CAP 6135: Malware and Software Vulnerability Analysis

Spring 2016

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

Course Time: MoWe 12:00pm-1:15pm, ENG1 O386A

Office Hour: MoWe 9:45am-11:45am

Course Webpage: http://www.cs.ucf.edu/~czou/CAP6135-16/

Prerequisite: Good programming skill (preferring C or C++);
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.

Textbook: No require 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 Teaching Tools:

We will use the new Panopto system for video streaming of each face-to-face lectures. Recorded videos can be accessed via Webcourse. Both face-to-face session (0R01) and online session (0V61) students can access the lecture videos. Each class video will be available in late afternoon after each face-to-face lecture. Webcourse will be used for assignment release and submission.

We will also utilize the Unix machines in department for some assignments and teaching of Linux usage.

Grading: +/- grading system will be used (A, A-, B+, B, etc). The tentative weights are:

	Face-to-face students	Online session students
In-class presentation	14%	N/A
Paper review reports	N/A	14%
Written and lab assignments	20%	20%
Program projects	36%	36%
Term project	30%	30%