Information Assurance: Homework 5 Answers and Comments

Not graded

1. A system allows the user to choose a password with a length of one to ten characters inclusive. Assume that 15,000 passwords can be tested per second. The system administrators want to expire passwords once they have a probability of 0.10 of being guessed. Determine the expected time to meet this probability under each of the following conditions.
    a. Password characters must be digits ("0" through "9").

1/10 = Number of Passwords explored/ Total number of passwords

*Number of passwords explored = 15,000*T, where T is the number of seconds running*

Total number of passwords = N = sum_i(1, 10, 10^i) = 11,111,111,110

*0.1 = 15,000*T/N*

*N*0.1/15,000 = T = 74074 seconds = 20.5 hours*

   b. Password characters may be capital letters ("A" through "Z") and numerics ("0" through "9").

N = sum_i(1, 10, 36^i) = 3760620109779060 passwords

T = 25070800731.8604 seconds = 794 to 795 years

   c. 12 bits of salt are added for both a and b.

Multiple the results of a and b by 4096. With the salt, the attacker should try all 4096 hash algorithms to see if any of the variants are represented in the password file. The salts are stored in the password file, so the attacker can note that only k salts are used in this particular file and only test those hash variants, but at worst it will increase his work by a factor of 4096.

Some of you noted that salt does not deter the attacker when attacking a specific user offline or attacking the system online.

2. Try running the John the Ripper password cracking program http://www.openwall.com/john/. You should be able to install it local to your environment for an unprivileged account. Obtain a password file from

http://www.cs.uiuc.edu/class/fa07/cs461/class07-passwd This file contains nine accounts with passwords from a linux system. At least one password should be cracked very easily. If you have access to a private system, try running the program for a while longer to see if you get more passwords cracked. Submit the account names and passwords that you crack. As long as you get the quickly cracked passwords, you will get full credit.

Alice: Alice.
Bob: bobbob
Carol: carol77
dave: 10-10-72
ellen: qghrlz
grace: maclusbar
fred: class-test
helga: cs461
ivan: xylophone

Everyone got Alice and Carol. Many people got Helga's password. Six of you got passwords for Alice, Carol, Helga, and Ivan.

3. An organization implements a biometric authentication system. All employees register their fingerprints, and the organization stores the resulting templates on a central server. Eve hacks the server and gains access to the template. What harm can occur from this breech? How does it compare to hacked passwords?

The template is not an exact copy of the fingerprint. Rather it is a measure of some key features of the registered fingerprint. Eve could use this information to generate a fingerprint facsimile. Eve knows exactly what the reader is looking for. In theory she could manufacture a fingerprint measurement sequence that matches what the reader is looking for.

Of course, we leave fingerprints all over the place. So if Eve wants to create a copy of someones fingerprint, she could get that information without hacking into the server. See "Impact of Artificial "Gummy" Fingers on Fingerprint Systems" http://www.lfca.net/Fingerprint-System-Security-Issues.pdf for more information on fooling fingerprint readers. This is not necessarily the case with other biometric measurements like iris scans.

In general stealing the biometric template is worse than having a password hacked. You can change your password. It is more difficult if not impossible to change a physical characteristic.

Some of you noted that once you have a person's fingerprint data, you can correlate every other account owned by this person, even accounts at other organizations as long *as they use the same biometric. Another one of you noted that you need to be physically present to use the hacked biometric, whereas a hacked password can be used over a network connection-- and on the other side of the coin, it can gain you physical access where a password may not (depending on the policy, of course).*

There is ongoing work in the biometric area to verify biometric characteristics while keeping the specifics of the registered biometric data hidden.