Cloud-based OTA On Trusted Execution Environment

DP Group 33: Alex Wei, Chenyi (Alice) Xu, Fengqi Zhang, Zhanyue Zhang
Supervisor: Prof. Zeljko Zilic

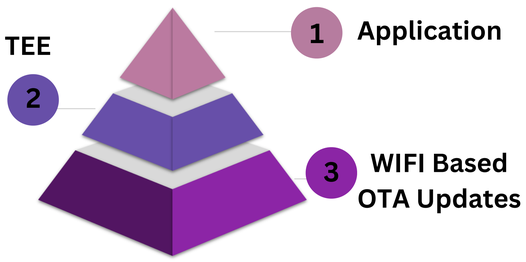
Motivation

The team worked together in ECSE 444 where we discovered a common interest toward microcontroller related topic. After discussion with our supervisor, we decided to pursue a TEE-supported OTA update for STM32H5 MCU.

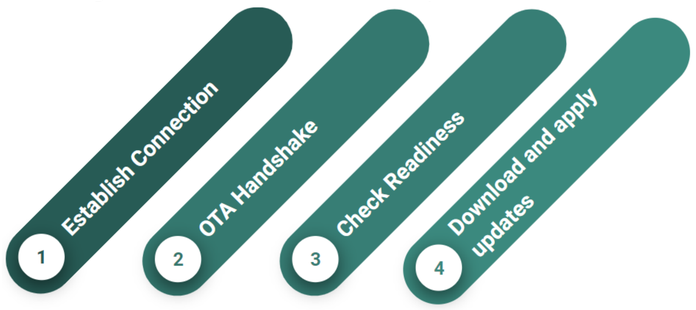
Objective

To develop an AI Interaction application that use the system with Trusted Execution Environment (TEE) supported Over-the-air Updates (OTA).

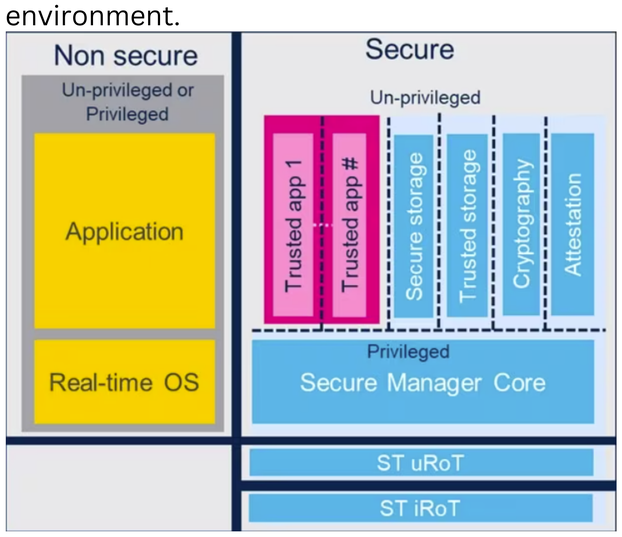
Introduction



Base Layer -> Firmware remote Update Mechniams



Middle Layer -> A secure area in the processor of a connected device that ensures sensitive data is stored and processed within a trusted and isolated environment.



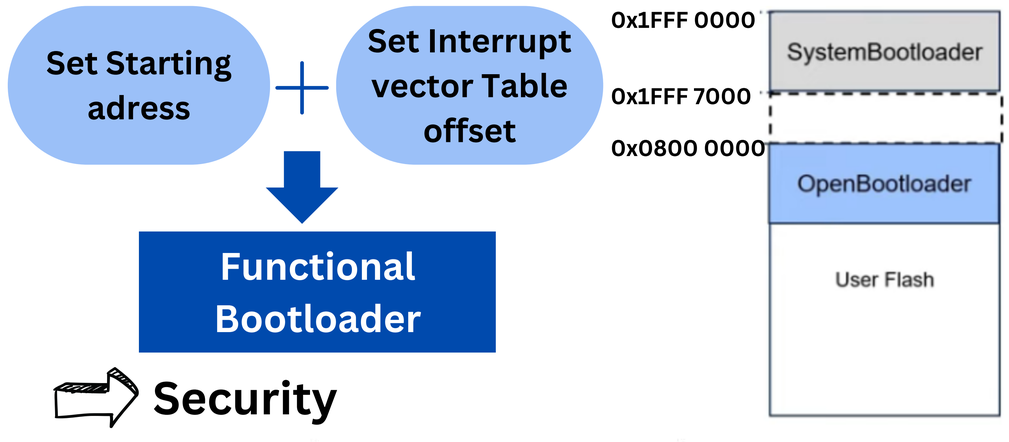
Top Layer -> A visual representation of System

