CS 458 – A1

Name: Dweep Shah
U.W. ID: dm2shah
Student Number: 20511868

Trust me, I'm a social engineer...

a. Confidentiality is violated in the following example since you are able to access Alice's data without authorization.
b. Integrity is violated in the following example since you are able to change Alice's information, which means next time she retrieves her data it will be incorrect.
c. Availability is violated in the following example since you are able to close Alice's account, so the next time the account will not be available for Alice.
d. Confidentiality is violated in the following example since you are able to retrieve Alice's address without her consent.
e. Reading all the conversation examples, it seems obvious that Sam was able to impersonate Alice without any authentication. In the last example he was also able to impersonate a person from retention in another department of the company.
f. First, the call center can improve its authentication by asking some knowledge question about personal information and historical account data to verify their identity. Second, they could use a PIN to allow access to more critical data. Third, they could use the caller id as a verification tool to know common calling patterns and have a way to give general information without much hassle.

Something isn't right...

a. I think I am experiencing interception in this case because some unauthorized party has gained access to my call without consent. A loss of the asset is not necessary for an interception threat.
b. I think I am experiencing interruption in this case because my credit card became unusable, causing an interruption in my usage of the asset.
c. I think I am experiencing interruption in this case because someone seems to have make the credit card customer service unusable using the personal phone number,
d. I think I am experiencing fabrication in this case because new counterfeit records are being created on the system. These transactions have been added and they are not modifications of my previous transactions.

S.O.S.

a. Update your public profile with false/decoy information. This may fool ToqToq (who else could it be?) into misallocating resources during their assault on you.
b. Encrypt data sent through the voice line so it can not be intercepted, and lock the bank account for further use.
c. Let the bank company know I have been compromised and to let me know when anybody tries to access the account. Also, the phone can be backtraced to detect when the phone is being wiretapped.
d. Change my phone number and credit card number and make sure it is not available anywhere else, and not given to anybody else.

Sploit3.c

This exploit leverages the vulnerability of having the pwgen –w option that overwrites the password of the user who is currently using pwgen. Using this write option to generate the password the password is printed to stdout. This output can be captured and written to a file, and read from the file to be accessed in the program. This new password is used to invoke a new superuser bash shell to open a shell with root access.

This is possible because the generated password is printed to stdout when using the pwgen –w option. This allows us to use the output the fetch the password. This printf statement should be removed so this vulnerability could not be exploited.

```
printf("Generated password (length %d): %s\n", PASSWD_SZ, passwd);
```