Cover Sheet: Request 14852

CAP 4XXX – Malware Reverse Engineering

Info

Process	Course|New|Ugrad/Pro
Status	Pending at PV - University Curriculum Committee (UCC)
Submitter	Joseph Wilson jnw@cise.ufl.edu
Created	4/5/2020 8:34:54 PM
Updated	3/1/2021 1:59:50 PM
Description of request	New Course Proposal

Actions

Step	Status	Group	User	Comment	Updated
Department	Approved	ENG - Computer and Information Science and Engineering 19140000	Arunava Banerjee		6/2/2020
No document changes					
College	Recycled	ENG - College of Engineering	Heidi Dublin	Notes from Curriculum Committee: Take out co-listing part. Get Graduate Course uploaded simultaneously, include safety and inclusion statement, provide detail on attendance grade, remove wording about critical tracking if it's not a critical tracking course.	9/6/2020
No document changes					
Department	Approved	ENG - Computer and Information Science and Engineering 19140000	Christina Gardner-McCune		9/30/2020
No document changes					
College	Approved	ENG - College of Engineering	Heidi Dublin	Approved by Curriculum Committee and Faculty Council.	10/9/2020
No document changes					
University Curriculum Committee	Recycled	PV - University Curriculum Committee (UCC)	Casey Griffith	Please respond to Review comments regarding; attendance grade and more detail regarding differences between undergrad and graduate versions of the course (see review email).	11/17/2020
No document changes					
College	Recycled	ENG - College of Engineering	Heidi Dublin	Please see comments made by UCC. When sending item back up to college level please note in comments that all items have been addressed.	12/1/2020
No document changes					

Step	Status	Group	User	Comment	Updated
Department	Approved	ENG - Computer and Information Science and Engineering 19140000	Christina Gardner-McCune	Requested changes have been made.	2/26/2021
ugradMalwareReverseEngineeringSyllabus.pdf gradMalwareReverseEngineeringSyllabus.pdf					2/25/2021 2/25/2021
College	Approved	ENG - College of Engineering	Heidi Dublin	Department indicates that changes have been made.	3/1/2021
No document changes					
University Curriculum Committee	Pending	PV - University Curriculum Committee (UCC)			3/1/2021
No document changes					
Statewide Course Numbering System					
No document changes					
Office of the Registrar					
No document changes					
Student Academic Support System					
No document changes					
Catalog					
No document changes					
College Notified					
No document changes					

Course|New for request 14852

Info

Request: CAP 4XXX – Malware Reverse Engineering
Description of request: New Course Proposal
Submitter: Joseph Wilson jnw@cise.ufl.edu
Created: 9/30/2020 2:49:49 PM
Form version: 4

Responses

Recommended Prefix

Enter the three letter code indicating placement of course within the discipline (e.g., POS, ATR, ENC). Note that for new course proposals, the State Common Numbering System (SCNS) may&nbsp;assign a different prefix.

Response:
CAP

Course Level

Select the one digit code preceding the course number that indicates the course level at which the course is taught (e.g., 1=freshman, 2=sophomore, etc.).

Response:
4

Course Number

Enter the three digit code indicating the specific content of the course based on the SCNS taxonomy and course equivalency profiles. For new course requests, this may be XXX until SCNS assigns an appropriate number.

Response:
XXX

Category of Instruction

Indicate whether the course is introductory, intermediate or advanced. Introductory courses are those that require no prerequisites and are general in nature. Intermediate courses require some prior preparation in a related area. Advanced courses require specific competencies or knowledge relevant to the topic prior to enrollment.

Response:
Advanced

- *1000 level = Introductory undergraduate*
- *2000 level = Introductory undergraduate*
- *3000 level = Intermediate undergraduate*
- *4000 level = Advanced undergraduate*
- *5000 level = Introductory graduate*
- *6000 level = Intermediate graduate*
- *7000 level = Advanced graduate*
- *4000/5000= Joint undergraduate/graduate*
- *4000/6000= Joint undergraduate/graduate*

**Joint undergraduate/graduate courses must be approved by the UCC and the Graduate Council)*

Lab Code
Enter the lab code to indicate whether the course is lecture only (None), lab only (L), or a combined lecture and lab (C).

