**HOMEWORK 10**

A short summary on “An Administrator's Guide to Internet Password Research”

What’s new to me?

- Salts are similar to nonce.

- Account categories:

• don’t-care accounts (unlocked doors).

• low-consequence accounts (latched garden doors).

• medium-consequence accounts.

• high-consequence accounts (essential/critical).

• ultra-sensitive accounts (beyond passwords).

- For an offline attack to improve an attacker’s lot over guessing online, three conditions must hold.

i) He must gain access to the system (or a backup) to get to the stored password file.

ii) He must go undetected in gaining password file access.

iii) The file must be properly both salted and hashed.

- If the password file is accessed, and the access goes undetected, then:

i) The file is plaintext.

ii) The file is hashed but unsalted.

iii) The file is both unsalted and hashed.

iv) The file has been reversibly encrypted.

- Concept of Rainbow table.

What I thought was important?

A simple blacklist offers excellent protection against breadth-first online attacks and good improvement for depth-first online attacks, but not much protection against offline attacks.

Login attempts can be restricted to devices a server has previously associated with successful logins for a given username, e.g., by browser cookies or IP address; login attempts from other devices (assumed to be potential online guessing machines) require both a password and a correctly answered CAPTCHA.

After reading this paper, I realized how insecure all my passwords are. For instance, having the login username as email id and the same password is such a major threat. If a hacker breaks one of the passwords, he can essentially hack into all the accounts which have the same password.

Also, I was the person who used the first letter of the password in Uppercase and ending with a special character, making the password itself vulnerable. Time to reset all my passwords!

Questions?

None I could think of.