Formal Methods for Systems Security

Bulletin Description

Formal methods provide a rigorous, mathematically grounded analysis of a system. Used as part of a security analysis, formal methods can provide verification that a system meets its security requirements. In this course students will learn about and gain experience using a variety of techniques, including symbolic execution, model checking, and proofs of equivalence and refinement. Students will develop an understanding of different specification logics and what can and cannot be expressed in each. Topics include assertion-based verification, simulation relations, linear temporal logic, information flow analysis, and hyperproperties.

General Course Information

Term:	Spring 2025
Department:	COMP
Course Number:	590/790
Section Number:	132
Time:	Mondays/Wednesdays 11:15 – 12:30
Location:	FB 007
Website:	COMP 590/790-132: Formal Methods for Systems Security
Schedule:	Spring 2025 Course Schedule

Instructor Information

Name:	Cynthia Sturton
Office:	FB354
Email:	csturton@cs.unc.edu
Website:	http://www.cs.unc.edu/~csturton
Office Hours:	Calendar

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, and proof checkers to a range of security-critical systems, including operating systems, firmware, 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, 311, and 455.

Course Requirements

Students will read 1 paper 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. There will be bi- or tri-weekly in-class quizzes. 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 minute presentation in class describing their work.

Key Dates

Project Groups:	1/26/25
Project Proposals:	2/23/25
Progress Report:	3/23/25
Final Paper:	4/22/25
Code Artifact:	4/27/25
Presentations:	4/30/25 4-7 PM (scheduled final exam time)

Grading Criteria

Project:	40%
In-class quizzes:	40%
Paper reviews + discussion:	19%
First OH visit:	1%

The two lowest in-class quiz grades and two lowest paper review grades will be dropped from the final calculation.

Grades will be assigned according to the following scale.
A >= 95
A- >= 90
B+ >= 86 ⅔
B >= 83 ⅓
B- >= 80
C+ >= 76 ⅔
C >= 73 ⅓
C- >= 70
D+ >= 65
D >= 60
F < 60

Course Policies

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

Paper reviews are due 11:59 pm the night before the class discussion. Paper reviews submitted anytime after that and before the start of class will incur a 10% late penalty. Paper reviews will not be accepted after the start of class in which the paper is discussed. Exceptions will be made

only for students with a letter from the University Approved Absence Office. In those cases, I will work with the student to find a suitable alternative, either in the form of a make-up assignment or by dropping the review from the final, calculated grade.

AI Usage General Guidance

Carolina students are expected to follow these AI guidelines:

1. AI should help you think, not think for you. You may be able to use these tools to brainstorm ideas, research topics, and analyze problems, but you must decide what's appropriate and accurate.
2. Engage responsibly with AI. You must evaluate AI-generated outputs for potential biases, limitations, inaccuracies, false output, and ethical implications. Do not put personal or confidential data into these tools.
3. The use of AI must be open and documented. You should declare, explain, and cite any use of AI in the creation of your work using applicable standards (e.g., APA, MLA, course guidelines). Understand that you are ultimately 100% responsible for your final product.
4. Follow specific AI guidelines in this syllabus. If you are unsure, check with me. Guidance offered in this syllabus would be referenced should an issue be referred to Student Conduct for alleged academic misconduct.

AI Usage for Course Assignments

Assignments in this course will allow for one of three levels of AI use:

- **No AI Use:**
  AI tools are not permitted; all work must be completed independently by the student. For example, a student writes a paper or solves a math problem entirely on their own without any AI assistance. Should students have questions, they should seek clarification from the instructor.
- **Assistive AI Use Only:**
  AI tools can be used for non-content-generating tasks, such as grammar checking, formatting, or organizing ideas, but it cannot create new intellectual content. For example, a student might use AI to help them understand a paper they are reading or to check spelling and grammar for the project proposal, progress report, and final report, but not to write the paper reviews or project milestone submissions. All such uses of AI must be disclosed.
- **Partial Generative AI Use (Idea Generation and Research Exploration):**
  AI tools can assist with generating content for specific parts of the final presentation, but the student must refine and modify the AI-generated content and use proper citations. For example, AI might draft an outline of the presentation, draft text for some slides, or create figures for a slide that the student then edits and improves. All such uses of AI must be fully cited.

