CSCI 699: Quantitative Information Flow and Side Channels

Units: 4

Fall 2021—Wednesday—Time: 3:00pm – 6:20pm

Location: SOS B41

Instructor: Chao Wang

Office: SAL 334 and Zoom (https://usc.zoom.us/my/wang626)

Office Hours: Wednesday 10:00am – 12:00pm

Contact Info:

Email: wang626@usc.edu
Website: https://sites.usc.edu/chaowang/

Course Description

This course provides an introduction to techniques for analyzing and mitigating an important class of cyber security risks called "side-channel" attacks, where sensitive information may be leaked by nonfunctional properties of a software program such as the execution time, memory usage, or power consumption. While information leakage has always been a significant security concern in software systems, prior work focuses primarily on the "main channel"; recent attacks such as Meltdown/Spectre demonstrated its importance and impact in the context of side-channel attacks.

In this course, we will discuss foundational techniques in quantitative information flow analysis, which can be used to analyze and mitigate side-channel vulnerabilities. These are program analysis techniques aimed to quantify the amount of information leakage by using information-theoretic concepts such as entropy and conditional entropy. We will also discuss tradeoffs in designing such an analysis tool, e.g., to accurately detect security vulnerabilities due to harmful leaks while minimizing the number of false alarms due to benign leaks.

Learning Objectives and Outcomes

Students will gain an understanding of the foundational techniques in quantitative information flow analysis, as well as state-of-the-art research on analyzing and mitigating side-channel leaks.

Topics include:

- Basic static and dynamic program analysis techniques
- Advanced program analysis techniques such as probabilistic symbolic execution, abstract interpretation, type inference, constraint solving, and model counting
- State-of-the—art research results in side-channel analysis and mitigation

Prerequisite(s):

1. General proficiency in computer science (e.g., discrete mathematics)
2. Good programing skills (e.g., C++ or Java)

Course Notes

To accommodate the possibility of hybrid attendance (in-person and remote), this course will be taught on campus in a classroom that also supports synchronous online attendance. Copies of the lecture slides and other class information will be posted on a course website on Blackboard.

Students will be graded on paper reading, class presentation, class discussion, as well as a final project.

Required Readings and Supplementary Materials

There are no textbooks. Students are expected to read and present recent research papers.

Description and Assessment of Assignments

Grades will be based on reading research papers and writing paper summaries (20%), class presentation (30%), class discussion (10%), and a final project (40%).

The course will be discussion-based. At the start of each lecture, the instructor will give an introduction of the related technical background, followed by student-led discussions of 2-3 research papers.

Each paper is assigned to a student, who is responsible for giving a presentation and leading the discussion. All students are required to read all the assigned papers, and write a (1-page) summary for each paper.

The final project will be an open-ended research project. Students are expected to select a topic with the help of the instructor, and work on the project throughout the semester, and submit a (5-page) report at the end of the semester.

Paper summaries
Students are expected to read and understand the research papers. In addition, they are expected to write and submit a (1-page) summary for each paper.

Class presentation
Students are expected to present a subset of the research papers in class and lead the follow-up discussion. The goal is to inform others about the topic, so in the end everyone can have a better understanding of the recent developments in the field.

To get a good grade in paper presentation, you need to excel in the following aspects:

- Clarity in presentation (how well you understand the paper and handle questions, etc.)
- Quality of the slides (must to be informative and thorough, with technical depths, figures, etc.)

Class discussion
Students are expected to participate in the class discussion, e.g., listening to the paper presentation and then asking good questions.

Final project
The open-ended project could be developing new side-channel analysis techniques, enhancing existing techniques, identifying innovative uses of these techniques, or conducting a survey of the research field.

At the end of the project, each student must submit a project report. Your grade on the final project depends on the following aspects:

- Novelty of the project design,
- Thoroughness in the execution, and
- Clarity in the project report.

