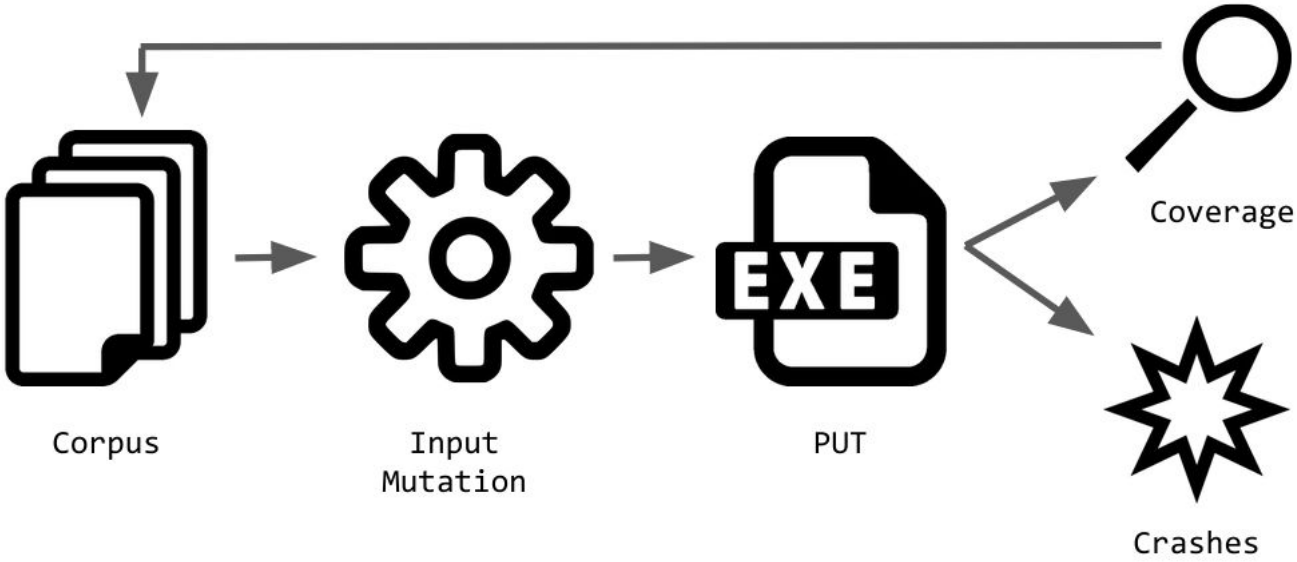
FuzzSplore: Visualizing Feedback-Driven Fuzzing Techniques

Andrea Fioraldi and Luigi Paolo Pileggi

Feedback-driven Fuzz Testing



A Fuzzing campaign

1. Start as soon as possible to fuzz
2. When there is a plateau we investigate in order to:
    a. Tune the selection of techniques during the fuzzing campaign
    b. Tune the parameters of single fuzzers
3. Restart the campaign
4. Go to 2 again if needed

A Fuzzing campaign

1. Start as soon as possible to fuzz
2. When there is a plateau we investigate **using a visualization** in order to:
    a. Tune the selection of techniques during the fuzzing campaign
    b. Tune the parameters of single fuzzers
3. Restart the campaign
4. Go to 2 again if needed

The AFL++ fuzzing framework

- New (2019) state-of-the art fuzzer, son of American Fuzzy Lop, implements multiple successful researches
- Used in industry (Google OSS-Fuzz, GitHub Security Lab, ...)
- Presented at USENIX Security Woot ‘20 [1]

[1] https://www.usenix.org/conference/woot20/presentation/fioraldi

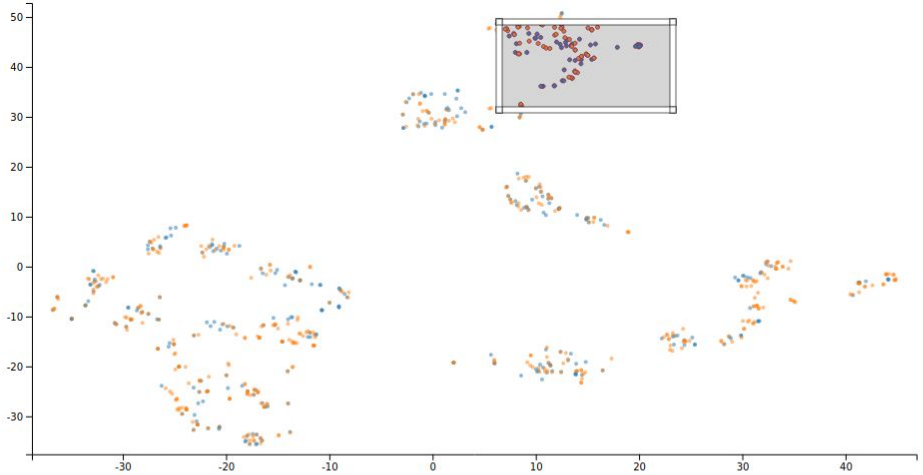
Extracted data

- The coverage of each testcase is described by a 65536 entries vector
- Each testcase has parents that generated it by mutation
- The growth in terms of coverage over time
- The number of new inputs for each second

