Yuvika Nibber

Assignment 7

1. The four means of authenticating a user’s identity are something an individual knows, possesses, static biometrics, dynamic biometrics.
2. The two common techniques used to protect a password file are storing passwords hashes or restricting the user access. Restricting the user access is when the passwords are stored in a password file, gives right to very few people, it is protected by encryption. Using password hashes is storing it as a hash function or value. The password is then compared with the hash value to see the authentication. If they match, it lets the user proceed and then view the file.
3. Password is used for the authentication of the user. Some common techniques for selection or assigning passwords are 1. education the user- tell the user the importance of having a strong password and how they should set their password. They should set a long password as it is hard to guess. 2. Use a computer-generated password as they are hard and long and harder to guess. 3. Run a password cracker program that keeps checking the vulnerability problem. 4. Use the strength checker to see how strong or weak the password is. It also locks the account when there have been multiple attempts.
4. Static Biometric authentication uses facial characteristics- eyes, nose, facial features, fingerprints- finger tips, ridges and furrows, Retina- digital image of the retina, retinal surface of the eyes, Iris etc. Dynamic biometrics uses signature and voice. Handwriting of every person is different, and voice can authenticate a person.
5. A. The password is selected from 4-character combinations out of the 26 characters. So, the total number of combinations are 26^4 = 456976. So, the expected time to get the correct password would be 456976/2 = 228488 sec.

B. The expected time to discover the password is 26\*4 = 104 sec and the expected password time would be 104/2 = 52 sec.

1. The number of passwords that can be generated using the 95 characters with the length of 10 is 95^10 = 6\*10^19. Total time = (6\*10^19)/ (6.4\* 10^6) = 9.4\*10^12 sec. There are 31,536,000 sec in one year. Therefore, the total time is (9.4\*10^12) \*(1/31,546,000 years) = 300,000 years.
2. Salt is found on all UNIX systems that use salt value and hashed passwords. It increases the security of the password. It stops the duplicity of password file. It makes it difficult to guess a password.
3. The salt size and the password being compromised are directly proportional to each other and the security is directly proportional to the user’s size. To make sure a password is secure, the user needs to increase the salts because the user only cracks the hashed password and not the salt.
4. The file that is readable to the public contains the user identifier, the public key, and the private key. The public key can be decrypted and verified using the private key. The public key and private key are needed to perform decryption and are inverse to each other.

B. The attacker can guess the private key by decrypting the public key. They can then encrypt all the public keys within that block and with the same password.

1. A. 1 (k = 1)

1/ N - > k / N

1 – k / N

Probability = (1-(k/N))^D = expected number of zero bits in the hash table.

B. expected number of one bits = 1 - ᵩ

P = (1- ᵩ)^k

C. P = (1- ᵩ)^k

ᵩ = (1-(k/N))^D

ᵩ ~ (e^(-k/n))^D = d^-(kd/n)

P = (1- ᵩ)^k = P ~(1-e^-(kD/N))^K