1. Suppose the other teams really had been observing all the bytes going across the network. Is your resulting network still secure? If so, explain why, and explain whether your answer would change if (1) you assumed the other teams had also tapped your keyboards and had observed all of your team's keystrokes, or (2) you are booting off USB and you assume the other teams temporarily had physical control of the USB. If not, explain any weaknesses of your team's setups, focusing on possible attacks by such outside observers.

1.

The network is still secure, since the communication is encrypted by session key,

and they does not know the session key and thus cannot decrypt the content.

(1)

It has two cases. If our team use key-based authetication, the network is secure.

Though the observer may record the passphrase from keystrokes, he/she still

cannot get the private key from either side, since passphrase is just a way to

protect the private key but cannot act as a private key. So if the observer wants

to pretend to be the server or try to log in as our team's client, he/she cannot

pass the challenge-resonse validation process. Also, there is no way the observer

can directly decrypt the content of communication, since the session key is

generated by using both client private key and each other's public key. Observer

cannot get the private key of either side.

The second case is that our team used password based authentication. I am not

sure whether this case is also what the spec intend to ask. In this case, if the

observer records the password the client entered, he/she can connect to the same

host with the password. But still, the observer has no way to directly decrypt

the content of communication. So if the question is about whether the process of

current communication is secure, the answer should still be "secure".

(2) it is no longer secure. The other team can find the private key in the USB,

and use it to log into our host and decrypt any message encrypted by public key.