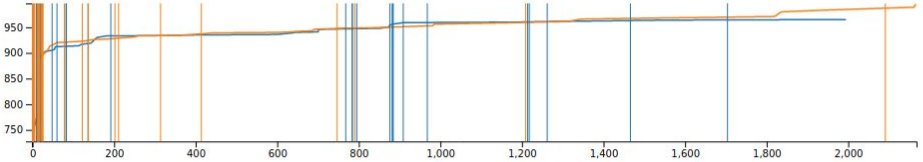
Extracted data

- The coverage of each testcase is described by a 65536 entries vector
    - Reduced to 2 coordinates with t-SNE
- Each testcase has a parent that generated it by mutation
- The growth in terms of coverage over time
- The number of new inputs for each second

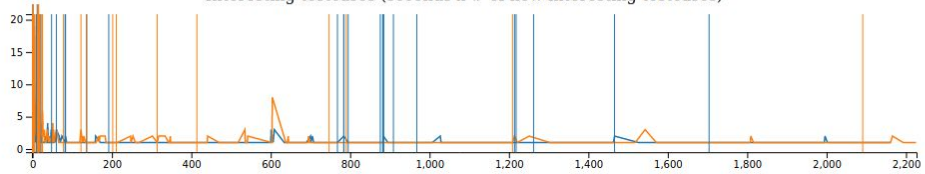
Testcases localities (hitcounts TSNE)



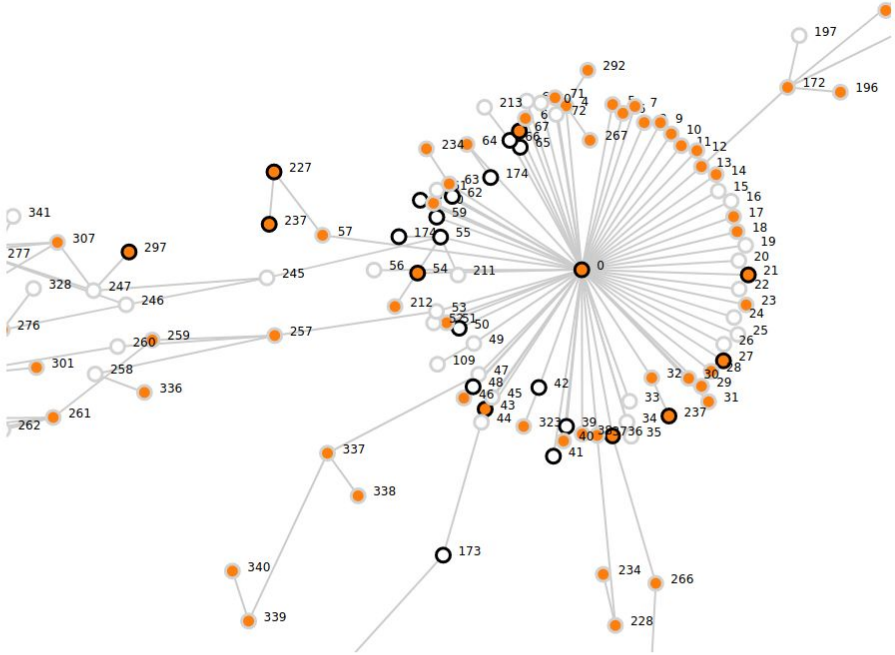
Coverage growth (seconds x # of edges)



Interesting testcases (seconds x # of new interesting testcases)



Generations Graph



User interactions

- Brush and zoom the scatterplot
- Zoom the Y axis of the plots
- Reduce the time window using the slider
- Select nodes in the graph
- Show the graph for a fuzzer using the current graph buttons
- Highlight nodes using the cross compare button
- Zoom the generations graph

Coordinated interactions

- Scatterplot brushing highlights points, selects nodes in the generations graph and inserts lines in the plots
- Selecting nodes in the generation graphs change the border color to black, highlights points in the scatterplot and insert lines in the plots
- The time slider updates all the views (the graph is not redrawn)
- Filter out fuzzers from scatterplot and plots using the buttons
- In the graph lowlight other nodes and edges when mouseover a node

Thank you

- FuzzSplore is OSS, available at https://github.com/andreafioraldi/FuzzSplore
- Technical report at https://github.com/andreafioraldi/FuzzSplore/report.pdf
- AFL++ is available at https://github.com/AFLplusplus