CSE 565 Solution to Homework 5

1. (20 points total; 10 points for each attack)

   First consider SKID2. In this 2-message authentication protocol, suppose Mallory tries to impersonate Bob by mounting a parallel session attack. After receiving the first message from Alice, Mallory will resend R_A back to Alice, wait for a reply, and then try to use the returned values to finish her own authentication session. This attack won't be successful because Alice's reply will include her identity A inside the MAC, which means that Mallory won't be able to create a correct response to her authentication message containing Bob's identity. SKID3 provides mutual authentication, which means that the knowledge of the second message doesn't help Bob (or Mallory) to correctly construct the third message. And mounting the above described parallel session attack, where this time Mallory aborts the parallel protocol session after obtaining Alice's reply, doesn't allow Mallory to construct a correct response to Alice's message for the same reason as before.

   In the two-message protocol, a successful man-in-the-middle attack would mean that Alice authenticates Mallory thinking that she authenticated Bob and Bob authenticates Mallory thinking that he authenticated Alice. Because all authentication information is based on a shared secret, which Mallory can't tamper with or learn, she won't be able to impersonate either Alice or Bob. The best Mallory can do to make Alice believe that she (Alice) is talking to Bob is to pass the authentication information to Bob, who will construct a reply, which Mallory will then relay back to Alice. This is simple message passing and doesn't constitute a successful man-in-the-middle attack. In the three-message version of the protocol, when Mallory (pretending to be Bob) initiates the protocol with Alice and obtains a reply back, she might try to use Bob to help in creating the final message. Bob would have no reason to reply, unless he actually initiated the protocol and Mallory is simply passing the messages (in which case she doesn't succeed at this attack).

   (There could be existing specific implementations of this protocol that are susceptible to the man-in-the-middle attack.)

2. (10 points) Answers might vary.

   The primary advantage of SSL over IPsec is its flexibility. IPsec supports only one configuration per host (which implies that it can be used by one user at a time) and all application will use exactly the same parameters and algorithms. In SSL, on the other hand, each application has control in terms of how it wants to use the available mechanisms and its use is not restricted to a single user.

   The primary advantage of IPsec over SSL is its transparency to the applications; that is, IPsec can be configured and used to protect communication of all applications without the need of the applications to do anything, while using SSL from a particular application requires awareness of the mechanism and setup on the application part. IPsec is also suitable for connectionless communication.

3. (30 points total; 10 points total) The answers are expected to be sufficiently detailed, especially when the question asks for technical details.