World Academy of Science, Engineering and Technology
International Journal of Educational and Pedagogical Sciences
Vol:17, No:12, 2023

A Comprehensive Approach to Mitigate Return-Oriented Programming Attacks: Combining Operating System Protection Mechanisms and Hardware-Assisted Techniques

Authors : Zhang Xingnan, Huang Jingjia, Feng Yue, Burra Venkata Durga Kumar

Abstract : This paper proposes a comprehensive approach to mitigate ROP (Return-Oriented Programming) attacks by combining internal operating system protection mechanisms and hardware-assisted techniques. Through extensive literature review, we identify the effectiveness of ASLR (Address Space Layout Randomization) and LBR (Last Branch Record) in preventing ROP attacks. We present a process involving buffer overflow detection, hardware-assisted ROP attack detection, and the use of Turing detection technology to monitor control flow behavior. We envision a specialized tool that views and analyzes the last branch record, compares control flow with a baseline, and outputs differences in natural language. This tool offers a graphical interface, facilitating the prevention and detection of ROP attacks. The proposed approach and tool provide practical solutions for enhancing software security.

Keywords : operating system, ROP attacks, returning-oriented programming attacks, ASLR, LBR, CFI, DEP, code randomization, hardware-assisted CFI

Conference Title : ICESET 2023 : International Conference on Education, Science, Engineering and Technology

Conference Location : Kuala Lumpur, Malaysia

Conference Dates : December 04-05, 2023

Open Science Index, Educational and Pedagogical Sciences Vol:17, No:12, 2023 publications.waset.org/abstracts/168825.pdf