Homework 6 (SPIN): COMS/CPRE/SE 412, COMS 512

Due-date: April 10 at 11:59PM (via Blackboard)

Homework must be individual's original work. Collaborations and discussions of any form with any students (except our TA) or other faculty members are not allowed. If you have any questions/doubts/concerns, post your questions/doubts/concerns on piazza and/or ask our TA or me.

---

1. Read the Section 2 of the pdf Merz.Needham.pdf. The author discusses the use of SPIN model checker for verifying the correctness of a Cryptographic Protocol (Needham-Schroeder protocol). The paper presents

   - description of the protocol
   - code samples for modeling the protocol
   - scenario for breaking the protocol

   (a) Complete the model based on the guidelines provided. Write the required property to generate at least one scenario for breaking protocol.

   (b) **512:** Suggest one possible solution to correct the protocol. Justify your solution.

   Submit via blackboard (`NS-<yournetid>.pml`)

2. You have developed a protocol using which one agent can share a secret with another.

   - Each agent has a private key
   - Each agent can encrypt and decrypt messages with his/her own private key. Given a message m, if it is encrypted using a key k, we denote it by $[m]_k$
   - Encryption is commutative, i.e., if a message is encrypted with key k_1 followed by key k_2, then the result is identical to the one obtained by encrypting the same message first by k_2 followed by k_1. That is,

   $$[[m]_{k_1}]_{k_2} = [[m]_{k_2}]_{k_1}$$

   The protocol followed by the agents is described below. Consider two agents Alice with a private key k_A and Bob with a private key k_B.

   (a) Alice sends $[m]_{k_A}$ it to Bob.

   (b) Bob, on receiving the encrypted message, sends back $[[m]_{k_A}]_{k_B}$) to Alice.

   (c) After receiving the message from Bob, Alice decrypts the message (resulting in $[m]_{k_B}$) and sends to Bob.

   (d) Bob receives the last message, decrypts it and obtains the secret m.

   Before you release the protocol, you need to verify that the protocol is not vulnerable to man-in-the-middle attacks. You will use Spin to do the verification.

   - Model Charlie's behavior such that in addition to normal behavior, he can
     (a) Intercept any message between Alice and Bob
     (b) Send any message he owns
   - Model Alice and Bob's behavior as per the above specification. Consider that Alice wants to share secret m_1 with Bob and secret m_2 with Charlie.
   - Assume that any message can be encrypted at most twice.

Verify whether Charlie can read a message/secret that Alice wanted to share only with Bob. Justify your findings.

You have been given partial code for the SPIN model (security-hw.pml). Update the file, write your answer as part of the comments at the top of the file and submit `security-<yournetid>.pml`.