Chapter 1

Implementation

1.1 Attestation TA

- Trusted Application
  - Hash NW memory pages
  - Store reference values in secure memory
  - Make comparison and notify user
- NW OS interaction
  - Retrieve address of memory page
  - Translate into physical address
  - Provide datastructures to TA
- Extensions
  - Notify user using trusted IO
  - Decrease dependency on NW OS
  - Attest more than just code pages (data structures, invariants,...)

The attestation is mainly implemented in a Trusted Application. This is done to allow the Secure World to store measurements in the secure memory and have access to the Normal World memory. Ideally the TA doesn't need to rely on the NW OS (Linux) for the memory addresses but this is the starting point for the implementation.