Date ____/____/____

MON TUE WED THU FRI SAT SUN

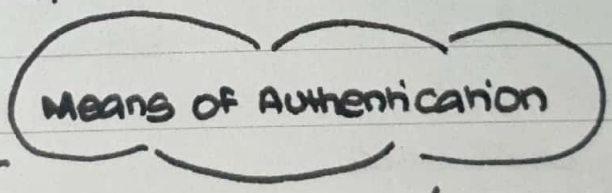
18 (MID 2)

SANDEN
SANPAK ENGINEERING INDUSTRIES (PVT) LTD.

=> User Authentication: 3.1

* User authentication has 2 functions - user identifies themselves through a credential and system verifies by exchange of authentication information.
* User authentication is basis for most types of access control and user accountability.
* User identifer & an item associated with that identifier (password) are typically used for authentication. Identifer can be used to send emails etc while item restricts someone from posing as that user.
* User authentication is distinct from message auth.
* User auth means to establish confidence in user's identity and to determine their access to functions.
* Authentication Architectural Model:
  - Required for user to be registered on the network.
  - To register:
    - Applicant applies to registration authority (RA). to become subscriber of credential service Provider (CSP)
    - CSP issues an electronic credential to subscriber.
    - Credential is a data structure that binds identity and token together.
      ↳ encrypted key/password. Set by CSP/ user / third party.

- To authenticate:
  - Party to be authenticated called claimant, party verifying called verifier.
  - Claimant successfully demonstrates possession & control of token to verifier.
  - Verifier passes on assertion about identify of subscriber to relying party (RP).
    - identity info about subscriber, name, identifier assigned at registration, other subscriber attributes verified in registration process.
  - RP uses authenticated info to make access control / authorization decision.



Something user is (static biometrics): recognition by fingerprints/ retina/ face.

Something individual knows - password/ PIN/ prearranget set of questions.

Something individual does: Recognition by voice pattern / handwriting/ typing rythm.

Something individual possesses - Electronic key cards/ smart cards / physical keys
Also called tokens.

* Means of authenication can be used alone or in combination.

* means of authentication can have issuses such as adversary can steal | forge token | password . significant overhead on systems in managing them . issue of false positive | negative, cost , convenience.

* Multifactor auth means use of more than one means of authentication .

* Strength of auth-systems deermined by no. of factors incorporated by systems.

* Assurance level - organizations degree of certainty that user has given a credential that refers to his | her identity.

↳ confidence in the vetting process to establish identity of user.

↓ Degree of confidence credential used by individual is the same individual it was issused to.

* level 3: high confidence enable clients to access restricted services multifactor authentication (2)

level 1 : little or no confidence - user supplied ID & password at time of transaction

Assurance level

level 2 : some confidence use secure authentication protocol along with means of authentication.

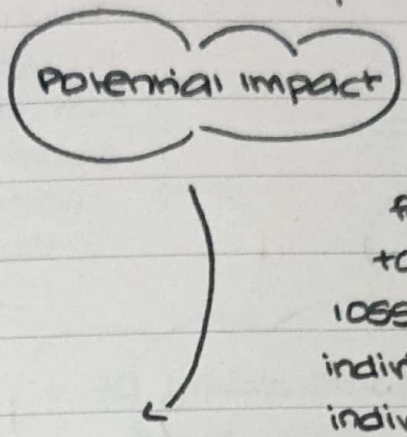
level 4 : very high confidence enable clients to access restricted services of high value
use multi-factor auth & in-person registration.

user identifier = ID

Date ___/___/___
MON TUE WED THU FRI SAT SUN

* Potential Impact - impact on organization incase of security breach.

*



LOW: limited effect on organization's operations / assets / individuals. causes reduction in effectiveness of a function, minor damage to assets, minor financial loss to organization / individuals, minor harm to individuals.

Moderate: serious effect. effectiveness of function seriously reduced (use significant with causes in LOW)

High: severe effect. Not able to perform functions. (use severe / major with causes in LOW)

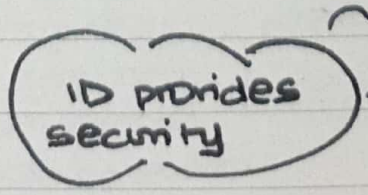
* Areas of risk - Mapping between potential impact & assurance level. LOW / Moderate / High.

* Potential impact LOW use AL 1, PI Moderate use AL 2/3, PI use AL 4.

3.2: Password based Authentication.

* Password provided is compared with password store previously against the ID.

