Malware Analysis - Course Syllabus

Course Information

Course Title: Malware Analysis
Course Number: CSCI 4976
Credit Hours: 4
Semester / Year: Fall 2015
Meeting Days: Tuesday/Friday 12-2PM
Room Location: Sage 2112
Course Website: http://security.cs.rpi.edu/courses/malware-fall2015/
Prerequisites (one of the following or permission of instructor):

- CSCI 2500 - Computer Organization
- ECSE 2660 - Computer Architecture, Networks, and Operating Systems

Instructor

Name: Bülent Yener
Office location: Lally 310
Email Address: yener@cs.rpi.edu

Teaching Assistant(s)

TAs: RPISEC
TA Office Location: Walker 5113
TA Office Hours: Wednesday 7-10PM
TA Email Address: malware_ta@cs.lists.rpi.edu

Course Description

With the increased use of the Internet and prevalence of computing systems in critical infrastructure, technology is undoubtedly a vital part of modern daily life. Unfortunately, the increasingly networked nature of the modern world has also enabled the spread of malicious software, or “malware”, ranging from annoying adware to advanced nation-state sponsored cyber-weaponry. As a result, the ability to detect, analyze, understand, control, and eradicate malware is an increasingly important issue of economic and national security.

This course will introduce students to modern malware analysis techniques through readings and hands-on interactive analysis of real-world samples. After taking this course students will be equipped with the skills to analyze advanced contemporary malware using both static and dynamic analysis.

Course Text(s)

Required Textbooks:

- “Practical Malware Analysis” by Michael Sikorski and Andrew Honig
  - ISBN: 1593272901
  - RPI: http://library.rpi.edu/update.do?artcenterkey=1671
- “The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System” Second Edition by Reverend Bill Blunden

Recommended Textbooks:

- “Rootkits: Subverting the Windows Kernel” by Jamie Butler and Greg Hoglund
  - ISBN: 0321294319
- “Practical Reverse Engineering” by Dang, Gazet, Bachaalany

Student Learning Outcomes

Upon successful completion of this course, students will:

1. Possess the skills necessary to carry out independent analysis of modern malware samples using both static and dynamic analysis techniques.
2. Have an intimate understanding of executable formats, Windows internals and API, and analysis techniques.
3. Extract investigative leads from host and network-based indicators associated with a malicious program.
4. Apply techniques and concepts to unpack, extract, decrypt, or bypass new anti-analysis techniques in future malware samples.
5. Achieve proficiency with industry standard tools including IDA Pro, OllyDbg, WinDBG, PE Explorer, ProcMon etc.

Course Assessment Measures

- **Labs:** Accompanying each lecture will be a lab that will solidify understanding of the topic of the lecture. Each lab will contain several malware samples, each with corresponding analysis goals and questions. These will be largely based on the labs included with the required text.

- **Malware Analysis:** There will be 4 large malware analysis projects over the course of the semester. Each project will require the student to demonstrate mastery of analysis skills learned up until that point. The students will be required to submit a formal writeup detailing their analysis of the sample. A rubric and sample report will be provided to avoid confusion about what is required.

- **Quizzes:** A quiz will be given each week that has assigned reading, with questions taken directly from the topics presented in that week’s reading. The quizzes will be straightforward, with their intended purpose being that students stay on top of pre-lecture reading, as lecture will be largely hands-on.

See the Grading Criteria and Course Calendar sections for further details.

Grading Criteria

Students will be able to calculate their standing at any time during the class by using the below percentages to calculate their grade.

- **Grading Scale:** A: 93%, A-: 90%, B+: 87%, B: 83%, B-: 80%, C+: 77%, C: 75%, C-: 70%, D: 50%, F: < 50%

- **Labs:** 48%, 12 labs equally weighted at 4%
  - Labs will typically consist of several problems, each with corresponding analysis goals and questions. Students will be graded on whether or not they met each goals and also on the sufficiency of their answers to each question.
  - If a student does not complete the first problem before the end of lab, they will receive a letter grade reduction for the assignment.
  - In order to receive full credit for a problem the student must submit a small write-up of how they completed the analysis goal along with their answers to each question. Students may be asked to explain their work upon submission to be checked off.
  - Labs problems will be introduced by the end of lecture. The first problem will be due in person **by the end** of the associated lab period. All other problems become homework, and are due **at the start of class, exactly one week after the associated lab period**.
  - Labs submitted late will receive a letter grade reduction and MUST be submitted no later than the class following their original due date, anything later will not be accepted.

- **Malware Analysis:** 40%, four projects equally weighted at 10%
  - Analysis specific grading breakdowns will be given when they are assigned.A rubric and sample report will be provided to avoid confusion about what is required.
  - A final analysis write-up/report will be due **two weeks after the analysis is assigned.**
  - Analyses submitted late will receive a -10% reduction per day late, and will not be accepted for credit after 5 days.

