Daniel Quiroga

Answers to Quiz 1:

1. Yes, a normal user would be allowed to execute this program since they would fall into the other permission group which has the flags r-x meaning they can read and execute this file.
2. So, the RUID and EUID would be set to the same which would be the normal user ID who is running the actual program.
3. No, this would not be possible since the user would not be able to read the actual contents of the file meaning that the user would not be able to encrypt the contents of said file.
   1. Scenario 1:
      1. Advantage: Makes it so that only you (the root user) can edit or add to the program and hence a level of security on your system is added since others can only read and execute.This would make it so that a hacker who was able to get into a single account would still not have ability to steal the contents enclosed since they would need to gain access to the root user to write into it.
      2. Disadvantage: Only user on the system and by having it in a restricted location, makes it a pain to go in to edit the program. Also, you would the program would be placed in an unconventional location and hence takes more work to go in to execute.
   2. Scenario 2:
      1. Advantage: These programs will be in locations that are very convenient and hence very easy to access it. The program would only be downloaded to the user and hence no worries about other users being able to access it.
      2. Disadvantage: Once in this location there is no option to edit the program, this program will only be in read and execute permissions. A hacker would easily be able to manipulate this file and hence would be easier to cause more harm to the machine.
4. Since this program is downloaded with user permissions it would have read access to all the restricted locations such as /user/, /bin, /etc. hence it would be able to read all the contents in that location and send all that information to evil host. It would also be able to execute the scrypt program easily since it is accessible locally.
5. I would say that option a is more secure since it will require a super user to run the program to begin with and not any user in the system. I would say the next in line for security would be option b since this would allow the user/group that installs the program would be able to execute the file – what we do here is change the owner to root and then add +s meaning that anyone in the current user/group would be able to execute this file without the sudo prefix. Lastly, we have an installation of the program that would allow anyone to who has access to it to run it without checking any of the permissions and hence someone could really monitor all the processes occurring due to the set CAP\_KILL capability.
6. I would say that b is more secure since when sent to the server it is already encrypted and hence has no real meaning. Rather in a we send a plaintext version of the password so the hacker would be able to know what input to use in the database to gain access to your account.
7. I would say that option b is more secure due to the number of possible ways to actual write out the passwords. In option we have 10^5 ways while in option b we have 5^10 ways to write out your password.
8. A salt is meant to decrease the vulnerability of having rainbow table attack but not to increase the effectiveness of a bad password. Hence, it would be better to have a longer password since this would be hard to crack than having one that is shorter with more salt. Essentially saying that 2 would be more secure than 1.