1. Catalog 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.

2. Pre-requisites and Co-requisites
   Pre-requisite: Computer Organization (CDA 3101 or consent of instructor)
   Co-requisite: Operating Systems (COP 4600 or COP 5615) or consent or 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 E471
   b. Telephone (personal cell): 352-514-2191
   c. E-mail address: jnw@cise.ufl.edu
   d. Class Web site: https://www.cise.ufl.edu/class/cap6137sp17/
   e. Canvas Site: https://ufl.instructure.com/courses/337630
   f. Office hours: TBA

7. Teaching Assistant
   a. Office location: TBA
   b. Telephone: TBA
   c. E-mail address: TBA
   d. Office hours:

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
    Unknown

12. Textbooks and Software Required
    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
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
- Practical Reverse Engineering..., B. Dang, A. Gazet, E. Bachaalany, S. Josse
- Intel® 64 and IA-32 Architectures Software Developer Manuals, Intel.

14. Course Outline (42 lecture hours)
1  Jan  4 Introduction
2  Jan  6 Basic Static Analysis
3  Jan  9 Netlab Intro
4  Jan 11 Basic Dynamic Analysis
5  Jan 13 x86 Crash Course I
6  Jan 18 x86 Crash Course II
7  Jan 20 IDA
8  Jan 23 Binary Ninja
9  Jan 25 C Code Constructs I
10 Jan 27 C Code Constructs II
11 Jan 30 Analyzing Malicious Windows Programs I
12 Feb  1 Analyzing Malicious Windows Programs II
13 Feb  3 Debugging and OllyDBG I
14 Feb  6 Debugging and OllyDBG II
15 Feb  8 Malware Behavior I
16 Feb 10 Malware Behavior II
17 Feb 13 Covert Malware Launching
18 Feb 15 Data Encoding
19 Feb 17 Malware Focused Network Signatures
20 Feb 20 Practical I Debriefing
21 Feb 22 Malware Classification
22 Feb 24 Anti-Disassembly
23 Feb 27 Anti-Debugging
24 Mar  1 Anti-Virtual-Machine Techniques
25 Mar  3 Packers and Unpacking
26 Mar 13 Shellcode Analysis
27 Mar 15 C++ Analysis
28 Mar 17 Catch-up Class
29 Mar 20 Kernel Debugging
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
   Graduate section grading is based on:
   - 20% Quizzes
   - 50% 4 Practical exercises
   - 30% Final examination
   Undergraduate section grading is based on:
   - 10% Attendance
   - 20% Quizzes
   - 50% 3 Practical exercises
   - 20% Final examination

17. Grading Scale
   Numeric grade g is mapped to a letter grade as specified below

   \begin{align*}
   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 
   \end{align*}

   Graduate students, in order to graduate, must have an overall GPA of 3.0 or better (B or better). Note: a B- average is equivalent to a GPA of 2.67, and therefore, it does not satisfy this graduation requirement.
For undergraduate students, 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/sscc/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/sscc/procedures/honorcode.php

20. Accommodation for Students with Disabilities – Students Requesting classroom accommodation must 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.

21. UF Counseling Services – Resources are available on-campus for students having personal problems or lacking clear career and academic goals. The resources include:
   - 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 by completing online evaluations 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/.