Written Response Questions

Question 1:

a)

Confidentiality and privacy.

Because the person spies their partner's phone. There is no privacy to their partner, everything through their phone will be acknowledged by the person who installs spying software. and the person is more likely without authorization to spy those cell.

b)

Privacy.

Google sells your information to malicious hacker. You most likely don't want to let google sells your information to other people. therefore, google sells your information without your permission, which compromised the privacy.

c)

Confidentiality and privacy.

After someone break, and steals user account information, user information no longer controlled by user themselves, non authorized person may be able to access user data, therefore privacy and confidentiality are compromised.

d)

All four.

If hacker replace the software/firmware in your car. hacker can stop give you data from their software, or they can give you wrong data. and you personal information for example location is known by hacker. therefore I think this compromised all four.

e)

All four.

After government replace the site, you will not be able to get what you want but get a malware from government, which may cause your personal information lose.

f)

Availability.

After internet shut down, user can not access their data online.

Question 2:

Interception: insider man can be track where a kind of drug goes.

Interruption: delivery truck can be robbed.

Modification: change the request mount of drugs that there can have extra drugs be sold to black market.

Fabrication: replace the real drug with placebo and sell to patients.

b)

patients has to pick up their medicine form one location with government issued ID. (Prevent: no transportation)

armour transportation.(Deter: harder to rob)

patients' drug are sent with small packages, which are delivered by EMS. (Deflect: less notice, same outfit as other packages)

when armour robbery occur, call 911 for backup. (Detect)

send police force to stop the robbery. (Recover)

spoilt3.c

this exploit performs a format string attack. which aim at print_version function return address.

I pass the arg[0] as my attack string by using execv passed in to submit.c with a option -v. submit goes to print_version function. after snprintf. my string is add to a string to a unguarded printf. In printf, attack string changed the return address of print_version to the address where we stored shellcode. To avoid that change printf (txt) to printf (“%d\n”, txt)

spoilt4.c

This exploit also is a format string attack. which aim at check_forbidden function return address.

I passed the attack string as arg[1], and when we are in the check_forbidden function. there is a unguarded printf, which can used to overwrite the return address of check_forbidden. After I overwrite address to our shellcode, we can return check_forbidden to run our shellcode. To avoid that change printf (txt) to printf (“%d\n”, txt)