Auto-Evaluation Questions
(Authentication / User-Authentication)

1. Considering in general the main authentication factors used as means of authenticating a user's digital identity, what are those means, exemplifying technologies related to each one.
2. List and briefly describe the principal dangers and threats against the secrecy of passwords.
3. What are the common techniques used to protect a password-file or in general, passwords in storage repositories of passwords.
4. List and briefly describe possible techniques for selecting or assigning passwords.
5. What is the difference between a memory card and a smart card, and how the difference is relevant when used for authentication purposes
6. List and briefly describe the principal characteristics used for biometric authentication, from the presented and discussed biometric technology
7. In the context of the use of biometric user authentication, explain what means the enrollment, verification and identification phases.
8. When using biometric factors, define the terms false match rate (FMR) and false nonmatch rate (FNR) and explain the use of threshold values in relationship of those two rates.
9. Describe the general concept of challenge/response authentication protocolos and give examples of three standard protocols that use the challenge/response method for authentication, indicating in each case if they support mutual (two-way) or unilateral (one-way) authentication guarantees

- - -

10. Explain the suitability or unsuitability of the following passwords:
    a. YK 334
    b. mfmitm (for "my favorite movie is tender mercies")
    c. Natalie
    d. Washington
    e. Aristotle
    f. Tv9stove
    g. 12345678
    h. dribgib

11. An early attempt to force users to use less predictable passwords involved computer-supplied passwords. A solution for this purposes is the following:

The passwords were eight characters long and were taken from the character set consisting of lowercase letters and digits.

They were generated by a pseudorandom number generator with 2^{15} possible starting values.
Using the technology of the time, the time required to search through all character strings of length 8 (in brute force guessing strategy) from a 36-character alphabet was 112 years.
Unfortunately, this is not a true reflection of the actual security of the system. Explain why.

12. Assume that passwords are selected from four-character combinations of 26 alphabetic characters. Assume that an adversary is able to attempt passwords at a rate of one per second.

a. Assuming no feedback to the adversary until each attempt has been completed, what is the expected time to discover the correct password?

b. Assuming feedback to the adversary flagging an error as each incorrect character is entered, what is the expected time to discover the correct password?

13. Assume that source elements of length k are mapped in some uniform fashion into a target elements of length p. If each digit can take on one of r values, then the number of source elements is r^k and the number of target elements is the smaller number r^p. A particular source element x_i is mapped to a particular target element y_j.

a. What is the probability that the correct source element can be selected by an adversary on one try?

b. What is the probability that a different source element x_k ($x_i \neq x_k$) that results in the same target element, yj, could be produced by an adversary?

c. What is the probability that the correct target element can be produced by an adversary on one try?

14. A phonetic password generator picks two segments randomly for each six-letter password. The form of each segment is CVC (consonant, vowel, consonant), where V = 6 a, e, i, o, u 7 and C = $\bar{V}$.a. What is the total password population?b. What is the probability of an adversary guessing a password correctly?

15. Assume that passwords are limited to the use of the 95 printable ASCII characters and that all passwords are 10 characters in length. Assume a password cracker with an encryption rate of 6.4 million encryptions per second. How long will it take to test exhaustively all possible passwords on a UNIX system?

16. Because of the known risks of the UNIX password system, the SunOS-4.0 documen- tation recommends that the password file be removed and replaced with a publicly readable file called /etc/publickey. An entry in the file for user A consists of a user's identifier ID_A, the user's public key, PU_a, and the corresponding private key PR_a.

This private key is encrypted using DES with a key derived from the user's login pass- word P_a. When A logs in, the system decrypts E(P_a, PR_a) to obtain PR_a.a. The system then verifies that P_a was correctly supplied. How?b. How can an opponent attack this system?

17. It was stated that the inclusion of the salt in the UNIX password scheme increases the dif- ficulty of guessing by a factor of 4096. But the salt is stored in plaintext in the same entry as the corresponding ciphertext password. Therefore, those two characters are known to the attacker and need not be guessed. Why is it asserted that the salt increases security?

