Addressing the Challenges of Software Build Process on LLVM-based Information Flow Tracking Implementation

國立陽明交通大學 資電亥客與安全碩士學位學程 學生: 彭珮婷 指導教授: 吳育松

Abstract

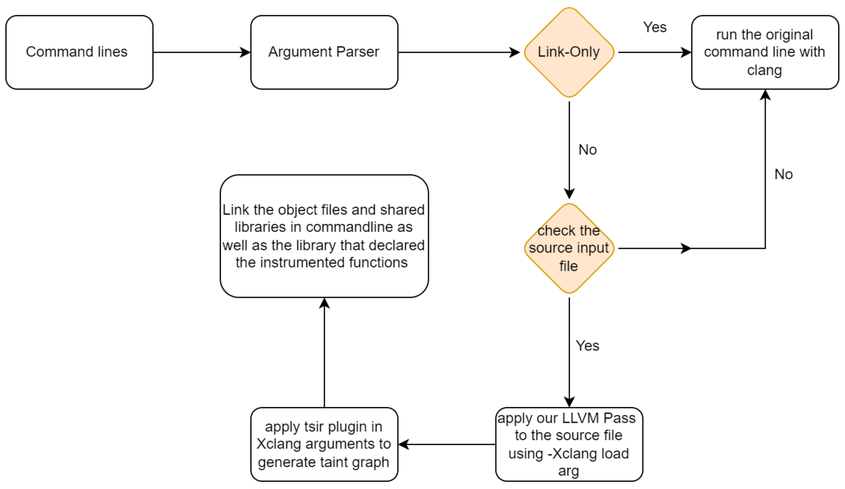
- This thesis is an extension of HIT. HIT is an LLVM-based dynamic information-flow tracking technique proposed by Yu-Hsing Hung, it decouples the information flow tracking logic from application execution to reduce the performance overhead incurred by dynamic analysis. We aim to apply HIT to large real-world projects, make this mechanism accommodate a variety kinds of build processes, and handle multiprocessing programs.

Challenges

- LLVM Instrumentation to applications that are built in different ways
- Information flows in Shared Libraries
- Multi-processing programs

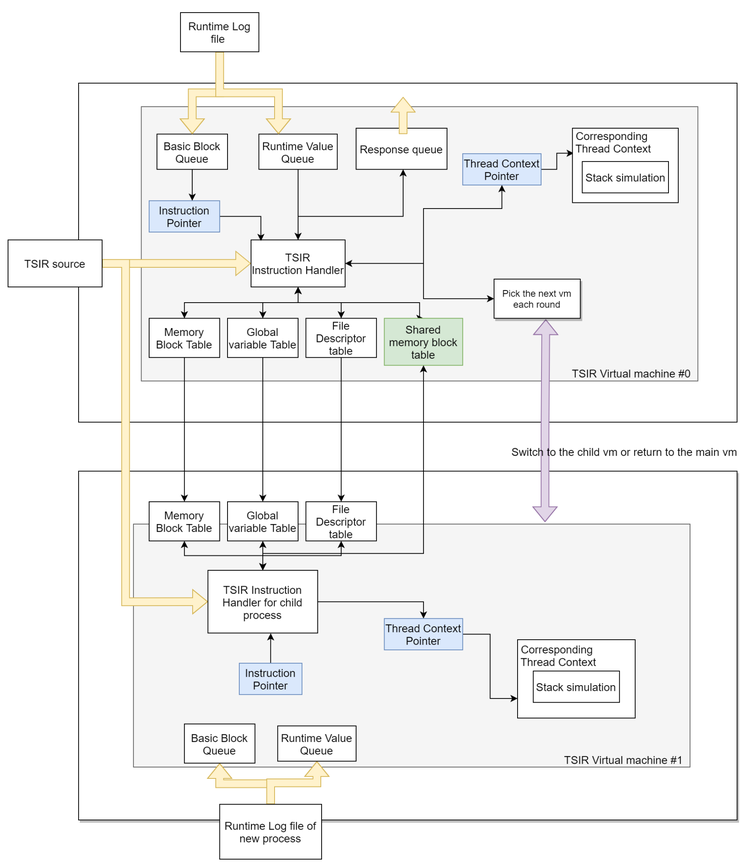
Design - Compiler Wrapper

- We design a compiler wrapper that can instrument our LLVM plugin, generate a taint semantic map during compilation



