CAP 6135: Malware and Software Vulnerability Analysis

Spring 2023

Instructor: Dr. Cliff Zou (HEC 243), 407-823-5015, changchun.zou@ucf.edu

Course Time: TuTh 9am - 10:15am, BA1-216

Office Hour: TuTh 10:30am - 12:00pm. My office is HEC-243. You can either come to my office physically, or call my office phone (407-823-5015), or join office hour Zoom meeting via
link: https://ucf.zoom.us/j/94378849490?pwd=bExIc3pjNzRpbXEwRCt1dDVlYjYzZz09 Links to an external site.

Prerequisite: (MSDF major) or CDA5106 or COT5405

Good programming knowledge (the course has 3 programming assignments);

Knowledge on computer architecture, algorithm, and networking;

Knowledge of basic usage of Unix machine.

Description:

This course will provide an introduction to several important aspects about malicious codes and software security, including Internet virus/ worm/ spam, typical software vulnerabilities (e.g., buffer overflow), software fuzz testing, secure programming, vulnerability prevention techniques, etc. In addition, we will provide representative research papers on software security and malware research for students to read, present and discuss in order to learn the frontier of software security research. Students will have a research-format term project to work on a software security related research topic selected by themselves. During the semester, we will have about three programming projects on topics such as buffer-overflow exploit, fuzz testing, network traffic monitoring, etc. We will also utilize Unix machines in CS department for some assignments and teaching of Linux usage.

Textbook: No required textbook. We will use research papers, online resources, and some contents from the following reference books.

1. 19 Deadly Sins of Software Security (Security One-off) by Michael Howard, David LeBlanc, John Viega
2. The Basics of Hacking and Penetration Testing (2nd edition) by Patrick Engebretson
3. Hacker Techniques, Tools, and Incident Handling (2nd edition) by Sean-Philip Oriyano

Course Learning Objectives:

1. Gain knowledge on the causes of software vulnerability such as buffer overflow or cross-site scripting.
2. Gain basic analytical skill and utilization of tools on analyzing software vulnerabilities.
3. Possess the skills to analyze malware samples using both static and dynamic analysis techniques.
4. Understand principles on detect malware from host and network-based indicators.
5. Learn state-of-art academic research on malware and software security.
6. Able to conduct independent academic research on general cybersecurity topics, and be able to write and present a research oriented term project paper.

Planned Outline of Topics:

1. Course introduction; software security introduction
2. Basic networking security
3. Buffer overflow – Attack
4. Buffer overflow – Defense
5. Finding software bugs – Fuzzing test
6. Email spam and email Phishing
7. Discrete-time simulation and Internet worm introduction
8. Academic paper presentation

Zoom-based real-time lecturing and video streaming:

We will use WebCourse's integrated Zoom system for real-time online lecturing and video streaming. Both face-to-face session (0V01) and online session (0V61) students have the freedom to either join or not join in the real-time Zoom lecturing on the lecture time via the "Zoom" tab link in the webcourse (TuTh 9am-10:15am). Everyone can access the recorded lecture video via the "Zoom" tab link in Webcourse after each lecture time (clicking the 'Cloud Recordings' tab). Webcourse will also be used for lecture content dissemination, assignment release and submission.

Grading: +/- grading system will be used (A, A-, B+, B, etc). The final grade will be curved and each student GPA grade is determined not only by the absolute cumulative scores, but also by his/her relative ranking among all students in this class. The tentative grading weights are shown below (subject to change).

Paper review reports	15%
Lab assignments (1)	10%

Program assignments (3)	45%
Term project	30%

Attention to students who receive federal student aid: all faculty members are required to document students' academic activity at the beginning of each course. In order to document that you began this course, please complete the first created assignment on WebCourse by the end of the first week of classes or as soon as possible after adding the course. Failure to do so may result in a delay in the disbursement of your financial aid. This first homework assignment will not be graded or counted in final grading.