Just-In-Time Malware Detection

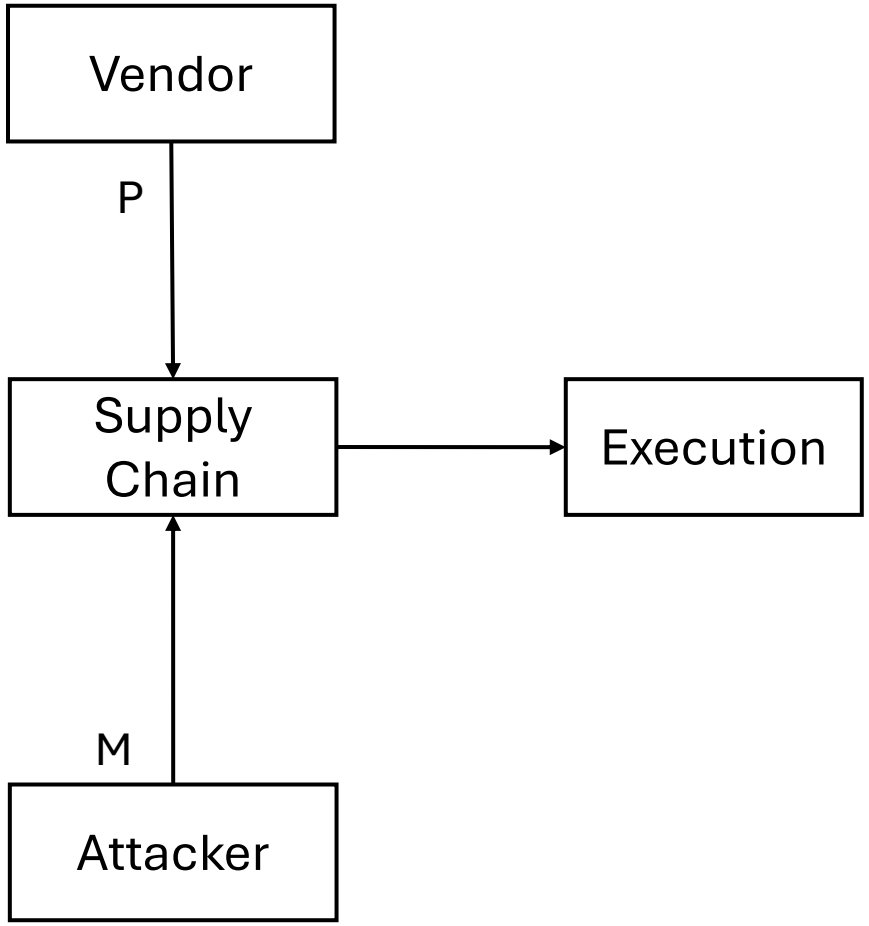
Gregor Haywood

