OP-TEE Hello World TA Debug & Modification Report (Updated)

Setup Overview

Board / OS: Raspberry Pi 3
TEE Environment: OP-TEE (REE-FS secure storage)
TA: Modified `hello_world` Trusted Application
Objective:
Modify Hello World TA to **store and retrieve a file** (`abc.bin`) securely inside the TEE.

Implementation Summary

New TA Commands Added

Two secure storage commands introduced:

- **STORE_BLOB:** Writes data to secure storage
- **LOAD_BLOB:** Reads stored data and verifies integrity

Secure Storage APIs used:

- `TEE_CreatePersistentObject()`
- `TEE_WriteObjectData()`
- `TEE_OpenPersistentObject()`
- `TEE_ReadObjectData()`

Host-Side Enhancements

Host application (`main.c`) updated to:

1. Send `"Hello Secure World!"` → `"abc.bin"`
2. Read back the file from secure storage
3. Verify contents
4. Use `TEEC_MEMREF_TEMP_INPUT/OUTPUT` for buffer transfer

Program Flow

Step	Action	Description
1	`TEEC_InitializeContext()`	Connect to TEE
2	`TEEC_OpenSession()`	Start TA (prints *Hello World!*)
3	`TEEC_InvokeCommand(INC_VALUE)`	Increment test value (42 → 43)
4	`TEEC_InvokeCommand(STORE_BLOB)`	Store data securely
5	`TEEC_InvokeCommand(LOAD_BLOB)`	Retrieve and verify data
6	`TEEC_CloseSession()`	Graceful TA shutdown

Errors and Investigation Timeline

#	Error / Symptom	Root Cause (Suspected / Confirmed)	Action Taken	Result

1	`TA panicked with code 0xffff0001` right after increment	Internal crash inside TA (usually due to param mismatch or binary mismatch)	Rechecked `paramTypes` on both sides, verified correct macros (`VALUE_INOUT`, `MEMREF_INPUT` etc.)	Panic persists
2	`STORE_BLOB failed: 0xffff3024` (origin 0x3)	Panic killed TA; session invalid before store command	Dependent on first error	Panic persists
3	Confusion about `/data/tee` mount (tmpfs vs ext4)	Misunderstanding of REE-FS secure storage	Confirmed tmpfs is fine; OP-TEE handles storage internally(mounted on root 16GB)	Not related
4	“Chunk size” uncertainty	Suspected need to specify data chunk sizes	Clarified chunking handled internally by OP-TEE kernel	Not related
5	`TA not found` and `failed to find an OP-TEE supplicant device` in `teec.log`	Supplicant or driver not initialized / TA missing	Restarted `tee-supplicant`, ensured `/dev/tee*` exists	Supplicant running
6	Duplicate TA files in `/lib` and `/lib64`	Host modified `/lib`, system loaded from `/lib64`	Verified with `strace` & `dmesg`; replaced correct `.ta` in `/lib64/optee_armtz/`	Path confirmed, but panic persists
7	Persistent Panic	Possible causes: memory corruption, wrong build flags, or invalid TA ABI	Rebuilt TA cleanly (`make clean && make`), verified UUID/header match	Still not resolved