Gianforte School of Computing
Norm Asbjornson College of Engineering
Montana State University

Course Syllabus

Course: CSCI 591 – Malicious Code Analysis

CRN: 25740

Course Time & Location: TR 12:15-13:30pm & BARNAR 126

3 Credit Hours

Instructor: Fangtian Zhong
Email: fangtian.zhong@montana.edu
Office Hours: By appointment or
CSCI 591: T 09:30 – 12:00pm

Office: Barnard Hall 352
Phone: 202-460-7413

Textbook

Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski, Andrew Honig, No Starch Press, 2012

Windows 64-bit Assembly Language Programming Quick Start: Intel X86-64, SSE, AVX by Robert Dunne,Gaul Communications, 2018

Prerequisite

a operating systems course, a C/C++ course, a Python course, and a data structures/algorithms course

Course Description

Introduction to malware analysis issues from end-user perspectives. Topics include assembly basics, malware classification, malware retrofiting, malware analysis and malware detection. Hands-on tools to identify and generate signatures for malware analysis will be introduced.

Student Learning Outcomes

Outcome 1: Be able to use current techniques, skills, and tools necessary for computing practice.
Outcome 2: Apply algorithmic principles and formal models to solve advanced problems in cybersecurity and computing.
Outcome 3: Apply security principles and practices for maintaining operations in the presence of risks and threats.
Outcome 4: Evaluate and maintain cyber systems for secure and reliable operations.

Course Objectives

Upon completion of this course, the student should be able to:

- Master the interaction between assembly codes and registers, and memory and manually analyze the changes in the stack by instruction execution.
- Grasp the rationale for the malware taxonomy and learn to classify malware files manually.
- Grasp binary retrofitting techniques to modify malware binaries.
- Analyze and predict the potential malicious operations in different types of malware.
- Understand security risks related to malicious content in malware and be able to recognize and respond the threats by using static or dynamic analysis.

Course Structure

This class will meet face to face on its scheduled days. This course will have assignments, quizzes, projects, a midterm exam, and a final exam.

Technology Requirements

You are expected to have the computing resources necessary to complete this course through personal and/or University channels (e.g., computer labs). Below is a list of some helpful computer requirements for full participation for this class:

- A x64-based laptop or desktop with Windows10 or above operating system.
- The latest version of VMware Workstation Player available from: https://www.vmware.com/products/workstation-player.html
- The latest version of Win10 available from: https://www.microsoft.com/en-us/software-download/windows10ISO
- The latest version of Microsoft Visual Studio available from: https://visualstudio.microsoft.com/zh-hans/downloads/
- The latest version of PE Tools available from: https://petoolse.github.io/petools/#pe-editor
- The latest version of Python available from: https://www.python.org/

  The latest version of Git available from: https://git-scm.com/download/win
- The latest version of angr available from: https://docs.angr.io/introductory-errata/install
- The latest version of Windbg available from: https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/debugger-download-tools
- The latest version of Cuckoo available from: https://cuckoosandbox.org/download

Learner Support

Students can get technical support from the Academic Technology and Outreach online at https://ato.montana.edu/technologies/learning/, by phone (406) 994-6550, and in person at, Location: 128 Barnard Hall.

Course Content Outline

1. Chapter 1: Assembly Basics
   a. Environment Setup and Basic Syntax
   b. Arithmetic Instructions and Logical Instructions
   c. Condition Instructions
   d. Procedures and Macro
   e. File Management and Memory Management

2. Chapter 2: Malware Taxonomy
    a. Viruses and Worms
    b. Logic Bombs and Trojan Horse
    c. Rootkits and Backdoors
    d. Bots and Botnets
    e. Spyware and Adware

3. Chapter 3: Programming Malware
    a. PE Structure
    b. Import Table
    c. Import Address Table
    d. Bound Import Table
    e. Relocation Table
    f. Export Table
    g. Retrofiting

