**Class Notes**

**September 2nd, 2021**

Video Response Tips:

1.) Reference links go to the bottom of the slide

2.) Fast talking is hard to understand

3.) Check the video examples for how to explain the harder subjects

4.) Go into deeper detail when explaining the harder part of the question

**Passwords**

**Creation Policy:**

* Length (Min & Max)
* Special Chair
* Blacklist of Words (Must keep updated)
* Numbers
* Uppercase & Lowercase
* No reuse of passwords
* No sequences

Makes passwords less predictable

Password Hashes:

Rainbow Table:

Online attack: Brute force with known passwords

Offline attack: List of password hashes that you. Take a list of common passwords, throw them into the password hash function, and compare the hashes that come out to what you have.

Plaintext + SALT + Cost Factor -> FUNCTION -> Hash Value

The SALT adds extra data to encrypt the hash in case two people sue the same password, the hash will not be the same.

HASH functions are one way, meaning you cant turn the hash back into the plaintext version.

HASH functions always put out the same length of HASH, regardless of the input

Attackers Perspective:

* Dictionary Attacks (Use list of most common words in passwords)
* Mangling Rules (Transformations that we would expect in the dictionary. Ex: apple -> 4pple

Information Entropy: Created to understand the size of messages that needed to be transmitted. It’s used to measure the amount of uncertainty/information that individual characters contain

H(x) = SUM 0 -> N p(Xi) \* log base 2 P(Xi)

Example: A Fair Coin

= H (0.5) log2 ( 0.5)

= T (0.5) log2 (0.5)

= 1 bit of entropy in each flip, each additional flip adds another bit of entropy

Entropy does not take into account passwords that are easy to guess.