Bug Finding in Pointer Analysis

Theodoros, Sandeep

9th August 2015

Outline

Symbolic Execution

- Symbolic execution using klee
- Migration from Klee to Zesti (a variant of klee)

Checker Logic

- Instrumenting the code to add checks.
- Incorporating the checker logic in zesti.

Implicit klee_assumes

Which variable to make symbolic

Making Input variable symbolic

```
int main() {
  int x=1 , y=2;
  int*  p = (int *)malloc(sizeof(int));

  klee_make_symbolic(&x, sizeof(x), "x");
  //klee_make_symbolic(&y, sizeof(y), "y");

  if(0 != x*y) {
    p = (int *)malloc(4);
  } else {
    if(y == 0) {
      p = (int *)malloc(4);
    }
  }
  return *p;
}
```

Testing

Outline