REVERSE ENGINEERING: SY485J

Course Policy

Fall 2019

INSTRUCTOR: Mr. Mark De Bels, debels@usna.edu, NSA Visiting Professor

COURSE DESCRIPTION:

In this course, students will learn why software is reverse engineered and the fundamentals of how it's done. Fundamental topics will be introduced: compilers, differences in programming languages when reverse engineering, assembly language, as well as static and dynamic analysis tools. Hands on work will develop the skills and knowledge used to reverse engineer a binary without access to the original source code.

In the first portion of the class, some reasons for software reverse engineering will be discussed and time will be spent examining the background material necessary for an understanding of the subject. This will include discussion of computer architecture, the evolution of programming from assembly language to modern languages, as well as the fundamentals of compilation.

In the second portion of the class, we will apply this newly acquired knowledge while learning about static and dynamic analysis tools used by practitioners of software reverse engineering. Students will perform reverse engineering of several representative examples of software, including malware.

COURSE OBJECTIVES:

1. Learn what reverse engineering is and why it is used. Understand the legal aspect of reversing.
2. Learn and understand assembly language code and how it relates back to a higher level language.
3. Learn different static and dynamic reverse engineering techniques. Understand how to use reverse engineering tools to reverse binary code back to assembly language and possibly a higher level language.
4. Reverse engineer cryptographic applications in order to understand how they function and to modify execution.
5. Reverse engineer malware to understand what it is doing and perform analysis of the code.

COURSE MATERIALS:

Required: none

Recommended: “Reversing: Secrets of Reverse Engineering” by Eldad Eilam

Wiley; 1 edition – ISBN: 0764574817

- Course Instructor will be using this book as a partial guide for course content

GRADING AND ASSIGNMENTS:

Your grade will consist of:

	6-Week Grade	12-Week Grade	Final Grade
Labs / Homeworks	45%	45%	25%
Final Project			20%
6-Week Exam	45%	20%	12.5%
12-Week Exam		25%	12.5%
Final Exam			20%
Instructor Option	10%	10%	10%

Lab Assignments: Most weeks, a portion of the class time will be used to work on lab assignments which will allow you to explore the ideas covered in lecture. Reverse engineering is hard work, and greatly benefits from collaboration with colleagues. Some labs will be working on your own, while others will be working collaboratively in groups of 2-3 students. Collaboration will be clearly defined for each assignment.

Homework: Reading assignments will be provided each week. They will include applicable real world examples of reverse engineering. This is required reading. Other homework assignments will be occasionally given to reinforce non-programming concepts from class. These assignments will be the main way to check if you understand the material, so please take them seriously and seek help if you are having trouble. You may not collaborate on homework.

Projects: There will be one final project in this course. No collaboration or online assistance is allowed on this project.

Exams: There will be a 6-Week, 12-Week and Final Exam for this course.

Instructor Option: Largely includes participation in class discussions. This course requires that you participate actively in class discussions, and work with your group as appropriate during lab time. It is highly recommended that you read any assigned reading ahead of time – this will provide you with a base knowledge necessary to aid in your class participation.

LATE ASSIGNMENTS:

This is a Senior Level course and as such, assignments/homework/projects are expected to be handed in / submitted to the instructor at the beginning of class the day they are due.
Assignments handed in within 24 hours of the due date/time can receive at best a score of 75%.
Assignments handed in within 48 hours of the due date/time can receive at best a score of 50%.
Assignments handed in greater than 2 days late will receive no credit.

WEEKLY BREAKDOWN OF TOPICS:

1. Introduction to Reverse Engineering, Legal aspects
2. Computer Architecture, Compilers, and Programming Languages
3. Assembly Language Introduction (objdump, GDB)
4. Reverse Engineering Mindset
5. Static and Dynamic Analysis Intro / Basic RE Tools (Ghidra)
6. 6-Week Exam; Reversing Cryptographic Applications
7. Deeper Dive into Programming Languages (C and Assembly)
8. Reconstructing Source Code
9. Other Reverse Engineering Tools (IdaPro, Radare2)
10. Stack Buffer Overflows: Finding and Controlling Execution
11. Windows Fundamentals and API usage
12. 12-Week Exam; Reversing Challenges: Data at Rest vs Data in Transit Applications (Communications Protocols)
13. Introduction to Malware & Start Final Project: Reverse Engineering Malware
14. Reversing C++
15. Anti-Reverse Engineering Techniques
16. Final Exam

HONOR:

You are expected to follow the guidance given in:

1. Honor Concept of the Brigade of Midshipmen, USNAINST 1610.3F (or newer)
2. Policies concerning graded academic work, USNAINST 1531.53 (or newer)

CLASSROOM EXPECTATIONS:

1. No food or smokeless tobacco is permitted in the classroom. Drinks with closeable caps are permitted.
2. Sleeping is not allowed in class. If found sleeping, this will affect your instructor option grade and will likely be reported to your Company Officer. If you feel you may fall asleep, stand in the back of the room.
3. You must bring your laptop to every class.
4. While class is in session, there will be no use of computer equipment for any other purpose than class activity/work. Other uses (not limited to the following), such as reading emails not related to the course, playing games, messaging, social media, etc., will not be tolerated.
5. Please inform the instructor in advance if you will miss class for an excused reason.

EXTRA INSTRUCTION:

Please contact the instructor in person or through email (debels@usna.edu) if you would like EI. Please make sure to do so in advance of due dates on assignments. It is crucial that you seek EI as soon as you are having problems understanding the material. You will not be provided answers; you will be provided with further information to help you understand the topic.

Mr. Mark De Bels

CDR Tracy Emmersen

_____

Course Coordinator

_____

Cyber Science Dept. Chair