

2018 Research Interest/Project Ideas

Byoungyoung Lee (byoungyoung@purdue.edu)

<https://lifeasageek.github.io/>

MEDS: Fast/Better Memory Error Detection System

MEDS is a practical memory error detector. MEDS significantly enhances its detection capability by approximating two ideal properties, called an infinite gap and an infinite heap. The approximated infinite gap of MEDS setups large inaccessible memory region between objects, and the approximated infinite heap allows MEDS to fully utilize virtual address space. The key idea of MEDS in achieving these properties is a novel user-space memory allocation mechanism using page-aliasing. This allows MEDS to maximize the virtual memory space utilization but minimize the physical memory uses. To highlight the detection capability and practical impacts of MEDS, we evaluated and then compared to Google's state-of-the-art detection tool, AddressSanitizer. When used for a fuzz testing, MEDS was able to identify 68.3% more memory errors than AddressSanitizer for the same amount of a testing time, highlighting its practical aspects in the software testing area.