**Course description**

**CIS4930/5930 Intro to Reverse Engineering with IDA Pro and Hex-Rays**

**General Information**

**Tentative Schedule:** Weekly meeting on Tuesday at 5:15 to 7:45 in Love 151 / SAIT Lab

Individual Lab Time with access to the machine in SAIT Lab.

* Instructor: John Connor McLaughlin & Mike Burmester
* Office, Office hours: 268 Love Bldg, TR 11:00-12:00 noon,
* email: burmester@cs.fsu.edu

**Prerequisites**

Familiarity with the basics for analyzing malware and/or subverting the security of software.

The course will be mostly hand-on and project based.

**Textbook** (*I shall order four copies*)

* The IDA Pro Book by Chris Eagle

 **Extra Reading** (I shall order four copies)

* *Practical Malware Analysis: hands-on guide to dissecting malicious software, Michael Sikorski and Andrew Honig, No Starch Press, San Francisco, Ca*, 2012

**Objectives**

Techniques for: (i) analyzing malware and, (ii) subverting the security mechanisms of native binary executables, by employing the IDA Pro Dissembler and the Hex-Rays Decompiler. This will involve studying reverse engineering techniques in the literature and experimentation involving IDA Pro. This is essentially a hands-on course, complemented with group discussions. Students taking part in this course should be able to analyze executables and are expected to submit a report and participate in at least one CTF reverse engineering activity to demonstrate their ability in reverse engineering.

N.B. Hands-on reverse engineering can be an exhaustive and long process, requiring patience and proficiencies in Machine code instructions. But it is very interesting and challenging.

Specific tasks will be shared out and a major part of the course will involve hands-on exercises and reporting. The tasks will start with static reverse engineering in which the source code is manipulated by dissemblers, and lead on to dynamic analysis of live binary sample targets using IDA Pro and Hex-Rays.

**Classes With Videos / Labs For References:**

<http://opensecuritytraining.info/IntroductionToReverseEngineering.html>

 <http://opensecuritytraining.info/ReverseEngineeringMalware.html>

**Lab Materials**

 <http://www.binary-auditing.com/>

 <http://pof.eslack.org/tmp/IOLI-crackme.tar.gz>

 <http://www.crackmes.de/>

**Assignments & Grading**

40% Group Project: IDA Pro Python Script / Addon

30% Final Project: Write Up / Demonstration on Practical Use of IDA Pro

30% Labs ( 10\* 3% )

**Labs**

Each lab we will do a number of crack.me’s. This involves loading up a specifically designed binary and reverse engineering how it works to find passwords that will work, or patch the binary to actually accept any password.

The binaries will be found on the websites listed above, and each class we will have everyone do a write-up on what was done.

**Tentative Schedule** (prepared by John Connor McLaughlin, based on Owen Redwood’s class)

Week 1: Tuesday 8/25/2015

Go over expectations of the course

Reading Assignment: Practical Malware Analysis Ch. 4

Week 2: Tuesday 9/1/2015

Crack Me Lab #1

Reading Assignment: IDA Pro Book Ch. 1, 2, 5

Week 3: Tuesday 9/8/2015

Crack Me Lab #2

Reading Assignment: Practical Malware Analysis Ch. 5

Week 4: Tuesday 9/15/2015

Crack Me Lab #3

Reading Assignment: Practical Malware Analysis Ch. 6

\*CSAW Qualifier CTF 9/18/2015-9/20/2015

Week 5: Tuesday 9/22/2015

Crack Me Lab #4

Reading Assignment: IDA Pro Book Ch. 9

Week 6: Tuesday 9/29/2015

Crack Me Lab #5

Reading Assignment: IDA Pro Book Ch. 7-8

Week 7: Tuesday 10/6/2015

Crack Me Lab #6

Reading Assignment: IDA Pro Book Ch. 15

Begin Project 1

Week 8: Tuesday 10/13/2015

Crack Me Lab #7

Reading Assignment: Practical Malware Analysis Ch. 1, 2, 3

Week 9: Tuesday 10/20/2015

Crack Me Lab #8

Begin Project 2

Practical Applications Code Obfuscation

Reading Assignment: IDA Pro Book Ch. 21

Week 10: Tuesday 10/27/2015

Crack Me Lab #9

Finish Project 1

Practical Applications Vulnerability Analysis

Reading Assignment: IDA Pro Book Ch. 20 and Ch. 22

\*CyberSEED 10/29/2015-10/30/2015

Week 11: Tuesday 11/3/2015

Crack Me Lab #10

Practical Applications Reversing Malware

Reading Assignment: IDA Pro Book Ch. 24

Week 12: Tuesday 11/10/2015

Special Guest

Practical Applications Reversing Malware

Week 13: Tuesday 11/17/2015

Special Guest

Practical Applications Reversing Malware

Week 14: Tuesday 11/24/2015

Thanksgiving Break

Week 15: Tuesday 12/1/2015

Present Project 2

Week 16: Tuesday 12/8/2015

Finals No Meeting

Schedule Subject To Change

**University Attendance Policy.** Excused absences include documented illness, deaths in the immediate family and other documented crises, call to active military duty or jury duty, religious holy days, and official University activities. Accommodations for these excused absences will be made and will do so in a way that does not penalize students who have a valid excuse. Consideration will also be given to students whose dependent children experience serious illness.

**Communication.** You are encouraged to use e-mail to ask questions and report problems.

If you experience difficulty or are concerned about your progress, please speak with me immediately.

**Disabilities.** Please notify the Department of Computer Science five working days prior to the event if a reasonable accommodation for a disability is needed. The Department’s telephone numbers are 644-2296 (Voice), and 644-0058 (Fax). This syllabus and other class materials are available in alternative format upon request.

**Academic Honor Code.** You are required to read the FSU Academic Honor Code and abide by it. By turning in work, or presenting work for a grade, you are representing it as being your own individual work. If an assignment permits teamwork, it will be explicitly stated so in the assignment, and then the work is required to only be that of the people on the team.

**University Academic Honor Policy.** The Florida State University Academic Honor Policy outlines the University’s expectations for the integrity of students’ academic work, the procedures for resolving alleged violations of those expectations, and the rights and responsibilities of students and faculty members throughout the process. Students are responsible for reading the Academic Honor Policy and for living up to their pledge to “. . . be honest and truthful and . . . [to] strive for personal and institutional integrity at Florida State University.” (Florida State University Academic Honor Policy, found at http://dof.fsu.edu/honorpolicy.htm.)

**Americans with Disability Act.** Students with disabilities needing academic accommodation should:

1. register with and provide documentation to the Student Disability Resource Center; and

2. bring a letter to the instructor indicating the need for accommodation and what type.

This should be done during the first week of class.

This syllabus and other class materials are available in alternative format upon request.

For more information about services available to FSU students with disabilities, contact the:

Student Disability Resource Center

874 Traditions Way

108 Student Services Building

Florida State University

Tallahassee, FL 32306-4167

(850) 644-9566 (voice)

(850) 644-8504 (TDD)

sdrc@admin.fsu.edu

http://www.disabilitycenter.fsu.edu/