ECE/CPSC 8830: Malware Reverse Engineering
Section 001 (Clemson Main Campus)
Section 843 (Charleston Zucker)

Part I: Course-Specific Information

Class Location/Time	Locations: Room 226, Riggs Hall, Clemson (Main Campus) Room 104, Charleston Zucker Grad Center Time: Tues. and Thurs., 5:00 p.m.– 6:15 p.m.
Instructor	Lu Yu (luy@clemson.edu), 300B Riggs Hall
Instructor's Office Hours	• In-person and online. Zoom link will be announced on Canvas. • 4:00 – 5:00 p.m.@Tues. • Other times **by appointment**. Email me directly and **Never** message me on Canvas.
Grader	Shuang Wang (swang8@g.clemson.edu)
Course Modality	In-person.
Prerequisites	Basic understanding of C, assembly and Windows OS.
Instructor being late	The students are expected to wait for **15 mins** for the instructor if the instructor is late for the class.
Important Dates	• Jan. 24th, Wed. – Last day to drop a class or withdraw from the University **without** a W grade. • Mar. 15th, Fri. – Last day to drop a class or withdraw from the University **without** final grades but **with** a W grade.

Course Description

Malware analysis is a critical skill in the information security community. Because understanding the purposes and capabilities of malware is critical to derive threat intelligence, respond to information security incidents, and produce effective countermeasures. This course will help the students understand the core skills required in malware investigations and analysis, and guide the students through the basic requirements and necessary skill sets required in order to take your knowledge to the next level. This course focuses on Malwares that target Windows because Windows is the most popular operating systems in the world, which makes Windows computers are the target of most malware attacks.

Student Learning Outcomes

Upon completion of this course, students should be able to:

1. Describe the basic flow of malware analysis.
2. Understand the differences between static analysis and dynamic analysis.

3. Use static malware analysis skills/tools to perform preliminary analysis of suspicious software.
4. Set up the safe environment for dynamic analysis.
5. Use static malware analysis skills/tools to conduct basic dynamic malware analysis of suspicious software.
6. Read assembly and maybe infer basic source C code structs from it.
7. Get familiar with IDA Pro and use IDA Pro to perform some advanced static analysis of suspicious software.
8. Get familiar with debuggers and use the right debugger to perform some advanced dynamic analysis of suspicious software.
9. Have a better understanding of the world's most popular operating system – Windows.
10. Have some knowledge about the vulnerabilities of Windows.
11. Gain enough basics to continue self-study the rest of the chapters of the textbook.

Required Materials

Required textbook: Sikorski, M., & Honig, A. (2012). *Practical malware analysis: the hands-on guide to dissecting malicious software*. no starch press. (Available online at: http://dtors.net/Hacking/Practical%20Malware%20Analysis.pdf)

The binaries for the textbook labs can be downloaded from (**Warning**: The lab binaries contain malicious code and you should not install or run these programs without first setting up a safe environment, i.e., a VM!!!):
https://github.com/mikesiko/PracticalMalwareAnalysis-Labs

A number of security-related URL's, videos and other information will be provided. Use of open source tools for system implementation is strongly encouraged. Books worth referring to:

- Eldad Eilam, *Reversing: Secrets of Reversing Engineering*
- Chris Eagle, *IDA Pro Book*
- Abhijit Mohanta, Anoop Saldanha, *Malware Analysis and Detection Engineering*.

Topical Outline

Part 1: Introduction
Part 2: Basic static analysis
Part 3: Basic dynamic analysis
Part 4: Disassembly
Guest Lecture*
Part 5: IDA Pro
Part 6: C code construct
Part 7: Malicious Windows program
Part 9: Debugger

Part 10: Olly debugger

Note that we may have more than one guest lecture or none.

Grading Policies

Final grades will be based on the following weights:

- 50% homework (three assignments),
- 25% midterm exam (take home),
- 25% final (take-home)

The following are the point ranges/percentages associated with each letter grade.

A – 90% - 100%; B – 80 to < 90%; C – 70 to < 80%; D – 60 to < 70 & F – < 60%

Exams: No make-up exams will be given because both are all take-home exams.

Homework: Submission of homework will be electronical by uploading the scan of your report to Canvas throughout the semester. All assignments are due at the time and date specified on the assignment. No late assignments will be accepted, and they are due at the time class begins.

