Kieren Ng

2/14/18

Homework 4

1A)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Bit 0 | Bit 1 | Bit 2 | Bit 3 | Bit 4 | Bit 5 | Bit 6 | Bit 7 | Bit 8 | Bit 9 |
| 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |

1B)

If bit 9 was chosen, mouse would get rejected as a false positive, because bit 9 was already covered by dog’s hash2.

1C)

If bit 5 was chosen, mouse would be accepted because bit5 hasn’t been chosen before by the other passwords.

3.8.

False match rate is the probability that a system incorrectly matches an input pattern to a non-matching template in a database. (Source: Wikipedia)

False nonmatch rate is the probability that the system fails to detect a match between an input pattern and the matching template in a database. (Source: Wikipedia)

The threshold just changes the probabilities mentioned above, and by increasing one the other decreases, same with the other way around.

3.8

If there isn’t a salt, the attacker can match the results of the hash to your password, which would give them your password. With a salt, you would need to both guess the password, and add the salt of every user, which makes it harder to guess the password.

3.9

Well, if the attacker has the actual password file with the plaintext salts, the increase in size would not help at all, if the attacker were to try to attack a single user. Also, the increase in size doesn’t thwart completely, assuming the attacker is trying every salt, password, and user, it just lowers the chance- they could get super lucky and guess it quickly.

4.1

MAC is Mandatory Access Control, basically it controls access based on a user’s clearance and security labels, like the security levels and subsets from earlier.

DAC is Discretionary access control, which controls access based the identity of subjects and/or the groups to which they belong (Source: Wikipedia)

With MAC you can’t just give access if you’re the owner of a file, the user’s clearance is what needs to change to get access. With DAC you would be able to manually change it.

4.5

If you have protection mode 730, the people in the group have write and execute access to the file, but not read it. The file won’t then be compromised because it’s been read, but will be compromised because the person in the group could write to it or possibly delete it if they know the name of the file.