

Side-Channel Effects of Performance Optimizations in VM-Based Languages

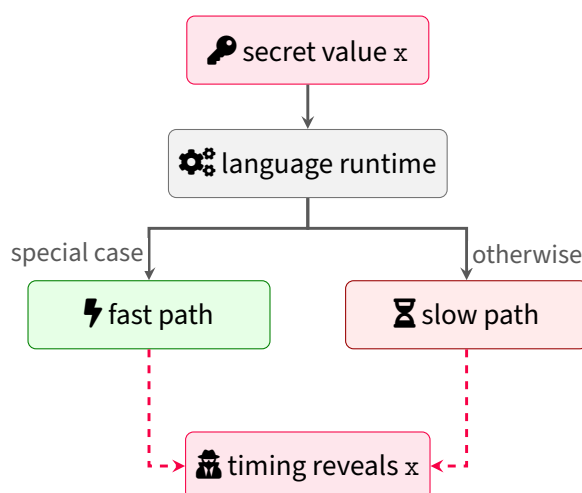
Advisor: **Hannes Weissteiner**

Motivation

Managed language runtimes, e.g., for Java, C#, Python, or JavaScript, contain many special cases to improve performance. As a result, the runtime may behave differently depending on the values a program processes. Runtime optimizations like JIT compilation are known to leak secrets [1, 2], but these special cases have not been studied systematically.

Goals and Tasks

-  Find value-dependent special cases in popular language runtimes
-  Measure their effects and exploit them in a real-world application
-  Evaluate mitigations and their performance cost



Value-dependent runtime optimizations can leak secrets through timing.

Literature

- > T. Brennan, N. Rosner, and T. Bultan
JIT Leaks: Inducing Timing Side Channels through Just-In-Time Compilation
IEEE S&P
<https://doi.org/10.1109/SP40000.2020.00007>
- > S. Nilizadeh, Y. Noller, and C. S. Păsăreanu
DifFuzz: Differential Fuzzing for Side-Channel Analysis
ICSE
<https://arxiv.org/abs/1811.07005>

Courses & Deliverables

☒ Master Project

Project code
Report
Presentation

– OR –

☒ Master's Thesis

Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

☒ CS ☒ ICE ☒ SEM

Prerequisites

- > Interest in side-channel attacks and language runtimes
- > Programming (e.g., Java, Python)
- > Basic understanding of compilers