UMBC UGC New Course Request: CMSC449 – Malware Analysis

Date Submitted: 11/1/2019 Proposed Effective Date: 1/1/2020

	Name	Email	Phone	Dept
Dept Chair or UPD	Jeremy Dixon	jdixon@umbc.edu	5-8866	CSEE
Other Contact	Mohamed Younis	younis@umbc.edu	5-3968	CSEE
Other Contact	Charles Nicholas	nicholas@umbc.edu	5-2594	CSEE

COURSE INFORMATION:

Course Number(s)	CMSC449
Formal Title	Malware Analysis
Transcript Title (≤30c)	Malware Analysis
Recommended Course Preparation	
Prerequisite : Unless otherwise indicated, a prerequisite is assumed to be passed with a "D" or better.	CMSC313 and CMSC 341 both with a "C" or better
# of Credits Must adhere to the UMBC Credit Hour Policy	3
Repeatable for additional credit?	Yes No
Max. Total Credits	3 This should be equal to the number of credits for courses that cannot be repeated for credit. For courses that may be repeated for credit, enter the maximum total number of credits a student can receive from this course. E.g., enter 6 credits for a 3 credit course that may be taken a second time for credit, but not for a third time. Please note that this does NOT refer to how many times a class may be retaken for a higher grade.
Grading Method(s)	Reg (A-F) Audit Pass-Fail

PROPOSED CATALOG DESCRIPTION (Approximately 75 words in length. Please use full sentences.):

Malicious software (malware) is a constant threat to the information and intellectual property of organizations. By analyzing malware using both static and dynamic methods, students will be introduced to these increasingly sophisticated attacks. This course will provide a foundation for understanding emerging trends in malware design, including efforts to deter analysis. Discussions and hands-on exercises will cover object file formats, and the use of tools such as debuggers, virtual machines, and disassemblers. Finally, obfuscation and packing schemes will be discussed, along with various issues related to operating systems internals.

RATIONALE FOR NEW COURSE:

a) Why is there a need for this course at this time?
We are continuing to grow our offerings in the field of cybersecurity as the demand continues to grow. We have offered this course several times previously as a special topics course with great success.

b) How often is the course likely to be taught?
We hope to offer it every semester if possible but at least once per year.

c) How does this course fit into your department's curriculum?
It fits well as an elective for all CS majors or as a course in our cyber security track.

d) What primary student population will the course serve?

e) Why is the course offered at the level (ie. 100, 200, 300, or 400 level) chosen?
It builds on many concepts in CMSC 313. As such, it is perfect as a 400 level course.

f) Explain the appropriateness of the recommended course preparation(s) and prerequisite(s).
This course builds on concepts in CMSC 313 which has prerequisites of CMSC 201, CMSC 202, and CMSC 203. Therefore, students should be familiar with programming in C++ and assembly.

g) Explain the reasoning behind the P/F or regular grading method.
Students can take this course for a letter grade, P/F, or audit although we continually have problems with large waitlists.

h) Provide a justification for the repeatability of the course.
This course cannot be repeated.

ATTACH COURSE SYLLABUS (mandatory):

CMSC 491/691 Malware Analysis

Spring 2019

Prof. Charles Nicholas
410-455-2594
nicholas@umbc.edu
ITE 356
Office hours: MWTh 4-5pm, or by appointment

The teaching assistants will be:

Robert Joyce	joyce8@umbc.edu	MW 1-2:15	ITE 366
Joshua Mpere	jmpere1@umbc.edu	WF 10am-noon	ITE 366

Spring 2019 Lecture Topics

A much condensed version of this course can be presented as a half-day tutorial. The most recent such tutorial was presented at CIKM 2017 in Singapore.

Course information

Monday and Wednesday 5:30-6:45pm
the room is ENG 231, but I hope to get to get a bigger room!

