Update Logic Specification

Dhruv Sunil Bhatia
24CSB0A19
CSE - A

Q119 - Secure OTA Update Compiler

1 Overview

Firmware update logic refers to all code segments responsible for receiving, validating, and installing firmware images on an embedded or IoT device.

2 Scope of Update Logic

This includes functions that perform:

- Cryptographic signature verification
- Firmware version checks and rollback prevention
- Trusted source validation
- Firmware installation procedures

3 Update Logic Identification

Update logic is identified based on the presence of:

- Firmware installation calls (e.g., `install_firmware`, `apply_update`)
- Cryptographic verification functions (e.g., `verify_signature`)
- Version comparison or rollback prevention logic
- Network or storage interfaces used to retrieve firmware images

The compiler assumes that any function directly or indirectly invoking firmware installation APIs is part of the update logic.

4 Security Invariant Enforcement

All control-flow paths leading to firmware installation must satisfy mandatory security invariants enforced by the compiler.

5 Out of Scope

The compiler does not enforce:

- Runtime security policies such as secure boot
- Hardware trust anchors
- Cryptographic key provisioning

The compiler's responsibility is limited to static analysis and compile-time enforcement of firmware update security correctness.