SENG2250/6250 System and Network Security
Self-Quiz Week 4, Semester 2, 2020

True/False Questions.

1. User authentication is typically based on something the user knows, is, or has.
   True.

2. In general, secret information is compulsory for user identification.
   False. Secret information is optional for user identification.

3. For good practice, we can choose a very strong password like **jw3U&0]Rm5tb0@Xo** so an adversary can never guess the password.
   False. An adversary always has a probability of guessing the password, but a strong password results in low (guessing) probability.

4. Salt is a random component used to distinguish identical passwords.
   True.

5. Hash chain based authentication protocol is under threat by Denial-of-Service attacks (DoS) without using overwhelming network traffic.
   True. Recall that hash chain based authentication is essentially a codebook-like authentication. It means that the user and server have to be synchronised on which password (of the codebook) will be used in the next authentication. An adversary can attempt to desynchronise the user and server. Then, the legitimate user cannot be authenticated in the future.

Short-Answer Questions

6. What are the differences between the identification and verification mode of biometric authentication?
   Identification Mode
   Given an input of biometric information, the system outputs the corresponding identity if the biometric is registered.
   Verification Mode
   Given an input of biometric information and the claimed identity, the system outputs "Yes", if the (biometrics, identity) pair is valid, otherwise, outputs "No".

7. What is a common client attack of user authentication? What are the countermeasures?
   Attack: masquerade as a legitimate user (e.g., guess the password or try all passwords)
   Countermeasure: strong passwords; limit number of attempts