Final Notes on Authentication

Final Notes on Authentication

- Combining various authentication techniques Is more effective than using a single authentication technique.

- We have discussed some disadvantages of using biometric authentication alone.

- However, if you combine biometric authentication with another technique, such as a password or a token, then the authentication process becomes more effective.

- The term *two-factor authentication (2FA)* is used to describe the case in which a user is to be authenticated based upon two (independent) methods.

- ATM cards- another example of two-factor authentication at work.

Final Notes on Authentication

- ATM cards have magnetic stripes that have the user's name and account number.

- When the card is used, the user is required to enter not only the card into the teller machine, but also a PIN, which can basically be thought of as a password.

- In such an example of *2FA*, the bank requires the user to be authenticated based upon two methods—in this case, something that the user has and something that the user knows.

Final Notes on Authentication

- There are other factors that can be taken into account when conducting authentication. E.g. Alice's location.

- Alice may carry around a cellphone that has a GPS chip inside of it.

- When Alice stands in front of an ATM requesting to withdraw money, Alice's bank could ask her cellphone company's computer system where she currently is.

- If the cellphone company's computer responds with a latitude and longitude that corresponds to the expected location of the ATM, the bank can approve the withdrawal request.

Final Notes on Authentication

- However, if Alice's ATM card and PIN were stolen by a bad guy who is trying to withdraw money, then taking Alice's location (or specifically, the location of her cell phone) into account could help thwart such a fraudulent withdrawal request.