Nicholas Garrett
garrnic3@isu.edu
Professor Zibran
CS 4416
10/17/2021

Reading/Critique: IntEQ

Paper:

IntEQ: Recognizing Benign Integer Overflows via Equivalence Checking Across Multiple Precisions
Authors: Hao Sun, Xiangyu Zhang, Yunhui Zheng, and Qingkai Zeng

Summary:

Integer overflow vulnerabilities represent one of the largest vulnerability types. In the IntEQ paper, a system to analyze code to identify Integer Overflows is described, which finds differences between the original code and an edited version of the code that uses precise variable sizes.

Strengths:

1. This paper made sure to give information about the background of its topic before throwing information at the reader.

2 The paper works to explain what weaknesses of it already exist, and tells what these weaknesses mean, making it easier to read for someone not thoroughly knowledgeable on the topic.

3 The paper provides examples of what it is trying to convey, which help with giving another way of thinking about the principle.

Weaknesses:

1. The paper is long and takes time to get to the point. Perhaps explaining principles more concisely would help to cut down on unnecessary "fluff".

2. As someone not thoroughly familiar with the programming language they use as example, it is difficult to know what exactly the authors are trying to explain. Instead of simply referring to the code, if they had explained what principle it follows, the explanations would be a bit easier to follow.

3. The evaluations for the IntEQ performance were run on an Intel Dual Core 2.4 GHz with 4GB of memory on Linux-3.5.0. This could lead to system-specific results which may differ across processors, operating systems, and RAM levels. Having either run tests on multiple systems or re-evaluating tests using more modern machines could improve the accuracy of the performance tests.