Contribution ID: **16** Type: **not specified**

Twenty years later: Evaluating the Adoption of Control Flow Integrity

Wednesday, 5 June 2024 10:50 (15 minutes)

Memory corruption vulnerabilities still allow compromising computers through software written in a memory-unsafe language such as C/C++. This highlights that mitigation techniques to prevent such exploitations are not all widely deployed. In this paper, we introduce SeeCFI, a tool to detect the presence of a memory corruption mitigation technique called control flow integrity (CFI). We leverage SeeCFI to investigate to what extent the mitigation has been deployed in complex software systems such as Android and specific Linux distributions (Ubuntu and Debian). Our results indicate that the overall adoption of CFI (forward- and backward-edge) is increasing across Android versions (~30% in Android 13) but remains the same low (<1%) throughout different Linux versions. Our tool, SeeCFI, offers the possibility to identify which binaries in a system were compiled using the CFI option. This can be deployed by external security researchers to efficiently decide which binaries to prioritize when fixing vulnerabilities and how to fix them. Therefore, SeeCFI can help to make software systems more secure.

Length

15 minutes

Optional: Speaker / convener biography

Primary author: HOUY, Sabine (Umeå University)

Co-author: Prof. BARTEL, Alexandre (Umeå University)

Presenter: HOUY, Sabine (Umeå University)

Session Classification: Talks and presentations

Track Classification: Talks and presentations