Grading Breakdown

Assignment	**% of Grade**
Paper summaries	20%
Class presentation	30%
Class discussion	10%
Final project	40%
TOTAL	**100%**

Additional Policies
Students are expected to submit their paper summaries and final project report in time. Late submissions will be accepted up to 24 hours after the announced deadline, with a penalty of 20%. Submissions received more than 24 hours late will receive a grade of 0.

If you feel that an error has been made in grading, please notify the instructor within one week after the material is graded. For the final project, please present a short written appeal to the instructor.

Course Schedule: A Weekly Breakdown

	Topics	Readings
Week 1	Introduction	
Week 2	Quantifying Information Leakage	*Geoffrey Smith. On the Foundations of Quantitative Information Flow. FOSSACS 2009* *Geoffrey Smith. Quantifying Information Flow Using Min-Entropy. QEST 2011*
Week 3	Modeling Adaptive Attacks	*Boris Köpf, David Basin. An information-theoretic model for adaptive side-channel attacks. CCS 2007* *Boris Köpf, David Basin. Automatically deriving information-theoretic bounds for adaptive side-channel attacks. JCS 2011*
Week 4	Analysis Technique -- Symbolic Execution	*Edward Schwatz, Thanassi Avgerinos, and David Brumley, All you Ever Wanted to Know about Dynamic Taint Analysis and Forward Symbolic Execution (but Might Have Been Afraid to Ask), S&P 2010.* *"Z3: An Efficient SMT Solver," Leonardo Mendonça de Moura, Nikolaj Bjørner. TACAS 2008*
Week 5	Analysis Technique -- Probabilistic Symbolic Execution	*Jaco Geldenhuys, Matthew B. Dwyer, Willem Visser. Probabilistic symbolic execution. ISSTA 2012* *Mateus Borges, Antonio Filieri, Marcelo d'Amorim, Corina S. Pasareanu, Willem Visser. Compositional solution space quantification for probabilistic software analysis. PLDI 2014*
Week 6	Model Counting for Boolean Constraints	*Elazar Birnbaum, Eliezer L. Lozinskii. The good old Davis-Putnam procedure helps counting models.* *Supratik Chakraborty, Kuldeep Meel, Moshe Vardi. A Scalable Approximate Model Counter. CP 2013.*
Week 7	Boolean Combinations of Constraints	*Antonio Filieri, Corina S. Pasareanu, Willem Visser. Reliability analysis in symbolic pathfinder. ICSE 2013* *Feifei Ma, Sheng Liu, Jian Zhang. Volume Computation for Boolean Combination of Linear Arithmetic Constraints. CADE 2009*
Week 8	Model Counting using BDDs and Automata	*Randal E. Bryant Binary Decision Diagrams. Handbook of Model Checking 2018* *Abdulbaki Aydin, Lucas Bang, Tevfik Bultan. Automata-Based Model Counting for String Constraints. CAV 2015*
Week 9	Quantitative Information Flow using Symbolic Execution and Model Counting	*Michael Backes, Boris Köpf, Andrey Rybalchenko. Automatic Discovery and Quantification of Information Leaks. IEEE Symposium on Security and Privacy 2009* *Lucas Bang, Abdulbaki Aydin, Quoc-Sang Phan, Corina S. Pasareanu, Tevfik Bultan. String analysis for side channels with segmented oracles. SIGSOFT FSE 2016*
Week 10	Abstract Interpretation and Type Inference	*Meng Wu and Chao Wang. Abstract interpretation under speculative execution, PLDI 2019* *Jun Zhang, Pengfei Gao, Fu Song, and Chao Wang. SCInfer: Refinement-based verification of software countermeasures against side-channel attacks, CAV 2018*
Week 11	Hyper properties, HyperLTL	*Michael R. Clarkson, Fred B. Schneider: Hyperproperties. CSF 2008* *Michael R. Clarkson, Bernd Finkbeiner, Masoud Koleini, Kristopher K. Micinski, Markus N. Rabe, César Sánchez: Temporal Logics for Hyperproperties. POST 2014*

