Engineering Faculty Document No. 29-25
September 6, 2024
Page 1 of *1*

TO: The Faculty of the College of Engineering

FROM: Elmore Family School of Electrical and Computer Engineering

RE: New Graduate Course, ECE 60852 Holistic Software Security

The faculty of the School of Electrical and Computer Engineering has approved the following new course. This action is now submitted to the Engineering Faculty with a recommendation for approval.

ECE 60852 Holistic Software Security
Sem. 1, Lecture 3, Cr. 3.
Prerequisite: graduate student standing

Description:
The goal of the course is to bootstrap students into software security research. The course provides a complete overview of different aspects of software security and standard techniques used to solve various software security problems. We discuss generic techniques such as data flow analysis/type inference/dynamic analysis that are also needed to perform research in other areas such as software engineering and program analysis. The course is composed of four components: (i) Vulnerability Finding, (ii) Automated Patching, (iii) Patch Propagation, and (iv) Vulnerability Prevention. For every component, we will start with the basics and cover state-of-the-art techniques. We will also be reading research papers and try to analyze the pros and cons critically.

Reason:
This course provides the necessary background, i.e., theory, technique, and tools, to conduct research in various aspects of software security. This background is also useful for other streams of research in computer engineering, such as compilers, software engineering, and operating systems.

The course also helps in critical reasoning of program analysis techniques, such as proving soundness and verifying guarantees.

Course History: Fall 2021 – 8, Fall 2022 – 9, Fall 2023 – 7, Fall 2024 – 7

T.S. Mith

Mithuna Thottethodi,
Associate Head for Teaching and Learning
Elmore Family School of Electrical and Computer Engineering

PurS3

Purdue University

Holistic Software Security

Fall 2023

HOME SCHEDULE LECTURES ASSIGNMENTS PROJECT MATERIALS

Holistic Software Security / Fall 2023

Updates

- New Lecture is up: Introduction [slides]
- New Lecture is up: Vulnerability Detection - Static analysis [References]
- New Lecture is up: Vulnerability Detection - Fuzzing
- New Lecture is up: Vulnerability Detection - Sanitizers

Course Description

The goal of the course is to bootstrap you into software security research. The course provides a complete overview of different aspects of software security and standard techniques used to solve various software security problems. We discuss generic techniques such as Data flow analysis/ type inference/ dynamic analysis that are also needed to perform research in other areas such as Software engineering and program analysis. The course is composed of four components: (i) Vulnerability Finding, (ii) Automated Patching, (iii) Patch Propagation, and (iv) Vulnerability Prevention.

- Vulnerability Finding: We understand the basics of vulnerability finding techniques: Static analysis (Pattern-based/ Dataflow based/ Type-based/DSL based), Dynamic Analysis (Different Flavors of Fuzzing and dynamic symbolic execution), Machine Learning, and a combination of all the above.
- Automated Patching: Automated Program repair techniques: Pattern-based/ Dynamic analysis based/ Machine learning etc.

- Patch Propagation: Understanding the problem of propagating patches caused by software diversity and potential solutions.
- Vulnerability Prevention: Type-safe languages (Rust, Go, etc.), Retrofitting techniques (Sanitizers: ASAN, etc.), Type-safe dialects (Checked C/Cyclone/etc.).

For every component, we will start with basics and cover the state-of-the-art techniques. We will also be reading research papers and try to analyze the pros and cons critically.

Grading and Evaluation

We will use the following distribution for grading:

- Four assignments (10% each, Total: 40%).
- Midterm 1 (10%).
- Midterm 2 (10%).
- Paper presentation (10%).
- Course Project (30%).

This is a project-heavy course with one-third of the grade depends on the successful completion of the project.

Course Project

The goal of the course project is to enable students to experience various aspects of software security research. The result of the project will be a conference-style presentation. This is a semester-long project and is recommended to be done in groups of up to three students. Each project group is expected to decide milestones and will receive grades based on the satisfactory completion of these milestones and the presentation. Potential project ideas are here. Although, students can pick a project of their choice after discussing it with the professor.

Prerequisites and Expectations

This is a hands-on graduate-level course, with most of the assignments involves writing C/C++ code. I am expecting the students to have the following background:

- Should be very comfortable with writing C/C++ code: We will be working with clang/LLVM, which requires considerable experience with C/C++ codebases.

