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. The technique has been researched and improved upon by researchers and been integrated into products such as LLVM. Current CFI evaluations usually use the SPEC2006 benchmark to measure performance and Average Indirect-target Reduction (AIR) to measure security assurance. The authors in [1] propose a novel

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.