WAFFLE: Exposing Memory Ordering Bugs Efficiently with Active Delay Injection

THE UNIVERSITY OF CHICAGO

Bogdan Stoica, Shan Lu, Madan Musuvathi, Suman Nath

Microsoft Research

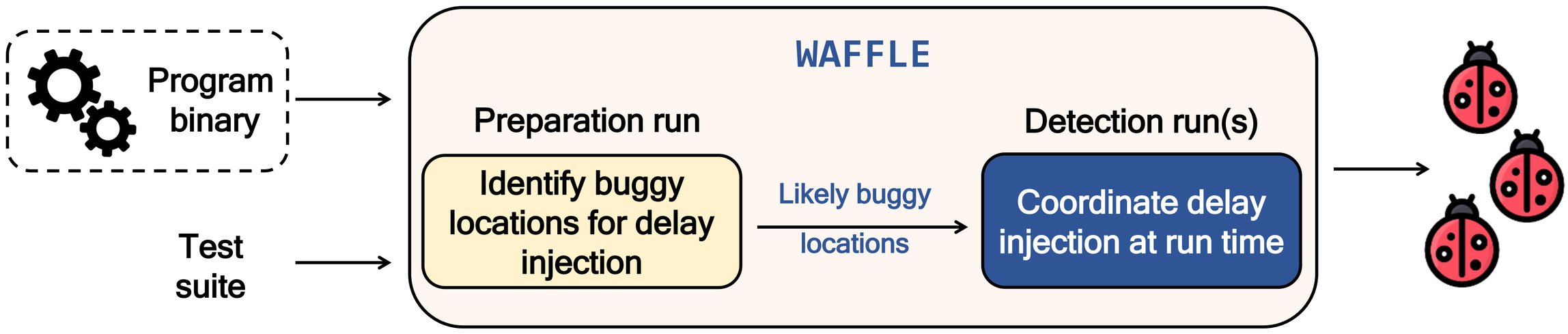
MemOrder Bugs

Thread #1	Thread #2
`myList = new T()`	
	`myList.Add(x)`
...	...
	`myList.Add(y)`
`myList.Dispose()`	
`myList = NULL`	