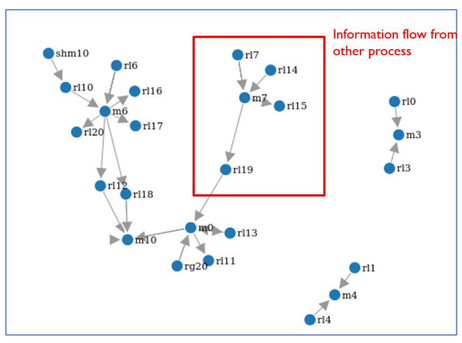
Design – Replay Engine

- Handle information flows in shared memory

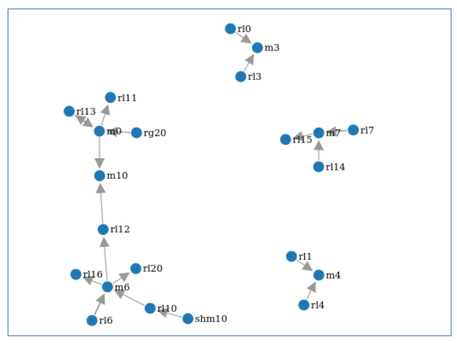


Information Flow Graph

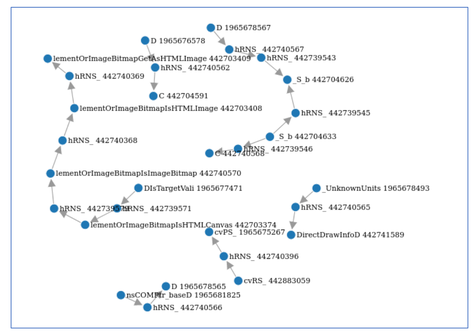
- Information flow of shared memory segment from multiple processes



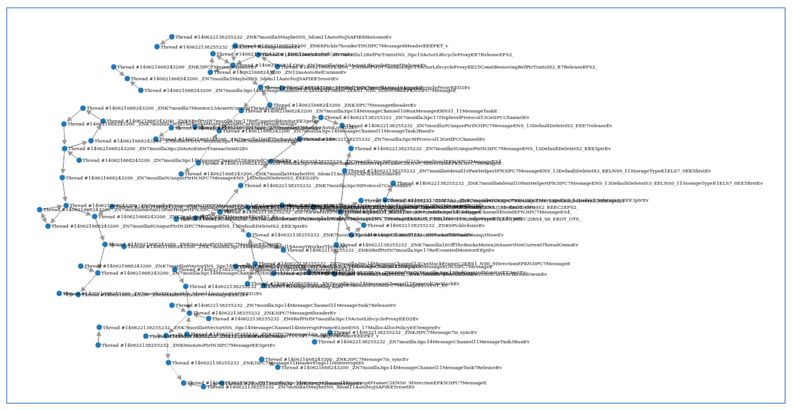
CVE-2020-16012



CVE-2020-6796

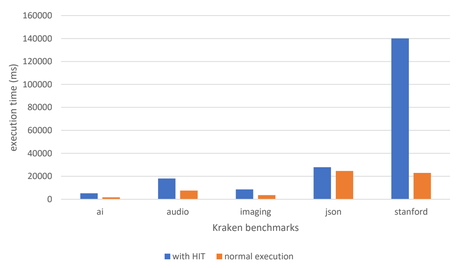


Firefox: browsing a website

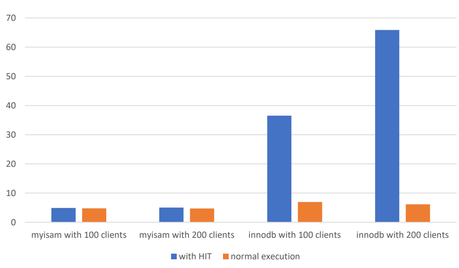


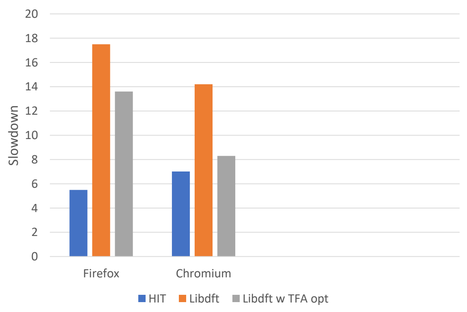
Performance

Firefox JS engine



MySQL Server





- Firefox & Chromium JS engine Performance compared to LibDFT (With Dromaeo benchmark)