Course Title

Introduction to Program Analysis

Course Description

A course on program analysis topics, focusing on control flow and data flow analysis, program slicing, pointer analysis, intra-procedure and inter-procedure analysis, fuzzing, symbolic execution, and applications of program analysis for addressing software and security issues.

Prerequisites

CSC 373 or consent of the instructor

Instructor

Instructor: Dr. Zhen Huang
Office: Room 735, CDM Buildingg, 243 S. Wabash Avenue
Email: zhen.huang@depaul.edu
Phone: (312)362-8239
Homepage: `http://facsrv.cs.depaul.edu/~zhuang28/`

Office Hours

My office hours are held via zoom meetings in two sessions:
1:00 pm – 2:30 pm on Tuesdays
1:00 pm – 2:30 pm on Thursdays

Course Format

To provide optimal experience for students in both in-person and online sections, this course will be delivered as follows:

- **Course website:** The course website is on D2L. It hosts the lecture slides, the asynchronous lecture videos, the live lecture recordings, and the homework/project assignments. Please check the course web page and the discussion forum regularly.
- **Asynchronous lecture videos:** The asynchronous lecture videos are pre-recorded and posted on the course website. They are designed to provide the best experience for students in both sections.
- **In-person lectures:** The in-person lectures for students attending the in-person section are held in Lewis 1005 from 5:45 pm to 9:00 pm on Tuesdays.

- **Discussion forum:** A Discord server serves as the discussion forum for the class. Please use it to ask questions relevant to the class. I encourage you to answer the questions of other students. The Discord server invite is posted on D2L. I am also available for one-on-one meetings during my virtual office hours. If you need to contact me or soutside of office hours, feel free to email me directly.

Textbooks

Anders Møller and Michael I. Schwartzbach (2022). *Static Program Analysis*

Learning Outcomes

After finishing the course, students will be able to

- formulate a software development problem in a way so that it can be solved using program analysis
- implement and use program analysis techniques, such as control flow analysis and data flow analysis, to address software debugging and testing problems
- use state-of-art program analysis tools to solve software development problems

Weekly Schedule

Week 1	Introduction to program analysis; Fuzzing; Review of assembly language
Week 2	Control flow analysis; Dominators and post-dominators
Week 3	Control dependency analysis; Data flow analysis
Week 4	Reaching definiton analysis; Liveness analysis
Week 5	Available expression analysis; Symbolic execution
Week 6	Use-def chain; Static single assignment; Data flow framework
Week 7	Constraint-based analysis; Type systems
Week 8	Pointer analysis; Inter-procedural analysis
Week 9	Common software vulnerabilities; Vulnerability repair and mitigation
Week 10	Security Workaround for Rapid Response (SWRR); Code synthesizing
Week 11	Final project presentations; Final exam

Assessment

Course assessments consist of six homework assignments, a project, and a final take-home exam. The course grade will be computed as follows:

- Homework Assignments: 30%
- Final exam: 25%
- Project: 30%
- Final Presentations: 15%

Homework Assignments

You will learn to use the following program analysis tools for homework assignments.

- AFL – fuzzing tool
- Pin – binary instrumentation tool
- angr – binary analysis framework
- LLVM – compiler infrastructure
- KLEE – dynamic symbolic execution engine
- RVM – software vulnerability mitigation tool

Project

You need to finish a project using or extending program analysis tools. The project will span the duration of the course. Students will form teams of at most two and pick a topic in consultation with the instructor. Students will need to submit a project proposal. The project will consist of three milestones to report project progress and for the instructor to provide feedback. Students need to submit a milestone report for each milestone. The project concludes with an in-class final presentation. Below is the schedule of the project:

- Project proposal – Week 4
- Project milestone 1 – Week 6
- Project milestone 2 – Week 8
- Project milestone 3 – Week 10
- Final presentation – Week 11

Changes to Syllabus

This syllabus is subject to change as necessary during the quarter. If a change occurs, it will be thoroughly addressed during class, posted under Announcements in D2L and sent via email.

Online Course Evaluations

Evaluations are a way for students to provide valuable feedback regarding their instructor and the course. Detailed feedback will enable the instructor to continuously tailor teaching methods and course content to meet the learning goals of the course and the academic needs of the students. They are a requirement of the course and are key to continue to provide you with the highest quality of teaching. The evaluations are anonymous; the instructor and administration do not track who entered what responses. A program is used to check if the student completed the evaluations, but the evaluation is completely separate from the student's identity. Since 100our goal, students are sent periodic reminders over three weeks. Students do not receive reminders once they complete the evaluation. Students complete the evaluation online in Campus Connect: `http://campusconnect.depaul.edu/`

Academic Integrity and Plagiarism

This course will be subject to the university's academic integrity policy. More information can be found at `http://academicintegrity.depaul.edu/`.

Academic Policies

All students are required to manage their class schedules each term in accordance with the deadlines for enrolling and withdrawing as indicated in the University Academic Calendar. Information on enrollment, withdrawal, grading and incompletes can be found at: `http://cdm.depaul.edu/enrollment`.

Incomplete Grades

An incomplete grade is a special, temporary grade that may be assigned by an instructor when unforeseeable circumstances prevent a student from completing course requirements by the end of the term and when otherwise the student had a record of satisfactory progress in the course. All incomplete requests must be approved by the instructor of the course and a CDM Associate Dean. Only exceptions cases will receive such approval. Information about the Incomplete Grades policy can be found at `http://www.cdm.depaul.edu/Current%20Students/Pages/Grading-Policies.aspx`.

Students with Disabilities

Students who feel they may need an accommodation based on the impact of a disability should contact the instructor privately to discuss their specific needs. All discussions will remain confidential. To ensure that you receive the most appropriate accommodation based on your needs, contact the instructor as early as possible in the quarter (preferably within the first week of class), and make sure that you have contacted the Center for Students with Disabilities (CSD) at: csd@depaul.edu. Lewis Center 1420, 25 East Jackson Blvd. Phone number: (312)362-8002 Fax: (312)362-6544 TTY: (773)325.7296