COMPSCI 590J  
Cyber Effects: Reverse Engineering, Exploit Analysis, and Capability Development  
SYLLABUS

Instructor: TBA  
Last revised: October 21, 2019

1 Important Details

Credits: 3  
Teaching Assistants:  
TBA  
When/Where: TBA (two days a week)  
Readings: There is no textbook for this class. Instead, we will be using prepared notes supplemented by selected readings and research papers.  
Office Hours: TBA. My email is xxx@cs.umass.edu.  
Prereqs: Undergraduate students: (1) COMPSCI 230 or ECE 322; and (2) COMPSCI 460 or ECE 371 (or any Introduction to Computer/Network Security course at the 300-level or higher), both with a "C" grade or better; or permission of instructor. No restriction on major. Graduate Students: No pre-requisites for CS and ECE graduate students. Other students with permission.

2 Introduction

This course covers a broad range of topics related to cyber security and operations. Our focus is on real world studies of reverse engineering, exploit analysis, and capability development within the context of computer network operations and attack. The course has an emphasis on hands-on exercises and projects. Topics covered include computer architecture and assembly language, principles of embedded security, the essentials of exploit development and analysis (including using industry standard tools such as Ghidra, and utilizing computer security databases such as CVE), and discussion of real-world events and techniques.

The structure of the course includes weekly lectures, discussions, technical assignments, and a final capstone project. Assignments will include programming assignment (both take home and in-class), readings, and some written work.

The specific objectives for the course are as follows:

- To gain a deep understanding of reverse engineering, exploit analysis, and capability development.
- To gain an understanding of practitioner’s tools.
- To gain experience in making well-reasoned arguments during class discussion.

2.1 List of Topics

Below are an overview of topics covered in this course. The course web site has more specifics and last-minute changes.

Course Schedule (Weekly):
1. Machine Architecture Refresher
2. Assembly and Reverse Engineering Refresher
3. Crypto refresher
4. Embedded Security 1
5. Embedded Security 2
6. Embedded Security 3
7. Ghidra: basic/old methods (stack smashing, ROP, etc)
8. Ghidra: why old methods don’t work anymore
9. Ghidra: overcoming new protections
10. Weaponization of CVEs
11. Command & Control of deployed exploits + covert communication for exfil
12. Case Studies + Capstone kickoff
13. Real world scenarios (Apt-1, Stuxnet, etc)
14. MITRE ATT&CK
15. Capstone Presentations
3 Inclusive Discussion

In this course, each voice in the classroom has something of value to contribute. Please take care to respect the different experiences, beliefs and values expressed by students and staff involved in this course. I support the commitment of the UMass Amherst College of Information and Computer Sciences to diversity, and welcome individuals of all ages, backgrounds, citizenships, disability, sex, education, ethnicities, family statuses, genders, gender identities, geographical locations, languages, military experience, political views, races, religions, sexual orientations, socioeconomic statuses, and work experiences.

4 Grading

Your overall grade for the course will be derived from three components. At a high-level grading is based on the following formula:

- 65% Assignments (including assignments completed during discussion)
- 25% Capstone
- 10% Class participation (including attendance in discussion and online participation)

Additionally, without a grade of 50% or higher on the capstone, students cannot pass the class.

Each assignment will have a slightly different number of points. Your score will be the total number of points earned over total number of points available for all assignments. Late homeworks are NOT accepted.

I will assign a B grade to students with a final numeric grade equal to the mean of the class. The range of each letter will be based on the standard deviation (sd) of the class grades. An A is 1 sd above B; A− is 0.7 sd above; B+ is 0.3 above; C+ is 0.7 below; C is 1 sd below. Graduate students at UMass cannot be assigned a grade below a C other than a failing grade. I may curve grades or individual assignments.

Don’t underestimate the Class Participation component — full credit versus none can move your final grade by quite a bit. Furthermore, in-class exercises that are missed due to unexcused absences will lower your grade.

4.1 Homeworks

I will use web interfaces exclusively to accept assignments, which must be in the form of a PDF (no word, text, or other formats), with your name clearly visible. In the case that an assignment involves code, please submit a tar-ball or zip file. I will not accept assignments late, and I will assign a score of zero for work that is not submitted on time (or at all).

If class participation is generally low, or if I get the sense that students aren’t reading, I will give in-class quizzes. These quizzes will be pre-announced. They will become part of the homework component of your grade. Assignments that do not compile will receive no credit.

4.2 Class Participation

I will assign this portion of your grade on the basis of your presence and participation in class. Obviously, I expect you to always attend class. Further, I expect you to participate in class discussion, posing and answering questions as appropriate. Also, I expect that you’ll leave room for others to speak their minds as well. I will provide feedback about halfway through the semester as to the status of this portion of your grade.

