Witch 3

Validation of Violation Witnesses in the Witness Format 2.0

Paulína Ayaziová, Jan Strejček

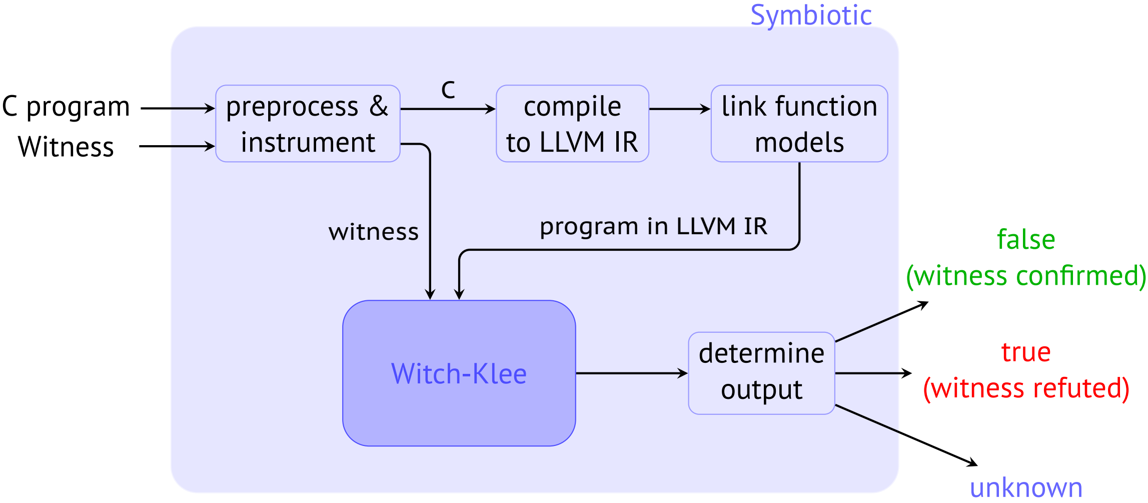
Masaryk University

April 8, 2024

Witch 3

- Validator of violation witnesses in the format 2.0
- For sequential C programs
- Accepts witnesses of all errors supported by the format
  - reachability of an error function
  - overflow
  - invalid pointer dereference
  - invalid memory deallocation
- Based on the symbolic executor for LLVM programs (Jet)Klee

Architecture



Validation approach

- Execute the program symbolically and simultaneously traverse the witness
  - Associate each state of SE with one witness segment
  - Upon encountering a branching waypoint from the segment:
    - Avoid: insert negation of constraint to path condition
    - Follow: insert constraint to path condition, move to next segment
    - Kill states with infeasible path condition
- Verdict:
  - *false* if we find a violating run matching the witness
  - *unknown* if the witness is not confirmed possibly due to concretisation
  - *true* otherwise

Witness feature support

	Symbiotic-Witch 2	Witch 3
line number	✓	✓
column number (offset)	✗	✓
function enter	✓	✓
function return	✓	✓
constraints on return values	✓	✓
branching	✓	✓
constraints on program variables	✗	✓
specifying target instruction	–	✓

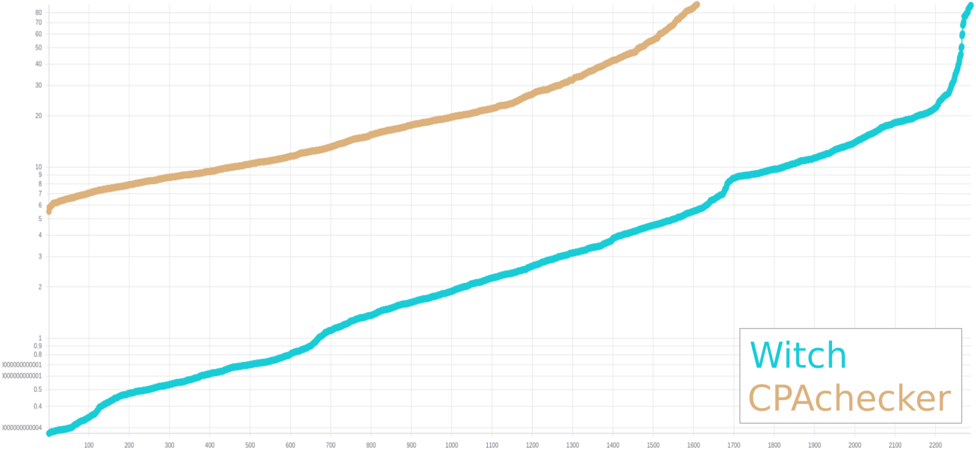
✓ supported ✗ not supported ✓ partially supported – not applicable

Results

	CPAchecker	Witch
ReachSafety	3147	3148
Overall	1569	1557

- Scores very similar due to the scoring schema based on voting

Results: Raw


80
70
60
50
40
30
20
10
9
8
7
6
5
4
3
2
1
0.9
0.8
)000000000001
)000000000001
0.5
0.4
)000000000004
100
200
300
400
500
600
700
800
900
1000
1100
1200
1300
1400
1500
1600
1700
1800
1900
2000
2100
2200
Witch
CPAchecker