TrustZone Face Recognition

Shivam Shekhar (ss6960)

…

Ritwik Goel (rg3546)

Estimated Total Hours: 12

Plans (Past Week)

1. Develop the face recognition algorithm in OP-TEE: Choose a face recognition algorithm and implement it within OP-TEE. Focus on modular and efficient code design. Implement communication between the Android app and OP-TEE: Establish a secure communication channel between the app and OP-TEE. Use OP-TEE's inter-process communication (IPC) mechanisms.

2. Design a secure database for storing face recognition data: Choose a secure database solution (e.g., SQLite with encryption). Plan the database schema and encryption mechanisms for storing facial data securely.

What Actually Happened

Work completed:

- Got the OP-TEE Setup and Hello World Application working.
- Researched more into how SMC calls would work and help us getting the database work.

Major challenges+roadblocks: Working with SMC Calls and Integration of mobile application

Attribution: Integration with mobile app

Plans (Next Week)

- Start writing Trusted Application.
- Started coding the facial recognition algorithm and compare the overhead.
- Start integrating the mobile application and receive image data.

Summary/Overall Progress

- Worked on getting the OP-TEE Hello World application running.
- Researched how we can leverage Secure Storage APIs for secure storage.
- Chose the facial recognition algorithm.

Normal World

```
#
#
# optee_example_hello_world
Invoking TA to increment 42
TA incremented value to 43
# ▯
```

Secure World

```
I/TA: Hello World!
D/TA:  inc_value:105 has been called
I/TA: Got value: 42 from NW
I/TA: Increase value to: 43
D/TC:? 0 tee_ta_close_session:512 csess 0xd56fa7f0 id 1
D/TC:? 0 tee_ta_close_session:531 Destroy session
I/TA: Goodbye!
D/TA:  TA_DestroyEntryPoint:50 has been called
```