<g.haywood@abertay.ac.uk>

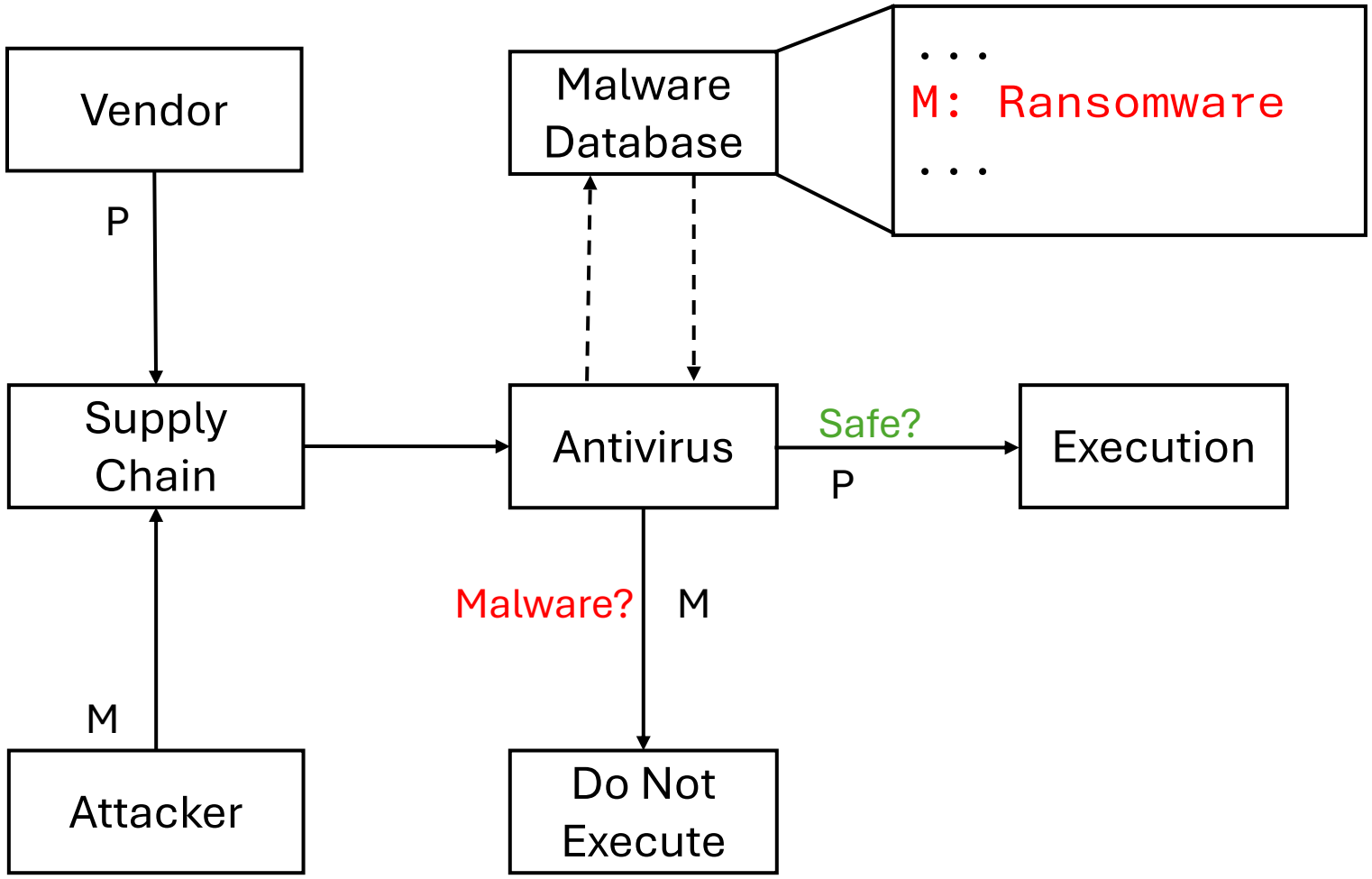
Abertay University

Interdisciplinary(-ish)

