CS3840 Introduction to Computer Security

Homework 6

1. An attacker is intent on disrupting the communication by inserting bogus packets into the communications.
2. Discuss whether such an attack would succeed in systems protected by IPsec. The packets would get rejected because they are not part of the trusted network.
3. Discuss whether such an attack would succeed in systems protected by SSL. The packets will not work because the attacker will not have the secret key that is used to form the MAC.
4. What do you call a fake hotspot used by hackers to prey on mobileworkers, and how does it work? An evil twin. These work by setting up a fake access point that seems to be the actual one the user wants to connect to. It then can ask the users for sensitive login information, which may be entered, since the users do not know it is not a legitimate access point. This can also monitor the traffic and pick up any sensitive information that the user enters on sites.