- **Quizzes:** 12%, 12 quizzes
  - Each “book” lecture will be preceded by a short and straightforward quiz.
  - Students will be given 5-10 minutes to answer a few questions about the chapters and/or the corresponding labs.

Grades and course progress will be made available to students throughout the semester. A grade can only be appealed within 5 days of the grade being made available to students. Questions regarding a grade on an assignment should first be directed at the class TAs.

Course Calendar

Date	Title	Topics	Chapter	Content
9/1	Introduction	Syllabus, Basic Static Analysis, Basic Dynamic Analysis	0/1/2/3	Lecture
9/4	Lab 1: Basic Analysis			Lab
9/8	Advanced Static Analysis	x86, IDA, Code Constructs	4/5/6	Lecture
9/11	Lab 2: Advanced Static Analysis			Lab
9/15	Analyzing Windows Programs	WinAPI, Handles, Windows Internals, Networking, COM	7	Lecture
9/18	Lab 3: Analyzing Windows Programs			Lab
9/22	Advanced Dynamic Analysis	Debugging Concepts and Tools	8/9	Lecture
9/25	Lab 4: Advanced Dynamic Analysis			Lab
9/29	**First Project Assigned** Malware Behavior	Malicious Activities and Techniques	11	Lecture
10/3	Lab 5: Malware Behavior			Lab
10/6	Data Encoding, and Malware Countermeasures	Hiding Data, Malware Countermeasures,	13/14	Lecture
10/9	Lab 6: Data Encoding, and Malware Countermeasures			Lab
10/13	******* **NO CLASS** ******* **First Project Due**	**COLUMBUS DAY**		
10/16	Covert Malware Launching	Covert Launching and Execution	12	Lecture
10/20	**Second Project Assigned** Lab 7: Covert Malware Launching			Lab
10/23	Anti-Analysis	Anti Disassembly, VM, Debugging, AV	15/16/17	Lecture

10/27	Lab 8: Anti-Analysis			Lab
10/30	******* **NO CLASS** *******	**CyberSEED**		
11/3	Packing and Unpacking **Second Project Due**	Packers, Packing, and Unpacking	18	Lecture
11/6	Lab 9: Packing and Unpacking			Lab
11/10	Intro to Kernel **Third Project Assigned**	Kernel Basics, Windows Kernel API, Windows Drivers, Kernel Debugging	PMA: 10 RA2: 3/4/5/6	Lecture
11/13	******* **NO CLASS** *******	**CSAW**		
11/17	Lab 10: Kernel Basics			Lab
11/20	Rootkit Techniques	Hooking, Patching, Kernel Object Manipulation	RA2: 11/12/13	Lecture
11/24	Lab 11: Rootkit Techniques **Third Project Due**			Lab
11/27	******* **NO CLASS** *******	**Thanksgiving Break**		
12/1	Rootkit Anti-Forensics and Covert Channels **Fourth Project Assigned**	Covert Channels, Anti-Forensics		Lecture
12/4	Guest Speaker: Grant Hollis	Duqu 2.0		Lecture
12/8	Lab 12: Modern Rootkit Analysis			Lab
12/11	**Fourth Project Due** Presentations			Lecture

Attendance Policy

Lecture is not mandatory, however, **attendance for labs is required** as the first problem of each lab set must be turned in in person during lab.

See Grading Criteria for more details

Academic Integrity

Student-teacher relationships are built on trust. For example, students must trust that teachers have made appropriate decisions about the structure and content of the courses they teach, and teachers must trust that the assignments that students turn in are their own. Acts that violate this trust undermine the educational process. The Rensselaer Handbook of Student Rights and Responsibilities defines various forms of Academic Dishonesty and you should make yourself familiar with these. In this class, all assignments that are turned in for a grade must represent the student's own work. In cases where help was received, or teamwork was allowed, a notation on the assignment should indicate your collaboration.

Submission of any assignment that is in violation of this policy will result in a penalty of **a zero for the assignment** for all parties involved. **Repeated offenses will result in a failing grade for the course.**

If you have any question concerning this policy before submitting an assignment, please ask for clarification.

Other Course-Specific Information

The labs and interactive exercises used in lecture should be treated as malicious. DO NOT run them on your host operating system. All analysis should be done inside of a virtualized environment. A pre-built VM that includes all of the tools needed for the class will be distributed during the first class. Proper handling of this VM and malicious/unknown samples will be taught in the first lecture.

Due to the experimental nature of the course and assignments being offered, the schedule, pacing, and other elements of the course may be modified depending on the rate at which students are progressing. Any changes made to the curriculum will be clearly defined and communicated to the students as well as being documented accordingly.