Response:
None

Course Title
Enter the title of the course as it should appear in the Academic Catalog. There is a 100 character limit for course titles.&nbsp;

Response:
Malware Reverse Engineering

Transcript Title
Enter the title that will appear in the transcript and the schedule of courses. Note that this must be limited to 30 characters (including spaces and punctuation).

Response:
Malware Reverse Engineering

Degree Type
Select the type of degree program for which this course is intended.

Response:
Baccalaureate

Delivery Method(s)
Indicate all platforms through which the course is currently planned to be delivered.

Response:
On-Campus

Co-Listing
Will this course be jointly taught to undergraduate, graduate, and/or professional students?

Response:
Yes

Co-Listing Explanation
Please detail how coursework differs for undergraduate, graduate, and/or professional students. Additionally, please upload a copy of both the undergraduate and graduate syllabus to the request in .pdf format. For more information please see the Co-Listed Graduate Undergraduate Courses Policy.

Response:

Graduate Course (CDA 6137) is currently in the catalog and being offered.

The differences between the courses are given here:

1. Grading Scale:

Graduates: 20% Quizzes, 50% Practical Exercises, 30% Final Examination
Undergrads: 10% Attendance, 20% Quizzes, 50% Practical Exercises, 20% Final Examination

2. Nature of the fourth practical assignment:

Graduates: Each student, individually, will select a malware specimen from one of a number of available repositories and then characterize and analyze that malware sample.
Instructor will approve choice of malware sample for complexity, understandability, and representativity. Graduates will present their analysis to the class.

Undergraduates: A single malware sample chosen by the instructor as being appropriate for the undergrad students level of experience and ability will be assigned to all students.
This assignment is optional and can be substituted for an assignment on which the student receives a lower grade.

3. Conceptual Differences reflected by these choices:

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

Effective Term
Select the requested term that the course will first be offered. Selecting "Earliest" will allow the course to be active in the earliest term after SCNS approval. If a specific term and year are selected, this should reflect the department's best projection. Courses cannot be implemented retroactively, and therefore the actual effective term cannot be prior to SCNS approval, which must be obtained prior to the first day of classes for the effective term. SCNS approval typically requires 2 to 6 weeks after approval of the course at UF.

Response:
Spring

Effective Year
Select the requested year that the course will first be offered. See preceding item for further information.

Response:
2021

Rotating Topic?
Select "Yes" if the course can&nbsp;have rotating (varying) topics. These course titles can vary by topic in the Schedule of Courses.

Response:
No

Repeatable Credit?
Select "Yes" if the course may be repeated for credit. If the course will also have rotating topics, be sure to indicate this&nbsp;in the question above.

Response:
No

Amount of Credit

Select the number of credits awarded to the student upon successful completion, or select "Variable" if the course will be offered with variable credit and then indicate the minimum and maximum credits per section. Note that credit hours are regulated by Rule 6A-10.033, FAC. If you select "Variable" for the amount of credit, additional fields will appear in which to indicate the minimum and maximum number of total credits.

Response:
3

S/U Only?

Select "Yes" if all students should be graded as S/U in the course. Note that each course must be entered into the UF curriculum inventory as either letter-graded or S/U. A course may not have both options. However, letter-graded courses allow students to take the course S/U with instructor permission.

Response:
No

Contact Type

Select the best option to describe course contact type. This selection determines whether base hours or headcount hours will be used to determine the total contact hours per credit hour. Note that the headcount hour options are for courses that involve contact between the student and the professor on an individual basis.

Response:
Regularly Scheduled

- *Regularly Scheduled [base hr]*
- *Thesis/Dissertation Supervision [1.0 headcount hr]*
- *Directed Individual Studies [0.5 headcount hr]*
- *Supervision of Student Interns [0.8 headcount hr]*
- *Supervision of Teaching/Research [0.5 headcount hr]*
- *Supervision of Cooperative Education [0.8 headcount hr]*

Contact the Office of Institutional Planning and Research (352-392-0456) with questions regarding contact type.

Weekly Contact Hours

Indicate the number of hours instructors will have contact with students each week on average throughout the duration of the course.

Response:
3

Course Description

Provide a brief narrative description of the course content. This description will be published in the Academic Catalog and is limited to 500 characters or less. See course description guidelines.

Response:
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.

