

Principled 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: Spring 2017
Department: COMP
Course Number: 790
Section Number: 132

Time: TTh 2:00-3:15
Location: FB 009
Website: <http://cs.unc.edu/~csturton/courses/verifiedsec/790-132-sp17.html>

Instructor Info

Name: Cynthia Sturton
Office: FB354
Email: csturton@cs.unc.edu
Phone: 919-590-6020
Website: <http://www.cs.unc.edu/~csturton>
Office Hours: By appointment

Textbook and Resources

Required readings will be posted on the course schedule. There are no required textbooks, however the following books may be useful as a reference.

“The Calculus of Computation; Decision Procedures with Applications to Verification,” A.R. Bradley and Z. Manna, Springer 2010.

“Logic in Computer Science; Modelling and Reasoning about Systems, 2nd ed.” M. Huth and M. Ryan, Cambridge University Press 2004.

“Model Checking,” E.M. Clarke, O. Grumberg, and D.A. Peled, MIT Press 1999.

Course Description

In this class we will discuss the use of formal verification methods for proving security properties of computer systems. We will study the application of model checking and theorem proving to 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

There are no prerequisites for this class. The class is meant for students who are interested in software, hardware, 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 the 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

Classes will be organized around paper discussions: we will read and discuss one paper per class; reading the paper is necessary in order to contribute to the discussion. For each paper, students will write a short synopsis and review. The discussion will be student-led; each student will be responsible for leading 2–3 paper discussions in the course of the semester.

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 (15 min) presentation in class describing their work.

Key Dates

Project proposals due: 2/23/2017
Final in-class presentations: 4/25/2017
Final project report due: 4/28/2017

Grading Criteria

Final project: 50%
Paper reviews and discussion: 20%
Paper presentations: 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 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 the right to make changes to the syllabus, including project due dates. These changes will be announced as early as possible.