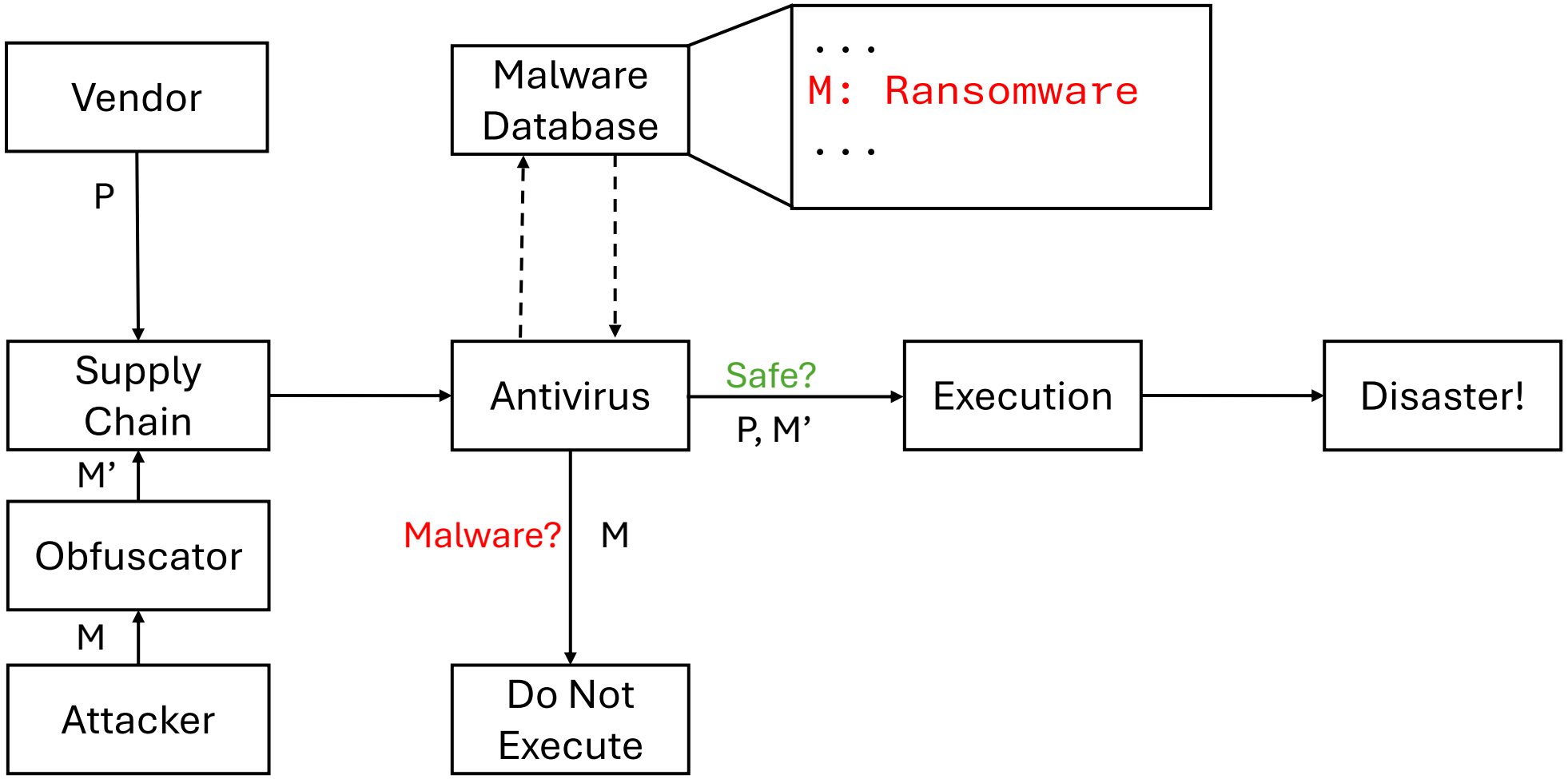
Background: Malware



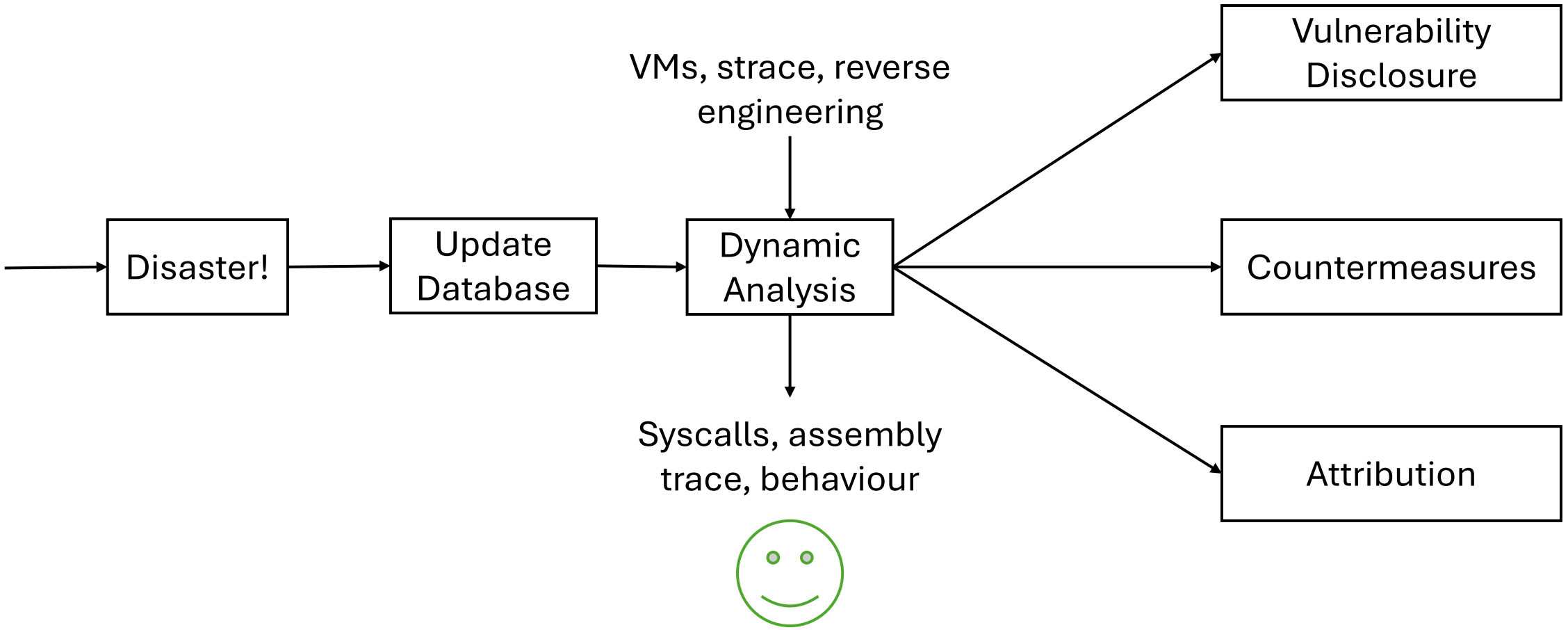
