Patrick Austin

9/21/2017

CS 450 Homework 1

1. A strategy that uses salt in conjunction with a hash function can protect user passwords even when both the salt and the password file, containing the password’s hash, are publicly available. The attacker can pre-calculate hashes for common passwords into a rainbow table, but that table is useless for passwords that have been concatenated with the salt and then hashed. Knowing the salt value and the hash, the attacker can attempt to calculate a salt-specific rainbow table, but this amounts to a brute-force attack since nothing has been pre-calculated. As the next problem shows, this is likely to be prohibitively time-consuming for a strong password. In this way the password is defended by the salt strategy, even when the salt and hash are available to an attacker.

2. If there are 95 possible characters and passwords are 10 characters in length, then there are 9510 possible passwords. If a cracker can crack 6.4 x 106 passwords each second, then it will take 9.355 x 1012 seconds, or about 300,000 years, to crack every password.

3. -Password: ~m32(yJEF%q.i] Strength: 327 centuries

-Password: =$![|!uFKe;=v)&6 Strength: 3261 centuries

-Password: :R1tpHGw$5K1mz=qvXl{ Strength: 10,000+ centuries

-Password: "mBeGW2zY2y%x]u Strength: 3261 centuries

-Password: ~7I<G,v6'<aj Strength: 4 centuries