DFOR 761-001: Malware Reverse Engineering

Digital Forensics Program
Department of Electrical and Computer Engineering
George Mason University
Fall 2021

Instructor

Joseph Opacki
Email: jopacki@gmu.edu
Telephone: 202.355.3521
Office Hours: Schedule by email over Zoom or Slack
Office Location: Virtually Online

Location and Time

Nguyen Engineering Building 5358
Tuesdays, 7:20-10:00PM

Course Description

The Malware Reverse Engineering course is for students who have limited or no experience with the practice of reverse engineering. Reverse engineering is generally accepted as reviewing the disassembled code of a potentially malicious binary, or piece of malware, usually using a disassembler or hex editor, to gain a better understanding of how a binary function operates when executed. This type of analysis is geared toward capturing the behavioral aspects of the malicious binaries as they are executed in a controlled environment. Analytical information such as environment changes (file, system, network, process, etc.), communication with the rest of the network, communications with remote devices, and so on are closely observed for actionable information. This information is analyzed, and a complete picture is reconstructed as to what the binary is doing to a computer when executed. It is important to extract information from the malware that can be used to establish actionable information. As such, emphasis is placed on analyzing the way the malware interacts with any associated networks, identifying the type of information being targeted, and finding commonalities with previously analyzed malware. Although not always known, features such as vulnerabilities exploited are of interest and are identified as possible malware infection vectors.

Prerequisites

CFRS 661 – Digital Media Forensics, a working knowledge of computer programming, and a familiarity with Assembly Language is preferred.

Course Objectives

The objective of this course is to familiarize students with the practice of reverse engineering suspicious files by utilizing static and dynamic tactics, techniques, and procedures in order to gain an understanding as to what impact the suspicious file may have on a particular computer system when executed.

Grading

Raw scores may be adjusted to calculate final grades. Grades will be assessed by the following components:

Class Participation:	5%
Homework:	25%
Midterm:	30%
Final Project:	40%

The components are outlined in the following sections.

Homework

Three homework labs will be provided to students over the course to allow students to apply the methods discussed in class. These assignments will be provided in class and announced via the course website. Homework assignments are due two weeks following the assigned date. Homework assignments are worth twenty-five percent (25%) of your overall grade. Late homework assignments will be assessed a penalty of twenty-five (25%) of the assignment grade for each day of tardiness. No homework will be accepted after the third day.

Midterm

A midterm exam will be given during week seven and will cover information provided during lectures, labs, required and supplemental readings, and any information derived from homework assignments.

Final Project

The capstone of the class will consist of an analytic paper of at least ten pages in length detailing your analysis on a piece of malware demonstrating the analytic fundamentals learned in the course. The final report is due in week 15 of the class. If a binary is selected for analysis other than the instructor provided, the binaries analyzed for the final project will need to be provided with the final report so that the results can be authenticated.

Software Requirements

All students will need the ability to virtualize the Windows operating systems. While VMWare is preferred, other software such as VirtualBox, Qemu, Parallels, and Microsoft Virtual PC are also sufficient. Students will be provided a copy of Windows 7 that will be used via virtualization for the execution and detonation of malware samples. All other software discussed in the course can be downloaded from the Internet and is either freeware, shareware, or available as trial software. All additional software requirements will be discussed in the lecture material.

Textbooks

The following books are a requirement for this course.

REQUIRED

Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware

Paperback: 510 pages

Publisher: Packt Publishing (June 29, 2018)

ISBN-10: 1788392507

ISBN-13: 978-1788392501

RECOMMENDED

Practical Malware Analysis

Publisher: No Starch Press; 1 edition (February 1, 2012)

Language: English

ISBN-10: 1593272901

ISBN-13: 978-1593272906

These books provide students with a basic primer on reverse engineering to include computer internals, operating systems, and assembly language. In addition, they also provide students with practical, in-depth techniques for software reverse engineering utilizing reverse engineering tools.

Additional course material will be given to students via lecture. Recommended reading will be discussed during lecture. Students are encouraged to review recommended reading as needed.