Static Analysis



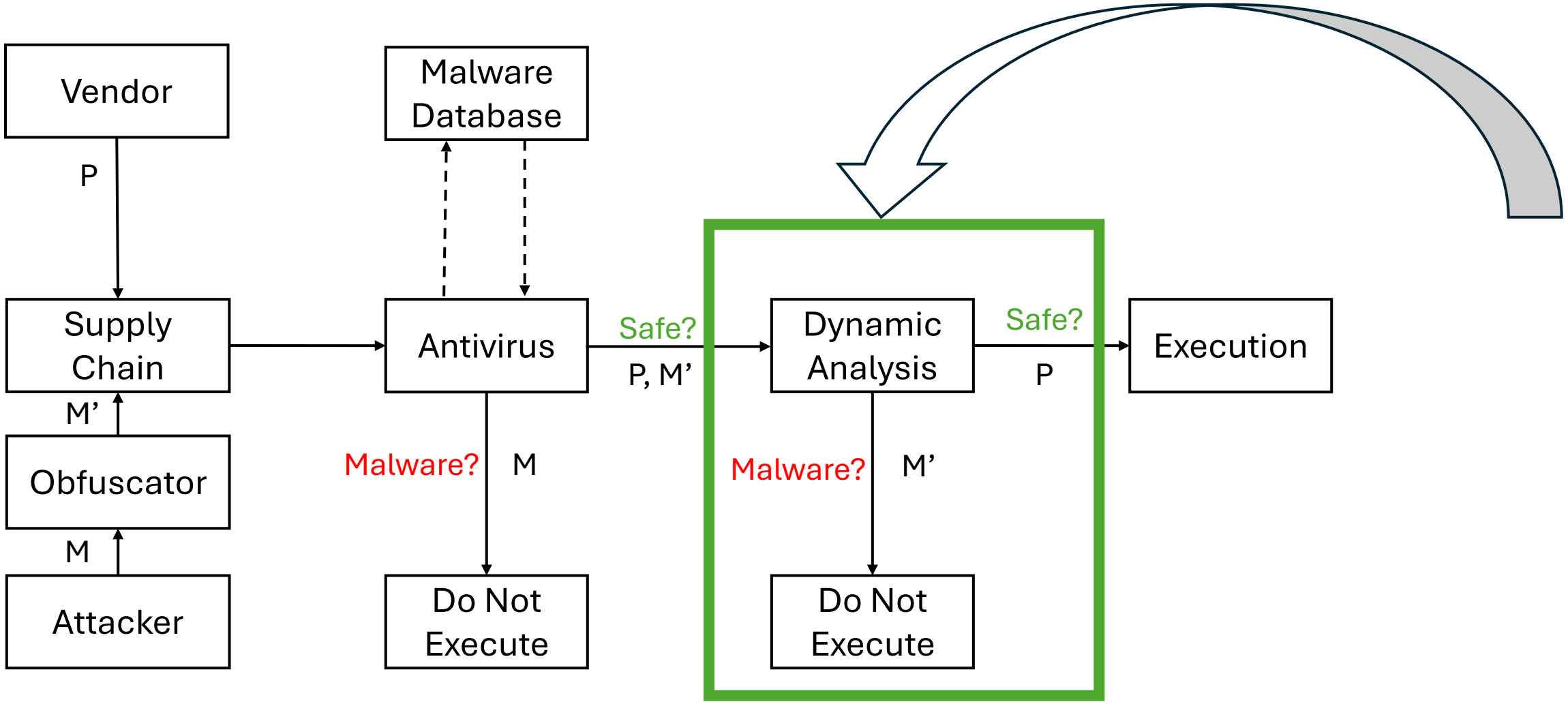
Obfuscation



