Nicholas Garrett
garrnic3@isu.edu
Professor Zibran
CS 4416
11/67/2021

Reading/Critique: Testing Static Analysis Tools using Exploitable Buffer Overflows from Open Source Code

Paper:

Testing Static Analysis Tools using Exploitable Buffer Overflows from Open Source Code
Authors: Misha Zitser, Richard Lippmann, and Tim Leek

Summary:

Software analysis tools have inconsistent returns on the accuracy of buffer overflow exploit scans. As a rseult, this paper attempts to analyze several detection programs and tests their accuracy in identifying bad lines of code.

Strengths:

1. The paper explained (generally) how the various analysis tools operate, so an understanding of the analysis for each can be better understood.

2 The vulnerable code used to test each of the tools was open-source, so it is unlikely data would be program-dependent.

3 The accuracy of error detection was described using simple equations, which are easier to understand for those with a mathematics background.

Weaknesses:

1. The results of this paper do not seem to be of very much value out side of understanding what weaknesses exist in software analysis tools. Perhaps if the authors had made a recommendation based on their results, the findings would be more useful..

2. The analyzed analysis tools were stated to be very different and had different methods of scanning for vulnerabilities. For this paper to be more useful in determining effective scanning systems, running the tests for more tools with similar scanning systems would improve the effectiveness of this paper.

3. There is no mention of repetitions in experimentation being made, so errors in initial data collection are not smoothed. A way to solve this problem would have been to test each of the programs several times.