Re-grades: Re-grade requests must be sent to the instructor via email within one week of the return of the graded item.

Attendance Policy

Physical attendance is mandatory. At least five roll calls[1] are expected throughout the semester in addition to the pop-up quizzes. 0.5 points will be deducted for each missing attendance. The roll calls start from the second week of the semester.

In the case of an absence from class, the student should use the Notification of Absence module in Canvas to notify the instructor (via an email) of and provides for the following categories: court attendance, death of immediate family member, illness, illness of family member, injury, military duty, religious observance, scheduled surgery, university function, unscheduled hospitalization, other anticipated absence, or other unanticipated absence.

[1] Canvas submission of an in-class selfie with the on-whiteboard mark in the background by 5:30 p.m.

Part II: University Policies and Student Support

Academic Integrity

As members of the Clemson University community, we have inherited Thomas Green Clemson's vision of this institution as a "high seminary of learning." Fundamental to this vision is a mutual commitment to truthfulness, honor, and responsibility, without which we cannot earn the trust and respect of others. Furthermore, we recognize that academic dishonesty detracts from the value of a Clemson degree. Therefore, we shall not tolerate lying, cheating, or stealing in any form.

All infractions of academic dishonesty by undergraduates must be reported to Undergraduate Studies for resolution through that office. In cases of plagiarism instructors may use the Plagiarism Resolution Form.

See the Undergraduate Academic Integrity Policy website for additional information and the current catalogue for the policy.

For graduate students, see the current graduate student handbook for all policies.

Access Accommodations

Clemson University values the diversity of our student body as a strength and a critical component of our dynamic community. Students with disabilities or temporary injuries/conditions may require accommodations due to barriers in the structure of facilities, course design, technology used for curricular purposes, or other campus resources. Students who experience a barrier to full access to this class should let the instructor know and make an appointment to meet with a staff member in Student Accessibility Services as soon as possible. You can make an appointment by calling 864-656-6848, by emailing studentaccess@lists.clemson.edu, or by visiting Suite 239 in the Academic Success Center building. Appointments are strongly encouraged – drop-ins will be seen, if at all possible, but there could be a significant wait due to scheduled appointments. Students who have accommodations are strongly encouraged to request, obtain and send these to their instructors through the AIM portal as early in the semester as possible so that accommodations can be made in a timely manner. It is the student's responsibility to follow this process each semester.

You can access further information at the Student Accessibility website. Other information is at the university's Accessibility Portal.

Anti-Harassment and Non-Discrimination

The Clemson University Title IX statement: Clemson University is committed to a policy of equal opportunity for all persons and does not discriminate on the basis of race, color, religion, sex,

sexual orientation, gender, pregnancy, national origin, age, disability, veteran's status, genetic information or protected activity in employment, educational programs and activities, admissions and financial aid. This includes a prohibition against sexual harassment and sexual violence as mandated by Title IX of the Education Amendments of 1972. This Title IX policy is located on the Campus Life website. Ms. Alesia Smith is the Clemson University Title IX Coordinator, and the Executive Director of Equity Compliance. Her office is located at 223 Brackett Hall, 864.656.0620. Remember, email is not a fully secured method of communication and should not be used to discuss Title IX issues.

Emergency Procedures

Emergency procedures have been posted in all buildings and on all elevators. Students should be reminded to review these procedures for their own safety. All students and employees should be familiar with guidelines from the Clemson Police Department. Visit here for information about safety.

Clemson University is committed to providing a safe campus environment for students, faculty, staff, and visitors. As members of the community, we encourage you to take the following actions to be better prepared in case of an emergency:

a. Ensure you are signed up for emergency alerts
b. Download the Rave Guardian app to your phone (https://www.clemson.edu/cusafety/cupd/rave-guardian/)
c. Learn what you can do to prepare yourself in the event of an active threat (http://www.clemson.edu/cusafety/EmergencyManagement/)

Copyright Statement

Materials from published sources (books, articles, and even videos) are protected under copyright. When used for educational purposes, they are intended for use only by students enrolled in a particular course and only for instructional activities associated with the course. They may not be retained in another medium or disseminated further as described in the provisions of the Teach Act. Students should refer to the Clemson Libguide Use of Copyrighted Materials and the "Fair Use Guidelines" policy on the Clemson University website f