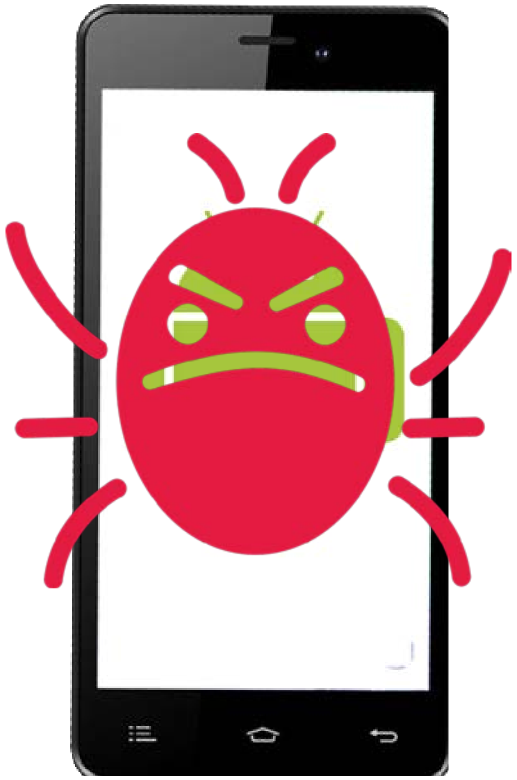
Exposing Android Event-Based Races by Selective Branch Instrumentation

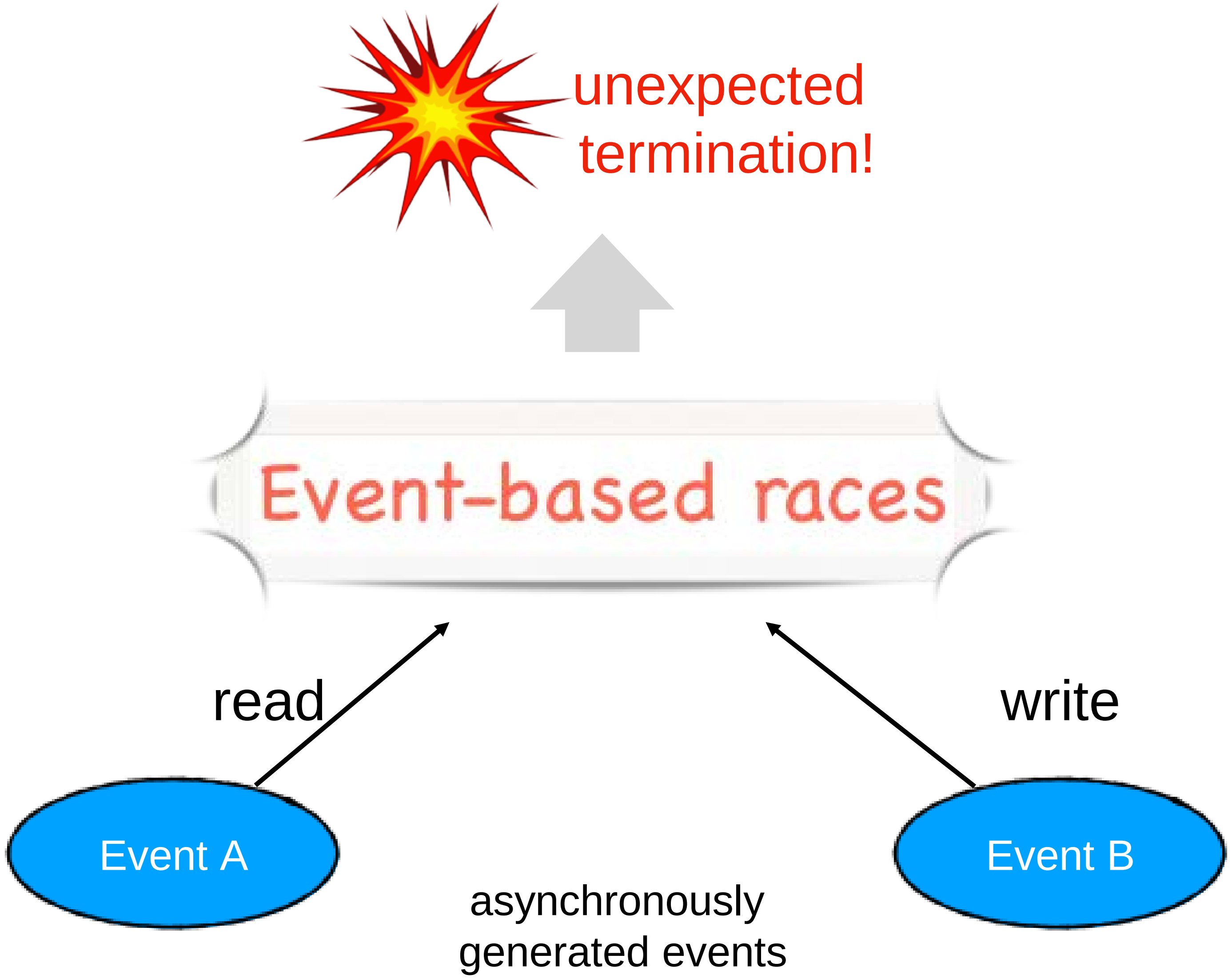
Diyu Wu, Dongjie He, Shiping Chen and Jingling Xue

