Graduate School of Science and Technology Master's Thesis Abstract

Laboratory name (Supervisor)	Cyber Resilience (Youki Kadobayashi (Professor))		
Student ID	2411430	Submission date	2026 / 1 / 18
Name	YAMEOGO KISWENDSIDA ARISTIDE CHILDERIC		
Thesis title	SecureWear: Toward a Security-Oriented Firmware Framework for BLE-Based Devices		

Abstract

Wearable devices increasingly rely on Bluetooth Low Energy (BLE), where practical security weaknesses often arise from firmware-level misconfigurations rather than flaws in the protocol itself. In wearable firmware, insecure pairing settings, missing access control on GATT operations, and inconsistent enforcement of security requirements remain common under tight resource and development constraints.

This thesis proposes SecureWear-FW, a modular, security-oriented firmware framework designed to reduce avoidable BLE firmware weaknesses under embedded constraints. SecureWear-FW is organized into three modules: (i) a secure BLE firmware baseline that enforces conservative pairing configurations and fail-closed, encryption-gated access to sensitive GATT operations; (ii) lightweight, on-device statistical monitoring that provides interpretable early-warning signals from BLE-visible events with minimal overhead; and (iii) a policy-driven compliance and validation pipeline that maps deterministic static analysis findings to explicit policy rules via traceable evidence objects, with optional and strictly guarded LLM-assisted triage for ambiguous cases.
An experimental evaluation on an ESP32-class platform assesses baseline enforcement, monitoring feasibility, policy compliance, and resource overhead. The results indicate that SecureWear-FW enforces a conservative BLE security posture, supports auditable compliance checking, enables stable on-device monitoring, and introduces modest Flash and RAM overhead compatible with wearable-class microcontrollers.
Overall, this work shows that combining secure-by-default firmware enforcement, lightweight runtime visibility, and policy-driven validation can improve the security posture of BLE-based wearable firmware without sacrificing deployability.