Overview

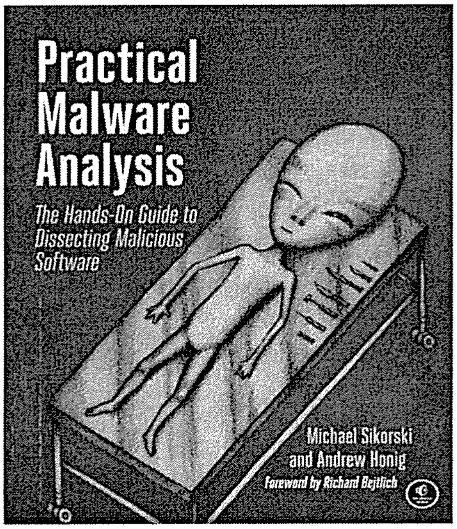
- Malware is in the news all the time!
- See, for example, the latest issue of Cyberwire
- Cyber in general, and malware analysis specifically, is an active area of research.
- Fortunately, there is no shortage of data to use. There is a lot of security related data located at http://www.secrepo.com, including links to several large malware corpora. Google's archive of Android malware is probably the biggest of them all, even though it's not available to the public.
- Tools for malware analysis include a disassembler such as IDA Pro, a debugger such as Olly, and others. Use of virtual machine software such as Virtual Box is essential, but is not without trade-offs.
- We'll look at static as well as dynamic analysis
- Much malware nowadays is polymorphic, and toolkits such as (the now quite ancient) Poison Ivy make this easy to achieve. Exploit kits such as Blackhole serve to automate the distribution of malware.
- This class is designed to be interactive!
- You can get started now! Before the class starts, you might want to
  - Make sure your laptop works. You'll probably want to bring it to class every time.
  - Download and install Virtual Box on your laptop.

- Install your favorite version of Linux. I prefer Ubuntu, but you can use other versions, including Kali.
- Apply for an Imagine Premium account. When you have this, you have access to Microsoft operating systems and compilers.
- You can also join the Microsoft Developers' Network, commonly known as the MSDN
- If your laptop doesn't have enough memory to run a VM or two, you might consider adding more. Eight gigs may be enough.

Prerequisite:

CMSC 313 or equivalent. You'll be expected to have a solid grasp of programming in assembler as well as a high-level language such as C. If you don't know assembly language you will need to take the course in a later semester. Knowledge of operating systems and networks will be useful but is not required.

Textbook(s):


Practical Malware Analysis
The Hands-On Guide to Dissecting Malicious Software
Michael Sikorski and Andrew Honig
Foreword by Richard Bejtlich

Practical Malware Analysis
Sikorski and Honig
ISBN 978-1-59327-290-6
Publisher: no starch press
this book is **Required**
(electronic and paper versions are available, student may purchase format of their choice)
(zipfile of labs for UMBC only. Use right click and "save link as" to download this password-protected zipfile. The password is 'malware' without the quotes.)

This book is available for the Kindle, but the chapters are numbered differently than the print edition. This book is the best available for the beginning malware analyst, in my opinion, but it focuses on Windows XP. However, this book is still useful because the tools and techniques are still relevant for newer versions of Windows, and indeed for malware on other systems.

The following books are **not required**, but may be helpful:

Malware Analyst's Cookbook and DVD
Ligh, Adair, Harstein and Richard
Publisher: Wiley
(save link as tarfile of DVD for UMBC only)

Reversing: Secrets of Reverse Engineering
Eldad Eilam
Publisher: Wiley
this book is not required, but it may be helpful

Windows Internals, Part 1 and Part 2
Russinovich, Solomon and Ionescu
Sixth edition
Publisher: Microsoft Press

Be careful when dowloading "free" copies of these books! Use VirusTotal to examine any PDFs you get. Additional books, varying in quality, can be found on Wikibooks and other places.

Objectives:

We explore both static and dynamic malware analysis. Although malware takes many forms, we focus on executable binaries. We will cover object file formats, and the use of tools such as debuggers, virtual machines, and disassemblers. Obfuscation and packing schemes will be discussed, along with various issues related to Windows internals.

Students will acquire knowledge of relevant system internals, and experience in using various malware analysis tools. Students will also acquire insight into emerging tends in malware design, including efforts to deter analysis.

This will be a "hands on" course, and students are encouraged to bring their laptops to every class session.

