# Review Questions

1- Define suppress-replay attack.

2- What is the problem that Kerberos was designed to solve. Explain the network environment and possible threats?

3- Explain the difference between SSL connection and session. How this difference is related to the Change Cipher Specs protocol and the Handshake Protocol?

4- Is there any advantage of not including the MAC in the scope of packet encryption in SSH Transport Protocol?

# Problems

1. Consider the following protocol:

A 🡪 AS: IDA || IDB

AS 🡪 A: E(PRas, [IDA || PUa || T] || E(PRas, [IDB || PUb || T])

A 🡪 B: E(PRas, [IDA || PUa || T) || E(PRas, [IDB || PUb || T) || E(PUb, E(PRa, [Ks || T]))

a. What are A and B trying to do in this protocol?

b. What is the main problem with this protocol?

c. Suggest a modified version of the protocol to solve the problem you answered in (b).

2. Show how SSL can protect against the following attacks:

a. Replay Attack: Earlier SSL handshake messages are replayed.

b. Man-in-the-Middle Attack: An attacker interposes during key exchange, acting as the client to the server and as the server to the client.

c. IP Spoofing: Uses forged IP addresses to fool a host into accepting bogus data.

3. You have a server in the university lab that you want to remote access from home. The server is behind a firewall, which allows outgoing connections but doesn’t allow incoming connections. You have a DSL connection at home. Show using a diagram how to use SSH to enable access to the university’s server from a PC at home. Then, explain the steps required to accomplish this task.

Hint: Check <http://www.walkernews.net/2007/07/22/ssh-port-forwarding-local-vs-remote/> for help.