RT-DFI : Optimizing Data-Flow Integrity for Real-Time Systems

Nicolas Bellec*†[1], Guillaume Hiet‡[2], Simon Rocicki§[3], Frédéric Tronel¶[2], and Isabelle Puaut‖[1]

[1]Pushing Architecture and Compilation for Application Performance (PACAP) – Inria Rennes – Bretagne Atlantique, ARCHITECTURE – Campus de Beaulieu 35042 Rennes cedex, France
[2]Centrale Supélec – SUPELEC – France
[3]Architectures matérielles spécialisées pour l'ère post loi-de-Moore (TARAN) – Inria Rennes – Bretagne Atlantique, ARCHITECTURE – Campus de beaulieu 35042 Rennes cedex, France

Résumé

The emergence of Real-Time Systems with increased connections to their environment has led to a greater demand in security for these systems. Memory corruption attacks, which modify the memory to trigger unexpected executions, are a significant threat against applications written in low-level languages. Data-Flow Integrity (DFI) is a protection that verifies that only a trusted source has written any loaded data. The overhead of such a security mechanism remains a major issue that limits its adoption.
In this presentation, we present RT-DFI, a new approach that optimizes Data-Flow Integrity to reduce its overhead on the Worst-Case Execution Time. We model the number and order of the checks and use an Integer Linear Programming solver to optimize the protection on the Worst-Case Execution Path. Our approach protects the program against many memory-corruption attacks, including Return-Oriented Programming and Data-Only attacks. Moreover, our experimental results show that our optimization reduces the overhead by 7% on average compared to a state-of-the-art implementation.

*Intervenant
†Auteur correspondant: nicolas.bellec@inria.fr
‡Auteur correspondant: guillaume.hiet@centralesupelec.fr
§Auteur correspondant:
¶Auteur correspondant: frederic.tronel@inria.fr
‖Auteur correspondant: isabelle.puaut@irisa.fr