COM S 641 (2014 Fall) Assignments

Wei Le

2014.9
Reading - Week 1

- Reading 1: A Survey of Automated Techniques for Formal Software Verification: Sections 1, 2 and 5
- Reading 2: New results on the computability and complexity of points-to analysis

Reading notes (within a page) due Fri 2:15pm: a list of 1) questions and 2) insights and ideas
Reading - Week 2

- Reading 1: The Concept of Dynamic Analysis
- Reading 2: The Heartbleed bug
  (http://www.pl-enthusiast.net/2014/07/01/how-did-heartbleed-remain-undiscovered-and-what-should-we-do-about-it/)
Assignment - Bug Analysis: Week 3

Select one of the important, well-known, interesting or yourself-discovered bugs in an open source program, and write an report on:

- meta information of the bug: when it is discovered, how it is found, what is the consequence of the bug, where is the bug report (if applied)
- analysis of the bug: what is the source code that contains the bug, what are the tests (if any) that can trigger the bug
Assignments

Assignment - Finding and Constructing a Benchmark Suite: Weeks 4-5 (Due Sept 26)

**Deliverables**

- A set of programs: code, makefile, bugs (if relevant to the benchmark) ($\geq 5$ programs)
- A readme file: how to use the benchmarks
- An analysis report (2 pages) about the benchmarks (answering the above following questions)
  - What is a criterion? What to evaluate? (e.g., bugs, versions, software productline, numerical computation, event-driven systems)
  - Static profile: Size (LOC), the number of program constructs (statements, loops, methods). Please take a look at: http://programanalysisandtesting.org/2013/04/05/software-release-static-code-profiler/
  - How the benchmark satisfies the criterion
Assignment - SOOT and LLVM Exercise: Weeks 6-7 (Due Oct 10)

Steps
- Install SOOT and LLVM
- Walk through examples, tutorials and documentation
- Generate Callgraphs, CFGs, and Dependence Graphs for 2 programs of Java and 2 programs of C/C++

Deliverables
- Soot and LLVM code
- A report (2 page) on:
  - Your experience with SOOT and LLVM, what you like, what you don’t like, how long it takes you to learn, what is the most challenges
  - Data collected from the graph:
  - Examples: part of the graph

<table>
<thead>
<tr>
<th>benchmark</th>
<th>size (LOC)</th>
<th>node</th>
<th>edge</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Reading Assignment: Dataflow and Abstract Interpretation

- Precise Interprocedural Dataflow Analysis via Graph Reachability: POPL1995 (reference: Program Analysis via Graph Reachability - article 1997)
- Precise Interprocedural Chopping: FSE1995