The University of New South Wales, Australia

ISSRE 2020

Problem





unexpected termination!

Event-based races

read

write

Event A

Event B

asynchronously generated events

Previous Work

ASE'16

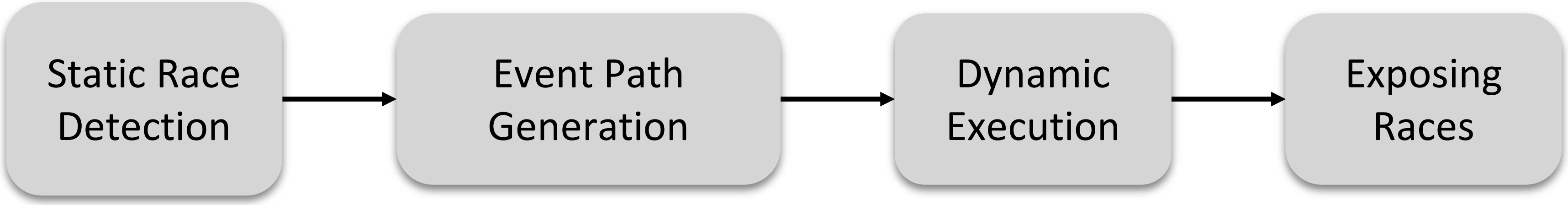
ASE'19

ISSTA'16

APSEC'16

CAV'15

Hybrid Analysis



Static Race Detection

Event Path Generation

Dynamic Execution

Exposing Races

complicated conditionals!

Our Work

- Selective Branch Instrumentation:

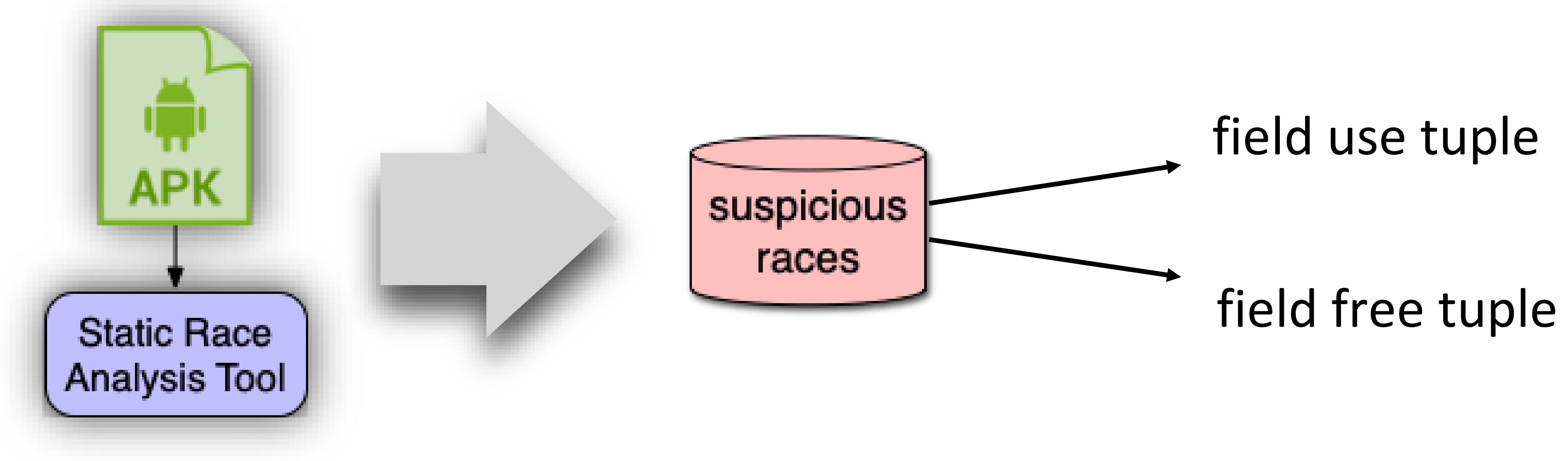
if(condition) → if(true/false)

