EEL 6805—Adv. Malware Reverse Engineering

Department of Electrical & Computer Engineering
Florida International University
Spring 2018

Classroom	**:**	EC 3239
Class Time	**:**	8:00 am—12:30 pm (Wednesday/Mar. 6-Apr. 29)
Faculty	**:**	Dr. Alexander Pons
Office Hours	**:**	T & R 9:00-11:00 am or by Appointment
Office	**:**	EC – 3145
Phone	**:**	305.348.7253
Email	**:**	apons@fiu.edu
Prerequisite	**:**	Basic knowledge about computer and windows operating system or Successful completion of a Programming language course Or permission from the instructor

Textbook

The lectures will be substantially based on technical papers from literature most of which can be found from on-line databases such IEEE eXplore and ACM digital library (accessible on-line in FIU campus). It is your responsibility to print and read related papers. Lecture material will also be drawn from various books and other resources, some of them are listed as follows.

- Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Adrew Honig (Feb, 2012), ISBN: 1593272901
- The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler by Chris Eagle (Jul, 2011), ISBN: 1593272898
- The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory by Michael Hale Ligh, Andrew Case, Jamie Levy, and AAron Walters, Wiley (2014) ISBN: 978-1-118-82509-9

Course Description

The objective of this course is to familiarize students with the practice of performing reverse engineering on suspicious files and firmware by utilizing static and dynamic techniques and procedures. The student will gain an understanding of how firmware is compromised and how to validate and restore its integrity. Analytical information such as environment changes (file, system, network, and process), communication with the rest of the network and the malware's impact on mobile devices will be closely observed and analyzed for actionable information.

Course Objectives

1. To give the student an understanding of Malware Reverse Engineering approaches.
2. To give the students a hands-on exposure to the latest tools and techniques to find, extract, and analyze malicious code from various types of hardware.
3. To provide analysis on the way the malware interacts with any associated networks, identifying the type of information being targeted.
4. Apply Machine learning to identify malware behavior using Weka
5. Apply Volatility and Python to detect memory resident malware
6. Develop kernel and user space malware to demonstrate common hooking techniques and process injection.

Topics Covered

1. Memory scraping and Volatility Framework
2. Machine Learning and WEKA
3. Sandboxing executable and extracting information by performing runtime analysis.
4. Static /dynamic analysis of malware.
5. Packers, Compression and Obfuscation techniques
6. Analysis malware using IDA Pro Disassembler
7. Analyzing malicious browser based exploits.
8. Recognize commonly used anti-debugging techniques and overcome them in IDA
9. Recognize commonly used anti-virtual machine techniques and overcome them in IDA
10. Recognize buffer overflow vulnerabilities in disassembled files
11. Recognize and decode commonly used encoding algorithms in disassembled files
12. Recognize and overcome commonly used obfuscation techniques in disassembled files
13. Coding for kernel/user space hooking techniques and process injection.
14. Linux device drivers and rootkit analysis
15. Develop Ground Truth of sample malware
16. Create your own Malware variant

Relationship of course to program objectives

In this course, the student will have to show:

1. An ability to apply knowledge of mathematics, science, and engineering,
2. an ability to design and conduct experiments, as well as to analyze and interpret data,
3. an ability to design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability,
4. an ability to identify, formulate, and solve engineering problems (homework),
5. the broad education necessary to understand the impact of engineering solutions in a global, economic, environmental, and societal context
6. an ability to communicate effectively (through teamwork),
7. an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice,
8. a knowledge of contemporary issues,

Tentative Grading Scale

Grading Scale:		
A	**95-100**	**"Florida International University is a community dedicated to generating and imparting knowledge through excellent teaching and research, the rigorous and respectful exchange of ideas, and community service. All students should respect the right of others to have an equitable opportunity to learn and honestly to demonstrate the quality of their learning. Therefore, all students are expected to adhere to a standard of academic conduct, which demonstrates respect for themselves, their fellow students, and the educational mission of the University. All students are deemed by the University to understand that if they are found responsible for academic misconduct, they will be subject to the Academic Misconduct procedures and sanctions, as outlined in the Student Handbook."**
A-	**90-94**	
B+	**86-89**	
B	**82-85**	
B-	**78-81**	
C+	**74-77**	
C	**70-73**	
D	**69-60**	
F	**0-59**	

Grading Scheme

Malware or Tool Development	**15%**
Topic Paper Presentation	**15%**
Group Research Paper/Project	**20%**
Classwork and Homework	**10%**
Final Exam	**40%**
Total	**100%**

Tentative Dates

- **Final Exam** is scheduled on the last Wednesday of the semester.
- **Group Presentations** will also be done on the last Wednesday of the semester

Topic Research Presentation

1. Groups will present a topic every week for approximately 30 minutes.
2. The group contains 2-3 students working together throughout the semester.
3. Students will give oral presentations and distribute their material as part of the course, based on an academic paper.

