In the name of God

Sharif University of Technology
Department of Computer Engineering

CE 442K: Data and Network Security

Mehdi Kharrazi *Azar 16th, 1390*

Homework 2

Please email your answers/report in **PDF format** to Zhaleh Milanian "zhaleh.milanian@gmail.com" and CC me at "kharrazi@sharif.edu". The HW file name should be **"Your Lastname-442k-HW-2"**. It should be used as the subject of your email, too. In order for us not to miss your homework please follow the formatting. This homework is due by **Azar 22nd, 11:59 PM**. There may also be a face-to-face delivery, the time of which will be announced later.

Part I

Consider the following protocol for user authentication. Alice and the host share a secret key K_A which is communicated securely once at the outset. After that, every time Alice wants to log on she used the following protocol:

- Alice sends to the host her ID and a nonce R_1.
- The host returns a nonce R_2 and also the encrypted nonce R_1 using the secret key that the host shares with Alice, that is $E_{K_A}(R_1)$.
- Alice returns $E_{K_A}(R_2)$.

1. Is the following protocol susceptible to a replay attack? Explain your answer.
2. Show how the above protocol is susceptible to a *reflection attack*, where Oscar starts multiple instances of the protocol claiming he is Alice. He then uses information obtained from one instance to complete the other. So for example, Oscar initiates a login and goes through the first two steps above. He then initiates a second instance using R_2 as the nonce. Explain in more detail how the reflection attack will succeed.
3. Suggest how the protocol can be modified to resist the attack.

Part II

A KDC shares unique secret keys with nodes in a network, hence a secured communication link between all nodes and the KDC. User A want to send a secret message M to B, he does this by:

1. $A \longrightarrow KDC : A||B||E_{K_a}[R]$ (*note: K_a is shared by node A and KDC, R is a random number generated by A*)
2. $KDC \longrightarrow A : E_{K_b}[R]$
3. $A \longrightarrow B : E_R[M]||E_{k_b}[R]$
4. B has K_b, thus obtains R, which is used to get M.

Are there any security issues with this protocol?