Nikkolas Irwin

University of Nevada Reno

CS 450 – Fundamentals of Integrated Computer Security

Ansari Business Building 106

Homework 1

1. Salt-Strategy

The salt strategy can be used to protect user passwords even when the salt and password file are publicly available because the salt is added to the hashing process and this allows the stored password to have an increased complexity without increasing the user-requirements. The salt-strategy allows a user's password to be protected from different attack vectors such as rainbow-tables, dictionary, and brute-force attacks. The reason why a salt-strategy works is because it provides a fixed-length cryptographically strong random value which is added to the input of the hash function. Although the hash function is deterministic (i.e. predictable), the addition of the salt-value makes the output much harder to crack from a possible attacker. For example, we could store the username, the salt value, and the hash in cleartext in a database which makes these attributes publicly available so that we can use them to verify logins. Storing these attributes in this manner is acceptable because even if an attacker can crack one password, cracking every other user's password would not be practical since each input is salted with unique random data and the attacker would have to computer a rainbow table for each user's hash. This bottleneck makes the salt-strategy viable and allows data breaches to be detected before they become widespread.

2. Password Testing

Number of Characters ^ Password Length = 95^{10} = $5.987*10^{19}$ passwords

Possible Passwords / Encryption Rate = $5.987*10^{19}$ passwords / $6.4*10^{6}$ passwords per second

= $9.355*10^{12}$ seconds

$9.355*10^{12}$ seconds / 60 seconds per minute / 60 minutes per hour / 24 hours per day

= ~ 296,653 years

In summary, it would take an estimated 296,653 years to exhaustively test all possible passwords on a UNIX system.

3. Strong Passwords

1. 1Tb7%2jnM.!
    a. 33 Years to be brute forced, strength = 10/10

2. nJH&*.posy^^MZ$
    a. 3261 Centuries to be brute forced, strength = 10/10
3. 19JHBKD@@312*&
    a. 327 Centuries to be brute forced, strength = 10/10
4. Ab*7ty2EFg%$1
    a. 33 Centuries to be brute forced, strength = 10/10
5. &Il1mJph$##.9832gHb
    a. 10,000+ Centuries to be brute forced, strength = 10/10