Writing problem

1.

a.In this case,the confidentiality of personal information is violated.The TCS reveal customer's balance information to other without any identity checking.

b.The Integrity is violated.The TCS allow a person who is not the account owner to change status of the account.Then the real account owner will recive wrong data when he check the account status.

c.The Availability is violate.The TCS remove a customer's account without identity checking.Then the real account owner lost all his data in the account.

d.The confidentiality of information is violated.The address of customer is private information that should not be provide to any other people.

e.The TCS violate customers' security and privacy easily,which is irresponsible.In case a,b and c,the TCS did not do enough identity check before providing or changing customer's information.In case d,the TCS provide customer's information to a person that is clearly not account owner,which is dereliction of duty.

f.First,do more identity check to make sure that the other side is the real account owner.For example,asking some question of privacy information such as date of birth and mailing address.

Second,for important change,such as close account,or change record credit card number,use caller number display to make sure that caller is the onwer of the account,or use the record email address to let account owner comfired.

Third,never provide any personal information to a person that cannot prove himself is the account owner.

2.

a.Interception,recording the call is one of the interception,which do not effect your communitction,but stealing information and data during your call.

b.Modification,the credit card was denied might because the credit card is already out of balance because someone else use all your money,or the relate credit card is change to another unavailable card.These are both case of modification,that someone not only accesses but tampers with your asset.

c.Interruption,the communicate between the phone and bank is interrupte,which mean the connecting between then is block.

d.Modification,same as b,the asset is tampers by others.

S.O.S

Preventing:Do not use talking about important pravite information in telephone(such as bank password,or some company secrets),use email or some SNS software instead.This could not stop the interception threats,but at least would preventing big lost by the recording.

Detecting:It might be hard to detect the threat by technology.However,when you relize some prvate information is revealed and you have talk about it in a call,you should watch out for it.You can even give some fake information in the call, to see if this fake information is leak to other,then you can detect if someone is stealing your information.

Recorvering:Communication with bank to make sure what happen with your credit card and your fund,make sure that if your funs is really been transferred. If you really lost your money,call the police for help.After that,change all the password that your have mentioned in telephone before,and change a telephone number.

Sploit1:
Sploit1 exploit a buffer overflow Vulunable in the function strcpy() in method parse_args.
This method try to copy arg2 as a string and without any length check.This give attacker a changes to overflow
and cover the return address to the shell,and get root privilege.
This is not the only function that have this Vunlnerability.For fixing this problem,add a length check before every sprintf() or strcpy() function,
and make sure that attacker can not reach the return address.Or simply use strncpy(),which have length check inside,instead of strcpy().

Sploit2:
Sploit2 exploit a format string Vulunable in the function printf() in method print_usage.
This printf() input a buffer that have part of user input without strict type check,which give attacker changes to locate the buffer
address by inputing format string(such as %x) and rewrite the return address by %n.
This problem can be fix by adding strict type check in evert printf(include sprintf(),fprintf(),ect).

Sploit3:

Sploit3 use a TOCTTOU attack in the fill_entropy method.This method call the get_entropy method,which allow user input arbitrary data into a buffer,
and the write it into a file that depend on user input.This allow user to writing data in a file that user not owns.To fix this,we should use a
a constant to store the result of check_perms() instead of the none constant various res.Then we can make sure that attacker can not change the
checking result during check and write.