Schedule

Date	Week	Topic
24 Aug	1	Course and Syllabus Overview, Introduction to Malware, Analysis
31 Aug	2	Initial Infection Vectors, Malware Discovery, and Static Analysis
7 Sep	3	Sandboxing Malware and Gathering Information through Static and Dynamic Analysis
14 Sep	4	Introduction to the Portable Executable File Format
21 Sep	5	Identifying Executable Metadata and Executable Packers
28 Sep	6	Assembly Language Primer
5 Oct	**7**	**Midterm Examination**
12 Oct	**8**	**NO CLASS**
19 Oct	9	Introduction to Disassemblers
26 Oct	10	Utilizing Software Debuggers to Examine Malware
2 Nov	11	Malware Self-Defense, Compression, and Obfuscation Techniques
9 Nov	12	Memory Dumping and Forensics
16 Nov	13	Analyzing Malicious Microsoft Office and Adobe PDF Documents, Advanced Infection Techniques
23 Nov	14	Automating Malware Analysis
30 Nov	**15**	**Final Projects are Due**

This schedule is subject to revision before and during this course.

Call 703-993-1000 for recorded information on campus delays or closings (e.g. due to weather).

Attendance Policy

Students are expected to attend the class periods of the courses for which they register. In-class participation is important not only to the individual student, but also to the class as a whole. Because class participation may be a factor in grading, instructors may use absence, tardiness, or early departure as de facto evidence of nonparticipation. Students who miss an exam with an acceptable excuse may be penalized according to the individual instructor's grading policy, as stated in the course syllabus.

Students are expected to make prior arrangements with Instructor if they know in advance that they will miss any class and to consult with the Instructor if they miss any class without prior notice.

Absences from final exams will not be excused except for sickness on the day of the exam or other cause approved by the student's academic dean or director. The effect of an unexcused absence from an undergraduate final exam shall be determined by the weighted value of the exam as stated in the course syllabus provided by the instructor. If absence from a graduate final exam is unexcused, the grade for the course is entered as F. See the Additional Grade Notations in the Grading System section for information on being absent with permission.

Communications

Communication on issues relating to the individual student should be conducted using email or telephone. Email is the preferred method – for urgent messages, you should also attempt to contact the Instructor via telephone. Email messages from the Instructor to all class members will be sent to students' GMU email addresses – if you use another email account as your primary address, you should forward your GMU email to that account.
Lecture slides are complements to the lecture process, not substitutes for it. Access to lecture slides will be provided as a courtesy to students provided acceptable attendance is maintained.

Honor Code

Students are required to be familiar and comply with the requirements of the GMU Honor Code. Students must NOT collaborate on the homework or projects without explicit prior permission from the Instructor.

Mason shares in the tradition of an honor system that has existed in Virginia since 1842. The code is an integral part of university life. On the application for admission, students sign a statement agreeing to conform to and uphold the Honor Code. Students are responsible, therefore, for understanding the code's provisions. In the spirit of the code, a student's word is a declaration of good faith acceptable as truth in all academic matters. Cheating and attempted cheating, plagiarism, lying, and stealing of academic work and related materials constitute Honor Code violations. To maintain an academic community according to these standards, students and faculty members must report all alleged violations to the Honor Committee. Any student who has knowledge of, but does not report, a violation may be accused of lying under the Honor Code.

The complete Honor Code is as follows:

To promote a stronger sense of mutual responsibility, respect, trust, and fairness among all members of the George Mason University community and with the desire for greater academic and personal achievement, we, the student members of the university community, have set forth this honor code: **Student members of the George Mason University community pledge not to cheat, plagiarize, steal, or lie in matters related to academic work.**

The material provided in the course is proprietary. Uploading this material anywhere without the express permission of the instructor is strictly prohibited and a violation of the Mason Honor Code. https://oai.gmu.edu/

Office of Disability Services

If you are a student with disability and you need academic accommodations, please see me and contact the Office of Disability Services (ODS) at 993-2474. All academic accommodations must be arranged through the ODS.