ECE: Advanced Information and Network Security
Homework 5
Spring 2007

1. Suppose Bob is a server, and Alice is a client. Bob is not allowed to store any challenges he issues to Alice (perhaps he is resource limited). To bypass this issue, the following protocol is proposed in which Alice sends back the challenge (nonce) to Bob:

$$A \rightarrow B : ID_A$$

$$B \rightarrow A : r$$

$$A \rightarrow B : \{r, E_{K_{AB}}(r)\}$$

where r is the nonce, and K_{AB} is a key shared between Alice and Bob. Does this protocol achieve mutual authentication? Is it secure?

2. Consider the following authentication protocol. Alice generates a random message r and encrypts it with the key K she shares with Bob, and sends

$$A \rightarrow B : E_K(r)$$

to Bob. Bob deciphers it and adds 1 to r and sends

$$B \rightarrow A : E_K(r+1)$$

to Alice. Alice deciphers and compares it with r. If the difference is 1, she knows that her correspondent shares the same key and is therefore Bob. If not, she assumes that her correspondent does not share K and so is not Bob. Does this protocol authenticate Bob to Alice? Why or why not?

3. Needham and Schroeder suggested the following variant of their protocol

$$\begin{aligned}
A \rightarrow B: &\quad ID_A && (1)\\
B \rightarrow A: &\quad E_{K_B}(\{ID_A, r_3\}) && (2)\\
A \rightarrow C: &\quad \{ID_A, ID_B, r_1, E_{K_B}(\{ID_A, r_3\})\} && (3)\\
C \rightarrow A: &\quad E_{K_A}\{ID_A, ID_B, r_1, K_S, E_{K_B}(\{ID_A, r_3, K_S\})\} && (4)\\
A \rightarrow B: &\quad E_{K_B}(\{ID_A, r_3, K_S\}) && (5)\\
B \rightarrow A: &\quad E_{K_S}(r_2) && (6)\\
A \rightarrow B: &\quad E_{K_S}(r_2 - 1) && (7)
\end{aligned}$$

Here K_A is Alices shared key with the center C, K_B is Bob's shared key with the center. K_S is the session key. Show that this protocol solves the problem of replay as a result of stolen session keys.