Journal Paper - Topics research (2 ~ 3 students per group): 15%

1. One page written proposal submitted in time and approved by the instructor (5%)
2. Prepare slides and perform a 25 - 30 minutes presentation in class (5%)
3. Three-page introduction and summary (5%).

Group Research/Project Paper

1. The course includes a substantial group project (20%) requiring the review and the implementation of a topic related to Malware.
2. The group contains 2-3 students working together throughout the semester.
3. Students will give oral presentations and show their demos on the last day of the class.
4. Final paper can be a composition of the various Topic presentations.

Projects (2 ~ 3 students): 20%

1. One page written proposal submitted in time and approved by the instructor (0%)
2. Research efforts, ideas, and results (5%)
3. A 25-30 minutes oral presentation in class (5%)
4. Formal project report (10%).

- Please form the group, select the group leader, and send the research project proposal by the indicated deadline. Failure to do so will incur a penalty resulting in a reduced grade.
- The **Graduate groups** comprise of 2 to 3 students.
- The group project requires substantial amount of research work towards the review, implementation, and/or demo of any issues related to mobile malware reverse engineering. Accordingly, the group is asked to clearly differentiate and understand the requirements of this group research project.
- The group members will give oral presentations and show their demos on the last day of the class. Everyone in the group must participate in the presentation.
- The **graduate groups** must submit a **publishable research paper**, properly formatted utilizing the IEEE conference paper format guidelines. (http://www.ieee.org/conferences_events/conferences/publishing/templates.html)

Homework/Classwork

Homework/Classwork mainly comprises of downloading, analyzing, attributing, and providing a detailed written report of different malwares.

University's Code of Academic Integrity

Florida International University is a community dedicated to generating and imparting knowledge through excellent teaching and research, the rigorous and respectful exchange of ideas, and community service. All students should respect the right of others to have an equitable opportunity to learn and honestly to demonstrate the quality of their learning. Therefore, all students are expected to adhere to a standard of academic conduct, which demonstrates respect for themselves, their fellow students, and the educational Mission of the University. All students are deemed by the University to understand that if they are found responsible for academic misconduct, they will be subject to the Academic Misconduct procedures and sanctions, as outlined in the Student Handbook.
More information can be found at http://academic.fiu.edu/academic_misconduct.html

Department Regulations Concerning Incomplete Grades

To qualify for an Incomplete, a student:

1. Must contact (e.g., phone, email, etc.) the instructor or secretary before or during missed class.
2. Must be passing the course prior to that part of the course that is not completed
3. Must make up the incomplete work through the instructor of the course
4. Must see the Instructor. All missed work must be finished before last two weeks of the next term.

University policies on sexual harassment, and religious holidays, and information on services for students with disabilities

Please visit the following websites: http://academic.fiu.edu/ http://drc.fiu.edu

Course Policies

- **Attendance:** Attendance in the course is **mandatory** and student is not allowed to miss any class during the semester. There is a **penalty** for missing classes and it may affect your final grade.
- **Academic Misconduct:** For work submitted, it is expected that each student will submit their own original work. Any evidence of duplication, cheating or plagiarism will result at least a failing grade for the course.
- **Unexcused Absences:** Two unexcused absences are permitted during the term. More than two will result in the loss of points from your final grade. (1 point per absence above two, 3 points per absence above 5).
- **Excused Absences:** Only emergency medical situations or extenuating circumstances are excused with proper documentation. After reviewing documentation you are required to email a description of the excuse and absence dates as a written record to apons@fiu.edu.
- **On Time:** As in the workplace, on time arrival and preparation are required. Two "lates" are equivalent to one absence. (Leaving class early is counted the same as tardy.)
- **Deadlines:** Assignments are due at the beginning of the class period on the date specified. Assignments submitted late (within 1 week) will receive half credit.
- To get assistance try to see me by an appointment.
- Students are encouraged to ask questions/discuss course topics with the instructor and each other.
- **Any work submitted should display Panther ID number and should be signed, as the students' own work, and that no unauthorized help was obtained.**
- Cell phones, communicators, MP3 players, head sets are not allowed to be used in the class.
- **DO NOT** send assignments by email.
- Instructor reserves right to change course materials or dates as necessary.