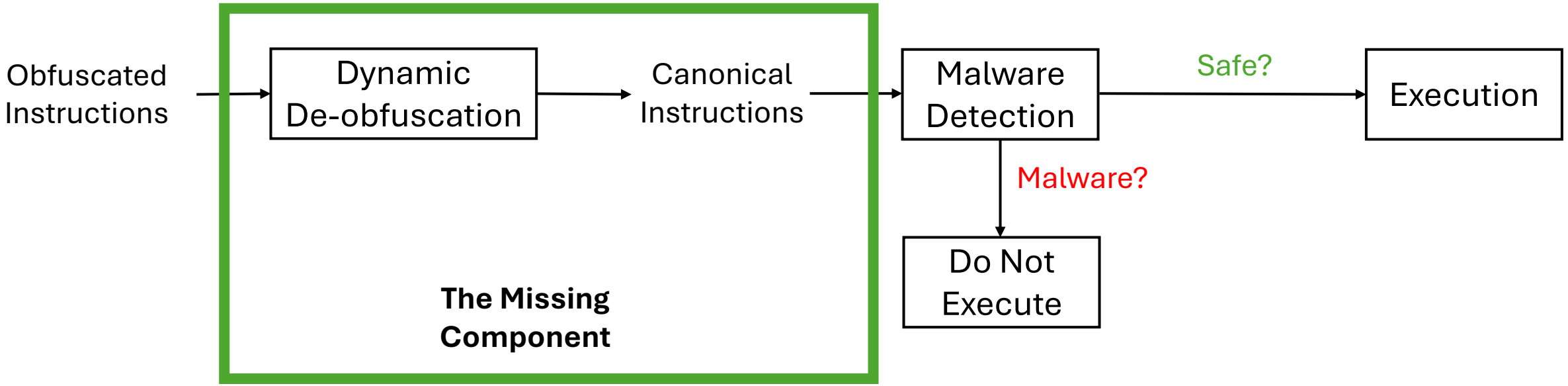
Dynamic Analysis



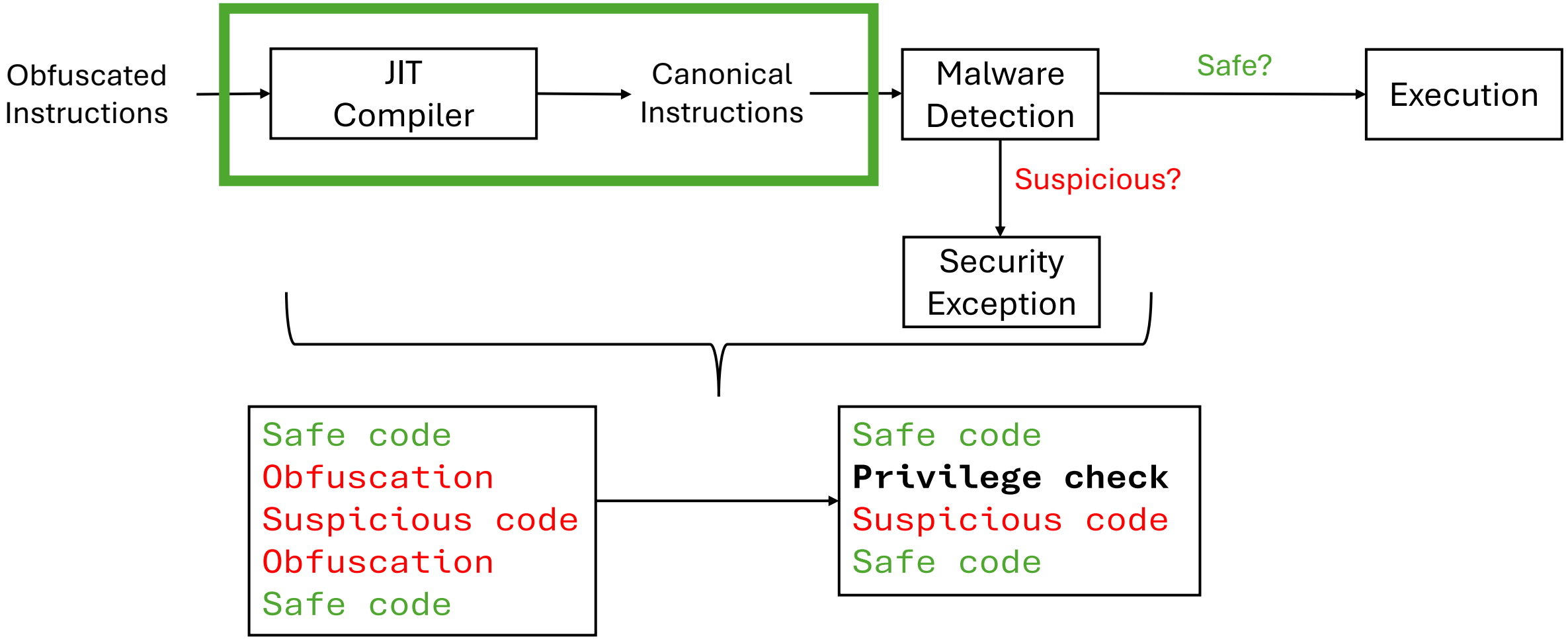
The Problem: