Scott Christensen

10/26/16

C.S. 465

Project #7: Password Cracking

1.

2.

3.

4.

5. Yes it does. They increase the cost of offline attacks by making all password guesses salt specific and it prevents duplicate password generation.

6.

7. Should the day come that minimal password lengths are too large for a typical person to remember, there will be far more security breaches unrelated to the algorithms employed. My thought is that should this scenario arise, more people will have to write their passwords down so there will be more security breaches based off of people having their written passwords stolen or shoulder surfing attacks since people will be spending more time typing in their passwords or some kind of social engineering attack that pretends to offer saving your long passwords to cookies so that people will not have to remember them.

My recommendation for the next step in password evolution is to increase the minimum password length by a little, mandate the use of non-alpha characters, and if possible find another secure encryption algorithm that could be employed on our passwords in addition to those currently being used.

8.