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

Reading/Critique: Finding Security Vulnerabilities in Java Applications with Static Analysis

Paper:
Finding Security Vulnerabilities in Java Applications with Static Analysis
Authors: V. Benjamin Livshits and Monica S. Lam

Summary:
This paper proposes a system for finding vulnerabilities of a certain type in code by statically scnning thhe code.

Strengths:
1. Explanations of injection and attacks were given in the paper, which helped to explain what they did and helped me to understand how the program proposed to detect these vulnerabilities.

2 The program was written to analyze Java code. I liked this choice as Java is a popular programming language with a similar base as many other languages.

3 I think that it is imreseive the range of vulnerabilities the system is capable of finding or analyzing.

Weaknesses:
1. The paper explained attacks and vulnerabilities beyond what seemed strictly necessary. It seems like the explanation of vulnerabilities composes more of the paper than how the proposed system intended to detect them. I would recommend putting more emphasis in detection methods, or less emphasis in explanations.

2. The program runs in the Java programming language. As a result, open options for other languages are closed by default. If the writers had instead chosen to include some implementations in their system for other languages, it would have allowed for better expandability and ability to conform to other situations than just Java.

3. The system proposed uses a user-kprovided specification system for analyzing code and finding errors. The paper itself mentions that erros may be missed if the specifications provided by the user are incomplete, though it does nothing to try and implement some fix to it. If the system were to have some sort of remotely-updated specifications list (which the user could customize), this problem could be possibly fixed–or at lease minimized.