Design and Application

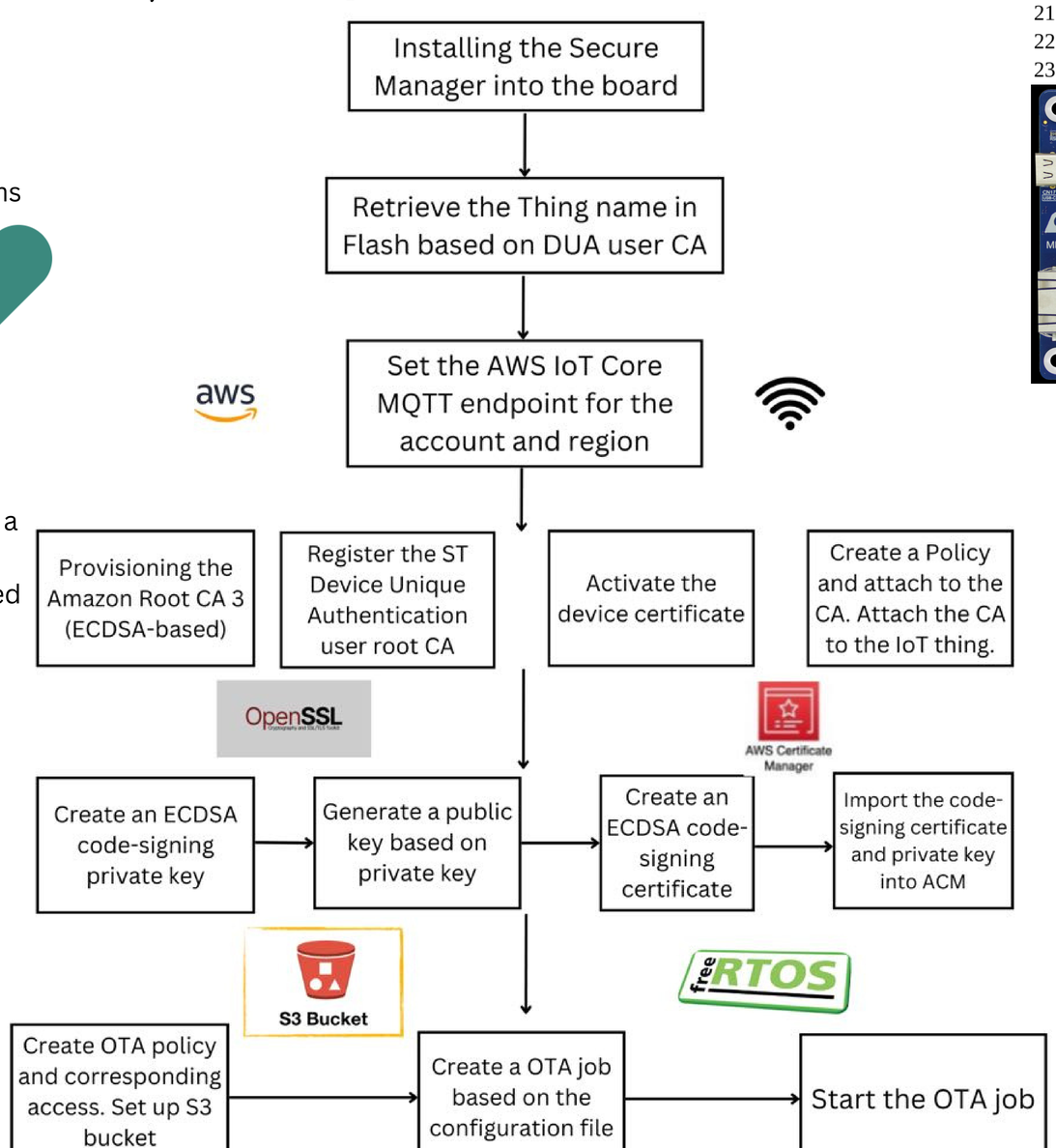
OTA

Step 1: Transfer files via WIFI

Step 2: Using Bootloader to Write Files Into Flash



Security



Application

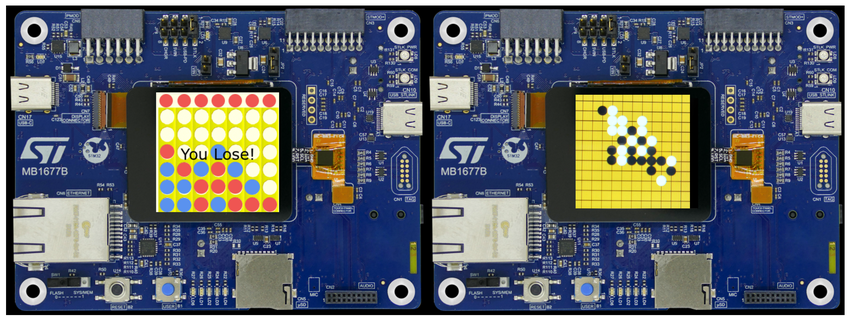
With previously deisgned system, we implemented *Connect Four* and *Gomoku* directly playable on H5 touchscreen. The games can be updated remotely.

Core methodology: *Minimax algorithm*

```
01: IF (depth = 0 OR depth ≥ remaining unoccupied)
02:    FOR (every linear n cells)
03:       score += its score
04:    ENDFOR and RETURN score
05: END IF

06: IF (opponent wins)
07:    RETURN extremum // COMP: INT_MIN; USER: INT_MAX
08: ENDIF

09: FOR (every cell)          // α-β pruning and optimizations omitted
10:    IF (unoccupied AND near occupied)
11:       copy ← current board
12:       score ← MINIMAX(copy, depth-1, opponent)
13:       IF (player is COMP)
14:          IF (score > old score)
15:             update score and record current cell
16:          ENDIF
17:       ELSE                // player is USER
18:          IF (score < old score)
19:             update score and record current cell
20:          ENDIF
21:       ENDIF
22:    ENDIF
23: ENDFOR
```



Challenge

- The 1.54'' onaboard touchscreen is too small, therefore compromising the touch accuracy.
- Only one board available.
- The OTA update is not quite user friendly.
- Firmware upgrade file has size limit.

Conclusion

The team was able to design an AI interaction application that can be securely updated remotely.

Acknowledgement

We would like to express our deepest gratitude toward Professor Zilic, Shaluo Wu, and Guanyi Heng for supports and guidance throughout the project.