Review “Driller”

Name: Wenhui Zhang

Paper Name：

Stephens, N., Grosen, J., Salls, C., Dutcher, A., Wang, R., Corbetta, J., ... & Vigna, G. (2016, February). Driller: Augmenting Fuzzing Through Selective Symbolic Execution. In *NDSS* (Vol. 16, pp. 1-16).

Contribution:

This paper proposes a new technique for fuzzing which combines symbolic execution with fuzzing. AFL fuzzer with symbolic execution of angr (a reverse engineering tool with symbolic execution). It puts these two in a loop for input generation for the new fuzzer. In Driller, performance of path selection of the AFL fuzzer is enhanced with angr’s symbolic execution algorithms.

Motivation:

Lots of memory corruption bugs exists. However there are problems with test-case generation techniques for fuzzing.

Related works:

Symbolic Execution is good at finding solutions for specific conditions, however it spends too much time iterating over general conditions.
Fuzzing is good at finding solutions for general conditions, however it is bad at finding solutions for specific conditions.

Methodology:

Symbolic Execution is good at find solutions for specific input. Fuzzing is good at finding solutions for general input. This paper generated a feedback loop for these two methods.
Symbolic Execution checks each state for safety violations. It holds a symbolic program counter, and writes/reads from symbolic address.

Results:

71 / 128 binaries crashes for the old solution: (1) Symbolic Execution (angr) catches 16 in total; (2) Fuzzing (AFL) catches 68 in total; (3) these two methods shared of 13 in total.
77 / 128 binaries crashes for the new solution. Driller catches 77 crashes in total.
Driller is greater than the sum of its parts:

1. It offers a >10% increase in crashes over pure AFL
2. Driller curbs path explosion

Take away:

Fuzzing beyond the hash is still a problematic.
Why not generate the constraints for a smallest set possible, while still make the constraints legal (works for all conditions), and solve the problem once for all, instead of using a feedback system with a loop.