Week 12	k-Safety and Self-Composition	*Tachio Terauchi, Alexander Aiken: Secure Information Flow as a Safety Problem. SAS 2005* *Marcelo Sousa, Isil Dillig: Cartesian hoare logic for verifying k-safety properties. PLDI 2016*
Week 13	Quantifying Information Leaks using Bounded Model Checking	*Jonathan Heusser, Pasquale Malacaria. Quantifying information leaks in software. ACSAC 2010*
Week 14	Hardware and Software Side-Channels	*Shengjian Guo, Meng Wang, and Chao Wang. Adversarial symbolic execution for detecting concurrency-related cache timing leaks, ESEC/FSE 2018* *Tegan Brennan, Nicolás Rosner, and Tevfik Bultan. JIT Leaks: Inducing Timing Side Channels through Just-In-Time Compilation, SP 2020*
Week 15	Wrap-up	
FINAL	(Project report due) no exam	

Statement on Academic Conduct and Support Systems

Academic Conduct:

Plagiarism – presenting someone else's ideas as your own, either verbatim or recast in your own words – is a serious academic offense with serious consequences. Please familiarize yourself with the discussion of plagiarism in SCampus in Part B, Section 11, "Behavior Violating University Standards" policy.usc.edu/scampus-part-b. Other forms of academic dishonesty are equally unacceptable. See additional information in SCampus and university policies on scientific misconduct, policy.usc.edu/scientific-misconduct.

Support Systems:

Student Health Counseling Services - (213) 740-7711 – 24/7 on call
engemannshc.usc.edu/counseling
Free and confidential mental health treatment for students, including short-term psychotherapy, group counseling, stress fitness workshops, and crisis intervention.

National Suicide Prevention Lifeline - 1 (800) 273-8255 – 24/7 on call
suicidepreventionlifeline.org
Free and confidential emotional support to people in suicidal crisis or emotional distress 24 hours a day, 7 days a week.

Relationship and Sexual Violence Prevention Services (RSVP) - (213) 740-4900 – 24/7 on call
engemannshc.usc.edu/rsvp
Free and confidential therapy services, workshops, and training for situations related to gender-based harm.

Office of Equity and Diversity (OED) | Title IX - (213) 740-5086
equity.usc.edu, titleix.usc.edu
Information about how to get help or help a survivor of harassment or discrimination, rights of protected classes, reporting options, and additional resources for students, faculty, staff, visitors, and applicants. The university prohibits discrimination or harassment based on the following protected characteristics: race, color, national origin, ancestry, religion, sex, gender, gender identity, gender expression, sexual orientation, age, physical disability, medical condition, mental disability, marital status, pregnancy, veteran status, genetic information, and any other characteristic which may be specified in applicable laws and governmental regulations.

Bias Assessment Response and Support - (213) 740-2421
studentaffairs.usc.edu/bias-assessment-response-support
Avenue to report incidents of bias, hate crimes, and microaggressions for appropriate investigation and response.

The Office of Disability Services and Programs - (213) 740-0776
dsp.usc.edu
Support and accommodations for students with disabilities. Services include assistance in providing readers/notetakers/interpreters, special accommodations for test taking needs, assistance with architectural barriers, assistive technology, and support for individual needs.

USC Support and Advocacy - (213) 821-4710
studentaffairs.usc.edu/ssa
Assists students and families in resolving complex personal, financial, and academic issues adversely affecting their success as a student.

Diversity at USC - (213) 740-2101
diversity.usc.edu
Information on events, programs and training, the Provost's Diversity and Inclusion Council, Diversity Liaisons for each academic school, chronology, participation, and various resources for students.

USC Emergency - UPC: (213) 740-4321, HSC: (323) 442-1000 – 24/7 on call
dps.usc.edu, emergency.usc.edu
Emergency assistance and avenue to report a crime. Latest updates regarding safety, including ways in which instruction will be continued if an officially declared emergency makes travel to campus infeasible.

USC Department of Public Safety - UPC: (213) 740-6000, HSC: (323) 442-120 – 24/7 on call
dps.usc.edu
Non-emergency assistance or information.