A Preliminary Taxonomy of Techniques Used in Software Fuzzing

Poster Presentation
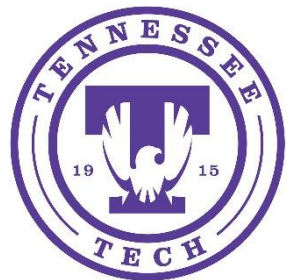

Raunak Shakya and Dr. Akond Rahman

Tennessee Technological University

September 22, 2020

FUZZING

Software Testing Technique

Goal of the paper

Help researchers in performing software fuzzing by categorizing different techniques used in *software fuzzing literature*

Research Questions

- RQ1: **What techniques** are used to perform software fuzzing?

- RQ2: **How frequently** do the identified software fuzzing techniques appear in software fuzzing literature?
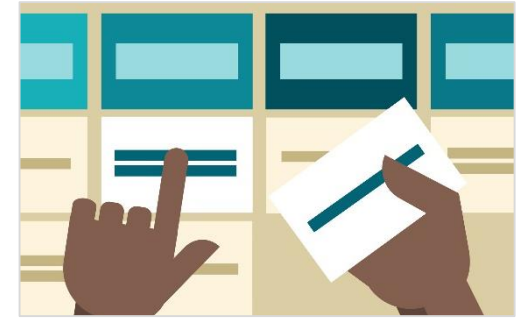
Methodology

Papers from major
conferences:
*ICSE, FSE, CCS, USENIX
(2009 – 2019)*
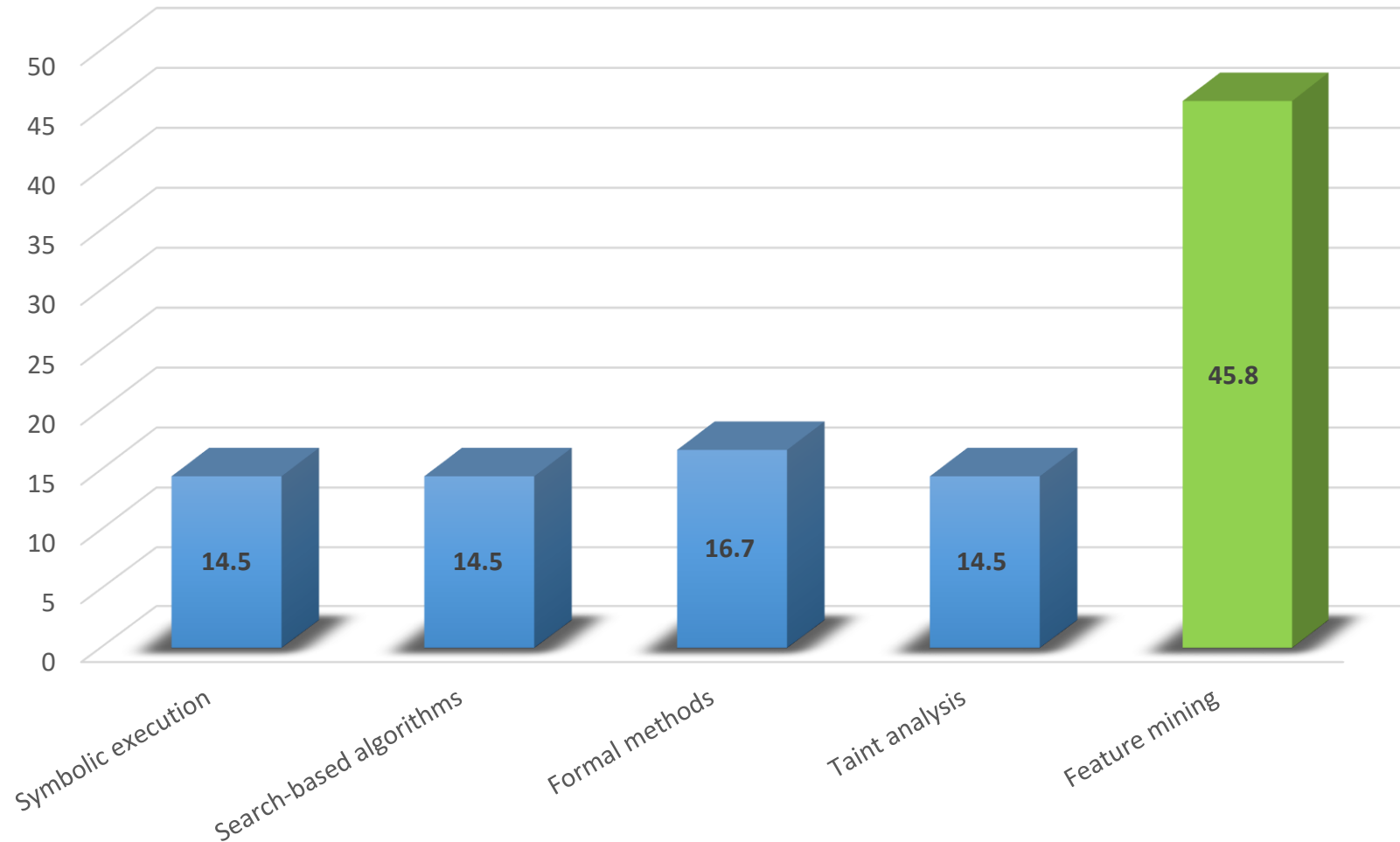
Determine if a paper
relates to fuzzing

