CAP 6137/COP 4930 Malware Reverse Engineering, Spring 2015
University of Florida

Note: Differences between the method of evaluation in this course and the like-named graduate course are underlined in item 16.

1. Catalog Description – (3 credit hours) Introduction to the theory and practice of software reverse engineering applied to analysis of malicious software (malware). Students learn techniques of static and dynamic analysis to help identify the behavior of programs presented without documentation or source code and to identify possible remediation and avoidance techniques.
2. Pre-requisites and Co-requisites
   Pre-requisite: Computer Organization (CDA 3101)
   Co-requisite: Operating Systems (COP 4600) or consent of instructor
3. 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.
4. Contribution of course to meeting the professional component
   This course provides 2 credit hours of engineering design.
5. Relationship of course to program outcomes:
   a, b, g, h, i, j, k.
6. Instructor
   a. Office location: CSE E472
   b. Telephone: 352-514-2191
   c. E-mail address: jnw@cise.ufl.edu
   d. Class Web site: http://www.cise.ufl.edu/~jnw/cis4930sp14/
   e. Office hours: TBA
7. Teaching Assistant: Jeremiah Blanchard
   a. Office location: Offsite
   b. Telephone: jeremiah.blanchard@gmail.com
   c. Office hours: TBA

   Undergraduate Assistant
   a. Office location: None
   b. email: vincent.moscatello@gmail.com
   c. Office hours: None

8. Meeting Times
   MWF 6
9. Class/laboratory schedule, i.e., number of sessions each week and duration of each session
   Class meetings only, 50 minutes per class
10. Meeting Location
    CSE E309
11. Material and Supply Fees
    $??
12. Textbooks and Software Required
    a. Title: Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software
    b. Author: Michael Sikorski and Andrew Honig
    c. Publication date: 2012,
    d. ISBN: ISBN 978-1-59327-290-6

    Software: 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.
13. Recommended Reading
    PC Assembly Language, Paul Carter, June 2006.
    Intel® 64 and IA-32 Architectures Software Developer Manuals, Intel.
    The IDA Pro Book, 2nd Ed. Chris Eagle, No Starch Press, June 2011.
    Malware Analysis Lab Safety Poster, Wesley McGrew, Mississippi State University, National Forensics Training Center.
14. Course Outline (43 lecture hours)
    a. 7 Jan. (0) Malware Analysis Primer, Class Intro, Group formation, Malware Analysis Primer, NDG NetLab
    b. 9, 12 Jan. (1) Basic static techniques (2) Malware analysis in virtual machines
    c. 14, 16, 21 Jan. (3) Basic dynamic analysis
    d. 23, 26 Jan. (4) Crash course in x86 disassembly
    e. 26,28 Jan. (5) IDA Pro
    f. 2, 4 Feb. (6) Recognizing C code constructs in assembly
    g. 6, 9 Feb. (7) Analyzing malicious windows programs
    h. 11, 13 Feb. (8) Debugging, (9) OllyDbg
    i. 16 Feb. (10) Kernel debuggins with WinDbg
    j. 18 Feb (18) Packers and unpacking
    k. 20, 23 Feb. (11) Malware Behavior
    l. 25, 27 Feb. (12) Covert malware launching
    m. 9, 11 Mar. (13) Data encoding
    n. 13, 16 Mar. (14) Malware-focused network signatures
    o. 18, 20 Mar. (15) Anti-disassembly
    p. 23, 25 Mar. (16) Anti-debugging
    q. 27, 30 Mar. (17) Anti-virtual-machine techniques
    r. 1, 3 Apr. (19) Shellcode analysis
    s. 6, 8 Apr. (20) C++ analysis

t. 10, 13, 15, 17 Apr. Malicious Documents
u. 20, 22 Apr. Review

Final Examination (Period): 1 May 3:00 p.m. - 5:00 p.m.

15. Attendance and Expectations
Students are expected to attend every class. University of Florida policy for excused absences applies. Requirements for make-up exams, assignments, and other work in this course are consistent with university policies that can be found in the online catalog at: https://catalog.ufl.edu/ugrad/current/regulations/info/attendance.aspx.
16. Grading – methods of evaluation
Attendance is equally weighted for every class period. Excused absences (see course catalog) will not be deducted nor will three unexcused absences. Any other absence is deducted from your attendance grade. A quiz will be given in each class after the first class meeting.
Grading is based on:
10% Attendance CIS 4930 (0% Attendance CAP 6137)
20% Quizzes
50% 3 Practical exercises CIS 4930 (50% 4 Practical exercises CAP 6137)
20% Final examination CIS 4930 (30% Final examination CAP 6137)
17. Grading Scale
Numeric grade g is mapped to a letter grade as specified below

A $93 \leq g \leq 100$
A- $90 \leq g < 93$
B+ $87 \leq g < 90$
B $83 \leq g < 87$
B- $80 \leq g < 83$
C+ $77 \leq g < 80$
C $73 \leq g < 77$
C- $70 \leq g < 73$
D+ $67 \leq g < 70$
D $63 \leq g < 67$
D- $60 \leq g < 63$
F $0 \leq g < 60$

A C- will not be a qualifying grade for critical tracking courses. In order to graduate, students must have an overall GPA and an upper-division GPA of 2.0 or better (C or better). Note: a C- average is equivalent to a GPA of 1.67, and therefore, it does not satisfy this graduation requirement. For more information on grades and grading policies, please visit:
https://catalog.ufl.edu/ugrad/current/regulations/info/grades.aspx
18. Requirements for class attendance and make-up exams, assignments, and other work are consistent with university policies that can be found at:
https://catalog.ufl.edu/ugrad/current/regulations/info/attendance.aspx
19. 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 (http://www.dso.ufl.edu/sccr/process/student-conduct-honor-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.

Note that failure to comply with this commitment will result in disciplinary action compliant with the UF Student Honor Code Procedures.
See http://www.dso.ufl.edu/sccr/procedures/honorcode.php

20. Accommodation for Students with Disabilities – Students Requesting classroom accommodation must first register with the Dean of Students Office. That office will provide the student with documentation that he/she must provide to the course instructor when requesting accommodation.
21. UF Counseling Services –Resources are available on-campus for students having personal problems or lacking clear career and academic goals. The resources include:
    - UF Counseling & Wellness Center, 3190 Radio Rd, 392-1575, http://www.counseling.ufl.edu/cwc/Default.aspx, counseling services and mental health services.
    - Career Resource Center, Reitz Union, 392-1601, career and job search services.
    - University Police Department 392-1111
22. Software Use – All faculty, staff and student 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.
23. Students are expected to provide feedback on the quality of instruction in this course based on 10 criteria. These evaluations are conducted online at https://evaluations.ufl.edu. Evaluations are typically open during the last two or three weeks of the semester, but students will be given specific times when they are open. Summary results of these assessments are available to students at https://evaluations.ufl.edu/results.