基于硬件分支事件的控制流劫持攻击防御方法[[1]](#footnote-1)∗

李威威1,2,王俊杰1,高伟毅1,2,杨秋松1,李明树1

1(中国科学院软件研究所基础软件国家工程研究中心,北京 100190)

2(中国科学院大学,北京 100190)

通讯作者: , E-mail: weiwei@nfs.iscas.ac.cn

摘 要: 控制流劫持攻击是当今安全领域面临的主要威胁之一，面向返回编程（Return-Oriented Programming，简称ROP）攻击是最常见的控制流劫持攻击方式。控制流完整性（Control Flow Integrity，简称CFI）是针ROP攻击的一种主要防御方式，已有的控制流完整性方法通常面临以下几个问题：1）需要修改源码或者通过反汇编重写二进制代码；2）需要针对所有间接分支进行检查，检查点过多；3）依赖有限资源的历史纪录，容易遭受历史覆盖攻击；4）对短配件链构成的ROP攻击不能进行有效检测，这些问题的存在大大影响了防御效果和性能。本文针对这些问题，提出了一种基于硬件分支处理的控制流劫持攻击防御方法。该方法基于最近分支记录（Last Branch Record，简称LBR）获取精确的分支信息，通过性能监控单元（Performance Monitoring Unit）得到预测失败的间接分支，结合内存信息和系统调用信息，识别出ROP攻击可能利用的配件链（gadget chain），并设计了相应的检测规则进行控制流劫持攻击检测。实验表明，该方法能够有效减少检测点，并解决历史覆盖攻击问题，在有效检测ROP攻击的同时，仅引入极小的性能开销。

关键词: ROP攻击，控制流劫持攻击，控制流完整性

**Control Flow Integrity Defense Approach Based on Hardware Branch Processing**

LI Weiwei1,2, WANG Junjie1,GAO Weiyi1,2,YANG Qiusong1, LI Mingshu1

1(Institute of Software Chinese Academy of Science, Beijing, China 100190)

2(University of Chinese Academy of Sciences, Beijing, China 100190)

**Abstract**: Return-Oriented Programming (ROP) attack is the most prevalent control flow hijacking attack and is one of the major security threats in the field of software security. Control Flow Integrigy (CFI) is a major defense against ROP attacks. However, traditional CFI methods usually face two major drawbacks: 1) introducing a large performance overhead; 2) need to modify the source code or rewrite the binary code through disassembly. To address these two drawbacks, this paper proposes a control flow integrity defense approach based on the hardware branch processing machnism. Our approach uses the hardware performance monitoring unit for data sampling, and the performance monitor interrupt triaggered by the branch sampling event is used as the ROP detection point. Experiment results show that our approach can effectively detect ROP attacks, and will only introduce neglectable performance overhead.

**Key words**: ROP attack, control flow hijacking attack, control flow integrity

1. ∗ 基金项目: xxxx

   Foundation item:xxxx

   收稿时间: 0000-00-00; 修改时间: 0000-00-00; 采用时间: 0000-00-00; jos在线出版时间: 0000-00-00

   CNKI在线出版时间: 0000-00-00 [↑](#footnote-ref-1)