1. non-existent races

2. crashes

Our Approach

- Statically detect suspicious races.



APK

Static Race Analysis Tool

suspicious races

field use tuple

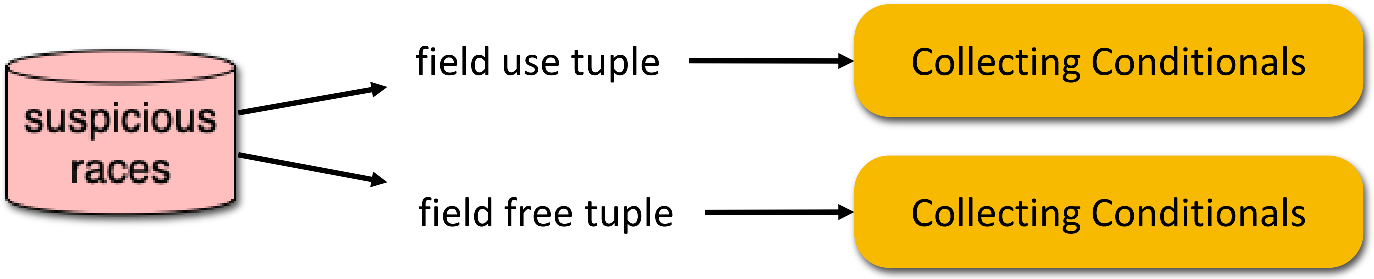
field free tuple

a suspicious race: $\langle \tau_u, \tau_f \rangle$

a tuple: $\tau = \langle s, e, ctx \rangle$

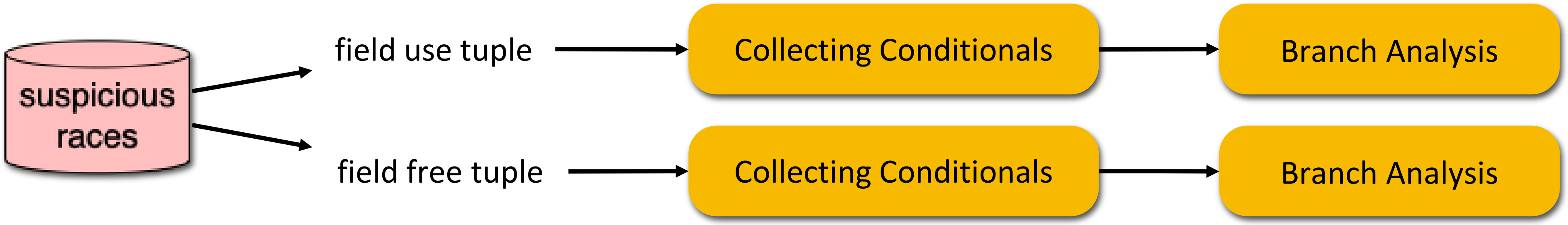
Our Approach

- Collecting Conditionals



Our Approach

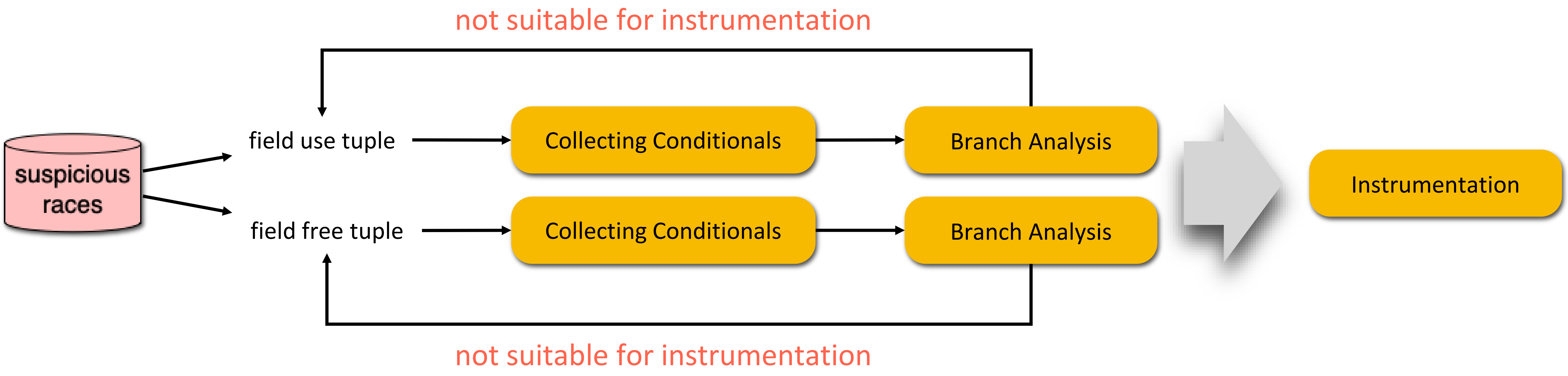
- Branch Analysis



  - Definition tracing
