IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, May 2024

Control Flow Integrity: Embedded System Code Reuse Defence

Chethan C V[1], Pavan Sai[2], Deepak U[3], Chirag S[4]
Students, Department of Computer Science & Engineering[1,2,3,4]
S J C Institute of Technology, Chikkaballapura, India

Abstract: *Hardware-based program Control Flow Integrity (CFI) components, centering on the state-of-the-art usage innovations. Control Stream Keenness may be a significant security degree pointed at moderating control- flow capturing assaults, such as Return Oriented Programming (ROP) and Jump Oriented Programming (JOP). Whereas software-based CFI arrangements have been compelling to a few degree, their restrictions have impelled the improvement of hardware-based approaches for improved security. This survey analyzes unmistakable innovations in this space, counting Intel CET (Control-flow Requirement Innovation), ARM Pointer Verification, AMD SEV-SNP (Secure Settled Paging), and RISC-V CFI Expansions. Each technology's highlights, usage strategies, and contributions to fortifying cyber security are analyzed to supply bits of knowledge into the current scene of hardware-based computer program CFI. By leveraging hardware-level protections, these progressions offer strong security against advanced control-flow capturing assaults, subsequently reinforcing the security pose of computing frameworks. As cyber dangers proceed to advance, the require for vigorous security components to ensure against control-flow capturing assaults gets to be progressively basic. This audit digs into the state-of-the-art execution innovations for hardware-based computer program Control Stream Astuteness*

Keywords: AMD SEV-SNP