Critique on
Hao Sun, Xiangyu Zhang, Yunhui Zheng and Qingkai Zeng (2016), "IntEQ: Recognizing Benign Integer Overflows via Equivalence Checking Across Multiple Precisions."

Astha Sharma
asharma6@uno.edu

Summary:
The author of this paper talks about the integer overflow (IO) vulnerability and measures associated with identifying its benign or malign nature. IO can sometimes be used by programmers to generate random numbers, hashing, coding and decoding, which determines its benign use. Therefore, there was initially a problem in determining the crucial fixes which were not just the false alarms. The authors came with a solution to recognize benign IOs via equivalence checking across multiple precisions. They named the tool 'IntEQ'. The tool was used to determine if an IO is benign or not by simply comparing the effects of the overflowed data and their corresponding data in the ideal world at the sink.

STRENGTHS:

1. It addresses a challenging issue of IO vulnerability (that basically includes more benign errors), to highlight critical bugs requiring immediate attention.
2. With IntEQ there are reduced number of false positives to help developers focus on fixing critical IOs and avoiding false alarms.
3. More accurate - gave 355 benign results out of 444 test case; whereas another similar study showed only 19 benigns.
4. Good for small projects.

WEAKNESSES:

1. The performance of the tool would affect its usability, which is not desirable.
2. Not suitable for big scale testing.
3. Its soundness depends on the group unrolling.
4. Providing equivalence for subpaths that ends at pointer dereference may lead to missing IOs.
5. There are manual evaluations in classifying errors in IntEQ that are subjected to human errors.