COM-301 Computer Security
Exercise 5: Authentication

1. Why are both (user, password) required for authentication? Why can't we use just a password for authentication?

2. Servers should store hashed passwords instead of storing them as plaintexts. Would hashing the password in the client, before sending it to the server through the encrypted channel bring any security advantage? How would the server side of the authentication process change if we have hashing at the client? How would the changes affect security?

3. In class, we talked a lot about how to counter offline attacks against password cracking. Please discuss online attacks (i.e., attacks where the adversary tries to guess a password by interacting with the system). Are they easier to thwart than offline attacks? What are the typical defenses against them? What is the rationale behind these defenses?

4. Why is having a slow hash function that hinders offline attacks not a problem for the authentication process?

5. Argue whether having the verifier (Morty, in the slides) sending two challenges to increase the security of a challenge response protocol is a good idea.

6. If you steal the biometric template from a database with server-side processing of biometrics, can you use it directly to fool authentication in another system with server-side processing?

7. If you were to implement a biometric authentication system for

   (a) Entering a military base

   (b) Using your loyalty card at the supermarket

   How would you select the parameters for the biometric algorithm? Justify.

8. In token-based authentication, the token produces a value by applying a number of times a cryptographic function on a pre-agreed "seed" value.

   (a) Can this cryptographic function be a hash function? If yes, what properties must this hash have? If no, what is the reason?

(b) Would the situation help if for each authentication the server could send a challenge?

9. EPFL is opening a new in-campus paying system. They task you with designing the authentication mechanism to reload the cards that hold the money. You decide that since this is money, it would be wise to have two-factor authentication. Argue whether each of the following combinations are good choices.

   (a) Ask users to present their Camipro to the loading machine and input their SCIPER.

   (b) Ask users to present their Camipro to the loading machine and input their Gastpar login

   (c) Ask users for Gastpar login/password

   (d) Ask users to present their Camipro and a code sent to their email