Using Formal Methods for Security

Bulletin Description

This is a senior level undergraduate and graduate course covering advanced topics in using formal methods for security. We will learn about and evaluate the use of formal verification methods applied to computer security problems. The course will be discussion based, with classes organized around reading and discussing papers. In addition, students will work in small groups on a semester-long research project of their choosing.

General Course Information

Term: Spring 2023  
Department: COMP  
Course Number: 590/790  
Section Number: 132  
Time: Mondays 11:00 – 12:15  
Location: FB 009  
Website: [https://cs.unc.edu/~csturton/courses/verifiedsec/790-132-sp23.html](https://cs.unc.edu/~csturton/courses/verifiedsec/790-132-sp23.html)

Instructor Information

Name: Cynthia Sturton  
Office: FB354  
Email: csturton@cs.unc.edu  
Website: [http://www.cs.unc.edu/~csturton](http://www.cs.unc.edu/~csturton)  
Office Hours: TBD

Textbook and Resources

There are no required textbooks. Required readings will be posted online in the course schedule.

Course Description

It is a well known adage in computer security that while the defender has to shore up every possible vulnerability in the system, the attacker only needs to find one to exploit. The attacker has the advantage.

In this class we will discuss one powerful tool for strengthening the defense: proving security properties of systems using formal verification methods. We will study the application of symbolic execution, model checking, language-based proof systems, and proof checkers to a
wide range of security-critical systems, such as operating systems, cryptographic protocols, and hardware designs. We will discuss the benefits and challenges of using formal methods for security in various settings.

Target Audience

The class is designed for students who are interested in aspects of formal verification methods and computer security. The course will be research focused: classes will be centered around discussion of published research in the formal verification and security communities, students will work on an original research project, and students will write a workshop-style paper describing their work.

Prerequisites

The 790 course is open to all CS graduate students. Graduate students outside the CS department who wish to take the class should attend the first week of class and speak to the instructor at the end of class. The 590 course is open to CS undergraduate students who have completed (with a grade of C or higher) COMP 283, 210, 211, 301, 455. A course in security (COMP 435, 535) or cryptography is recommended as a pre- or corequisite.

Course Requirements

Students will read 1–2 papers per class. Classes will be organized around a combination of lecture and paper discussions; reading the paper is necessary in order to contribute to the discussion. For each paper, students will write a short synopsis and review. Students will be responsible for presenting some yet-to-be-determined number of papers during the semester (two is the current plan). Students will work in groups of 2 or 3 on an original research project. At the end of the semester, each group will submit a workshop-style paper and give a 10–15 min presentation in class describing their work.

Key Dates

Project Groups: 1/18/23
Project Proposals: 2/08/23
Progress Report: 3/06/23
Final Paper: 4/24/23
Code Artifact: 4/26/23
Presentations: TBA (scheduled final exam time)

Grading Criteria
Group project: 50%
Leading paper discussion: 30%
Paper reviews & discussion: 20%

Course Policies

Classes are centered around discussions of papers; attendance is necessary in order to participate in the discussion.

Honor Code

Any outside source used as part of a paper review (other papers, textbooks, websites) must be properly cited. The final project must be original research. Students will work in groups of 2 or 3 for the final project, and submit one written report per group.

In the course of this class we may discuss known vulnerabilities and attacks on computer systems. This is not an invitation to exploit these vulnerabilities in real systems. You may not attempt to break into any system that is not your own; you may not attempt to thwart or circumvent the security of any system that is not your own. Doing so is, at a minimum, a violation of the honor code, and possibly a violation of the law.

Course Schedule
The course schedule will be posted on the course website.

Disclaimer

The professor reserves the right to make changes to the syllabus, including project due dates. These changes will be announced as early as possible.