4. Chapter 4: Malware Analysis
    a. Angr and Environment Setup
    b. Analyzing Malicious Program
    c. User Mode Debugging with Angr
    d. WinDbg and Environment Setup
    e. Kernel Debugging with WinDbg

5. Chapter 6: Malware Detection
    a. String Scanning
    b. Hashing
    c. Top-and-Tail Scanning
    d. Nearly Exact Identification
    e. Image Based Identification
    f. SandBoxing
    g. Encrypted and Polymorphic Virus Detection Using Emulation
    h. Graph Detection

Grading (100 points possible)

Deliverable	**Points**
Weekly Participation / Attendance	5%
Weekly Assignments / Quizzes	15%

4 Projects	40%
Midterm Exam	20%
Final Exam	20%
Total	**100%**

Grading Scale

(100 points possible)
A: 90%-100%,
B: 80%-89.9%, (89.5 will be rounded to 90%)
C: 70%-79.9%, (79.5 will be rounded to 80%)
D: 60%-69.9%, (69.5 will be rounded to 70%)
F: 0%-59.9%, (59.5 will be rounded to 60%)

Other Information and Policies

1. Your MSU email account will be used, frequently, by the instructor, to communicate messages. It is your responsibility to check this account regularly.

2. Class notes, announcements, and assignments, projects will be posted on Blackboard. It is the responsibility of the student to frequently check Blackboard for course changes and updates.

3. The assigned textbook is required.

4. Advanced arrangement for unavoidable absences should be made whenever possible. Neither absence nor notification of absence relieves you of the responsibility of meeting all course requirements.

5. Make-up exams will be given only for valid excuses with proof and have to be completed within 5 days of the regular exams. A make-up exam will be different from the regular exam.

6. Assignments, quizzes, projects, and tests are to be done independently unless otherwise indicated by the instructor.

7. During tests, no communication tools are allowed. **Any form of academic dishonesty will be dealt with according to the guidelines found in the Code of Conduct, Policies, Regulations, & Reports or at http://catalog.montana.edu/code-conduct-policies-regulations-reports/.**

8. **Accessibility Services**

Students with disabilities who are seeking accommodation should contact the The Office of Disability Services at 137 Romney Hall, 406-994-2824. If you want to share information about your needs that I should be aware of, such as emergency medical information or special arrangements for field trips or internships, please see me privately after class or during office hours.

9. **Sexual Discrimination and Sexual Misconduct Statement**

Montana State University seeks to foster a safe and healthy environment built on mutual respect and trust. Sex discrimination, including sexual harassment, sexual violence, and other forms of sexual misconduct will not be tolerated. All faculty and most staff are considered mandated reports by the University and must disclose all information they receive about sexual misconduct to the Title IX Coordinator. As a faculty or staff member of the University, I am a mandated reporter. This means I am required to report information shared with me regarding sex discrimination and sexual misconduct.

If you, or someone you know, has experienced sex discrimination or sexual misconduct, please know assistance and options are available. MSU strongly encourages all members of the community to seek support and report incidents of this nature to the Title IX Coordinator. Anyone who wishes to report sexual misconduct, to learn more about the University process and options available, or to utilize a confidential resource, please visit https://www.montana.edu/equity/nondisclosurestatement.html.

10. **Diversity, Equity, and Inclusion**

Montana State University strives to develop a campus environment that welcomes and recognizes all dimensions of diversity and inclusiveness. What this means is that all students are welcomed in the classroom, and differences are to be recognized rather than erased or denied. Dimension of diversity can include sex, race, age, national origin, ethnicity, gender identity and expression, intellectual and physical ability, sexuality, income, faith, and non-faith perspectives, socio-economic class, primary language, family status, military experience, and more. Inclusive learning is facilitated by creative and innovative thought and mutual respect; being in this classroom means that you, your faculty member, and your peers pledge to foster a welcoming and equitable environment for all.