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

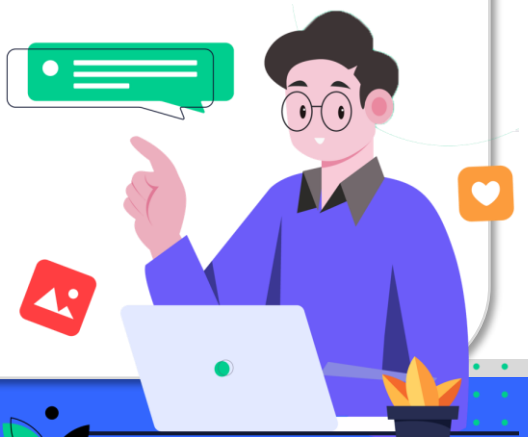
- Ph.D., George Washington University, 2021
- Postdoc., Pennsylvnia State University and University of Notre Dame

Research interests

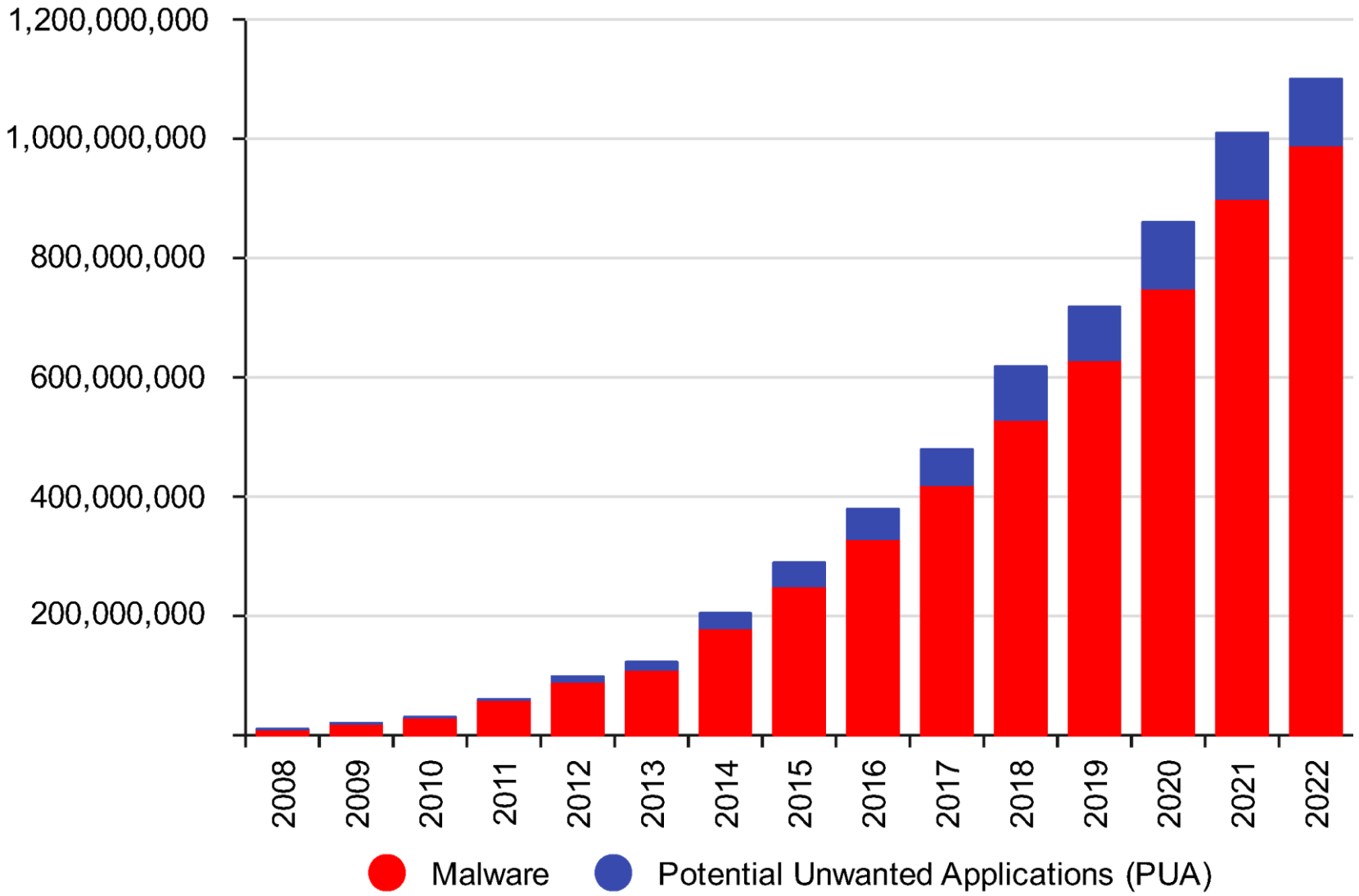
- Software security
- Program analysis
- Machine learning for cybersecurity

More

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



Necessity


1,200,000,000
1,000,000,000
800,000,000
600,000,000
400,000,000
200,000,000
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
Malware
Potential Unwanted Applications (PUA)

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: 13:00pm - 14:20pm and Thursdays 10:50am-12:10pm
- Office: Barnard Hall 356
- Email: 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

Late Penalties

- All 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 labs 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.

- Classwork cannot be submitted late.

Missed quiz policy

- Note that quizzes are taken in-class. Any conflicts with a quiz must be discussed with me prior to missing the quiz. I follow University policy on makeups, which allows that serious illness or a serious family emergency are valid reasons requiring an accommodation.

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 a quarter of a point. Only the first person to post about an error gets the points. You can earn a max of 1 total point toward your 100 for the course (for four errors).

Bonus

Course evaluation

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

Course Objectives

- Master assembly codes and analyze the changes in the stack by instruction execution.
- Classify malware files manually.
- Develop binary retrofitting techniques to modify malware binaries.
- 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 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.

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 lab/exam questions, and discuss any questions or concerns you may have about graded work.

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

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

Late Penalties

- All 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 labs 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.

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.