Computers & Security 163 (2026) 104817

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Attacks, defenses and perspectives for the runtime security of RISC-V IoT devices: A review

Wei Wang [a], Weike Wang [a,b,*], Jiameng Liu [a], Lin Li [c], Bingzheng Li [a], Zirui Liu [a], Xiang Wang [d]

[a] College of Electronic and Information Engineering, Shandong University of Science and Technology, Qingdao, 266590, China
[b] China Academy of Safety Science and Technology, Beijing, 100012, China
[c] National Computer Network Emergency Response Technical Team/Coordination Center of China Beijing Branch, Beijing, 100055, China
[d] College of Electronic and Information Engineering, Beihang University, Beijing, 100091, China

ARTICLE INFO

Keywords:
RISC-V
Runtime security
Side-channel attacks
Memory corruption
Network attacks
Defense schemes

ABSTRACT

With the extensive application of embedded devices in daily life, the security issues have gained escalating significance. There are numerous researches and countermeasures dealing with the security problems of mainstream processor architectures. As an emerging Instruction Set Architecture (ISA), RISC-V has drawn widespread attention owing to its openness, flexibility, and extensibility. With its popularization in diverse fields, ensuring the security becomes crucially important. Aiming at the runtime security of RISC-V IoT devices, this paper reviews all the published papers in RISC-V security, and investigates three mainstream attack approaches and corresponding defense solutions. We analyze five common side-channel attacks with distinct attack focuses, categorize defense schemes into three types based on different levels and strategies of defense technology, and summarize several existing defense schemes on RISC-V platforms. Then, in the context of program vulnerability exploitation attacks, we present the attack process and offer a comprehensive overview and comparison of hardware-assisted defense mechanisms that have been implemented on RISC-V platforms in the recent years. This analysis is carried out from four key strategies, namely Code Integrity, Control Flow Integrity, Data Flow Integrity, and Information Confidentiality. For higher-level network attacks that are less correlated with the underlying ISA, we provide a brief statement and introduce two mainstream mechanisms, namely Intrusion Detection System and Data Encryption. Besides, this paper offers the critical perspectives and future development directions for the defense strategies corresponding to each type of attack. It is convinced that this review will act as a valuable resource for fellow researchers in RISC-V security.

1. Introduction

Driven by the rapid advancement of the Internet of Things (IoT) and smart devices, embedded systems play an increasingly important role in daily life. Embedded devices are pervasive across a wide range of applications, encompassing smartphones and smart homes, as well as industrial controls and medical devices. However, while the extensive adoption of embedded systems enhances production efficiency and daily life convenience, it inevitably brings inherent security vulnerabilities. In recent years, the attack methods targeting embedded systems have exhibited an increasing level of diversification. Exploiting system vulnerabilities, hackers employ various forms of attacks that not only endanger individuals' property security but also pose a threat to human safety. For example, nearly 900,000 customers of Deutsche Telekom Internet Service Provider experienced internet service disruption due to a Mirai variant attack (Kolias et al., 2017) on their routers, significantly impacting their daily lives. Furthermore, the utilization of wireless RF communication protocol by the attacker enables them to manipulate the configurations of the affected insulin pump and exert control over insulin administration, thereby directly endangering individuals' lives. Therefore, ensuring the security of embedded systems has emerged as a prominent research area. Researchers have diligently investigated the security concerns associated with prevailing processor architectures such as x86 and ARM, proposing numerous countermeasures against diverse attack methods (Li et al., 2024a; Paul et al., 2022; Wang et al., 2023a,b). Consequently, a comprehensive defense system has been established.

The RISC-V architecture is an open standards-based ISA that originated from a research project at the University of California, Berkeley in 2010. As a recent emergence in the field of open-source ISAs, RISC-V has attracted significant attention from both academia and indus-

* Corresponding author.
E-mail address: wangweike@sdust.edu.cn (W. Wang).

https://doi.org/10.1016/j.cose.2025.104817
Received 31 August 2025; Received in revised form 27 November 2025; Accepted 26 December 2025
Available online 2 January 2026