Prerequisites

Indicate all requirements that must be satisfied prior to enrollment in the course. Prerequisites will be automatically checked for each student attempting to register for the course. The prerequisite will be published in the Academic Catalog and must be formulated so that it can be enforced in the registration system. Please note that upper division courses (i.e., intermediate or advanced level of instruction) must have proper prerequisites to target the appropriate audience for the course.
Courses level 3000 and above must have a prerequisite.

Response:
Computer Organization (CDA 3101) or consent of instructor

Completing Prerequisites on UCC forms:

- *Use "&" and "or" to conjoin multiple requirements; do not used commas, semicolons, etc.*
- *Use parentheses to specify groupings in multiple requirements.*
- *Specifying a course prerequisite (without specifying a grade) assumes the required passing grade is D-. In order to specify a different grade, include the grade in parentheses immediately after the course number. For example, "MAC 2311(B)" indicates that students are required to obtain a grade of B in Calculus I. MAC2311 by itself would only require a grade of D-.*
- *Specify all majors or minors included (if all majors in a college are acceptable the college code is sufficient).*
- *"Permission of department" is always an option so it should not be included in any prerequisite or co-requisite.*

Example: A grade of C in HSC 3502, passing grades in HSC 3057 or HSC 4558, and major/minor in PHHP should be written as follows:
HSC 3502(C) & (HSC 3057 or HSC 4558) & (HP college or (HS or CMS or DSC or HP or RS minor)

Co-requisites

Indicate all requirements that must be taken concurrently with the course. Co-requisites are not checked by the registration system. If there are none please enter N/A.

Response:
None

Rationale and Placement in Curriculum

Explain the rationale for offering the course and its place in the curriculum.

Response:
Reverse engineering is a critical skill for the information security professional who is often faced with identifying the intended behavior and risks associated with an executable artifact. By learning the methods associated with analyzing malware artifacts, students will learn about and employ the skills necessary to engage in effective reverse engineering. In addition, the student will learn about programming language and run-time system implementation as well as interactions between user and kernel code. In distinction to the like-named graduate course, the emphasis is more on practical understanding and skill-development than developing a theoretical model that supports the activities and methods.

Course Objectives

Describe the core knowledge and skills that student should derive from the course. The objectives should be both observable and measurable.

Response:
The student will be able to
understand and explain the behavior of assembly language programs;
identify and explain the purpose of and risks associated with various types of malware;
understand and be able to identify different types of encoding methods;
understand and be able to overcome a variety of code-obfuscation techniques employed to make reverse engineering difficult;
effectively employ a disassembler to understand the behavior of a program presented as object code;
understand and overcome methods of preventing execution of a program within a virtual machine or sandbox environment;
identify and analyze document files containing malicious executable code;
identify effectively employable indicators of compromise associated with a malware attack; and
prepare a professional report describing the methods, risks, and potential methods of risk mitigation associated with a malware infection.

Course Textbook(s) and/or Other Assigned Reading

Enter the title, author(s) and publication date of textbooks and/or readings that will be assigned. &nbsp;Please provide specific examples&nbsp;to evaluate the course.

Response:
Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software,
Sikorski Honig, 2012.

Malware Analyst's Cookbook and DVD, Ligh, Adair, Hartstein, and Richard, 2011.

Weekly Schedule of Topics

Provide a projected weekly schedule of topics. This should have sufficient detail to evaluate how the course would meet current curricular needs and the extent to which it overlaps with existing courses at UF.

Response:
1 Introduction, Basic Static Analysis
2 Netlab Intro, Basic Dynamic Analysis, x86 Crash Course I
3 x86 Crash Course II, IDA, Binary Ninja, Ghidra
4 C Code Constructs I, C Code Constructs II
5 Analyzing Malicious Windows Programs I, Analyzing Malicious Windows Programs II, Debugging and OllyDBG I
6 Debugging and OllyDBG II, Malware Behavior I, Malware Behavior II
7 Covert Malware Launching, Data Encoding, Malware Focused Network Signatures
8 Practical I Debriefing, Malware Classification Anti-Disassembly
9 Anti-Debugging, Anti-Virtual-Machine Techniques, Packers and Unpacking
10 Shellcode Analysis, C++ Analysis
11 Kernel Debugging, Memory Forensics I, Practical 2 Debriefing
12 Memory Forensics II, PDF Documents I, PDF Documents II
13 PDF Documents III, Malicious Office Documents I, Malicious Office Documents II
14 Malicious Office Documents III, Practical 3 Debriefing
15 Exam Review

Grading Scheme

List the types of assessments, assignments and other activities that will be used to determine the course grade, and the percentage contribution from each. This list should have sufficient detail to evaluate the course rigor and grade integrity. Include details about the grading rubric and percentage breakdowns for determining grades. If participation and/or attendance are part of the students grade, please provide a rubric or details &nbsp;regarding how those items will be assessed.