Just-In-Time Detection



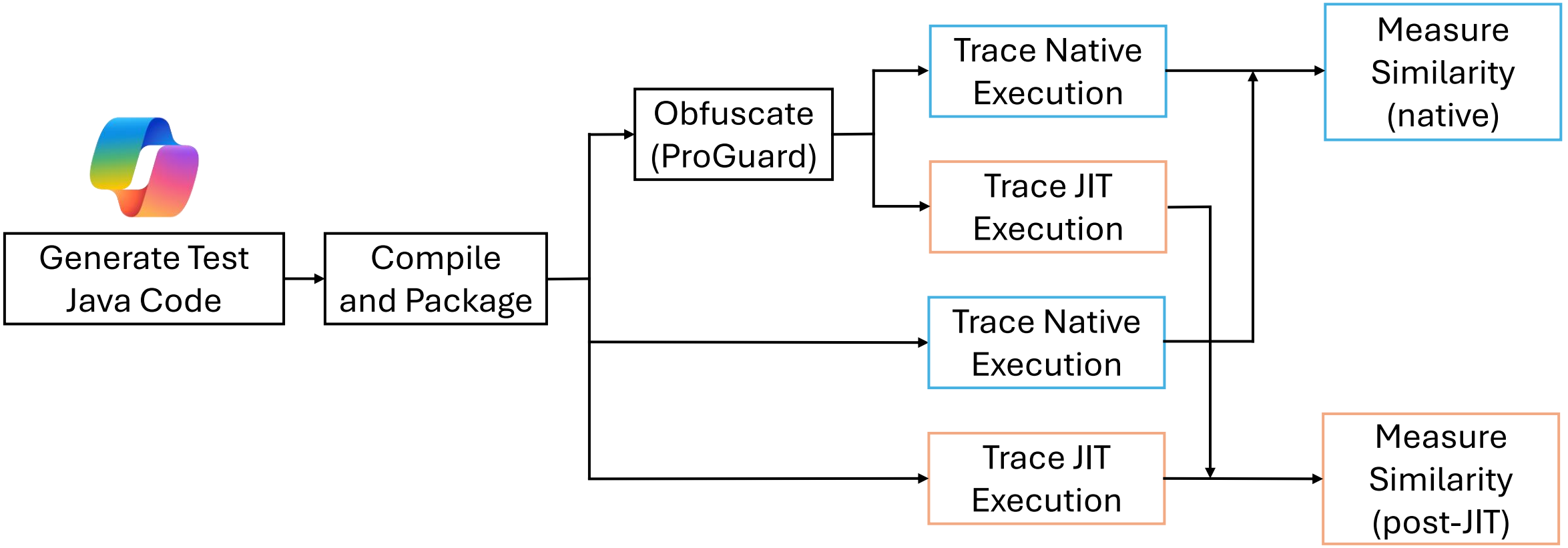
Instruction-Based Classification



