes all consist of three questions with multiple choice answers. Each question receives one point. The quizzes evaluate your concrete understanding of the material you will have been asked to study in order to prepare for class.

Practical Exercises require you to analyze an actual malware specimen. In each case, you are asked to analyze the malware specimen and write a report discussing its properties and the potential risk it poses to an organization. Your grade will be based on your highest three grades out of four exercises. Malware specimens on each of these assignments are the same for all students. Each student may work with other students in carrying out analysis of those malware samples, but the reports must be written entirely independently.

The *Final Examination* is a multiple-choice examination that assesses your understanding of the course material. If you attended the classes, worked on the in-class exercises, and carried out analysis of the malware provided in the practical exercises, then you should be able to do very well on the examination. It is used to ensure that you understood the course material.

Assignment	Total Points	Percentage of Final Grade
Quizzes (5 lowest dropped)	3 each	30%
Practical Exercises (best 3 of 4)	100 each	50%
Final Exam	100	20%
		100%

Grading Policy

Percent	Grade	Grade Points
93.4 - 100	A	4.00
90.0 – 93.3	A-	3.67
86.7 - 89.9	B+	3.33
83.4 - 86.6	B	3.00
80.0 - 83.3	B-	2.67
76.7 - 79.9	C+	2.33
73.4 - 76.6	C	2.00
70.0 - 73.3	C-	1.67
66.7 - 69.9	D+	1.33
63.4 - 66.6	D	1.00
60.0 - 63.3	D-	0.67
0 - 59.9	E	0.00

More information on UF grading policy may be found at:
https://catalog.ufl.edu/ugrad/current/regulations/info/grades.aspx

Differences Between This Course and CAP 6137

- Grading Scale:

  Graduates: 20% Quizzes, 50% Practical Exercises, 30% Final Examination
  Undergrads: 30% Quizzes, 50% Practical Exercises, 20% Final Examination

  For undergraduates, quizzes are used to provide more credit and final examination less credit than in the graduate section. This is a result of emphasizing and rewarding keeping a high level of engagement throughout the semester.

- Nature of the practical assignments:

  Each practical assignment consists of one or more malware samples to be analyzed. For the first three assignments, both undergraduate students and graduate students are assigned the same malware samples.

  The malware for the fourth assignment for undergraduates is chosen by the instructor to be appropriate to analyze with an undergraduate level of experience and ability. With experience gained during the semester, this malware should be readily analyzed by all students. This assignment is essentially optional because the grade on the highest three of four practical assignments are used to compute each student's course grade.

  Each graduate student, individually, will select a fourth malware specimen from one of a number of available repositories and then characterize and analyze that malware sample. The instructor will approve the choice of malware sample for complexity and representativity. Graduate students will present their analysis to the class.

- Conceptual Differences reflected by these choices:

  For undergraduates, the emphasis is more on practice that developing a deep understanding, thus the

emphasis on quizzes more than the final examination and the provision of an optional fourth practical exercise rather than what the graduate students will consider to be a *stretch* assignment. The undergraduates are not expected to be able to carry out as complete an analysis in general due to their lack of familiarity and background with operating systems, programming language implementation, and low-level architecture implementations.

The graduate students, on the other hand, are expected to hit the road running, developing a more sophisticated ability to understand both the methods employed by the malware samples as well as the potential risks and impact of their behaviors.

- Final Examination

  The same final examination is presented to both undergraduates and graduates.

Students Requiring Accommodations
Students with disabilities who experience learning barriers and would like to request academic accommodations should connect with the disability Resource Center by visiting https://disability.ufl.edu/students/get-started/. It is important for students to share their accommodation letter with their instructor and discuss their access needs, as early as possible in the semester.

Course Evaluation
Students are expected to provide professional and respectful feedback on the quality of instruction in this course by completing course evaluations online via GatorEvals. Guidance on how to give feedback in a professional and respectful manner is available at https://gatorevals.aa.ufl.edu/students/. Students will be notified when the evaluation period opens, and can complete evaluations through the email they receive from GatorEvals, in their Canvas course menu under GatorEvals, or via https://ufl.bluera.com/ufl/. Summaries of course evaluation results are available to students at https://gatorevals.aa.ufl.edu/public-results/.