- Should be comfortable with operating system concepts, especially: Process Isolation, Memory Management (Virtual memory/Demand paging), Processor privilege levels (e.g., x86 Rings: 0-3).
- Knowledge about basic software security concepts such as buffer overflows, return-oriented programming, etc.

Learning Objectives

This course is aimed at introducing students to various aspects of software security research. After finishing the course, the students should:

- Have a good understanding of software security problems at various stages of software development and deployment.
- Have a good understanding of principles behind solving various software security problems.
- Have the ability to use state-of-the art tools to implement software security solutions.
- Have the ability to systematically solve system security problems.

Course Policies

This course will be run under the "reasonable adults" policy wherein it is assumed that all students are reasonable adults that want to benefit the most of the course by attending the course regularly, completing the homework assignments and projects on time, asking questions during the course and if they run into problems, and checking back with the instructor and the TA (if there exists one) regularly to ensure good progress.
A more verbose version of the policy is available on Spaf's page. This course follows the policies listed on that page. If you have any question about the course policy, don't hesitate to ask the instructor or the TA.
As a short summary: (i) you are expected to attend all classes (modulo good reasons), (ii) you are supposed to hand in all work before the deadlines (there's a 10% point reduction per day for late hand-ins), (iii) if you need special treatment or have special circumstances, talk to the instructor or TA (if there exists one). - Copied from Prof.Payers course.

Nondiscrimination Statement

Purdue University is committed to maintaining a community which recognizes and values the inherent worth and dignity of every person; fosters tolerance, sensitivity, understanding, and mutual respect among its members; and encourages each individual to strive to reach his or her own potential. In pursuit of its goal of academic excellence, the University seeks to develop and nurture diversity. The University believes that diversity among its many members strengthens the institution, stimulates creativity, promotes the exchange of ideas, and enriches campus life. Link to Purdue’s nondiscrimination policy statement.

Students with Disabilities

Purdue University strives to make learning experiences as accessible as possible. If you anticipate or experience physical or academic barriers based on disability, you are welcome to let me know so that we can discuss options. You are also encouraged to contact the Disability Resource Center at: drc@purdue.edu or by phone: 765-494-1247

Emergency Preparation

In the event of a major campus emergency, course requirements, deadlines and grading percentages are subject to changes that may be necessitated by a revised semester calendar or other circumstances beyond the instructor’s control. Relevant changes to this course will be posted onto the course website or can be obtained by contacting the instructors or TAs via email or phone. You are expected to read your @purdue.edu email on a frequent basis.

Mental Health Statement

It is important to make sure that you maintain your mental health.

- If you find yourself beginning to feel some stress, anxiety and/or feeling slightly overwhelmed, try WellTrack. Sign in and find information and tools at your fingertips, available to you at any time.
- If you need support and information about options and resources, please see the Office of the Dean of Students for drop-in hours (M-F, 8 am- 5 pm).
- If you’re struggling and need mental health services: Purdue University is committed to advancing the mental health and well-being of its students. If you or someone you know is feeling overwhelmed, depressed, and/or in need of mental health support, services are available. For help, such individuals should contact Counseling and Psychological Services (CAPS) at 765-494-6995 during and after hours, on weekends and holidays, or by going to the CAPS office of the second floor of the Purdue University Student Health Center (PUSH) during business hours.
- TaskHuman offers private, real-time, on-demand, 1-on-1 video calls with wellness coaches covering over 800+ topics such as anxiety, mindfulness, reducing stress, clean eating, time management, in-home workouts, relationship tensions, financial issues, spiritual guidance and many more. You can access these wellness coaches from around the world 24/7. The College of Engineering has an exclusive agreement with TaskHuman which gives you FREE and UNLIMITED access to these resources. Over 3,200 calls have been made by College of Engineering students, staff, and faculty so far with an average satisfaction rating of 4.89/5. Learn more here: https://engineering.purdue.edu/ECE/TaskHuman.

Logistics

When: MWF 11:30 am - 12:20 pm, **Where:** Physics Building 201

Instructor Office Hours: Tuesday 2:00 pm - 4:30 pm @ EE 333

Join our Slack Channel for course related collaborations!

Instructors

Aravind
Machiry

Elmore Family School of Electrical and Computer Engineering
Purdue University
West Lafayette, IN, USA

machiry_msidc
engineering.purdue.edu/ECE