



2025.08.21

# Malicious Code Analysis

Fangtian Zhong  
CSCI 591

Gianforte School of Computing  
Norm Asbjornson College of Engineering





# Info About Me

## Fangtian Zhong

### ★ Education

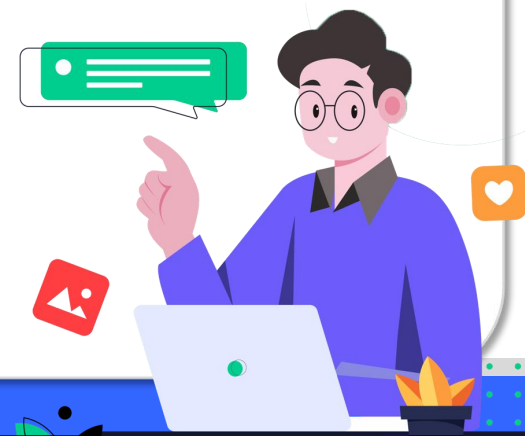
- Ph.D., George Washington University, 2021
- Postdoc., Pennsylvania State University and University of Notre Dame

### ★ Research interests

- Software security
- Program analysis
- Machine learning for cybersecurity

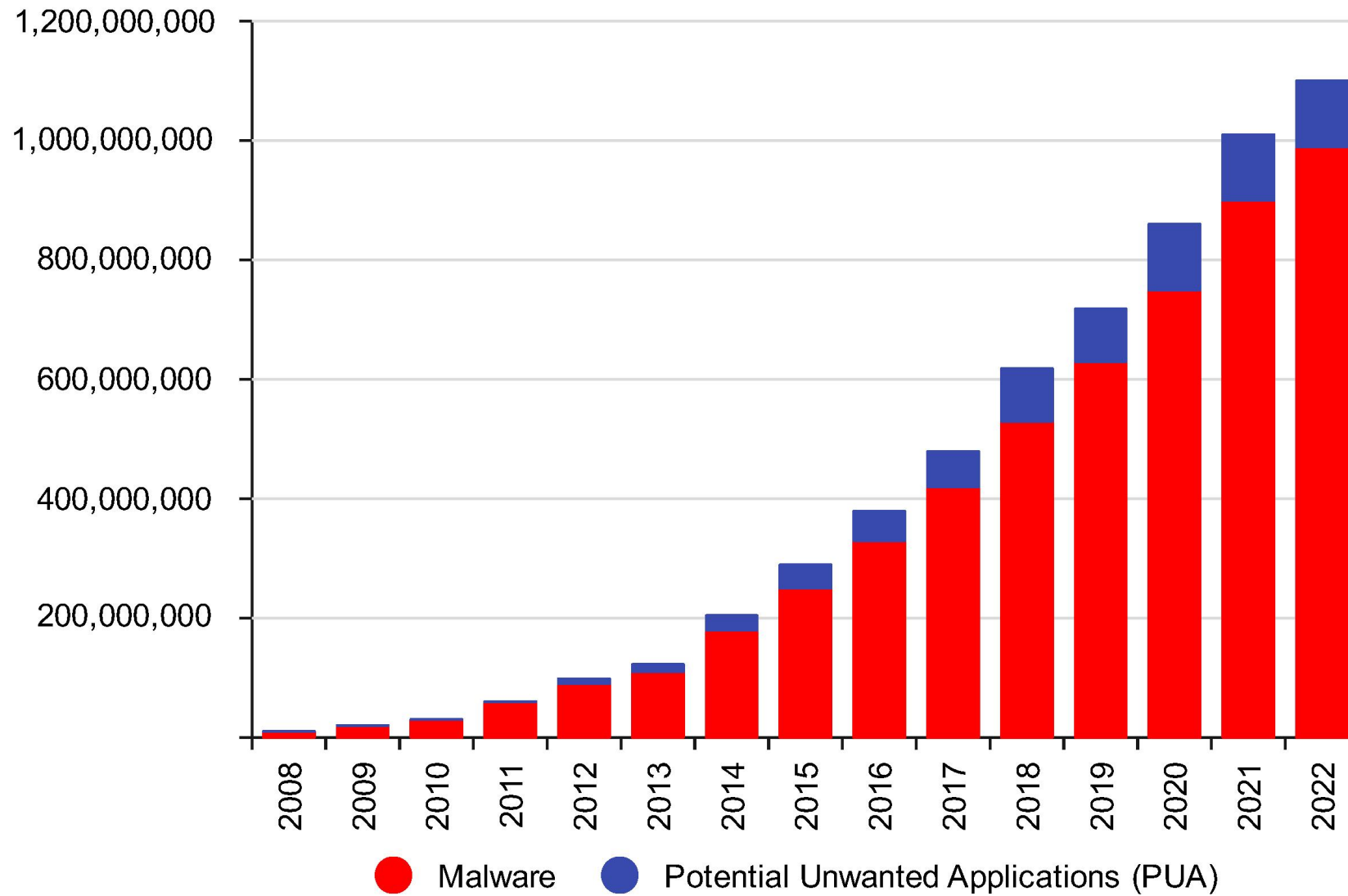
### ★ More

- <https://fangtian-zhong.github.io/>





# Necessity





# Course Information

---

- ★ Website: <https://fangtian-zhong.github.io/teaching/csci591-fall-2025/syllabus>
- ★ Time: TR 12:15-13:30pm
- ★ Location: REID 453
- ★ Office Hour: Tuesdays/Thursdays: 10:50am-12:10pm
- ★ Office: Barnard Hall 356
- ★ Email: [fangtian.zhong@montana.edu](mailto:fangtian.zhong@montana.edu)



## Text Books (Required)

---

- ❑ 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

**CSCI 107 Joy Beauty of Computing**

**CSCI112 Programming with C I**

**CSCI 232 — Data Structures and Algorithms**

**CSCI 460 — Operating Systems**





# Course Objectives

---

- ★ Write assembly programs and study the effects of instruction execution on the stack.
- ★ Classify malware programs manually.
- ★ Develop binary retrofitting techniques to modify and repurpose malware binaries.
- ★ Understand the security risks associated with malicious content in malware and develop the ability to recognize and respond to such threats using static and dynamic analysis techniques.

# Grade Breakdown

- ★ You will be graded on the following:
- ★ 6 assignments: 20%
- ★ 5 projects: 40%
- ★ 2 exams: 30
- ★ Quizzes/Absence (Lowest 5 dropped): 10%
- ★ Your grade will be determined by your total score as follows:  
93+: A; 90+: A-; 87+: B+; 83+: B; 80+: B-; 77+: C+; 73+: C;  
70+: C-; 67+: D+; 63: D; 60: D-.





# Grading

---

I am always happy to chat, review ideas from this course, try to clarify questions, and discuss any questions or concerns you may have about graded work.

I do not pre-grade assignments/projects. I typically do not curve grades.

