Winston Shine

ILC Database Theory/Security

Week 3 Progress Report

2/8/2023

My goal is to study Database Theories and Security through the book Translucent Databases. Some additional smaller goals I am trying to accomplish are doing my work this quarter with docker containers and If time allows study a bit about document-oriented databases.

This week I read about Fuzzy One-Way Functions. The difference between one-way functions and fuzzy one way functions is that fuzzy one way functions will have very little change in output when there’s only a slight change in input, where as standard one way functions output changes drastically with even the slightest change in input.

The type of fuzzy one-way function that I was able to understand the most is the block type. In this type of function the data would be separated into blocks and each block would be hashed separately. That way if one small change was made only the output of the block its in would change rather then overall hash. I think it’s important to note that standard hash functions also separate the input into blocks, but the calculation of one block is used to calculate the next block as well rather than each block’s calculations being independent.

The type of fuzzy one-way function I understood the least was the statistical function. This type would use various statistics, such as the occurrence of a specific letter or group of letters, in order to calculate the hash. I still don’t quite understand how those statistics are actually used to generate a hash, or why this method would result in little change to the output when small changes are made to the input.

Next week I plan to re-read the part of chapter 4 about statistical hashes and then move on to Chapter 5 and 6 titled ‘Translucent XML’ and ‘Quantization’.