Chapter 1

Discussion

Solution overview

Reproduction of the solution provided in the paper is the starting point of this thesis.

Extensions on this reproduced solution are necessary because the original solution does not achieve all goals.

Shortcomings

Attacker possibilities that are not accounted for are still present, the security measures taken in the solution are not adequate for the wide variety of attacks that it claimed to protect against.

Desired guarantees the solution should be able to provide are not entirely met.

Positives

Code for this thesis is made available as open source code to make it easier to reproduce the experiments and continue work on this research topic by other researchers.

Thorough comparison has been executed on the provided solution and solutions of related work to give an overview of what direction is most promising to achieve the security goals.