Aggiornamenti OTA con Secure-Boot e Flash encryption

UniVR - Dipartimento di Informatica

Fabio Irimie

Tesi di laurea 2025/2026

Indice

1 Introduzione **2**

2 Cenni teorici **2**

2.1 Aggiornamenti OTA (Over The Air) 2

2.1.1 Partizione OTA Data 3

2.1.2 App rollback 3

1 Introduzione

Questo progetto consiste nell'implementazione di un sistema che permetta di aggiornare il firmware dell'ESP32 da remoto (Over The Air) tramite Wi-Fi. L'obiettivo principale è quello di attivare le funzionalità di sicurezza del microcontrollore in modo da proteggere il dispositivo da accessi non autorizzati. Le funzionalità di sicurezza includono:

- **Secure OTA**: Garantisce che il nuovo firmware sia autentico e non compromesso
- **Secure Boot**: Impedisce l'esecuzione di firmware non autorizzato
- **Flash Encryption**: Protegge i dati memorizzati nella memoria flash del dispositivo

2 Cenni teorici

2.1 Aggiornamenti OTA (Over The Air)

Gli aggiornamenti OTA permettono di aggiornare il firmware del dispositivo durante la sua normale esecuzione, senza la necessità di collegarlo fisicamente a un computer. Le modalità di aggiornamento si distinguono in base alla vulnerabilità del sistema:

- **Modalità sicura**: L'aggiornamento di alcune partizioni è resiliente, cioè garantisce l'operabilità del dispositivo anche in caso di perdita di alimentazione o di errore durante l'aggiornamento. Solo il seguente tipo di partizione supporta la modalità sicura:
  - **Application**: OTA configura la partition table in modo da avere due partizioni per l'aggiornamento (`ota_0` e `ota_1`) e una partizione per lo stato di boot (`ota_data`). Durante l'aggiornamento il nuovo firmware viene scritto nella partizione OTA attualmente non selezionata per il boot. Una volta completato l'aggiornamento, la partizione `ota_data` viene aggiornata per indicare che la partizione OTA appena scritta deve essere utilizzata al boot successivo. Se la partizione `ota_data` non contiene alcun dato il dispositivo esegue il boot dalla partizione `factory`.

    La partition table con due partizioni OTA è la seguente:

    ```
    # ESP-IDF Partition Table
    # Name,   Type, SubType, Offset,  Size, Flags
    nvs,      data, nvs,     0x9000,  0x4000,
    otadata,  data, ota,     0xd000,  0x2000,
    phy_init, data, phy,     0xf000,  0x1000,
    factory,  app,  factory, 0x10000,  1M,
    ota_0,    app,  ota_0,   0x110000, 1M,
    ota_1,    app,  ota_1,   0x210000, 1M,

    ```

- **Modalità non sicura**: L'aggiornamento di alcune partizioni è vulnerabile, cioè in caso di perdita di alimentazione o di errore durante l'aggiornamento il dispositivo potrebbe non essere più operabile. Una partizione

temporanea riceve i dati della nuova immagine e, una volta completato il trasferimento, l'immagine viene copiata nella partizione di destinazione. Se l'operazione di copia viene interrotta potrebbero verificarsi problemi di boot. Le partizioni che supportano la modalità non sicura sono:

- **Bootloader**
- **Partition Table**
- **Partizioni data** (ad esempio NVS, FAT, ecc...)

2.1.1 Partizione OTA Data

Al primo avvio del dispositivo la partizione `ota_data` deve essere vuota (tutti i byte a 0xFF) in modo da far eseguire il boot dal'applicazione nella partizione `factory`. Se l'applicazione in `factory` non è presente viene eseguito il boot della prima partizione OTA disponibile (di solito `ota_0`).

Dopo il primo aggiornamento OTA, la partizione `ota_data` viene aggiornata per indicare quale partizione OTA deve essere utilizzata al successivo boot. La dimensione di `ota_data` è di due settori (0x2000 bytes = 8192 bytes) in modo da evitare errori mentre si scrive la partizione. I due settori sono cancellati indipendentemente e scritti con gli stessi dati. In questo modo se i dati dei due settori non coincidono viene usato un counter per determinare quale settore è stato scritto più recentemente.

2.1.2 App rollback

L'obiettivo dell'app rollback è quello di tenere il funzionante il dispositivo dopo un aggiornamento e permette di tornare alla versione precedente del firmware se la nuova versione non funziona correttamente (solo le partizioni OTA possono effettuare il rollback). Dopo un aggiornamento OTA con rollback attivo si hanno le seguenti possibilità:

- Se l'app funziona bene `esp_ota_mark_app_valid_cancel_rollback()` imposta lo stato dell'applicazione a `ESP_OTA_IMG_VALID`.
- Se l'app non funziona correttamente il dispositivo esegue il rollback alla versione precedente e `esp_ota_mark_app_invalid_rollback()` imposta lo stato dell'applicazione a `ESP_OTA_IMG_INVALID`.
- Se l'impostazione `CONFIG_BOOTLOADER_APP_ROLLBACK_ENABLE` è abilitata e viene effettuato un reset, allora viene effettuato un rollback senza chiamare nessuna funzione nell'applicazione. Questa opzione permette di intercettare la prima esecuzione di una nuova applicazione per confermare che funzioni correttamente.

Gli stati che controllano il processo di selezione dell'applicazione sono:

Stato	Restrizioni sulla nuova app
ESP_OTA_IMG_VALID	Nessuna restrizione. Verrà selezionata
ESP_OTA_IMG_UNDEFINED	Nessuna restrizione. Verrà selezionata
ESP_OTA_IMG_INVALID	Non verrà selezionata
ESP_OTA_IMG_ABORTED	Non verrà selezionata
ESP_OTA_IMG_NEW	Se l'opzione CONFIG_BOOTLOADER_APP_ROLLBACK_ENABLE è abilitata, l'app verrà selezionata solo una volta. Nel bootloader lo stato viene subito impostato a ESP_OTA_IMG_PENDING_VERIFY.
ESP_OTA_IMG_PENDING_VERIFY	Se l'opzione CONFIG_BOOTLOADER_APP_ROLLBACK_ENABLE è abilitata, l'app non verrà selezionata. Nel bootloader lo stato viene impostato a ESP_OTA_IMG_ABORTED.

L'impostazione di questi stati avviene nei seguenti casi:

- ESP_OTA_IMG_VALID: impostato dalla funzione esp_ota_mark_app_valid_cancel_rollback().
- ESP_OTA_IMG_UNDEFINED: impostato dalla funzione esp_ota_set_boot_partition() se l'impostazione CONFIG_BOOTLOADER_APP_ROLLBACK_ENABLE è disabilitata.
- ESP_OTA_IMG_NEW: impostato dalla funzione esp_ota_set_boot_partition() se l'impostazione CONFIG_BOOTLOADER_APP_ROLLBACK_ENABLE è abilitata.
- ESP_OTA_IMG_INVALID: impostato dalla funzione esp_ota_mark_app_invalid_rollback() o esp_ota_mark_app_invalid_rollback_and_reboot().
- ESP_OTA_IMG_ABORTED: impostato se l'operabilità dell'applicazione non è stata confermata e avviene un reboot quando l'impostazione CONFIG_BOOTLOADER_APP_ROLLBACK_ENABLE è abilitata.
- ESP_OTA_IMG_PENDING_VERIFY: impostato nel bootloader se l'impostazione CONFIG_BOOTLOADER_APP_ROLLBACK_ENABLE è abilitata e l'applicazione selezionata è nello stato ESP_OTA_IMG_NEW.