Week 11 Questions

Lecture 59

1. There are so many different ways attacker may use. There are also many different protocols that knowing one piece of information may not get you more information. An attack could be one that no had thought of previously.
2. You don't know when the attacker will use the messages. The attacker could be interjecting messages from just a few minutes ago or they could be interjecting messages from a year ago.
3. Yes, the attacker could simply be looking to disrupt communication between two parties.
4. It is assumed that the attacker does not have the ability to create arbitrary messages.
5. Each party is only aware of its own surroundings so attacks cannot compromise another party by getting information from one party. Each party does not know it is a part of a protocol until a message is sent to it therefore an attacker cannot just choose one particular party and assume that there will be messages sent between the two.

Lecture 60

1. Yes, however there is no confirmation if the message sent back was a relay or not. The probability is the message being a relay is highly unlikely though.
2. A
    a. A tells S that it wants to communicate with B and gives S a nonce to generate keys. S believes that A sent the nonce.
    b. S returns to A the key generated, along with the nonce (so that A knows it's fresh),the receiver, and additional information that is encrypted k_{bs} (only B and S can decrypt). This is encrypted with k_{as} so only A and S can decrypt it. A believes it has received the keys generated by S.
    c. A sends to B the additional information. B believes it has the key sent from A and A wants to communicate with it.
    d. B sends to A a new nonce created by B, which is encrypted with K_{ab}. A believes that B has the key it sent to B.
    e. A sends to B the nonce -1 encrypted with K_{ab}. B believes that A has received the nonce and can use it.

Lecture 61

1. A can still be compromised because S does not know that A has changed its key.
2. Yes.
3. Add a way for B to confirm that the message coming from A is fresh.

Lecture 62

1. It seems to guarantee to A and B that the messages are fresh.
2. In Needham-Schroeder, B ensures no relay because the probability of finding a nonce that is the same is highly unlikely.
3. You can add an additional lock that it would have to be unlocked before sending it back.

Lecture 63

1. Verification is important because we want to make sure it's doing what it claims to be doing.
2. A belief logic is a formal system for reasoning beliefs.
3. Beliefs come in when reasoning and formalizing a protocol's behaviors and properties.

Lecture 64

1. A type of logic that includes operators expressing modality.
2. A believes that the key shared with B is the only instance of this key and therefore only B has this key. So when it sees this key it believes that it came from B.
3. A believes X is fresh and A believes B once said X, then A believes B believes X.
4. A believes B has jurisdiction over X and A believes B believes X, then A believes X. If you hear something from an expert, you are entitled to believe what they say.
5. Idealization is determining what a message or transaction is trying to accomplish. It is needed to turn it into a belief logic.

Lecture 65

1. It is omitted because the plaintext can be forged.
2. It can be used as a way to confirm that each step in the protocol is correct.
3. It could expose assumptions that you would not have thought of. This could lead to a better formalization of a protocol.