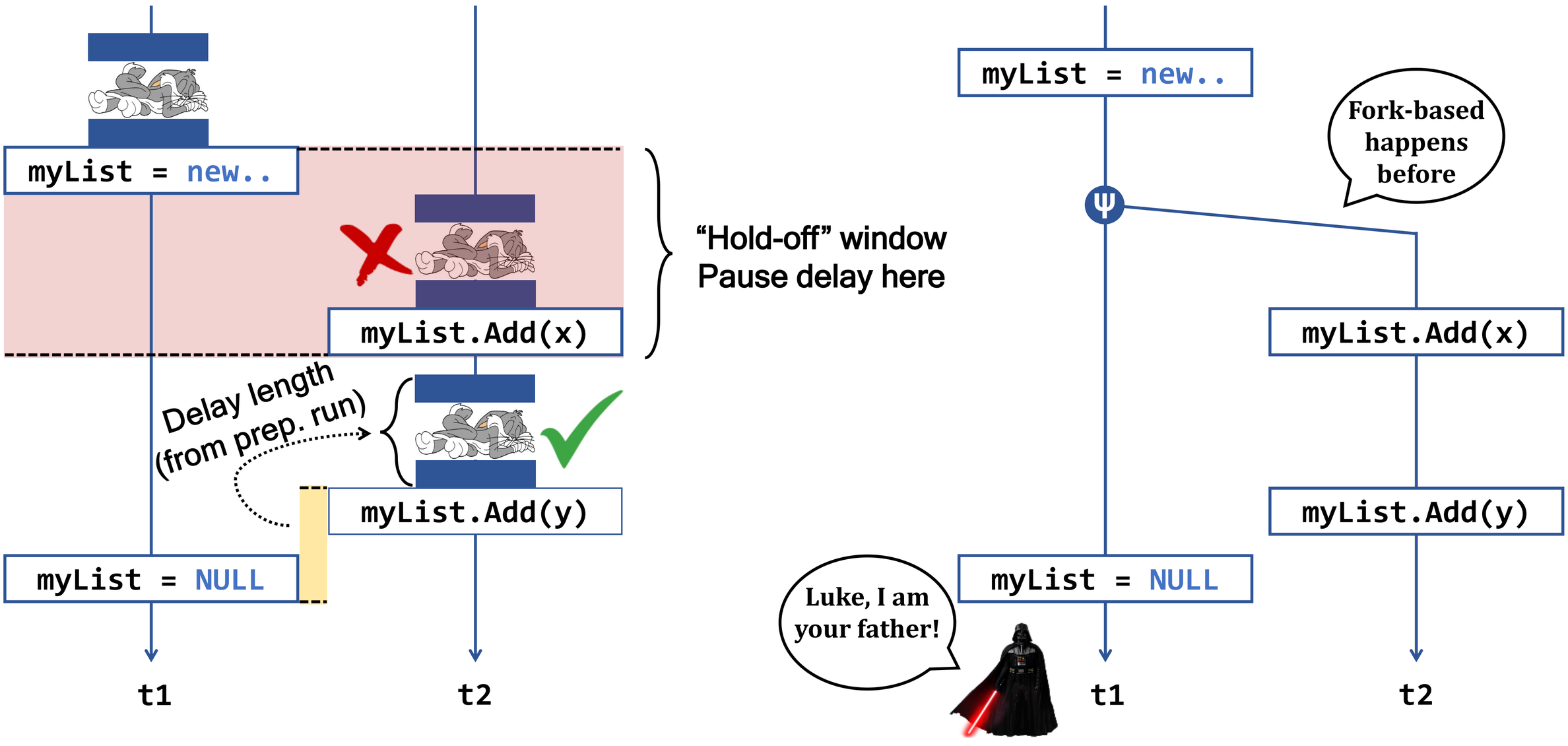
Key Insights

- Break down active delay injection into 4 design points
- Adapt each point to match MemOrder bugs properties
- Repurpose existing tests, no tailored inputs needed
- Maximize delays per run, minimize number of runs

Tool Overview

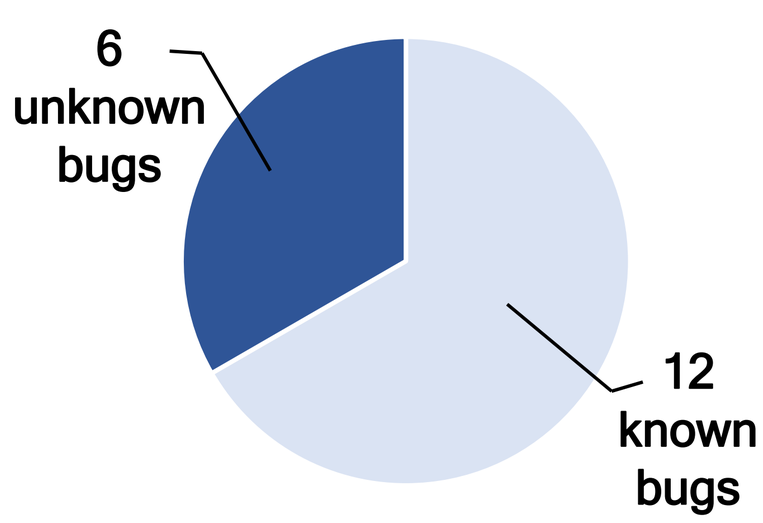


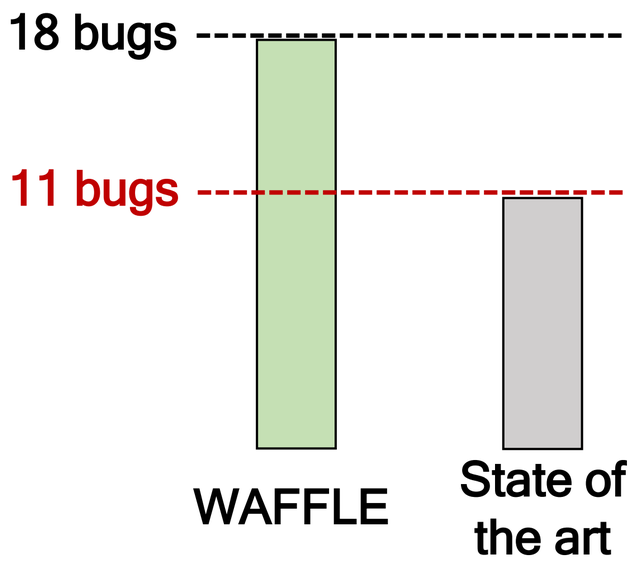
Under the Hood



Results at a Glance

- 11 open source large apps
- 80% bugs exposed in 2 runs
- 0 false positives bug reports





EuroSys '23: The Eighteenth European Conference on Computer Systems. 8-12 May, 2023. Rome, Italy.