Response:
Quizzes consist of three multiple choice questions each, based on assigned readings. Their goal is to insure students are prepared for activities engaged in during class.

Practical exercises are reports associated with analysis of specific malware artifacts. The contents of the reports are specified by the instructor. A typical report will contain an executive summary, static analysis section, dynamic analysis section, and a discussion of indicators of compromise as well as remediation procedures. Questions to stimulate student analysis are provided in the assignment. The grading rubric is shared with students before they prepare these reports.

The final examination is multiple choice and is used as a method to insure that the student actually carried out the assignments. The questions are such that they can be readily answered by students who carried out all assignments, but likely would be impossible to answer if a student did not actually carry out that work.

Instructor(s)

Enter the name of the planned instructor or instructors, or "to be determined" if instructors are not yet identified.

Response:
Joseph N. Wilson

Attendance & Make-up

Please confirm that you have read and understand the University of Florida Attendance policy.
A required statement statement related to class attendance, make-up exams and other work will be included in the syllabus and adhered to in the course. Courses may not have any policies which conflict with the University of Florida policy. The following statement may be used directly in the syllabus.

• Requirements for class attendance and make-up exams, assignments, and other work in this course are consistent with university policies that can be found at:
https://catalog.ufl.edu/ugrad/current/regulations/info/attendance.aspx

Response:
Yes

Accomodations

Please confirm that you have read and understand the University of Florida Accommodations policy.
A statement related to accommodations for students with disabilities will be included in the syllabus and adhered to in the course. The following statement may be used directly in the syllabus:

• Students with disabilities requesting accommodations should first register with the Disability Resource Center (352-392-8565, www.dso.ufl.edu/drc/) by providing appropriate documentation. Once registered, students will receive an accommodation letter which must be presented to the instructor when requesting accommodation. Students with disabilities should follow this procedure as early as possible in the semester.

Response:
Yes

UF Grading Policies for assigning Grade Points

Please confirm that you have read and understand the University of Florida Grading policies.
Information on current UF grading policies for assigning grade points is require to be included in the course syllabus. The following link may be used directly in the syllabus:

• https://catalog.ufl.edu/ugrad/current/regulations/info/grades.aspx

Response:
Yes

Course Evaluation Policy

Course Evaluation Policy
Please confirm that you have read and understand the University of Florida Course Evaluation Policy.
A statement related to course evaluations will be included in the syllabus. The following statement may be used directly in the syllabus:

• <span style="font-size:11.0pt">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&nbsp;https://gatorevals.aa.ufl.edu/public-results/. 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&nbsp;<a href="https://ufl.bluera.com/ufl/" target="_blank">https://ufl.bluera.com/ufl/</a>. Summaries of course evaluation results are available to students at&nbsp;<a href="https://gatorevals.aa.ufl.edu/public-results/">https://gatorevals.aa.ufl.edu/public-results/</a>.</span>

&nbsp;

Response:
Yes

Malware Reverse Engineering

CAP 6137

Class Periods: MWF, Period 6 (12:55-1:45)

Location: E309 CSE

Academic Term: Spring 2021

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: M 3:00-3:50, T 10:40-12:40

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

Students will learn how to safely and thoroughly analyze malicious software. Such analysis will be aimed at understanding the behavior and potential security impacts of such code. Students will learn a variety of static and dynamic analysis techniques that help them understand a program's structure and behavior. The class will cover a variety of anti-forensic techniques employed by malware and how to avoid or overcome them. A large number of software tools will be employed during the class and students will become familiar with them through hands-on application during analysis of actual malware samples. In addition to preparing students to be able to analyze new malware artifacts, the course will provide a very good background for understanding, analyzing, and developing low-level code.

