Initial Threat Overview

Dhruv Sunil Bhatia
24CSB0A19
CSE - A

Q119 - Secure OTA Update Compiler

Threats Addressed

Threat 1: Malicious Firmware Installation

An attacker attempts to install tampered or unauthorized firmware if update authenticity is not verified.

Impact:

- Device compromise
- Malware installation
- Loss of control over device behavior

Compiler Enforcement: Rejects update logic where firmware installation is reachable without signature verification.

Threat 2: Rollback Attack (Firmware Downgrade)

An attacker forces installation of an older but authentic firmware version containing known vulnerabilities.

Impact:

- Reintroduction of patched vulnerabilities
- Exploitation of known CVEs

Compiler Enforcement: Rejects update logic that does not enforce version monotonicity before installation.

Threat 3: Unauthorized Update Source

Firmware updates originate from spoofed or attacker-controlled sources if origin trust is not validated.

Impact:

- Malicious firmware delivery

- Integrity and trust failure

Compiler Enforcement: Rejects update logic where trusted source validation is missing or bypassable.

Threat 4: Information Leakage Through Debug Logs

Sensitive update information may be exposed through logs.

Impact:

- Exposure of firmware metadata
- Easier targeting of vulnerable firmware

Compiler Enforcement: Rejects update logic containing unsafe logging within the update routine.

Threat 5: Weak Cryptographic Validation

Use of weak cryptographic primitives in firmware validation.

Impact:

- Integrity verification bypass
- Spoofed firmware updates

Compiler Enforcement: Rejects update routines invoking banned weak cryptographic APIs.