Race Vulnerability Study and Hybrid Race Detection (CMU/University of Nebraska, Lincoln Collaborative Proposal) - July 2017

Submitted by Jamie Presken on Mon, 06/12/2017 - 9:13am

Yu, Tingting, Witty Srisa-an, and Gregg RothermelPublic Audience
Purpose: To highlight progress. Information is generally at a higher level which is accessible to the interested public.

PI(s): Jonathan Aldrich (CMU), Witawas Srisa-an (University of Nebraska, Lincoln)
Researchers: Joshua Sunshine (CMU)

1) HARD PROBLEM(S) ADDRESSED (with short descriptions)
This refers to Hard Problems, released November 2012.

a. Scalability: Improve the tradeoff between scalability and precision in race detectors. Existing race detectors suffer from either many false positives or unacceptably high overhead, which impedes their use in real world systems. Our hybrid race detection technique aims to be efficient and precise enough for practical large-scale applications.

b. Predictive Security Metrics: The empirical study of race vulnerabilities introduced by humans explores a rarely studied topic. If the study uncovers interesting relationships between races and security attacks, it can further contribute to security metrics research by providing another dimension of security assessment criteria. Of course, this study will open up opportunities to mitigate race-related vulnerabilities.

2) PUBLICATIONS - for current quarter

Tingting Yu, Witty Srisa-an, and Gregg Rothermel. SimExplorer: An Automated Framework to Support Testing for System-Level Race Conditions. *Software Testing, Verification and Reliability*.

Junjie Qian, Hong Jiang, Witawas Srisa-an, Sharad Seth, Stan Skelton, and Joseph Moore. Energy-efficient I/O Thread Schedulers for NVMe SSDs on NUMA. In *Proc. International Symposium on Cluster, Cloud and Grid Computing (CCGrid)*. Madrid, Spain. May, 2017

Yutaka Tsutano, Shakthi Bachala, Witawas Srisa-an, Gregg Rothermel, Jackson Dinh. An Efficient, Robust, and Scalable Approach for Analyzing Interacting

Android Apps. In *Proc. International Conference on Software Engineering (ICSE)*, Buenos Aires, Argentina, May, 2017.

Michael Coblenz, Whitney Nelsony, Jonathan Aldrich, Brad Myers, Joshua Sunshine. Glacier: Transitive Class Immutability for Java. In *Proc. International Conference on Software Engineering (ICSE)*, Buenos Aires, Argentina, May, 2017.

3) KEY HIGHLIGHTS

We developed a methodology to support cost-effective testing for data races. Concurrent programs are prone to various classes of difficult-to-detect faults, of which data races are particularly prevalent. Prior work has attempted to increase the cost-effectiveness of approaches for testing for data races by employing race detection techniques, but to date, no work has considered cost-effective approaches for re-testing for races as programs evolve. To address this need, we introduce SIMRT, an automated regression testing framework, for use in detecting races introduced by code modifications. SIMRT employs a regression test selection technique, focused on sets of program elements related to race detection, to reduce the number of test cases that must be run on a changed program to detect races that occur due to code modifications, and it employs a test case prioritization technique to improve the rate at which such races are detected. Our empirical study of SIMRT reveals that it is more efficient and effective for revealing races than other approaches, and that its constituent test selection and prioritization components each contribute to its performance. A paper based on this work appeared at the 2014 edition of the International Conference on Software Engineering.

Tingting Yu, A PhD student partially supported by this grant, graduated in August and is now an Assistant Professor at University of Kentucky-Lexington.

Approved by NSA Scalability and Composability Metrics CMU Race Vulnerability Study and Hybrid Race Detection FY14-18