Pohasii Serhii, Tkach Maksym, Holdobin Serhii, Brynza Natalia, Stetsenko Vadym, Tiutiunyk Olha

HARDWARE SECURITY EVALUATION OF IOT MICROCONTROLLERS: THREATS AND COUNTERMEASURES

Pohasii S. Hardware Security Evaluation of IoT Microcontrollers: Threats and Countermeasures / S. Pohasii, M. Tkach, S. Holdobin et al. // 2025 IEEE: 6th KhPI Week on Advanced Technology (KhPIWeek). – Kharkiv, Ukraine, 2025. – pp. 1-6.

Abstract. This study analyzes the susceptibility of IoT microcontrollers to reverse engineering, defined as unauthorized data access for replication, and proposes countermeasures. STM32F0 demonstrates superior resistance due to dense integration, rapid protection activation, and robust encryption, effectively countering attacks like Cold Boot Stepping, Glitch, Electromagnetic Analysis, and invasive methods. GD32 offers moderate security but is vulnerable to faster attacks. CH32 and MM32F0 show the least resilience due to weak protection. Architectural analysis highlights STM32F0's secure interfaces, while GD32's multi-chip design and CH32/MM32F0's simpler cores increase risks. Security metrics confirm STM32F0's lead, with GD32, CH32, and MM32F0 needing enhancements. Recommendations include hardware shielding, signal filters, and dynamic encryption, implementable in 2-14 days at $0.1-1.0 per device. STM32F0 suits high-security IoT, GD32 mid-level needs, and CH32/MM32F0 low-risk applications. Comprehensive hardware and software modifications are critical to mitigate reverse engineering threats across all microcontrollers.

Keywords: hardware attacks; IoT Security; microcontrollers; protection mechanisms; tncryption