If I have outside experts join us in class, not attending on these days will weigh more heavily against your participation grade.

One optional way to improve your class participation grade is to offer up to the entire class your scribe notes from discussion or the online videos. I’ll provide a google doc for each discussion meeting and video to add your comments to.

5 Policies

All official material for the class can be found on the UMass moodle/blackboard website. Any external course web page is more of an advertisement for the class and won’t be kept up to date.

Cell phones, laptops, and similar devices may not be used during in-class session.

5.1 Collaboration and Plagiarism

Please come see me if you are unable to keep up with the work for this class, for any reason, and I will work something out. Obviously, there isn’t anything I can do when the semester has already ended. I want to see you succeed and will do everything I can to help you out. The earlier you let me help, the more help I can offer. I’ve been here since last millennium and I’ve seen it all; please come by.

Please be cognizant of the University’s policies on cheating. You may discuss material with others, but your writing must be your own. When in doubt, contact me about whether a potential action would be considered plagiarism. When discussing problems with others, do not show any of your written solutions. When asking others for help, do not take notes about the solution other
than to jot down publicly available references. Use only verbal communication.

If you do discuss material with anyone besides the instructors, acknowledge your collaborators in each write-up. If you obtain a key insight with help (e.g., through library work or a friend), acknowledge your source, briefly state the insight, and write up the solution on your own. I expect to see citations if you use an outside source (other than the assigned articles) to complete an assignment. You may directly quote from a decision in order to complete a brief — provided you surround the text by quotation marks — without citation.

It is never permissible to distribute your completed assignments, my homework solutions, quiz/exam solutions to other persons nor to post these materials to Internet sites, including Github and Course Hero. Of course it is not permissible to use such resources as well. Both are obvious violations of the University’s academic honesty policies and I will pursue sanctions even after the course is over.

Never misrepresent someone’s work as your own. It must be absolutely clear what material is your original work. You must remove any possibility of someone else’s work from being misconstrued as yours.

As a condition of continued enrollment in this course, you agree to submit all assignments to the Turnitin and/or My Drop Box services for textual comparison or originality review for the detection of possible plagiarism. All submitted assignments will be included in the UMass Amherst dedicated databases of assignments at Turnitin and/or My Drop Box. These databases of assignments will be used solely for the purpose of detecting possible plagiarism during the grading process and during this term and in the future. Students who do not submit their papers electronically to the selected service will be required to submit copies of the cover page and first cited page of each source listed in the bibliography with the final paper in order to receive a grade on the assignment.

You can and should read the University’s policies on cheating as well at http://www.umass.edu/ombuds/honesty.php/. In short, intellectual honesty requires that students demonstrate their own learning during examinations and other academic exercises, and that other sources of information or knowledge be appropriately credited. Scholarship depends upon the reliability of information and reference in the work of others. Student work at the University may be analyzed for originality of content. Such analysis may be done electronically or by other means. Student work may also be included in a database for the purpose of checking for possible plagiarized content in future student submissions. No form of cheating, plagiarism, fabrication, or facilitating dishonesty will be condoned in the University community. (Some portions of the above plagiarized from http://www.umass.edu/academic honesty/Addressing Plagiarism.html!)

6 UMass Policies

Accommodation Statement. The University of Massachusetts Amherst is committed to providing an equal educational opportunity for all students. If you have a documented physical, psychological, or learning disability on file with Disability Services (DS), you may be eligible for reasonable academic accommodations to help you succeed in this course. If you have a documented disability that requires an accommodation, please notify me within the first two weeks of the semester so that we may make appropriate arrangements.

Academic Honesty Statement. Since the integrity of the academic enterprise of any institution of higher education requires honesty in scholarship and research, academic honesty is required of all students at the University of Massachusetts Amherst. Academic dishonesty is prohibited in all programs of the University. Academic dishonesty includes but is not limited to: cheating, fabrication, plagiarism, and facilitating dishonesty. Appropriate sanctions may be imposed on any student who has committed an act of academic dishonesty. Instructors should take reasonable steps to address academic misconduct. Any person who has reason to believe that a student has committed academic dishonesty should bring such information to the attention of the appropriate course instructor as soon as possible. Instances of academic dishonesty not related to a specific course should be brought to the attention of the appropriate department Head or Chair. Since students are expected to be familiar with this policy and the commonly accepted standards of academic integrity, ignorance of such standards is not normally sufficient evidence of lack of intent (http://www.umass.edu/dean_students/codeofconduct/acadhonesty/).