Scott Christensen

10/26/16

C.S. 465

Homework #10: Passwords

- Discuss the three primary things you learned from your reading.

1. I learned that there is a number of guesses a password should withstand to most optimally withstand both online and offline attacks, without expending too much effort by comparison. This region, referred to as the online-offline chasm, represents 8 orders of magnitude and in this gap, incrementally increasing the number of guesses the password will survive delivers little or no security benefit. This is mostly because offline attacks do not depreciate in effectiveness till about log10 14 attacks.

2. Even though there are many ways to store and encrypt passwords, the paper claimed that salted hashes are a preferred means to store passwords because they not only are based off of a very secure algorithm, but also because an attacker who has access to the password file, and exports it undetected, still faces a computationally expensive offline attack. While there are other algorithms that are more secure, like passwords that are reversibly hashed, it can be easy to get the password should the decryption key be leaked.

3. I learned about the existence of Blacklists, collections of common choice, weak passwords and that they are in fact stronger than having each user follow contain criteria. These passwords seek to eliminate words, number, or phrases usually seen together in pop culture and if someone uses them on popular sites, they are guaranteed to be at high vulnerability. Maintaining a up to date Blacklist can be difficult though as more elements such as new bands and songs come out but should be maintained to maintain optimal results.

- List the two best questions from your reading that you could bring to discuss in class.

1. The term rainbow table was used a number of times. From the sound of it, it seems to be a list of functions on could use to attack passwords that were not salted or generally weak passwords, but gave no indication as to what they truly were or what these functions are. So, what is in a rainbow table?

2. The article explained that the number one best way to ensure password security is to simply prevent and password file from ever being leaked. In today's world, this may be impossible to guarantee all the time, but I would like to know how this can be done at all, if it's a common goal among parties.