Oracle Labs, Australia: Research Assistant Position

Automatically Improving Security-Specific Test Coverage

Position: 6-month, full-time tenable during June 2018 to May 2019 with the Program Analysis group.

Project Details: Security testing is a challenging activity as

- it is not possible to test all behaviours and
- the attacker only needs to find one flaw to exploit the system.

The testing process is made more challenging as almost all real programs do not have an explicit security model and the desired security properties are not specified. We have developed a technique, derived from mutation testing, that can identify potential weaknesses in the test suite. Given a system under test and security-sensitive mutation operators, we identify behaviours that are not covered by the tests. These behaviours represent potential security issues that are untested.

The aim of the project is to develop new techniques that will generate tests to improve the security coverage of existing test suites. The focus of the generated tests will be to exercise behaviour that is not covered by any of the existing tests. The test generation process can adapt our work on security-related mutation testing to identify relevant security-sensitive behaviour. The techniques developed will also need to be scalable, i.e., work on systems that have millions of lines of code and thousands of tests. This research will be conducted in the context of large JEE applications.

Supervisor: Paddy Krishnan

Paddy Krishnan is a senior researcher at Oracle Labs in Brisbane, Australia. His current research interests are in the areas of program analysis, software security and automatic test generation. His work at Oracle has focused on finding vulnerabilities in the JDK and Java web applications.

Oracle Labs, the research arm for Oracle, focuses on applied research that produces new technologies of interest to the company. Oracle Labs Australia, based in Brisbane, focuses on Program Analysis as it applies to a variety of domains, including bug-checking, security analysis, productivity tools, testing, and more. The group is best known for its research on static code analysis that led to scalable and precise bug-checking algorithms embedded in the Oracle Parfait tool. For more information, visit `http://labs.oracle.com/locations/australia` Oracle internships give students valuable industry experience and the chance to work on cutting-edge research projects with real-world applications.

About this position:

Duties You will:

- work independently to research or develop a state-of-the-art test generation solution for security issues,
- meet with your supervisor daily for guidance and to discuss ways to solve the problem,
- attend team meetings and give updates on your work, and
- present your findings and outcomes to the group.

Prerequisites:

- Students must be currently enrolled in a PhD or research-based Masters degree in Computer Science or Software Engineering.
- Demonstrated expertise in the area of testing. Knowledge of mutation testing for Java and/or security analysis will be advantageous.
- Demonstrated ability to work independently and collaboratively.

Benefits:

- These positions are paid at current industry rates.
- Travel & visa costs associated with overseas applicants will be reimbursed.
- Ongoing learning is incorporated into our every week to keep us at the cutting edge.
- Building your research network as international speakers frequently present their research to us.

Contact Paddy Krishnan paddy.krishnan@oracle.com for more details. The position will commence interviewing immediately and remain open until filled.