Lauren Fromm
404751250

Homework 7

1. If the other teams were observing the bytes going across the network, the resulting network would still be secure. Although they will be able to see the public key, the private key would still be kept hidden. The private key is the only thing that will be able to decrypt the messages. The data remains secure since they can't access the private key, and since it's pretty much impossible for them to find the private key given the public key.

If the teams tap my keyboard and observe my keystrokes, the network would still be secured because the generate private key is created with random values and not keyboard input, so that the passphrase does not indicate what the private key is.

If a team has physical control of the USB, the network might not be secure, since the team can access the private key if the system files are located on drive. They can then use the private key to decrypt all of the messages and access the data.

2. The gpg --verify doesn't really verify that I personally created the tarbell because all it does is verifty if the signatures match. The signature is easy to be messed with since a hacker can replace the public key and recreate the tarbell. So the --verify would verify that the signature of the hacked file matches the hacker, so it doesn't really work with seeing that the original creator is still in charge of the file.

People now fix this using a trusted third party company that is used to track the origin of the public key, so the reciever can verify that the file is from

who they are expected for it to be from.