Problem Definition

Dhruv Sunil Bhatia
24CSB0A19
CSE - A
Q119 - Secure OTA Update Compiler

Firmware updates in IoT and embedded devices are commonly delivered through OTA mechanisms, allowing remote upgrades without physical access. While OTA updates are essential, insecure update logic introduces significant security risks.

Insecure firmware update code may still compile successfully even when missing critical security checks such as signature verification, rollback prevention, and trusted source validation. This enables attacks such as malicious firmware installation and downgrade attacks.

This project proposes a compiler-based enforcement approach where firmware update security requirements are treated as compile-time correctness rules. The compiler statically analyzes update logic and rejects programs violating mandatory security invariants.

Objective

To design and implement a compiler extension that enforces firmware update security invariants at compile time, ensuring firmware installation code is generated only when all required security checks are present.