Dynamic Recompilation

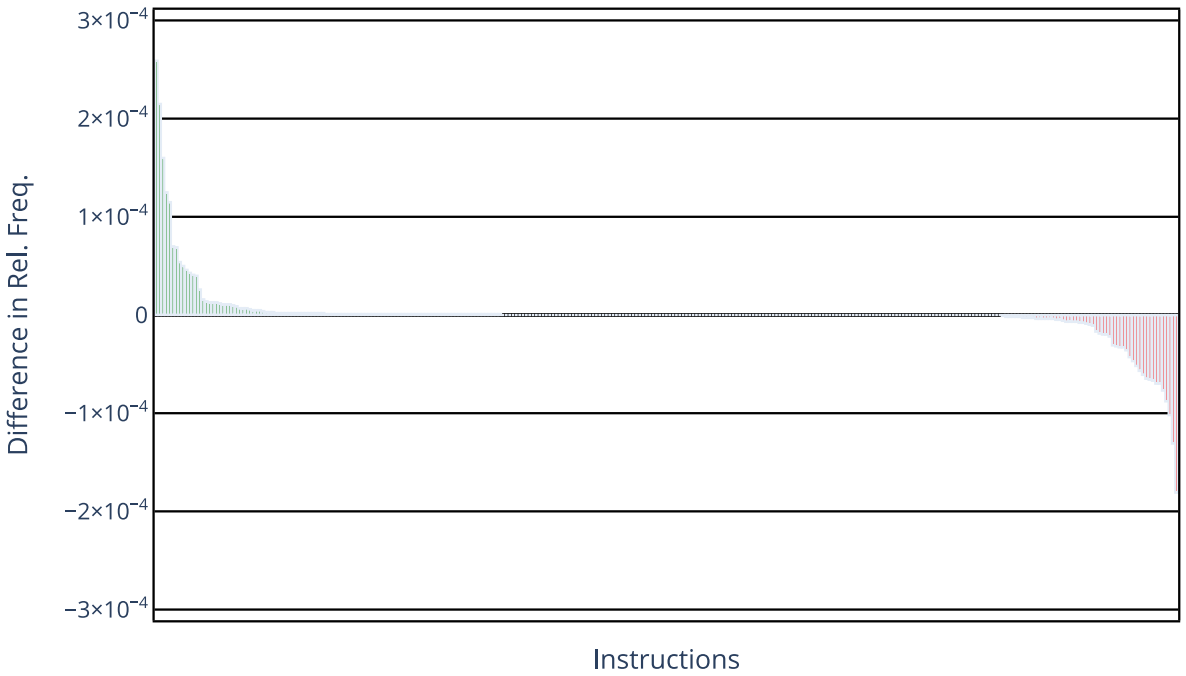


Does Optimisation Beat Obfuscation?

