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	10/9/2020 11:25:29 AM
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
ChangesFor2020-10-02CCMeeting.pdf					9/30/2020
College	Approved	ENG - College of Engineering	Heidi Dublin	Approved by Curriculum Committee and Faculty Council.	10/9/2020
ugradMalwareReverseEngineeringSyllabus.pdf gradMalwareReverseEngineeringSyllabus.pdf ChangesFor2020-10-04UCCMeeting.pdf					10/2/2020 10/2/2020 10/2/2020
University Curriculum Committee	Pending	PV - University Curriculum Committee (UCC)			10/9/2020
No document changes					
Statewide Course Numbering System					
No document changes					
Office of the Registrar					
No document changes					

Original file: Cover sheet.pdf

Step	Status	Group	User	Comment	Updated
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 CAP
Course Level 4
Course Number XXX
Category of Instruction Advanced
Lab Code None
Course Title Malware Reverse Engineering
Transcript Title Malware Reverse Engineering
Degree Type Baccalaureate

Delivery Method(s) On-Campus
Co-Listing Yes
Co-Listing Explanation
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 Spring
Effective Year 2021
Rotating Topic? No
Repeatable Credit? No

Amount of Credit 3

S/U Only? No
Contact Type Regularly Scheduled
Weekly Contact Hours 3
Course Description 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 Computer Organization (CDA 3101) or consent of instructor
Co-requisites None
Rationale and Placement in Curriculum 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 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 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 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 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) Joseph N. Wilson
Attendance & Make-up Yes
Accomodations Yes
UF Grading Policies for assigning Grade Points Yes
Course Evaluation Policy Yes

Changes:

1. Modified form 14852 to better explain co-listing.
   (CAP 6137, the graduate version of this course, is currently in our catalog and is being offered. The undergraduate class has been offered as CIS 4930 in the past.)
2. Modified both undergrad and grad syllabi to follow HWCOE 2020 syllabus structure.
3. Added description of differences between the undergrad and grad class to both syllabi.
4. Attached graduate syllabus to this new course request.
5. Provided more detail on attendance grade.
6. Updated schedule to match proposed UF spring calendar (starting one week late and deleting spring break).
7. Removed critical tracking language.
8. Removed instructor information from undergraduate course syllabus.
9. Attached this document to this new course request.

Changes:

1) Further modified language describing the differences between the graduate and undergraduate courses. I specifically noted that:

   a) In the undergraduate course Attendance is 10% and final exam is 20% vs. final exam being 30% for the graduate students. I want to ensure the undergraduates are exposed to more information and get credit for that activity. On the other hand, I want to ensure that graduate students take their learning role seriously and know the material well without having to be carried along.

   b) The undergraduates and graduates complete the same first three practical exercises, analyzing malware I have chosen. The graduate students must identify an appropriately complex and representative malware artifact to analyze for their fourth project. One can consider this to be a stretch assignment, as they will be working individually and will not be able to get guidance or assistance from others analyzing the same artifact. In addition, the graduate students are required to give a presentation discussing their analysis of this last malware artifact.

      Undergraduates are graded on their best three of four assignments. The fourth assignment for the undergraduates is one that I choose specifically to make sure that those who may have had difficulty with the first three assignments will have and assignment on which they can succeed. This is optional for those students who have done well enough on the first three assignments, but provides *safe harbor* for those who may have had trouble.

2) Attached this document to this new course request.

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.

Original file: gradMalwareReverseEngineeringSyllabus.pdf

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

  For undergraduates, attendance provides credit equivalent to 1/3 of the graduate final examination credit.

- Nature of the fourth practical assignment:

  Graduate students: Each student, individually, will select a 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. Graduates will present their analysis to the class.

  Undergraduates: A single malware sample chosen by the instructor as being appropriate for an undergraduate level of experience and ability will be assigned to all students. With the experienced gained during the semester, this malware artifact 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.

- Conceptual Differences reflected by these choices:
  For undergraduates, the emphasis is more on practice that developing a deep understanding, thus the emphasis on attendance 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.

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 defined by physical presence in class (for classes that meet in person) or virtual presence in classes meeting online. Each class provides one attendance point toward the attendance total. Excused absences must be consistent with university policies in the Undergraduate Catalog and require appropriate documentation. (https://catalog.ufl.edu/UGRD/academic-regulations/attendance-policies/#absencestext)

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

Assignment	Total Points	Percentage of Final Grade
Attendance (at 38 of 43 classes)	38	10%
Quizzes (best 35 of 40)	3 each	20%
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: 10% Attendance, 20% Quizzes, 50% Practical Exercises, 20% Final Examination

  For undergraduates, attendance provides credit equivalent to 1/3 of the graduate final examination credit.

- Nature of the fourth practical assignment:

  Graduate students: Each student, individually, will select a 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. Graduates will present their analysis to the class.

  Undergraduates: A single malware sample chosen by the instructor as being appropriate for an

undergraduate level of experience and ability will be assigned to all students. With the experienced gained during the semester, this malware artifact 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.

- Conceptual Differences reflected by these choices:
  For undergraduates, the emphasis is more on practice that developing a deep understanding, thus the emphasis on attendance 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.

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.