CS 4440/7440 MALWARE ANALYSIS & DEFENSE: SPRING SEMESTER 2017

Instructor	William L. Harrison, Ph.D	Phone	573 884 2436
Office	318 Engineering Building North	E-mail	harrisonwl@missouri.edu
Office Hours	By appointment only.		

TEXTBOOK:

- *The Art of Computer Virus Research and Defense*, Peter Szor, Symantec Press/Addison Wesley, 2005. Specific sections will be assigned; the whole book is a great reference, but contains more material than we can cover in a semester. You need to order this book online. You may enter the ISBN (0321304543) at http://www.bestbookbuys.com/ and compare new and used prices at various online retailers. *Beware of waiting for back-ordered items.*

DESCRIPTION:

Malicious software – a.k.a. "malware" – is a security threat that everyone has heard about. Most of us have even experienced its bite first-hand. What is malware? How do we recognize malware and what defense techniques are available to us? The best malware – if "best" is the right word – combines in equal parts a deep knowledge of computer systems and tools with diabolical cleverness. Malware analysis and defense is therefore a challenging and important activity for computer scientists and engineers.

The economic impact of malware is severe. Estimates of the economic damage due to malware vary between roughly $15B and $150B worldwide per year over the past decade. According to a well-known malware analyst, there are somewhere between 5 and 6 million known varieties of malware in existence today. "Black Hat" malware education is obviously too good. This course considers "white hat" malware education only.

GOALS:

1. Understand the nature and types of viruses and how they are threats to computer systems.
2. Learn the techniques used to prevent, detect, repair, and defend against viruses and worms.
3. Learn to use program binary examination tools to detect malicious code.
4. Understand the ethical issues surrounding computer security violations.

PREREQUISITES:

CS3280, ECE 3210 or equivalent.

RESOURCES:

An online resource with which you should become familiar is the Virus Bulletin, at the URL: http://www.virusbtn.com/. You can register for free to access archived articles and alerts about all types

of malicious software. Anti-virus professionals pay a substantial sum to subscribe to the monthly magazine, which would be overkill for this course.

EVALUATION:

Undergraduates: There will be two exams (20% each), a final exam (35%), various pop quizzes and class participation (10%), and programming assignments (15% total). Keep all graded material to provide evidence of grades in case there is an error in transcription. Attendance in class is noted. Excessive unexcused absences from class are grounds for receiving a failing grade. The grading scale is the standard A-F scale:

A+	98-100%
A	92-97%
A-	90-91%
B+	88-89%
B	82-87%
B-	80-81%
C+	78-79%
C	72-77%
C-	70-71%
D+	68-69%
D	62-67%
D-	60-61%
F	< 60%

Graduate students. Graduate students will be required to make a 20 minute presentation at the end of the semester on a subject related to malware analysis and defense; the subject of this presentation must be approved by the instructor. Graduate students will also perform all of the same tasks as undergraduates, although with a different weight: two midterms (20% each), one final exam (35%), programming assignments (15%), and the pop quizzes and presentation (10%). The grading scale is the standard A-F scale:

A	90-100%
B	80-89%
C	70-79%
C	60-69%
F	< 60%

COURSE SCHEDULE:

Here is a rough outline of the order of topics. The syllabus may change depending how quickly or slowly we move.

Week	Topic
1	Course introduction, ethics guidelines and pledge, threat models.
2	Categories of threats, terminology, overview of Intel X86 architecture.
3	Overview of Intel x86 architecture, binary disassembly tools; Boot viruses.
4	Viruses: Interrupt hooking, memory-resident viruses, executable file infections.
5	Viruses: Detecting viruses using patterns; regular expressions and lex.
6	Exam 1; obfuscation; defeating obfuscation.
7	Return-oriented Programming
8	Anti-anti-virus schemes: tunneling, armor, retroviruses.
9	Anti-virus analysis; SSA form.
10	Exam 2; Encrypted and oligomorphic viruses.
11	Polymorphic and metamorphic viruses, Strata SDT.
12	Software dynamic translation: security applications.
13	Vulnerabilities, exploits, buffer overflows; secure coding; static analyzers.
14	Root kits.
15	Wrap up.

COURSE RULES:

You are fully responsible for all material presented in class. There may be an occasional unannounced quiz. Exams and due dates are scheduled in advance. A grade of zero will be recorded for missed exams and late assignments unless prior arrangements are made. Assignments turned in after the due date, but before the next scheduled class, are penalized 10%. Assignments that are more than one class period late will not be accepted. You are free to develop assignments on any platform/OS you wish. However, you are responsible for porting your code to the system the class is using and ensuring that it runs correctly. Our reference system will be Windows XP.

Students are encouraged to discuss programs in general and to help one another find bugs in existing programs, but using another's code or writing code for someone else is cheating and a violation of the University's Honor System. This includes consulting solutions to assignments from previous years or tests from previous years. Keep listings to provide evidence of creative development.

ACADEMIC HONESTY

Academic integrity is fundamental to the activities and principles of a university. All members of the academic community must be confident that each person's work has been responsibly and honorably

acquired, developed, and presented. Any effort to gain an advantage not given to all students is dishonest whether or not the effort is successful. The academic community regards breaches of the academic integrity rules as extremely serious matters. Sanctions for such a breach may include academic sanctions from the instructor, including failing the course for any violation, to disciplinary sanctions ranging from probation to expulsion. When in doubt about plagiarism, paraphrasing, quoting, collaboration, or any other form of cheating, consult the course instructor.

STUDENTS WITH DISABILITIES

If you anticipate barriers related to the format or requirements of this course, if you have emergency medical information to share with me, or if you need to make arrangements in case the building must be evacuated, please let me know as soon as possible.

If disability related accommodations are necessary (for example, a note taker, extended time on exams, captioning), please register with the Office of Disability Services (http://disabilityservices.missouri.edu), S5 Memorial Union, 882-4696, and then notify me of your eligibility for reasonable accommodations. For other MU resources for students with disabilities, click on "Disability Resources" on the MU homepage.