Exam policy

1. Make sure to complete the assigned homework in order to do well in the exam.
2. All exams are closed book and closed notes.
3. Use of any electronic device with keyboard is prohibited. This also applies to cellphones with messaging system.
4. No discussion is permitted during the exams.
5. Instructor is not compelled to give credit for something he cannot read or follow logically.
6. Cheating is considered as a serious offense. Students who are caught will receive the appropriate consequences.

Class Schedule

Once a week, 240 minutes each session: Wednesday

Week	Date	Weekly Topic
1	3/6	Students form teams and conduct initial research into determining Team paper topic – at least 10 papers should be collected and reviewed.
2	3/13	Spring Break
3	3/20	Lecture/Labs 1 Topic Research Presentation
4	3/27	Lecture/Labs 2 Topic Research Presentation
5	4/3	Lecture/Labs 3 Topic Research Presentation
6	4/10	Lecture/Labs 4 Topic Research Presentation
7	4/17	Lecture/Labs 5 Topic Research Presentation
8	4/24	Lecture/Labs 6 Topic Research Presentation
9	5/1	Course Final Exam Final Paper Presentations

Course Hands-On Labs

Lab 1 – Sandbox and Basic Static and Dynamic Analysis
Practical Malware Analysis perform labs 1-4, 3-3, 3-4 using Cuckoo, limon, virusTotal and tools to monitor windows malware execution and static content, **Tools:** winmd5, strings, PEiD, UPX, dependencywalker, PRView, Resource Hacker, PE Explorer, ProcMon, RegShot, ApateDNS, Wireshark and INetSim.
Lab 2 – Advanced Static Analysis
Practical Malware Analysis perform labs 5-1, 6-3, 6-4 and 7-3 to perform Advanced Static Analysis identifying malware assembly language using IDA Pro disassembler. **Tools:** IDA Pro (The IDA Pro Book)
Lab 3 – Advanced Dynamic Analysis
Practical Malware Analysis, perform labs 9-2, 11-1, 12-1, 12-2, 13-1 and 13-2 to perform Advanced Dynamic Analysis using Olly Debugger**. Tools:** OllyDbg
Lab 4 – Memory Scraping with Volatility
Obtain the stuxnet.vmen sample and follow the tutorial to execute the same command and generate the output associated with each command. Make sure to understand the objective and result of each command. Make sure to extract evidence samples and verify that they are malicious in uploading to VirusTotal.com. Then, take sample sample003.bin and perform the same command as in stuxnet and/or any other you believe will provide you as much information as possible. Then write a description of what you learned from performing these command. Develop a ground truth description for each. Tools: Volatility Framework and Python
Lab 5 – Malware Behavior and Machine Learning (Extract Task-level features)
Use the given linux driver to extract data from two different type of processes CLI and GUI. Create a file for the following CLI programs: ls and ps, into ls.dat and ps.dat, now combine all of these into cli.dat. Create a file for the following GUI programs gedit file and firefox into gedit.dat and firefox.dat, now combine all of these into gui.dat. Using Weka, input these two data sets to train the classifier model j4.8, make sure to add a class attribute in each as CLI and GUI as the classification values. Please make a note of the confusion Matrix and use 10-fold cross-validation to test the model. Now, sample two applications, one CLI and one GUI and test how the model performs. Show the percentage of CLI and GUI generated, if above 75% then classify as such. Use cat as the CLI and nano as the GUI.
Lab 6 – Linux RootKit development (user and Kernel Space)
Develop a linux kernel diver that will hook the system call table for the open call, it should call the original open function, but also save into the kern.log file a message indicating every time a user space program call the open function. Write a test program to that open a file to test the hooking driver. Next, write a program that will perform hooking a library function like malloc and test and show how this would work. Once you have performed both of tasks, write a comprehensive description how these techniques work, their limitations and potential detection and prevention.