Cyber Effects: Intro to Reverse Engineering, Exploit Analysis, and Capability Development

SYLLABUS

Instructors: Nick Merlino, Jeff Hamalainen, Adam Woodbury, Seth Landsman, Ed Walters

Last revised: January 4, 2024

1 Important Details

Credits: 3

Location: In-person CS142 (preferred) or synchronous attendance online via Zoom

Meeting times:

Lectures: Once per week - likely Mondays 5:30-6:45pm

Discussions: Once per week - likely Wednesdays 5:30-6:45pm

Required Material: There is no required textbook.

Prereqs:

Undergraduate students: (1) COMPSCI 230 or ECE 322 ; and (2) COMPSCI 360 (or 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 lead instructor.

Graduate Students: No pre-requisites for COMPSCI and ECE graduate students. Suggested basic knowledge of reverse engineering and cybersecurity concepts.

Other students: Permission of lead instructor.

2 Introduction

This course covers a range of topics related to cyber security and operations. As each topic could be its own course, they will be presented broadly. The 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 a strong emphasis on hands-on exercises and projects. Industry standard tools such as Ghidra and CVE will be leveraged. Lectures will cover a lot of material and the assignments will likely be on material that students have not had experience in, so individual online research will be necessary. Students are not expected to be at a professional skill level in each of these topics by the end of the course, but instead the objective is to ensure that each student has at least a fundamental understanding of each topic and how they influence each other. Students should be prepared to learn about both COMPSCI and ECE concepts.

3 Course Objectives

1. To learn and understand the fundamentals of the different technical aspects of CyberEffects, including
   - Obtaining firmware from devices around potential memory protections
   - Investigating an unknown binary of unknown origin
   - Analyzing an executable for both behavior analysis and behavior modification
   - Building additional security protections into systems to mitigate threats
   - Designing meaningful cyber operations given a working exploit, including command and control and data exfiltration
2. To learn about real-world CyberEffects scenarios that have occurred throughout the world in order to better inform creation and analysis of future CyberEffect investigations
3. To learn how to use real-world tools as a professional in cybersecurity
4. To develop a real-world cyber effect in a lab environment using pre-developed vulnerabilities

4 Lecture Outline

1. 2/5 Real World Scenarios (Apt-1, Stuxnet, etc)
2. 2/12 Computer Architecture
3. 2/21 Assembly and Reverse Engineering
4. 2/26 Tools and Techniques for Analyzing a binary
5. 3/4 Cryptography
6. 3/11 Weaponization of CVEs
    - 3/13 Discussion: MITRE ATT&CK
7. 3/25 Covert Command & Control of Implants
8. 4/1 Offensive Methods (stack smashing, ROP, etc)
9. 4/8 Defensive Methods (ASLR, etc)
10. 4/12 Embedded Security
11. 4/22 Implementation Attacks
12. 4/29 Firmware Extraction + DPA
13. 5/6 Firmware Extraction + DFA
14. 5/8 Capstone Presentations
15. Final: Capstone presentation questions

5 Grading

- 50% Assignments
- 40% Capstone Project
- 10% Lecture Attendance

Additionally, without a grade of 60% or higher on the capstone, students will receive an F for the course.

5.1 Numeric/Letter Grading Scale

The following scale will be used to translate between numeric to letter grades for undergraduate students.

High	Low	Letter
100.0+	93.00	A
92.99	90.00	A-
89.99	87.00	B+
86.99	83.00	B
82.99	80.00	B-
79.99	77.00	C+
76.99	73.00	C
72.99	70.00	C-
69.99	67.00	D+
66.99	63.00	D
62.99	0.00	F

For graduate students, any grade below C is an F grade in the course, per university policy.

High	Low	Letter
100.0+	93.00	A
92.99	90.00	A-
89.99	87.00	B+
86.99	83.00	B
82.99	80.00	B-
79.99	77.00	C+
76.99	73.00	C
72.99	0.00	F

6 Assignments

The weekly assignments will be related to the material presented in lecture that week, but additional online research will be necessary to solve most problems.

Assignments will be posted after each lecture and will be due at the beginning of the following lecture. Late assignments won't be accepted. One re-submission per assignment will be accepted up until a hard deadline of 8pm on the day 1 week after the grade was posted, where students have the ability to earn back up to 50% of the points that they lost. Solutions will be posted at the re-submission deadline, so the assignment will be closed at this point.

7 Capstone Project

Students are expected to create a Cyber Effect in teams of up to 3 people, with complexity reflecting the size of the team. Teams must:

- Identify one or more CVEs on a platform of their choice and develop/locate a weaponized exploit. Metasploit implementations will not receive full credit. Github discovered implementations are suggested.
- Develop an implant that will leverage the weaponized exploit to allow it to execute. This implant must include exfil of meaningful data.
- Develop an effective command and control system for tasking the implant and receiving exfil data.
- Obfuscate the implant, the command and control communication, and the exfil communication. The methods for command and control and exfil obfuscation must be different.
- Ensure that all code is well commented and easily interpreted (only when appropriate for the use case - implants shouldn't have comments to make reversing harder!).
- Demonstrate knowledge from many aspects of the course, including software reverse engineering and hardware implementation security

In addition to the code, teams are expected to submit a professional pre-recorded presentation (10min maximum) about their project, including slides that describe:

- A hypothetical use case of their project, and why their specific design choices were appropriate for that use case with both hardware and software considerations
- What the implant does. How is this novel?
- How the implant is injected into the target device. Why is it realistic for your scenario?
- How the implant, the C2 comms, and exfil comms work and are obfuscated. Is this sufficient for your scenario?
- How the project is resistant to reversing if it is discovered (consider methods described in the course)
- If you were to defend against your project, how would you do so? (consider attacks on your command and control system, data exfiltration, the implant itself, etc)
- What would the team do differently next time?

Students shall not run their projects on any public network, including UMass networks. All tests should be done on private local networks that are not connected to the internet.

There is a hard deadline of the start of the session where we will watch the submissions together as a class. This includes the code (shared by Github link in a CampusWire post), the presentation video (uploaded to Google Drive), and presentation slides (uploaded to Google Drive). The code will be reviewed and tested as needed by the instructors before the final exam period, when the class and instructors will ask clarifying questions about the presentations.

8 Course Engagement

At every lecture session, attendance will be taken. Sometimes this will be by recording who is in attendance at the beginning and end of the lecture. Sometimes it will include random check-in quetsions to ensure engagement.

Attendance will not be taken in discussions, which will be time for students to collaborate and ask for assistance on assignments / the capstone project. It is strongly encouraged to use this time during the entire semester to actively work on your capstone projects. There won't be additional time at the end to work solely on the capstone project.

9 Course Resources

Canvas - Where all course material, including lecture recordings, lecture slides, course announcements, and assignments will be posted. Also, the location to submit assignments and questions for the class.

Zoom - Where we will stream to students joining remotely.

10 Policies

10.1 Fair Work

We acknowledge that many students have commitments outside of this course, whether it be other courses, work, family obligations, etc. Therefore, We will attempt to ensure that each assignment can be completed within 8 hours. If an assignment takes more than 8 hours, students are strongly encouraged to ask for guidance from first their peers and then the instructors. Students should not spend sleepless nights working by themselves if they are having a problem completing any assignment.

10.2 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. We 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.

10.3 Academic Honesty

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 the lead instructor about whether a potential action would be considered plagiarism. When discussing problems with others, do not show any of your written solutions.

It is never permissible to distribute completed assignments or homework 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 we will pursue sanctions even after the course is over.

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/`).

10.4 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.