University Honesty Policy
UF students are bound by The Honor Pledge which states, "We, the members of the University of Florida community, pledge to hold ourselves and our peers to the highest standards of honor and integrity by abiding by the Honor Code. On all work submitted for credit by students at the University of Florida, the following pledge is either required or implied: "On my honor, I have neither given nor received unauthorized aid in doing this assignment." The Honor Code (https://sccr.dso.ufl.edu/policies/student-honor-code-student-conduct-code/) specifies a number of behaviors that are in violation of this code and the possible sanctions. Furthermore, you are obligated to report any condition that facilitates academic misconduct to appropriate personnel. If you have any questions or concerns, please consult with the instructor or TAs in this class.

Commitment to a Safe and Inclusive Learning Environment
The Herbert Wertheim College of Engineering values broad diversity within our community and is committed to individual and group empowerment, inclusion, and the elimination of discrimination. It is expected that every person in this class will treat one another with dignity and respect regardless of gender, sexuality, disability, age, socioeconomic status, ethnicity, race, and culture.

If you feel like your performance in class is being impacted by discrimination or harassment of any kind, please contact your instructor or any of the following:
• Your academic advisor or Graduate Program Coordinator
• Robin Bielling, Director of Human Resources, 352-392-0903, rbielling@eng.ufl.edu
• Curtis Taylor, Associate Dean of Student Affairs, 352-392-2177, taylor@eng.ufl.edu
• Toshikazu Nishida, Associate Dean of Academic Affairs, 352-392-0943, nishida@eng.ufl.edu

Software Use

All faculty, staff, and students of the University are required and expected to obey the laws and legal agreements governing software use. Failure to do so can lead to monetary damages and/or criminal penalties for the individual violator. Because such violations are also against University policies and rules, disciplinary action will be taken as appropriate. We, the members of the University of Florida community, pledge to uphold ourselves and our peers to the highest standards of honesty and integrity.

VMWare Workstation (available freely via the CISE Department's VMWare Academic Program membership), a variety of Microsoft tools (available freely via UF's membership in Microsoft Dreamspark), and various free software tools.

Student Privacy

There are federal laws protecting your privacy with regards to grades earned in courses and on individual assignments. For more information, please see: https://registrar.ufl.edu/ferpa.html

Campus Resources:

Health and Wellness

U Matter, We Care:
Your well-being is important to the University of Florida. The U Matter, We Care initiative is committed to creating a culture of care on our campus by encouraging members of our community to look out for one another and to reach out for help if a member of our community is in need. If you or a friend is in distress, please contact umatter@ufl.edu so that the U Matter, We Care Team can reach out to the student in distress. A nighttime and weekend crisis counselor is available by phone at 352-392-1575. The U Matter, We Care Team can help connect students to the many other helping resources available including, but not limited to, Victim Advocates, Housing staff, and the Counseling and Wellness Center. Please remember that asking for help is a sign of strength. In case of emergency, call 9-1-1.

Counseling and Wellness Center: http://www.counseling.ufl.edu/cwc, and 392-1575; and the University Police Department: 392-1111 or 9-1-1 for emergencies.

Sexual Discrimination, Harassment, Assault, or Violence
If you or a friend has been subjected to sexual discrimination, sexual harassment, sexual assault, or violence contact the **Office of Title IX Compliance**, located at Yon Hall Room 427, 1908 Stadium Road, (352) 273-1094, title-ix@ufl.edu

Sexual Assault Recovery Services (SARS)
Student Health Care Center, 392-1161.

University Police Department at 392-1111 (or 9-1-1 for emergencies), or http://www.police.ufl.edu/.

Academic Resources

E-learning technical suppor*t*, 352-392-4357 (select option 2) or e-mail to Learning-support@ufl.edu. https://lss.at.ufl.edu/help.shtml.

Career Resource Center, Reitz Union, 392-1601. Career assistance and counseling. https://www.crc.ufl.edu/.

Library Support, http://cms.uflib.ufl.edu/ask. Various ways to receive assistance with respect to using the libraries or finding resources.

Teaching Center, Broward Hall, 392-2010 or 392-6420. General study skills and tutoring. https://teachingcenter.ufl.edu/.

Writing Studio, 302 Tigert Hall, 846-1138. Help brainstorming, formatting, and writing papers. https://writing.ufl.edu/writing-studio/.

Student Complaints Campus*:* https://care.dso.ufl.edu.

On-Line Students Complaints*:* http://www.distance.ufl.edu/student-complaint-process.