Control-Flow Integrity

Antonio Barresi[1], Mathias Payer[2] und Thomas Gross[3]

ETH Zürich

[1] antonio.barresi@inf.ethz.ch
[2]mathias.payer@inf.ethz.ch
[3]thomas.gross@inf.ethz.ch

Abstract: Various modern attacks change the instruction sequence executed by a system. Examples are ROP (return-oriented programming) and its variants that combine existing code snippet ("gadgets") in an application's code to divert program execution. Control-Flow Integrity (CFI) is an approach to protect a system against attacks that hijack an application's control flow, and this tutorial describes CFI and its practical implications. We pay special attention to recent developments of CFI-based techniques that make this approach more attractive for real-life settings and that further reduce the number and quality of "gadgets" available to an attacker. The objective of the tutorial is to raise the level of awareness both of the kinds of attacks a system may experience as well as to understand the benefits and limitations of CFI-based defenses.

The tutorial is presented in English. The target audience consists of software engineers and their managers.