Verified Security

Bulletin Description

This is a graduate seminar in computer security. We will learn about and evaluate the use of formal verification methods applied to computer security problems. Classes will be organized around paper reading and a final project.

General Course Info

Term:	Fall 2013
Department:	COMP
Course Number:	790
Section Number:	132
Time:	MW, 2:00 – 3:15
Location:	FB 331
Website:	http://cs.unc.edu/~csturton/courses/790-132-fa13.html

Instructor Info

Name:	Cynthia Sturton
Office:	FB 354
Email:	csturton@cs.unc.edu
Phone:	919-590-6020
Web:	http://www.cs.unc.edu/~csturton
Office Hours:	TTh, 10:00 – 11:00

Textbooks 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 model checking and theorem proving for a wide range of security-critical systems. A few examples include voting machines, operating systems, and cryptographic protocols. We will discuss the benefits and challenges of using formal methods for security in various settings.

Target Audience

The class is meant for students who are interested in software and systems security, as well as students interested in the application of formal methods. The class will be research focused: classes will be centered around discussion of published research in the security community, and students will work on an original research project and write a workshop-quality paper describing their work.

Prerequisites

There are no prerequisites. This class is open to all CS graduate students. Graduate students outside the CS department who wish to take this class should contact the instructor.

Goals and Key Learning Objectives

- Learn how formal verification techniques are useful as a tool for computer security, and become familiar with examples from the literature demonstrating ways in which formal methods have been applied to answer security questions.
- Understand the basics of how various formal verification techniques work.
- Understand the benefits and limitations of various formal verification techniques, and know when it makes sense to apply a particular technique, and when it does not.
- Produce original research that applies formal methods to address an open problem in computer security.

Course Requirements

Students will read 1 to 2 papers per class. Classes will be organized around 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. In addition, students will choose 2 papers for which they will write a full length review.

Students will work in groups of 2 on an original research project. At the end of the semester, each group will submit a workshop-quality paper and give a short (~10 min) presentation in class describing their work.

Key Dates

Project proposals due:	9/23/13
Final in-class presentations:	12/2/13, 12/4/13
Final project report due:	12/4/13

Grading Criteria

Final project: 50%
Paper reviews: 20%
Class discussion & short reviews: 30%

Course Policies

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

Honor Code

Discussion of the assigned papers outside of the classroom is encouraged; however, collaboration on the written paper reviews (short or full length) is not permitted.

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.

Course Schedule

The course schedule will be posted on the course website.

Disclaimer

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