CSS322 – Quiz 6 Answers

Name: _____

ID: _____ Mark: _____ (out of 6)

Question 1 [2 marks]

Forcing users to use certain types of passwords is one method to make passwords stronger against guesses. Two types of rules for users selecting passwords are: (a) random string; (b) pseudo-random pronounceable string. Explain the difference between them and compare them in terms of strengths against password guessing if the password must be a fixed length.

Answer

A password that is a random string is simply a random set of characters (e.g. selected from a-Z, numbers etc.). For example: oJ6fwmPc. A pseudo-random pronounceable string consists of random characters chosen but with the limitation that the resulting string can be pronounced. This can be achieved using an appropriate combination of vowels and consonants. For example: miGrufeN.

For a fixed length password, a random string is stronger because there are many more possible combinations that the attacker needs to try to guess the password. For example, assume an 8 character password using only the characters a..z. With a random string, there are 26 possible choices for the 1^{st} character, 26 for the 2^{nd} character, ... and 26 for the 8^{th} character, leading to 26^8 (approx. 2×10^{11}) possible combinations. As a simple rule, to create a pseudo random pronounceable string of 8 characters, assume the string must have 3 vowels (choosing pronounceable strings is more complex than this in practice). In English there are 5 vowels and 21 consonants. Therefore for 5 of the 8 characters there are 21 possible choices, and for 3 of the 8 characters there are 5 choices. Hence the number of combinations is: $21^5 \times 5^3$ approx. 5×10^8 which is much less than the random string.

Question 2 [2 marks]

Apart from making passwords harder to guess, give two examples of techniques that can be used to make a system more secure against online password guessing. For each technique also explain a disadvantage of the technique.

Answer

a. Limit the number of incorrect password attempts the user can make before the system is locked. This means the attacker cannot try many possible passwords. The disadvantage is that a malicious user could perform a denial of service attack on the system: make many incorrect password attempts on the accounts of other users, so that the other (normal) users are locked from their account.

b. Introduce a delay between each password attempt. This means it will take longer for an attacker to try many passwords. For example on a computer system the attacker may normally automate the password attempts at a rate of 1000 per second. To try a dictionary of 200,000 passwords

would take 200 seconds (about 3 minutes). However if the system introduces a delay of 1 second between each attempt, then the attacker can only make attempts at 1 per second. To try the dictionary would now take 55 hours. The disadvantage of this is that it may be inconvenient for the normal user when they accidentally enter the wrong password – they have to wait some time before trying again.

c. Log and monitor all password attempts. This means if an attacker is making attempts a user or system administrator will know about the incorrect attempts and can later either attempt to find the attacker or at least warn the user to use a secure password. The disadvantage of this is that it doesn't prevent attacks, only detects them (i.e. an attack is still possible).

Question 3 [2 marks]

a) Two users, A and B, have the certificate of their trusted CA X. Does user A know the public key of X? Explain your answer.

Answer

Yes, A knows the public key of X because the certificate of X contains the public key of X.

b) If user A sends its own certificate to B, explain how B validates the certificate.

Answer

When B receives the certificate of A, B decrypts the signature contained in the certificate using the CA's public key. The resulting answer should be the same as the hash of other parts of the certificate. If they are the same, then the certificate is valid.