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

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.
The IDA Pro Book, 2nd Ed. Chris Eagle, No Starch Press, June 2011.

Course Schedule (based on proposed UF schedule delaying class start and deleting spring break)

1 Jan 11 Introduction
2 Jan 13 Basic Static Analysis
3 Jan 15 Netlab Intro

4 Jan 20 Basic Dynamic Analysis
5 Jan 22 x86 Crash Course I

6 Jan 25 x86 Crash Course II
7 Jan 27 IDA
8 Jan 29 Binary Ninja

9 Feb 1 C Code Constructs I
10 Feb 3 C Code Constructs II
11 Feb 5 Analyzing Malicious Windows Programs I

12 Feb 8 Analyzing Malicious Windows Programs II
13 Feb 11 Debugging and OllyDBG I
14 Feb 13 Debugging and OllyDBG II

15 Feb 15 Malware Behavior I
16 Feb 17 Malware Behavior II
17 Feb 19 Covert Malware Launching

18 Feb 22 Data Encoding
19 Feb 24 Malware Focused Network Signatures
20 Feb 26 Practical I Debriefing

21 Mar 1 Malware Classification
22 Mar 3 Anti-Disassembly
23 Mar 5 Anti-Debugging

24 Mar 8 Anti-Virtual-Machine Techniques
25 Mar 10 Packers and Unpacking
26 Mar 12 Shellcode Analysis

27 Mar 15 C++ Analysis
28 Mar 17 Catch-up Class
29 Mar 19 Kernel Debugging

30 Mar 22 Memory Forensics I
31 Mar 24 Practical 2 Debriefing
32 Mar 26 Memory Forensics II

33 Mar 29 PDF Documents I
34 Mar 31 PDF Documents II
35 Apr 2 PDF Documents III

36 Apr 5 Malicious Office Documents I
37 Apr 7 Malicious Office Documents II
38 Apr 9 Malicious Office Documents III

39 Apr 12 Catch-up Class
40 Apr 14 Practical 3 Debriefing
41 Apr 16 Breaking Reverse Engineering Trends

42 Apr 19 Exam Review 1
43 Apr 21 Exam Review 2

F2F Course Policy in Response to COVID-19

We will have face-to-face instructional sessions to accomplish the student learning objectives of this course. In response to COVID-19, the following policies and requirements are in place to maintain your learning environment and to enhance the safety of our in-classroom interactions.

- You are required to wear approved face coverings at all times during class and within buildings. Following and enforcing these policies and requirements are all of our responsibility. Failure to do so will lead to a report to the Office of Student Conduct and Conflict Resolution.
- This course has been assigned a physical classroom with enough capacity to maintain physical distancing (6 feet between individuals) requirements. Please utilize designated seats and maintain appropriate spacing between students. Please do not move desks or stations.
- Sanitizing supplies are available in the classroom if you wish to wipe down your desks prior to sitting down and at the end of the class.
- Follow your instructor's guidance on how to enter and exit the classroom. Practice physical distancing to the extent possible when entering and exiting the classroom.
- If you are experiencing COVID-19 symptoms (Click here for guidance from the CDC on symptoms of coronavirus), please use the UF Health screening system and follow the instructions on whether you are able to attend class. Click here for UF Health guidance on what to do if you have been exposed to or are experiencing Covid-19 symptoms.
- Course materials will be provided to you with an excused absence, and you will be given a reasonable amount of time to make up work. Find more information in the university attendance policies.

Attendance Policy, Class Expectations, and Make-Up Policy

Attendance is optional. All students are expected to comport themselves in a professional manner. UF policies for absences, illness, etc. will be followed. (http://handbook.aa.ufl.edu/teaching/policies/)

Evaluation of Grades

Assignment	**Total Points**	**Percentage of Final Grade**
Quizzes (best 35 of 40)	3 each	20%
Practical Exercises (4)	100 each	50%
Final Exam	100	30%
		100%

Grading Policy

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:
http://gradcatalog.ufl.edu/content.php?catoid=10&navoid=2020#grades

Differences Between This Course and CAP 4XXX

- 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 a *safe-harbor* 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.

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.

