Winston Shine

ILC Database Theory/Security

Week 2 Progress Report

1/25/2022

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.

In week 2 I started reading chapter 2 titled ‘One-Way Functions’. Unfortunately I did not get around to putting these ideas in practice but I did plan out some ideas to try. The chapter introduces one way hash algorithms, Secret key functions, keying hash functions (from what I understood this is something we talked about last quarter but we referred to it as ‘salting’). I had heard of some of the hash functions the book talked about but not all, for example I had not heard of Tiger which is similar to SHA but has some more complexity to it.

I think I had the most difficulty this week in 2 different areas. One was the when the book described using public-key encryption as one way functions with trapdoors. To me these two seem very different and I struggle to see a use case for this. The second one was the sample java applet provided to demonstrate scrambling data on a client side application.

For week three I plan to recreate the applet provided in chapter 2 in order to understand it, and try out MySQL functions for data scrambling including: MD5, ENCODE, DECODE, ENCRYPT. Then I will read chapters 3 & 4. I don’t currently have any exercises planned out but I will decide on something once I finish the reading.