ECE 8930-011/843 & CPSC 8810-008/009
Malware Reverse Engineering
Spring 2020

Instructor and contact information:

Lu Yu
300C Riggs Hall
Email : luy@g.clemson.edu

Grader:

Chunpeng Shao
15C Riggs Hall
Email: chunpes@g.clemson.edu

Office hours:

Tues. 4:00 PM – 5:00 PM,
Or by appointment

Class meeting times and location:

Tues. & Thurs. 5:15PM – 6:30 PM
Riggs 223 (Clemson)
Charleston Zucker (Charleston)

Attendance Policy: Unless otherwise stated on the course specific syllabus, **students are expected to attend class, and to arrive on time**.

In the event of an **emergency**, students should contact the course instructor, preferably before class or the exam. Students should speak with instructors regarding any scheduled absence as soon as possible and develop a plan for any make-up work, if allowed by the instructor. It is the student's responsibility to secure documentation of emergencies, if required by the instructor. A student with an excessive number of absences may be withdrawn at the discretion of the course instructor.

If the instructor is late, students are expected to wait 15 minutes for the instructor to arrive.

Any further attendance policies in place will be listed on the course specific syllabus, and will serve to supplement these 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 professor 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 possible, but there could be a significant wait due to scheduled appointments. Students who receive Academic Access Letters are strongly encouraged to request, obtain and present these to their professors 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 here: https://www.clemson.edu/academics/studentaccess/index.html .

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. In instances where academic standards may have been compromised, Clemson University has a responsibility to respond appropriately to charges of violations of academic integrity.

Further information on Academic Integrity can be found in the *Undergraduate Announcements* and in the *Graduate School Policy Handbook*.

Anti-harassment and Non-Discrimination: 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 policy is located at http://www.clemson.edu/campus-life/campus-services/access/title-ix/. Ms. Alesia Smith is the Clemson University Title IX Coordinator, and the Executive Director of Equity Compliance. Her office is located at 110 Holtzendorff Hall, 864.656.3181 (voice) or 864.656.0899 (TDD).

Objectives and Outcomes: The objective of this course is to familiarize students with the practice of reverse engineering suspicious files by utilizing static and dynamic tactics, techniques, and procedures in order to gain an understanding as to what impact the suspicious file may have on a particular computer system when executed. We expect the students to gain lots of hands-on experience with malware analysis tools and techniques.

A note on ethics, legal issues and etiquette: In order to develop and maintain secure systems, it is necessary to fully understand system vulnerabilities. This understanding is best attained by mimicking the mindset of potential attackers. This course provides students with facilities and resources for exploring system vulnerabilities. It is expected that any exploits attempted will be carefully designed with a specific purpose in mind. Exploit designs will be documented and delivered to the instructor before implementation occurs. They will involve neither physical access to machines nor vandalism (including destruction of software or hardware infrastructure). Exploits will most often involve violating system confidentiality, consistency, and/or non-repudiation attributes.

- **All the exercises and assignments MUST be conducted on the provided Virtual Macine!!! Any consequences due to operations on a production machine will be your responsibility.**
- **Do NOT update the provided Windows XP VM!**
- **Always bring your laptop with the Windows XP VM installed. We might have some in-class exercises.**

Attacks on operational networks potentially violate existing laws with severe consequences. Illegal activity is not condoned and will be dealt with severely. Red team analysis of systems should be performed with the informed consent of the owners of the system being analyzed and not in connection with this course.

Resources: This course is project oriented. Students are expected to independently find the resources needed to fulfill their assignments. They will also write a number of reports and present their results. Most lectures will be run as a seminar with the instructor questioning the students. The instructor is available to the students for discussion of design alternatives and as an information resource.

Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software is the required text.

The binaries for the book 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*

Assignments: For assignments and presentations, 4-5 assignments will be given throughout the semester. Written assignments must be turned in before the start of class on the day they are due. No credit is given for late assignments.

Grading:

- Attendance (5%)
- Assignments (45%)
- Midterm (20%)
- Final (20%)

A – 90 or above
B – 80 to 89
C – 70 to 79
D – 60 to 69
F – Below 60

Deadlines are given when the assignments are given. Once given, deadlines are fixed. No extensions will be given. No late assignments will be accepted. This means that assignments are due at the start of class. No credit will be given for a late assignment. Printers printing slowly are not an adequate excuse for a late assignment. Presentations are interactive. Students must be prepared to answer questions from the instructor and other students. Documents must be professionally prepared. Sloppy and poorly written documents will be graded harshly. Students may be asked to re-write the document to make it fulfill professional standards. The documentation is due at the start of class on the due date. Presentations will be given during the week. A sign-up sheet will be circulated in class.