Malware Reverse Engineering

CAP 4XXX
Class Periods: MWF, Period 6 (12:55-1:45)
Location: E309 CSE
Academic Term: Spring 2021

Instructor:
TBA

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

Students will learn how to safely and thoroughly analyze malicious software. Such analysis will be aimed at understanding the behavior and potential security impacts of such code. Students will learn a variety of static and dynamic analysis techniques that help them understand a program's structure and behavior. The class will cover a variety of anti-forensic techniques employed by malware and how to avoid or overcome them. A large number of software tools will be employed during the class and students will become familiar with them through hands-on application during analysis of actual malware samples. In addition to preparing students to be able to analyze new malware artifacts, the course will provide a very good background for understanding, analyzing, and developing low-level code.

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

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.
The IDA Pro Book, 2nd Ed. Chris Eagle, No Starch Press, June 2011.

Course Schedule (based on proposed UF schedule delaying class start and deleting spring break)

1 Jan 11 Introduction
2 Jan 13 Basic Static Analysis
3 Jan 15 Netlab Intro

4 Jan 20 Basic Dynamic Analysis
5 Jan 22 x86 Crash Course I

6 Jan 25 x86 Crash Course II
7 Jan 27 IDA
8 Jan 29 Binary Ninja

9 Feb 1 C Code Constructs I
10 Feb 3 C Code Constructs II
11 Feb 5 Analyzing Malicious Windows Programs I

12 Feb 8 Analyzing Malicious Windows Programs II
13 Feb 11 Debugging and OllyDBG I
14 Feb 13 Debugging and OllyDBG II

15 Feb 15 Malware Behavior I
16 Feb 17 Malware Behavior II
17 Feb 19 Covert Malware Launching

18 Feb 22 Data Encoding
19 Feb 24 Malware Focused Network Signatures
20 Feb 26 Practical I Debriefing

21 Mar 1 Malware Classification
22 Mar 3 Anti-Disassembly

23 Mar 5 Anti-Debugging

24 Mar 8 Anti-Virtual-Machine Techniques
25 Mar 10 Packers and Unpacking
26 Mar 12 Shellcode Analysis

27 Mar 15 C++ Analysis
28 Mar 17 Catch-up Class
29 Mar 19 Kernel Debugging

30 Mar 22 Memory Forensics I
31 Mar 24 Practical 2 Debriefing
32 Mar 26 Memory Forensics II

33 Mar 29 PDF Documents I
34 Mar 31 PDF Documents II
35 Apr 2 PDF Documents III

36 Apr 5 Malicious Office Documents I
37 Apr 7 Malicious Office Documents II
38 Apr 9 Malicious Office Documents III

39 Apr 12 Catch-up Class
40 Apr 14 Practical 3 Debriefing
41 Apr 16 Breaking Reverse Engineering Trends

42 Apr 19 Exam Review 1
43 Apr 21 Exam Review 2

F2F Course Policy in Response to COVID-19

We will have face-to-face instructional sessions to accomplish the student learning objectives of this course. In response to COVID-19, the following policies and requirements are in place to maintain your learning environment and to enhance the safety of our in-classroom interactions.

- You are required to wear approved face coverings at all times during class and within buildings. Following and enforcing these policies and requirements are all of our responsibility. Failure to do so will lead to a report to the Office of Student Conduct and Conflict Resolution.
- This course has been assigned a physical classroom with enough capacity to maintain physical distancing (6 feet between individuals) requirements. Please utilize designated seats and maintain appropriate spacing between students. Please do not move desks or stations.
- Sanitizing supplies are available in the classroom if you wish to wipe down your desks prior to sitting down and at the end of the class.
- Follow your instructor's guidance on how to enter and exit the classroom. Practice physical distancing to the extent possible when entering and exiting the classroom.
- If you are experiencing COVID-19 symptoms (Click here for guidance from the CDC on symptoms of coronavirus), please use the UF Health screening system and follow the instructions on whether you are able to attend class. Click here for UF Health guidance on what to do if you have been exposed to or are experiencing Covid-19 symptoms.
- Course materials will be provided to you with an excused absence, and you will be given a reasonable amount of time to make up work. Find more information in the university attendance policies.

Attendance Policy, Class Expectations, and Make-Up Policy

Attendance is optional. 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, namely: attendance, 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.

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 (best 35 of 40)	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 a *safe-harbor* 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.