Control Flow Integrity: Security Precision and Performance - A Summary

Boakye Dankwa

January 23, 2018

Control-Flow Integrity (CFI) shows promise to defeat control flow modification attacks such as remote code injection, Return-Oriented Programing (ROP) and code-reuse, that expoit memory corruption vulnerabilities in C/C++ programs. The technique has been researched and improved upon by researchers and has been integrated into products such as LLVM and some Microsoft products. Current CFI evaluations usually use the SPEC2006 benchmark and Average Indirect-target Reduction (AIR) to measure performance and security precision respectively. Control-Flow Integrity: Security Precision and Performance [1] systematize various CFI implementations and their trade-offs, and propose a novel way of evaluating these implementations against security precision and performance.

The authors first explained the fundamental concept of CFI

References

[1] Nathan Burow, Scott A. Carr, Stefan Brunthaler, Mathias Payer, Joseph Nash, Per Larsen, and Michael Franz. Control-flow integrity: Precision, security, and performance. *CoRR*, abs/1602.04056, 2016.