  - Value range analysis : possible values of variables.
  - select conditionals : could be replaced with true/false.
    - Safety check
    - Satisfiability check

Our Approach

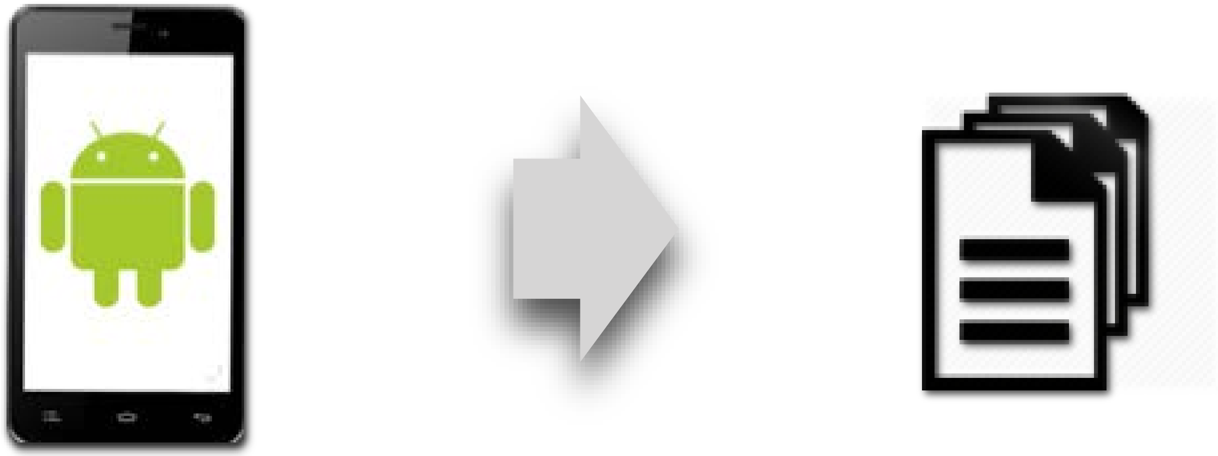
- Instrumentation



a tuple: $\tau = \langle s, e, ctx \rangle$

Our Approach

- Dynamic Execution



instrumented app

results

Evaluation

- 25 real world Android apps
  - 190 suspicious races
  - 18 true races
- Compare SIEVE with two baseline tools
  - Sieve-ZB: non-instrumentation
  - Sieve-FB: full-instrumentation

