CSCI 699: Quantitative Information Flow and Side Channels
Units: 4
Fall 2020—Wednesday—Time: 2:00pm – 5:20pm

Location: Online`

Instructor: Chao Wang

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

Office Hours: Wednesday 1:00pm – 2:00pm

Contact Info:
Email: wang626@usc.edu
Website: https://sites.usc.edu/chaowang/
Course Description
This course provides an introduction to program analysis and verification techniques for detecting and mitigating side-channel information leakage in computer systems. Information leakage has always been a significant security concern in computer systems, and recently, side-channel attacks such as Meltdown and Spectre further demonstrated their importance and impact. Instead of exploiting the main communication channel, side-channel attacks gain sensitive information by observing nonfunctional properties of a computer system, such as the execution time and the memory usage.

In this course, we discuss the recent developments in detecting and mitigating side-channel leaks based on quantitative information flow analysis. Quantitative information flow analysis is a technique aimed to quantify the amount of information leaked using information-theoretic concepts such as entropy and conditional entropy. We will discuss tradeoffs in designing such an analysis to enable the detection of vulnerabilities due to harmful leaks while minimizing false alarms due to benign leaks.

Learning Objectives and Outcomes
Students will gain a deep understanding of the foundational techniques in quantitative information flow analysis and recent developments on detecting and mitigating side-channel leaks. The topics include:

- Static and dynamic program analysis techniques for side-channel detection,
- Probabilistic symbolic execution, abstract interpretation, type inference,
- Model counting constraint solving, and
- Hyperproperties in temporal logics.

Prerequisite(s):
1. General proficiency in discrete mathematics, static and dynamic program analysis
2. Good programming skills

Course Notes
This is an online course. Lectures will be delivered using Zoom. Copies of the lecture slides and other class information will be posted on Blackboard.

The course will be graded on the basis of paper reading, class presentation, class discussion, as well as a semester-long project.

Required Readings and Supplementary Materials
There are no textbooks. Students are expected to read and present the most recent research papers.

Description and Assessment of Assignments
The grades will be based on reading research papers and writing paper summaries (20%), class presentation (30%), class discussion (10%), and a research project (40%).

The course will be discussion-based. At the start of each lecture, the instructor will give an introduction of the technical background, followed by student-led discussion of 1-3 research papers. Each paper is assigned to a student, who is responsible for giving a presentation and then leading the discussion. All students are required to read the assigned papers and submit a short (1-page) summary. Students will also work on an open-ended research project throughout the semester and submit a final 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 the detailed summaries.

Class presentation
Students are expected to present a subset of the research papers in class and lead the 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 presentation and asking good questions.

**Final project**
Final project is an open-ended research project that asks students to develop some new analysis techniques or identify some innovative uses of existing techniques. 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**

<table>
<thead>
<tr>
<th>Assignment</th>
<th>% of Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper summaries</td>
<td>20%</td>
</tr>
<tr>
<td>Class presentation</td>
<td>30%</td>
</tr>
<tr>
<td>Class discussion</td>
<td>10%</td>
</tr>
<tr>
<td>Final project</td>
<td>40%</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

**Additional Policies**
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 returned. For final projects, please present a short written appeal to the instructor.
## Course Schedule: A Weekly Breakdown

<table>
<thead>
<tr>
<th>Week</th>
<th>Topics</th>
<th>Readings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Topics</strong></td>
<td></td>
</tr>
<tr>
<td>Week 1</td>
<td>Introduction</td>
<td></td>
</tr>
<tr>
<td>Week 10</td>
<td>Abstract Interpretation and Type Inference</td>
<td>Meng Wu and Chao Wang. <em>Abstract interpretation under speculative execution</em>, PLDI 2019 &lt;br&gt;Jun Zhang, Pengfei Gao, Fu Song, and Chao Wang. <em>SCInfer: Refinement-based verification of software countermeasures against side-channel attacks</em>. CAV 2018</td>
</tr>
<tr>
<td>Week</td>
<td>Topic</td>
<td>References</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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       | Tegan Brennan, Nicolás Rosner, and Tevfik Bultan. JITLeaks: Inducing Timing Side Channels through Just-In-Time Compilation, SP 2020  
Shengjian Guo, Meng Wang, and Chao Wang. Adversarial symbolic execution for detecting concurrency-related cache timing leaks, ESEC/FSE 2018 |
| 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.