ECE497/CSSE490: Malware Analysis and Reverse Engineering Syllabus

Fall 2025-2026

Instructor: Dr. Sid Stamm
Office: D207
Email: stammsl@rose-hulman.edu
Office Hours: See http://www.rhit.edu/~stammsl/#schedule

Course Information

This course is meant to introduce you to the broad area of reverse engineering through examples focused on binary analysis. You will learn how to investigate software to see what it does and how to catch software that is behaving badly.

The topics covered include: Static Analysis, Dynamic Analysis, Executable packing, Disassembly/Decompiling, Anti-disassembly/Anti-debugging techniques, Malicious software behavior, Network and Host-level Malware Signatures, Analysis of Embedded Systems, and Current Topics in Binary Analysis (e.g., emulator based dynamic analysis and symoblic execution).

The course will meet four days a week and sessions will involve lectures with in-class activities. You are expected to actively participate during class sessions.

Catalog Description and Prerequisites

ECE332 or (CSSE232 and CSSE332).
Recommended: Proficiency in OS and Compiler Concepts

Course Requirements (Materials)

"Practical Binary Analysis: Build Your Own Linux Tools for Binary Instrumentation", Andreisse 2019. (ISBN-13: 978-1-59327-912-7)

Approximately 30GiB of Hard Drive space for Virtual Machines

Student Learning Outcomes

After successfully completing this course the student should be able to:

- Describe a process that would identify the purpose and behavior of a binary executable program.
- Given a binary executable, analyze and explain its purpose and what it does.
- Given sample malware, explain changes required to a system to make the malware ineffective.
- Use modern techniques to create unwanted software (packing, obfuscation, anti-debugging).
- Use modern techniques to detect and recover from installs of unwanted software (static/dynamic analysis, debugger tracing, manual decompiling).
- Research and define state of the art techniques in malware behavior, analysis, and reverse engineering.
- Describe and discuss the societal implications and ethics of malicious software

Grading

The topics covered in this class are extremely hands-on and students will demonstrate mastery of those techniques through mini-projects, written reflections, and a final project.

The percentage breakdown of your grade is:
40% Homework/Mini-Projects
10% Written Reflections
40% Final Project
10% Class Participation

The course will use the standard Institute grading scale (e.g., 90-100 is an A, 85-89 is a B+, etc...)

Late Assignment Policy

All homework will be submitted electronically and is due at 11:59 pm on the assigned due date. Late submissions are generally not accepted.

Academic Honesty

Be aware of the Rose-Hulman Honor Code and that honesty and integrity in one's work is of the utmost importance. Inappropriate sharing of work and information, including electronic sharing, will not be tolerated. For example, using tools other than those required for that

assignment is strictly prohibited (e.g., decompiling an assembly assignment).

Given the nature of the material covered in this course, you are expected to act ethically. You should not use the skills in this course in any context when you are not authorized to do so by the owner and maintainer of that system. Unethical behavior and in particular, the distribution or creation of malicious software is grounds for an automatic failure in the course. All incidents will be escalated to the appropriate authorities. There will be no second chances.

If you consult others in your submitted work you must acknowledge their specific contributions in writing on the assignments. A general guideline is that talking about tools and techniques is okay. Talking about how a challenge binary works is not okay. Discussing your final project with others is not okay. Looking at someone else's screen while they work on a problem is not okay.

Rose-Hulman has high expectations for its students, faculty, and staff. That is because we are in the business of educating students for challenging careers with high standards of professionalism, ethics, technical know-how, intellectual creativity, productivity, communication,teamwork, and academic integrity. The standards are also embraced by the faculty and staff so that they can achieve high standards and also serve as role models.

Academic integrity refers to maintaining a high standard of honesty in academic conduct. All students and faculty are encouraged and required to show academic integrity at all times. On the other hand, academic misconduct is a failure of academic integrity. Specifically, academic misconduct is cheating, plagiarism, or interfering with the academic progress of other students.

The Academic Rules and Procedures document http://www.rose-hulman.edu/offices-and-services/registrar/rules-procedures/discipline.aspx provides extensive rules and procedures for academic and other misconduct. The minimum penalty for such misconduct is for the instructor to award zero credit for whatever test, exam, project or quiz on which the misconduct occurs, even if it results in a lowered or failing grade. A report of the misconduct will be sent to the Dean of Students, Department Head, and the student's advisor. Faculty members may exact a higher penalty, up to and including failure in the course if they feel the misconduct warrants such action. Students may appeal the sanctions to the rules and discipline committee, per the cited web page.