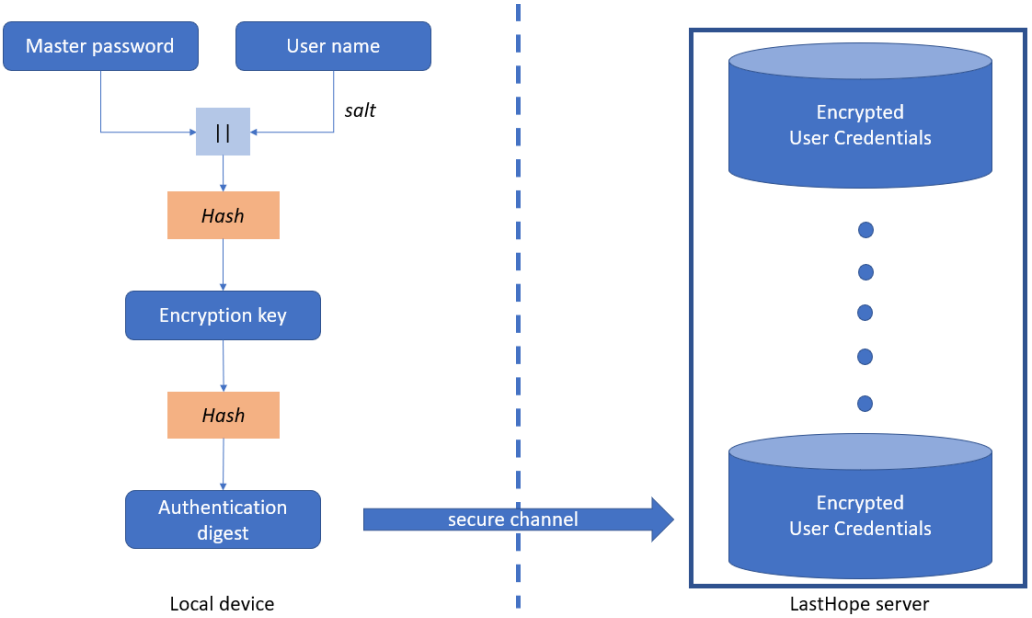
Jan 27, 2023

Introduction to Computer and Network Security

Part 1

Question 1 [50 points]

LastHope offers a password manager service structured as depicted in the figure.



When users create accounts on their devices, they set a *user name* and a *master password*. The former is used as a salt that is concatenated with the latter (see the box labeled with || in the figure) and then hashed to create a digest that is, in turn, used to generate an *encryption key* for encrypting all credentials of a user before sending them to the LastHope server.
Then, the *encryption key* is hashed again and an authentication digest is sent to the LastHope server over a secure channel. In the LastHope server, a database of credentials is created for each user where the *authentication digest* is stored together with all the user's credentials.

You are a security expert paid to comment on the password manager service and, in particular, to answer the following questions:

A. [10 points] Which of the available hash function algorithms would you advise using in the Local device? Motivate your answer, highlighting advantages and possible disadvantages.
B. [15 points] Is it secure enough to use the *user name* as the salt to derive the encryption keys? Motivate your answer and suggest, if the case, possible extensions.

C. [10 points] Which security service would you adopt to make the communication channel between the Local device and the LastHope server secure? Motivate your foganswer and discuss possible configuration problems of the proposed security service.
D. [15 points] Which encryption primitive would you suggest adopting by the LastHope server to encipher the credentials in each user database? Motivate your answer.

Part 2

Question 2 [40 points]

In the context of access control, describe the general architecture of an access control enforcement mechanism including (a) subjects, (b) requests, (c) guard, (d) policy, (e) isolation boundaries, (f) audit log, and (g) the role of authentication and authorization.

Question 3 [10 points]

Define the notions of Confidentiality, Integrity, and Availability.

Please, remember…

Be sure to annotate the following information on each used sheet of paper (possibly, 2 sheets at most)

- Name
- Surname
- Student ID number
- Question number