Fizzer

New Gray-Box Fuzzer

Martin Jonáš, Jan Strejček, Marek Trtík, Lukáš Urban

Masaryk University

April 11, 2024

```c
void main() {
    int x = nondet_int();
    if (x < 42) {
      // branch 1
    } else {
      // branch 2
    }
}
```

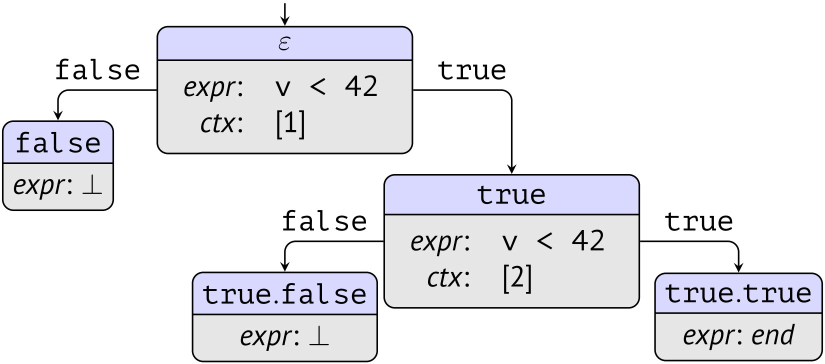
```c
void main() {
    int x = nondet_int();
    if (x < 42) {
      // branch 1
    } else {
      // branch 2
    }
}
```

distance: x - 42

```c
bool compare(int v) {
    return v < 42;
}

void main() {
    int x = nondet_int();
    bool res1 = compare(x);
    x++;
    bool res2 = compare(x);
    if (res1 || res2) {
      // branch 1
    } else {
      // branch 2
    }
}
```

```
bool compare(int v) {
    __instr_abe(1, v < 42, v - 42);
    return v < 42;
}

void main() {
    int x = nondet_int();
    __instr_call(1);
    bool res1 = compare(x);
    __instr_return();
    x++;
    __instr_call(2);
    bool res2 = compare(x);
    __instr_return();
    if (res1 || res2) {
      // branch 1
    } else {
      // branch 2
    }
}
```

```
bool compare(int v) {
    __instr_abe(1, v < 42, v - 42);
    return v < 42;
}

void main() {
    int x = nondet_int();
    __instr_call(1);
    bool res1 = compare(x);
    __instr_return();
    x++;
    __instr_call(2);
    bool res2 = compare(x);
    __instr_return();
    if (res1 || res2) {
      // branch 1
    } else {
      // branch 2
    }
}
```



ε
expr: v < 42
ctx: [1]
false
true
false
expr: ⊥
true
expr: v < 42
ctx: [2]
false
true
true.false
expr: ⊥
true.true
expr: end

1. Sensitivity analysis
    - Determine which bytes influence the distance value

1. Sensitivity analysis
   - Determine which bytes influence the distance value
2. Byteshare analysis
   - Use the input from a different calling context

1. Sensitivity analysis
   - Determine which bytes influence the distance value
2. Byteshare analysis
   - Use the input from a different calling context
3. Gradient descent
   - Minimize the absolute value of the distance

- Bronze medal in *Cover-Branches*

- Bronze medal in *Cover-Branches*
- Highest score in 3 sub-categories
  - *ReachSafety-Floats*
  - *SoftwareSystems-AWS-C-Common-ReachSafety*
  - *SoftwareSystems-BusyBox- MemSafety*