Assignment	Description	Learning Goals	AI Use Allowed
Paper readings	Read the research papers posted to the schedule before the class meeting time	● Learn the seminal and cutting edge research in the use of formal methods for systems security ● Develop skills in reading and understanding published research	Assistive AI Use Only
Paper reviews	Submit a short review of the paper we will be discussing in class the day before class	● Develop skills analyzing published research ● Understand the big picture and important technical details of a paper	No AI Use
Final project code artifact	Use a formal methodology to prove a security policy of a codebase, algorithm, data structure, or protocol of the students choosing	● Apply knowledge in formal methods and security learned during the semester ● Create new proofs of security for computer systems ● Gain experience using formal methods	No AI Use
Final project written deliverables	Submit a project proposal, progress report, and final paper	● Evaluate one's own research through the process of recognizing, organizing, and explaining the most important aspects of a research project in written form ● Develop skills teaching content in formal methods and computer security in written form	Assistive AI Use Only
Final presentation	Give a presentation to the class describing your research project	● Evaluate one's own research through the process of recognizing, organizing, and explaining the most important aspects of a research project in oral form ● Develop skills teaching content in formal methods and computer security in oral form	Partial Generative AI Use (Idea Generation and Research Exploration)

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 is available online.

Attendance Policy

University Policy: As stated in the University's Class Attendance Policy, no right or privilege exists that permits a student to be absent from any class meetings, except for these University Approved Absences:

1. Authorized University activities
2. Disability/religious observance/pregnancy, as required by law and approved by Accessibility Resources and Service and/or the Equal Opportunity and Compliance Office (EOC)
3. Significant health condition and/or personal/family emergency as approved by the Office of the Dean of Students, Gender Violence Service Coordinators, and/or the Equal Opportunity and Compliance Office (EOC).

University Approved Absence Office (UAAO): The UAAO website provides information and FAQs for students and faculty related to University Approved Absences.

Note: Instructors have the authority to make academic adjustments without official notice from the UAAO. In other words, it is not required for instructors to receive a University Approved Absence notification in order to work with a student. In fact, instructors are encouraged to work directly with students when possible.

Optional Mask Use Statement

UNC-Chapel Hill is committed to the well-being of our community – not just physically, but emotionally. The indoor mask requirement was lifted for most of campus on March 7, 2022. If you feel more comfortable wearing a mask, you are free to do so. There are many reasons why a person may decide to continue to wear a mask, and we respect that choice.

Disclaimer

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

Acceptable Use Policy

By attending the University of North Carolina at Chapel Hill, you agree to abide by the University of North Carolina at Chapel Hill policies related to the acceptable use of IT systems and services. The Acceptable Use Policy (AUP) sets the expectation that you will use the University's technology resources responsibly, consistent with the University's mission. In the context of a class, it's quite likely you will participate in online activities that could include personal information about you or your peers, and the AUP addresses your obligations to protect the privacy of class participants. In addition, the AUP addresses matters of others' intellectual property, including copyright. These are only a couple of typical examples, so you should consult the full Information Technology Acceptable Use Policy, which covers topics related to using digital resources, such as privacy, confidentiality, and intellectual property.

Additionally, consult the University website "Safe Computing at UNC" for information about the data security policies, updates, and tips on keeping your identity, information, and devices safe.

Accessibility Resources and Service

The University of North Carolina at Chapel Hill facilitates the implementation of reasonable accommodations, including resources and services, for students with disabilities, including mental health disorders, chronic medical conditions, a temporary disability or pregnancy complications resulting in barriers to fully accessing University courses, programs and activities.

