MCS: Secure Execution Environments 2023-2024

Practical Assignment:
SGX project (tamper-proof digital vault)

April 5, 2024 Due date: no date

Changelog

- v1.0 - Initial version (2024).

1 Introduction

The goal of this project is to implement a “"tamper-proof digital vault,” or TPDV for short, on an SGX enclave. The TPDV will store digital assets and will be write once, without any possibility of deleting information. A malicious operator may destroy the entire TPDV, but it may not change anything already stored in it without that being detected.

2 Work to be done

Write an application that implements the TPDV (unsafe part that interacts with the SGX enclave, and safe part that implements the TPDV). Your applications should have the following facilities:

- Create a new TPDV file. Arguments: name of the TPDV, file name where the sealed data will be stored, password, and the name of the creator of the TPDV.
- Add a digital asset (a binary file) to the TPDV. Arguments: file name.
- List all digital assets stored in the TPDV (insertion order, file name, size).
- Extract one (or perhaps all) digital assets.
- Compare a given message digest with the message digest of a digital asset stored in the TPDV.
- Password change
- Clone the TPDV contents, perhaps to another version of the TPDV SGX code and to another computer. This will requires special authentication. A manufacturer (the maker of the software) public key should be stored in the SGX enclave, and to clone the TPDV the operator has to demonstrate that he/she is in possession of the private key.

All of these facilities always require a password. Or course, the TPDV file name has also to be given.

3 Suggested implementation details

To store the TPDV data seal it and save it in a file. Store everything sequentially in an unsigned char array. Use a fixed size header to store the TPDV name, password, and number of stored digital assets. Consider placing a 4-byte nonce at the very start (can be a simplified message digest of the rest of the information), to avoid differential attacks that attempt to recover the sealing key (that's very likely overkill, but is costs almost nothing to implement — better safe than sorry). For each new digital asset, append its name and size and then its contents. The TPDV software should have a version string. To test the clone operation, duplicate your SGX code and change the version string of the copy; then load both enclaves in the same application (could be in a different application, but then you would have to implement some form of inter-process communication).