Error Conditions for Each Violation

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

---

1 Overview

This document defines the specific compile-time error conditions triggered when security invariants are violated within the `updateFirmware()` routine.

2 Verification Dominance Violation

Error Message:
Firmware installation reachable without prior signature verification.

Trigger Condition:
Raised when `install(pkg)` is not dominated by `verify_signature(pkg)` in the Control Flow Graph.

3 Rollback Protection Violation

Error Message:
Firmware installation without version monotonicity check.

Trigger Condition:
Raised when no condition enforcing

$$\texttt{pkg->version} > \texttt{current\_version()}$$

guards the `install(pkg)` call.

4 Trusted Source Violation

Error Message:
Firmware installation without trusted source validation.

Trigger Condition:
Raised when `source_is_trusted(pkg)` does not dominate the `install(pkg)` call or is absent from its controlling predicate.

5 Logging Safety Violation

Error Message:
Sensitive logging detected inside updateFirmware().

Trigger Condition:
Raised when logging APIs (e.g., `printf`, `fprintf`, `log`, `syslog`) are invoked within `updateFirmware()`.

6 Weak Crypto Violation

Error Message:
Weak cryptographic API usage inside updateFirmware().

Trigger Condition:
Raised when banned cryptographic functions such as `MD5`, `SHA1`, or `rand` are detected within the update logic.