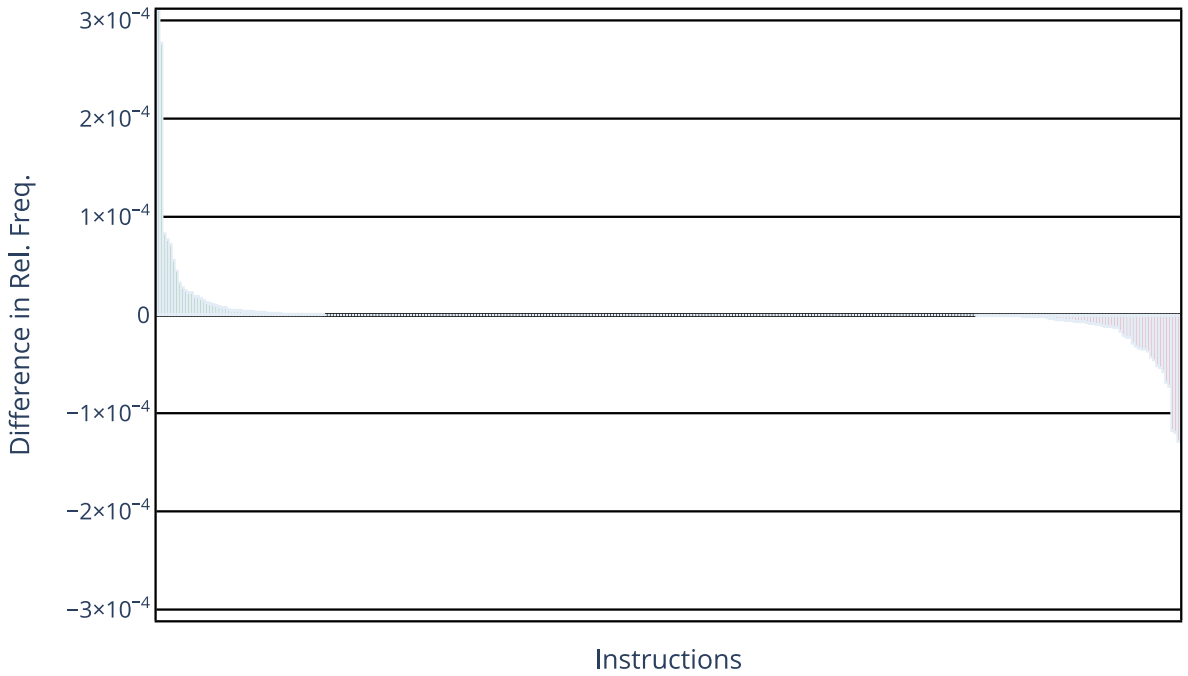


Frequency Distribution Difference

GameOfLife without JIT



GameOfLife with JIT



Similarity Metrics

Application	Normalised Taxicab Distance Without JIT	Normalised Taxicab Distance With JIT
Game Of Life	0.00316	0.00254
Traffic Simulator	0.00335	0.00298
Agent Simulator	0.00113	0.00424
Rule Engine	0.00368	0.00225

- Distance metric: sum of absolute difference in relative frequency of each assembly instruction
- Programs run >500,000 instructions
- Coarse analysis only!

Future Work & Questions?

- More programs!
  - Real malware?
- “Microscope” Analysis
  - (Large) Language Models, AST Analysis, Sliding Windows
- New security model: privileged/suspicious/unprivileged
- As a Hypervisor?
- In Hardware?