18. Assuming that you have successfully answered the preceding problem and under- stand the significance of the salt, here is another question. Wouldn't it be possible to thwart completely all password crackers by dramatically increasing the salt size to, say, 24 or 48 bits?

19. For the discussed biometric authentication protocols for static-biometric systems (using physical biometry) note that the biometric capture device is in general authenticated in the case of static biometric factors. However, the capture is not authenticated for a dynamic biometric. True or False ? Explain why authentication is useful in the case of a stable biometric but not needed in the case of a dynamic biometric. Is this a weakeness for dynamic behavioyral biometry? Analyze and discuss.

20. Consider the authentication proposal in Secure Quick Reliable Login (SQRL) described here: https://www.grc.com/sqrl/sqrl.htm. Write a brief summary of how SQRL works and indicate how it fits into the categories of types of user authentication and factors as studied.

- - -

21. In their internet banking platforms for retail-baking (individual accounts), two Portuguese banks use token-based authentication using a matrix of codes, as a second-factor authentication for access-control to certain operations. This factor is independent from the first factor based on a password provided by a visual (virtual) keyboard used to logon.

    For the two institutions, the matrix formats are different:

    Bank A uses a 8x8 matrix with three numbers (0 to 9) in each cell, and the authentication challenge consists in providing three numbers, asking for three coordinates in the following way: line, column position of the number in the cell

    Bank B uses a matrix in the form of a list (as a key-value store). The key in each line is a random integer (between 000 and 999) and the value is a random integer (between 0000 and 9999). The challenge in this case is to ask for a given key number, with the authentication proof provided by the respective value in the list.

    a) For brute force attack, how many attempts are necessary to have a probability ½ of guessing a valid challenge/response code in both cases?
    Note: the banks also combine the process of multi-factor authentication with possible challenge/response codes obtained via SMS, using registered mobile phone numbers by users in their contracts. The two methods are today used to answer to the requirements of the regulation (decreto-lei 91/2018 PCM):
    https://dre.pt/application/file/a/116940401

    b) From your comparison, what is the more effective method in terms of "usability" vs. "security"? Explain.

22. In classes we discussed the notion of multi-level authentication and possible combination of multi-level layered authentication. Explain the notion and give an example of using layered authentication combination.