Identifies topics using
Qualitative Analysis:
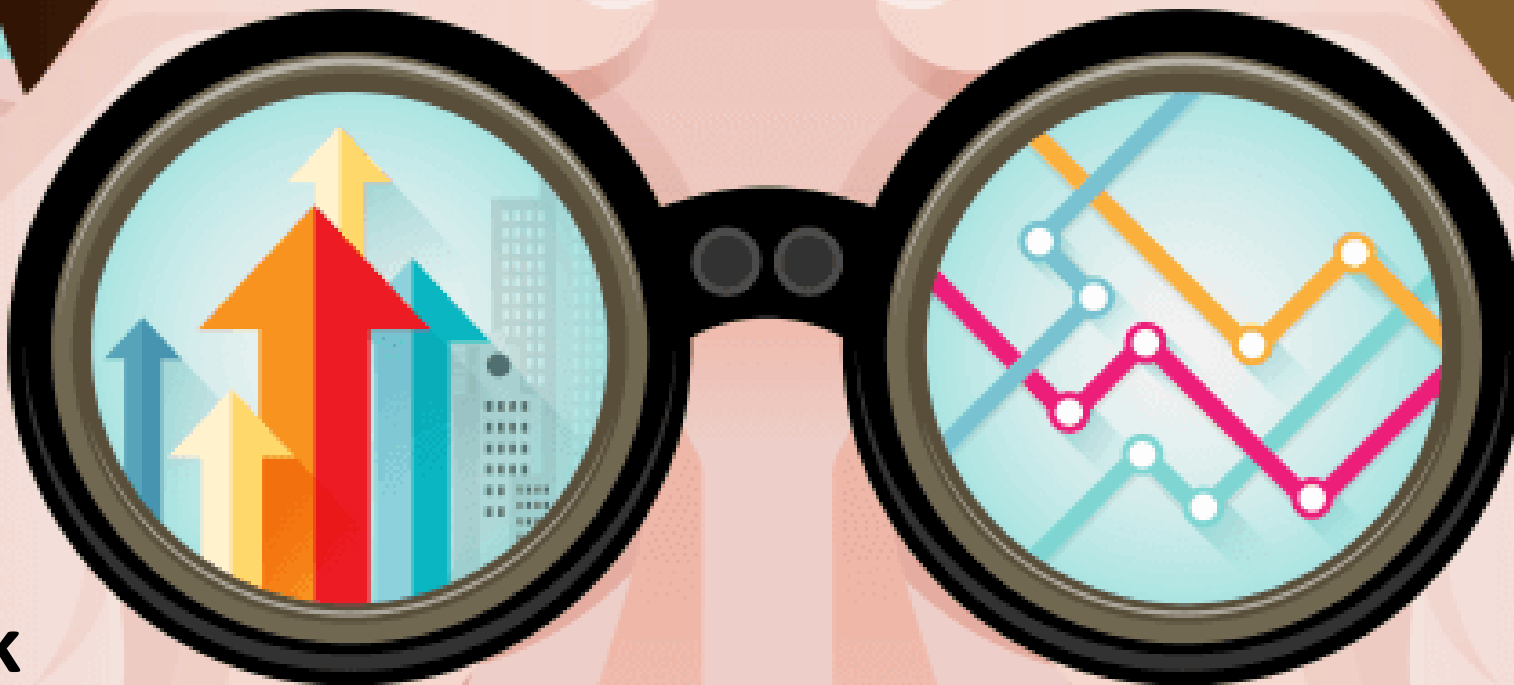(What fuzzing technique is
used by the authors?)

Card Sorting technique:
Identify high-level categories
from the identified topics

Results

Frequency of Identified Topics

Future Work

- Implement fuzzing for scientific softwares
- Derive a more comprehensive taxonomy

Thank you

Raunak Shakya
rshakya@tntech.edu

Dr. Akond Rahman
arahman@tntech.edu