Approximate Schedule:

We will be following the textbook, Practical Malware Analysis, closely. In general, we will cover a chapter per week.

The topics for class sessions here. The course notes are under almost continuous construction. Don't rely on what you see, I can revise at any time!

Course Policies

Grading

We will have a mid-term exam and a comprehensive final examination. Both will be take-home. There will be roughly one homework/programming assignment every two weeks. One or more of the homeworks may involve reading articles or papers and writing short essays. Regular class attendance is expected. In-class quizzes will be given from time to time, with appropriate notice given.

Points will be allocated as followed: 15% midterm, 20% final, quizzes/homework/programming assignments 65%.

Title IX

As an instructor, I am considered a Responsible Employee, per UMBC's Policy on Prohibited Sexual Misconduct, Interpersonal Violence, and Other Related Misconduct (located at http://humanrelations.umbc.edu/sexual-misconduct/umbc-resource-page-for-sexual-misconduct-and-other-related-misconduct/). While my goal is for you to be able to share information related to your life experiences through discussion and written work, I want to be transparent that as a Responsible Employee I am required to report disclosures of sexual assault, domestic violence, relationship violence, stalking, and/or gender-based harassment to the University's Title IX Coordinator.

As an instructor, I also have a mandatory obligation to report disclosures of or suspected instances of child abuse or neglect (www.usmh.usmd.edu/regents/bylaws/SectionVI/VI150.pdf).

The purpose of these reporting requirements is for the University to inform you of options, supports and resources; you will not be forced to file a report with the police. Further, you are able to receive supports and resources, even if you choose to not want any action taken. Please note that in certain situations, based on the nature of the disclosure, the University may need to take action.

If you need to speak with someone in confidence about an incident, UMBC has the following Confidential Resources available to support you:
The Counseling Center: 410-455-2472
University Health Services: 410-455-2542
(After-hours counseling and care available by calling campus police at 410-455-5555)

RETRIEVER ESSENTIALS

Retriever Essentials is a faculty, staff, and student-led partnership to tackle food insecurity in our university community. Our website, www.retrieveressentials.umbc.edu explains our 3 support programs to close the gap between food access and academic success.

Prepackaged bags of non-perishable groceries and other essentials can be anonymously picked up at one of six (6) food zone locations across campus: Honors College, Women's Center, Mosaic Center, Off Campus Student Services, Counseling Center, and Residential Life. If you feel you require additional assistance on top of food, please contact the Counseling Center, 410-455-2472, to make an appointment with Doha Chibani MSW, LCSW-C for a referral services appointment or to be assessed for the Save a Swipe Program (up to 10 free meals to True Grits). Any additional questions can be emailed to retrieveressentials@umbc.edu.

Abuse of Resources

Abuse of the knowledge or experience you gain in this course may subject you to discipline under UMBC policy and/or criminal prosecution. Do not expect your status as a student to protect you if you break the law! Hacking into campus computers (other than systems approved for such a purpose) is a violation of UMBC policy, and may result in disciplinary action possibly including expulsion, in addition to possible criminal charges.

Academic Honesty

Academic dishonesty of any kind will be handled in accordance with University policy.

> "By enrolling in this course, each student assumes the responsibilities of an active participant in UMBC's scholarly community, in which everyone's academic work and behavior are held to the highest standards of honesty. Cheating, fabrication, plagiarism, and helping others to commit these acts are all forms of academic dishonesty, and they are wrong. Academic misconduct could result in disciplinary action that may include, but is not limited to, suspension or dismissal. To read the full Student Academic Conduct Policy, consult the UMBC Student Handbook, the Faculty Handbook, or the UMBC Policies section of the UMBC Directory." [Statement adopted by UMBC's Undergraduate Council and Provost's Office.]

Resources

A collection of malware analysis resources, such as web sites, downloads, and so forth. Suggestions are welcome!

Reading List

Malware analysis is an active area of pure and applied research, and papers are appearing all the time. Students should know how to use the UMBC Library research port and other facilities to get copies of papers they want. I suggest this reading list. Again, suggestions for improving this list are welcome.

CMSC 491/691 Malware Analysis Spring 2019