Week 10 Attila Meeting notes: Composed by SR

***Action Items:***

- Complete Final Draft of Design Document by Thursday to Submit to Attila

- Meeting with TA Andrew Wednesday

- Meeting with team Friday (Also Sunday?) to complete Progress Report Paper/Video

- Final Week to Update OneNote for Blog Posts.

***Topics of discussion:***

- Design Document

- Timeline for Winter/Spring Term

- Thoughts about the Capstone Process.

***Notes on Design Document:***

**AES CTR**: Why is it parallelizable? (Research)

-High granularity

Comparing Throttle Speeds: Network VS Crypto

-Change the name of “Dumb Server” to “Storage Only Service” 🡪 Very important to security, server cannot communicate on its own.

- Fetch relevant part of data structure

**Forward Security:**

- Prevents many trivial attacks

- Simple yet effective

Impact on network on performance

-**Very Fast** Vs **Very Slow (**Wifi From home is slow Vs Very fast network)

Performance Difference:

128 Bit Block AES VS 1 Bit Block

What block size to us? Depends on network speed to determine where the Throttling is in the system.

**Optimization**: Iterative Process, Improve over time

**Spiral Model** for implementation?