**Any grade disputes must be resolved within one week of the release of the grade.**

# Late Penalties

- All projects/assignments are due on their due date by the Anywhere on Earth (AoE) timezone, which is 6 hours behind Bozeman (Actually, it's only 5 hours behind during standard time, but we'll go with 6 hours behind at all times). This means that the real due date is 6am the following day. If you submit projects within 24 hours of the due date, you get 25% off of whatever score you earn. If you submit within two days of the due date you get 50% off. Otherwise, no points are possible. You can submit as many times as you would like; only your last submission will be graded.
- Assignments cannot be submitted late.

# Missed quiz/attendance policy



Quizzes and attendance will be taken during class sessions. You may miss up to five classes without penalty, regardless of whether the absences are excused or unexcused.

# Bonus



## Catch errors in course materials

- If you find an error in any of the course materials (typo, incorrect statement, etc.), post in the #errors\_capture channel on Slack. I will decide whether it's truly an error and not a duplicate. If it is really an error, you get half of a point. Only the first person to post about an error gets the points. You can earn a max of 3 total points toward your 100 for the course (for six errors).



## Course evaluation

- If 75% or more of the class completes the course evaluation, the whole class gets 1 bonus point.



# Communication

---

We will use Slack for all course communication (except for sensitive stuff like grades!).

Please **do not** use other means of electronic communication (e.g., D2L, e-mail) **unless you absolutely have to**.

**I typically won't respond to emails or Slack direct messages (DMs) past 6 p.m. or so. Generally speaking, I will not respond on weekends and certainly not immediately.**

Please do not expect an instant answer if you send me an email or DM in Slack.

# Academic Honesty

 Please review [MSU's Code of Conduct, Policies, Regulations, & Reports](#). A couple of clarifications and additions:

- Although you may discuss and design with others, the work you hand in (e.g., code, write-ups) must be entirely your own. (Applies to individual assignments only.)
- Anything you submit that did not originate from you must be accompanied by attribution.
- Also, please do not share solutions or detailed information about solutions (e.g., specific code, non-trivial command line sequences) with others.