Politecnico di Torino
Dipartimento di Automatica e Informatica

PhD in Computer and Control Engineering
XXXVI cycle

Supervisor
Prof. Paolo Ernesto PRINETTO

Vulnerability-Tolerant Architectures for IoT Devices

PhD Candidate: *Vahid EFTEKHARI MOGHADAM* *vahid.eftekhari@polito.it*

1. Introduction

The rapid development and ubiquity of the Internet of Things (IoT) and its applications in many mission-critical and safety-critical domains, like automotive or aeronautics, make a huge attraction for attackers to exploit the vulnerabilities of the systems and benefit from their weaknesses. Consequently, the security of embedded IoT devices and their resilience is of paramount importance.

2. Objectives

Nowadays, IoT systems are often of mixed-criticality nature where high-critically tasks (e.g., an engine control) and low-criticality tasks (e.g., infotainment) coexist/operate within the same environment. Considering that, a secure system architecture design can be introduced to address the security needs of the critical system operations, improving vulnerability-tolerance of the design, while keeping the performance/cost of the overall system intact.

3. Method

Vulnerabilities in IoT devices like memory vulnerabilities introduced by the languages used to program these devices (e.g., C/C++) are the points attackers can use to get access and control data. E.g., return address stored on the call stack, which allows for control-flow hijacking. Control-Flow Integrity (CFI), is a general defense technique for control-flow hijacking attacks. CFI security policy ensures that the program execution flow strictly follows the path of the Control-Flow Graph (CFG) that can be defined by statical source-code analysis before binary execution.

4. Result

Asymmetric verification of control flow on multicore systems is a reference design to address the security needs of critical IoT systems, where the real-time behavior of the operations is preserved, while the integrity of the operations is verified using the CFI strategies.

By statically dividing the system resources through adoption of a hypervisor, separate operational environments can be created to accommodate the mixed-criticality nature of system designs. In this fashion, the task of auditing the CFI checks can be passed to the portion of the system where the real-time nature is not of concern. Improving the security of the critical system operations and detecting anomalies while preserving the performance requirements is the outcome of this layout where the mixed nature of the systems is exploited to gain fault tolerance.

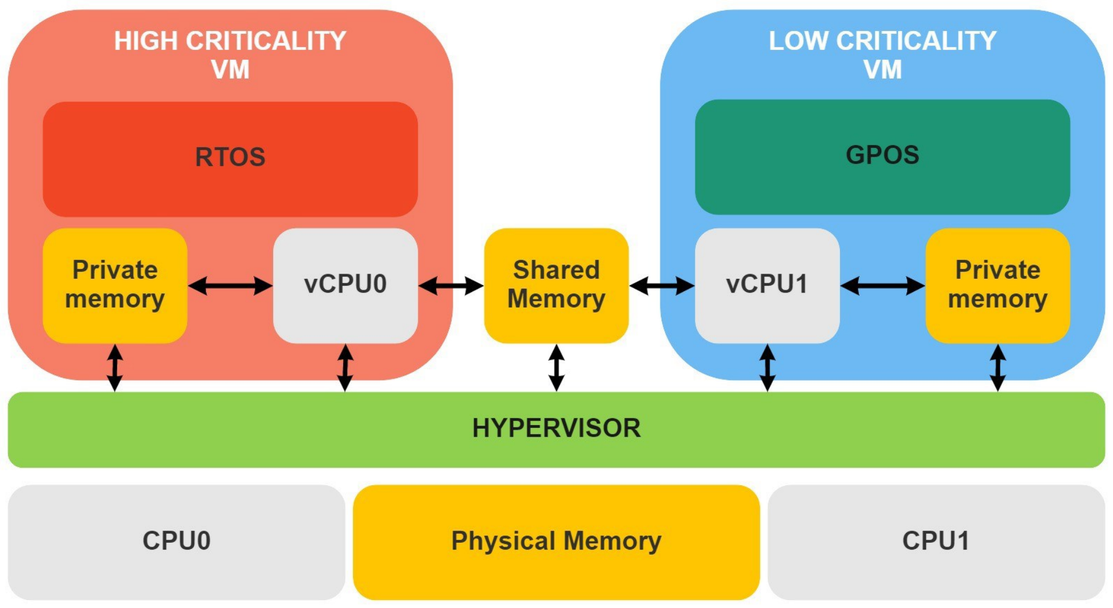

Fig: The described architecture for supporting multicore control-flow verification.

5. References

1. “Control-flow integrity for real-time operating systems: open issues and challenges”, 2021. Available at: https://iris.polito.it/handle/11583/2923694
2. “Real-Time Control-Flow Integrity for Multicore Mixed-Criticality IoT Systems”, 2022. Available at: https://iris.polito.it/handle/11583/2969412