Evaluation

- Sieve vs Sieve-ZB (non-instrumentation)
  - Reached races: reached racy statements in order
  - Reported races: reached races with NPE

90(47.3%) reached races
16(88.9%) reported races
no false positive

Sieve

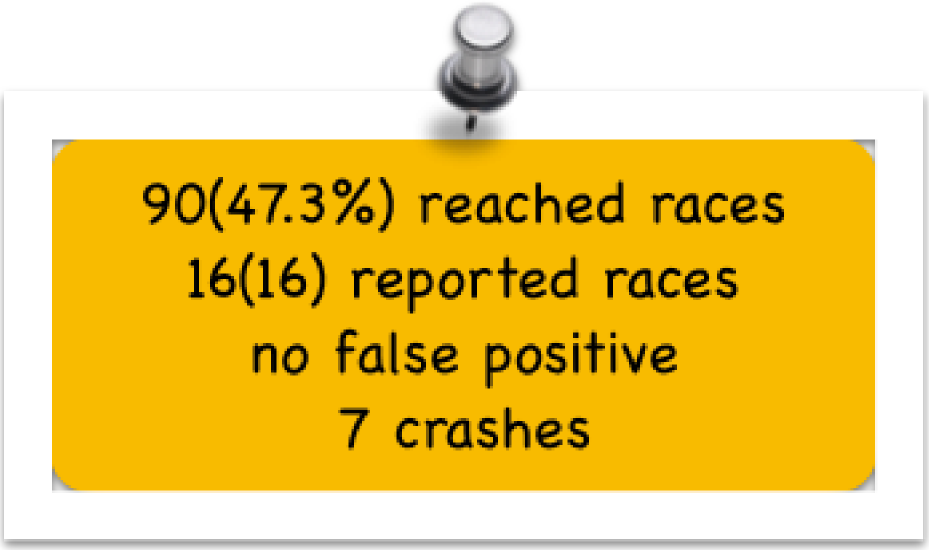
56(29.4%) reached races
14(77.8%) reported races
no false positive

Sieve-ZB

more effective!

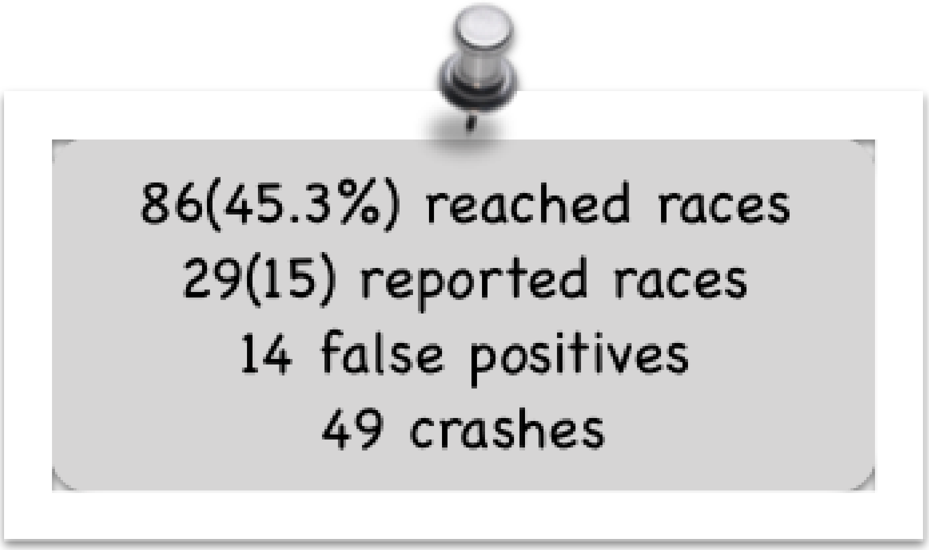
Evaluation

- Sieve vs Sieve-FB (full-instrumentation)



90(47.3%) reached races
16(16) reported races
no false positive
7 crashes

Sieve



86(45.3%) reached races
29(15) reported races
14 false positives
49 crashes

Sieve-FB

less false alarms and crashes!

Conclusion

- SIEVE: Selective branch instrumentation
  - Expose event-based races more effectively
  - Reduce negative ramifications of instrumentation

THANK YOU!