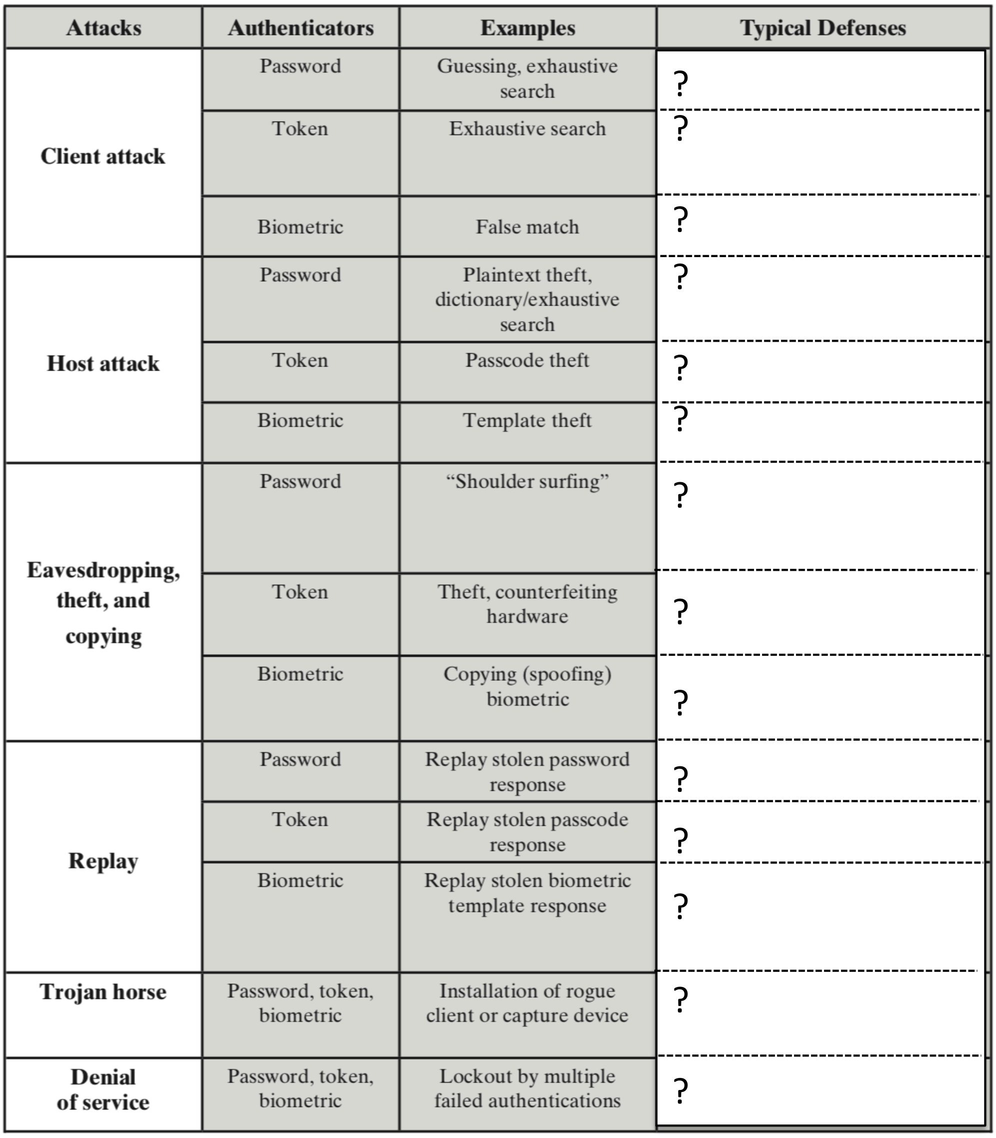
23. In the NIST SP 800-63-2 E-Authentication framework, different entities are involved: RA (Registration Authorities), CSP (Credential Service Providers), S/C (Subscribers/Claimants), ARP (Authentication Relying Parties) and V (Verifiers). Describe the roles of these entities in authentication protocols.
24. What is the relevance of using salts in password-based authentication ?

25. From your study and analysis, why the use of schemes like CRYPT, BCRYPT, Argon2, PBKDF2, are stronger than using simple secure hash-functions and salts to protect password-storage (for example in authentication servers' side)

26. In what consists and what is the advantage of Bloom-Filter based password checking in selecting and testing passwords with strong evaluation criteria?
27. What advantages you find in using hardware-based tokens versus matrix-codes for dynamic one-time passwords?
28. Try to identify the properties in the choice of biometric factors and technology to be used in authentication protocols and systems for user-authentication
29. What kind of new or emergent biometric factors you learned that are in the recent research of

biometric authentication

30. What means the decision threshold criterion in addressing the tradeoff between False Acceptance and False Rejection Rates in biometric authentication?
31. From the studied biometric factors, give an example of factors you found with lower false non-mismatch rates and lower false match rates
32. Given the following table, try to identify and summarize typical counter-measures against possible attacks to different authentication factors, when using such authentication factors



Attacks	Authenticators	Examples	Typical Defenses
Client attack	Password	Guessing, exhaustive search	?
	Token	Exhaustive search	?
	Biometric	False match	?
Host attack	Password	Plaintext theft, dictionary/exhaustive search	?
	Token	Passcode theft	?
	Biometric	Template theft	?
Eavesdropping, theft, and copying	Password	"Shoulder surfing"	?
	Token	Theft, counterfeiting hardware	?
	Biometric	Copying (spoofing) biometric	?
Replay	Password	Replay stolen password response	?
	Token	Replay stolen passcode response	?
	Biometric	Replay stolen biometric template response	?
Trojan horse	Password, token, biometric	Installation of rogue client or capture device	?
Denial of service	Password, token, biometric	Lockout by multiple failed authentications	?