Accommodations are determined through the Office of Accessibility Resources and Service (ARS) for individuals with documented qualifying disabilities in accordance with applicable state and federal laws. See the ARS Website for contact information: https://ars.unc.edu or email ars@unc.edu.

Counseling and Psychological Services

UNC-Chapel Hill is strongly committed to addressing the mental health needs of a diverse student body. The Heels Care Network website is a place to access the many mental resources at Carolina. CAPS is the primary mental health provider for students, offering timely access to consultation and connection to clinically appropriate services. Go to their website https://caps.unc.edu/ or visit their facilities on the third floor of the Campus Health building for an initial evaluation to learn more. Students can also call CAPS 24/7 at 919-966-3658 for immediate assistance.

Title IX Resources

Any student who is impacted by discrimination, harassment, interpersonal (relationship) violence, sexual violence, sexual exploitation, or stalking is encouraged to seek resources on campus or in the community. Reports can be made online to the EOC at https://eoc.unc.edu/report-an-incident/. Please contact the University's Title IX Coordinator (Elizabeth Hall, titleixcoordinator@unc.edu), Report and Response Coordinators in the Equal Opportunity and Compliance Office (reportandresponse@unc.edu), Counseling and Psychological Services (confidential), or the Gender Violence Services Coordinators (gvsc@unc.edu; confidential) to discuss your specific needs. Additional resources are available at safe.unc.edu.

Policy on Non-Discrimination

The University is committed to providing an inclusive and welcoming environment for all members of our community and to ensuring that educational and employment decisions are based on individuals' abilities and qualifications. Consistent with this principle and applicable laws, the University's Policy Statement on Non-Discrimination offers access to its educational programs and activities as well as employment terms and conditions without respect to race, color, gender, national origin, age, religion, genetic information, disability, veteran's status, sexual orientation, gender identity or gender expression. Such a policy ensures that only relevant factors are considered and that equitable and consistent standards of conduct and performance are applied.

If you are experiencing harassment or discrimination, you can seek assistance and file a report through the Report and Response Coordinators (see contact info at safe.unc.edu) or the Equal Opportunity and Compliance Office, or online to the EOC at https://eoc.unc.edu/report-an-incident/.

Diversity Statement

I value the perspectives of individuals from all backgrounds reflecting the diversity of our students. I broadly define diversity to include race, gender identity, national origin, ethnicity, religion, social class, age, sexual orientation, political background, and physical and learning ability. I strive to make this classroom an inclusive space for all students. Please let me know if there is anything I can do to improve. I appreciate suggestions.

Undergraduate Testing Center

The College of Arts and Sciences provides a secure, proctored environment in which exams can be taken. The center works with instructors to proctor exams for their undergraduate students who are not registered with ARS and who do not need testing accommodations as provided by ARS. In other words, the Center provides a proctored testing environment for students who are unable to take an exam at the normally scheduled time (with pre-arrangement by your instructor). For more information, visit http://testingcenter.web.unc.edu/.

Learning Center

Want to get the most out of this course or others this semester? Visit UNC's Learning Center at http://learningcenter.unc.edu to make an appointment or register for an event. Their free, popular programs will help you optimize your academic performance. Try academic coaching, peer tutoring, STEM support, ADHD/LD services, workshops and study camps, or review tips and tools available on the website.

Writing Center

For free feedback on any course writing projects, check out UNC's Writing Center. Writing Center coaches can assist with any writing project, including multimedia projects and application essays, at any stage of the writing process. You don't even need a draft to come visit. To schedule a 45-minute appointment, review quick tips, or request written feedback online, visit http://writingcenter.unc.edu.

Grade Appeal Process

If you feel you have been awarded an incorrect grade, please discuss with me. If we cannot resolve the issue, you may talk to our departmental director of undergraduate studies or appeal the grade through a formal university process based on arithmetic/clerical error, arbitrariness, discrimination, harassment, or personal malice. To learn more, go to the Academic Advising Program 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.