*

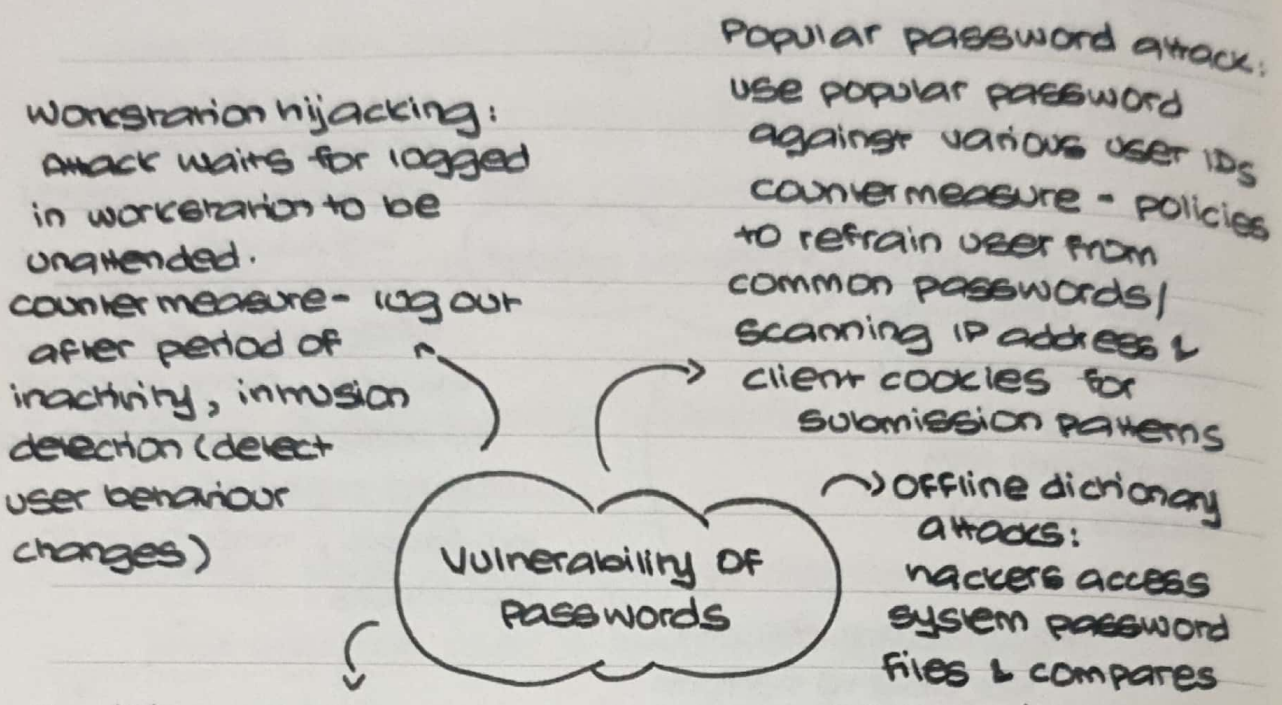


user authorized to access system

privileges accorded to user.

can be used for discretionary access control.

*


Vulnerability of Passwords
Workstation hijacking: attack waits for logged in workstation to be unattended. counter measure - log out after period of inactivity, intrusion detection (detect user behaviour changes)
Popular password attack: use popular password against various user IDs counter measure - policies to refrain user from common passwords/ scanning IP address & client cookies for submission patterns
Offline dictionary attacks: hackers access system password files & compares password hashes against commonly used passwords hashes. Gain access through the match. countermeasure - restrict unauthorized access/ intrusion detection/ rapid reissuance of passwords.
Specific account attack: target an account and keep guessing passwords until a match. counter measure - account lockout measure (5 attempts)
Password guessing against single user: Gain knowledge of user & system policies. use to guess passwords. countermeasures: Policies that make password guessing hard - secrecy, min length, character set, length of time before password change.
Exploiting user mistakes: user hold of shared/ written down password. use social engineering to trick users to reveal password. Pre-configured passwords not changed. counter measure - user training/ intrusion detection/ simple pass with auth mechanism.

Electronic monitoring:
Password communicated through a network can be evasdropped.
Password used to encrypt can be used by adversary to be reused.

continued ....

Exploiting multiple password use:
Network devices share same password makes attacks more effective.
counter measure + policy to restrict some passwords.

* Schemes relying on single sign on to multiple services using non password technique creates single point of failure

Popularity of Passwords ?

Need widespread instalment of biometrics on one side to encourage integration on other side too (client-server)

Automated password managers have poor support for roaming & synchronization across multiple client platforms.

Physical tokens are expensive & inconvient to carry around

* Use of hashed passwords & salt value found on all UNIX systems.
* The user selects | is assigned a password which is combined with a fixed length salt value.
* Password & salt serves as input to hashed ~~passwords~~ algo to generate hash code.

↳ Before - timestamp.
Now - pseudorandom number.

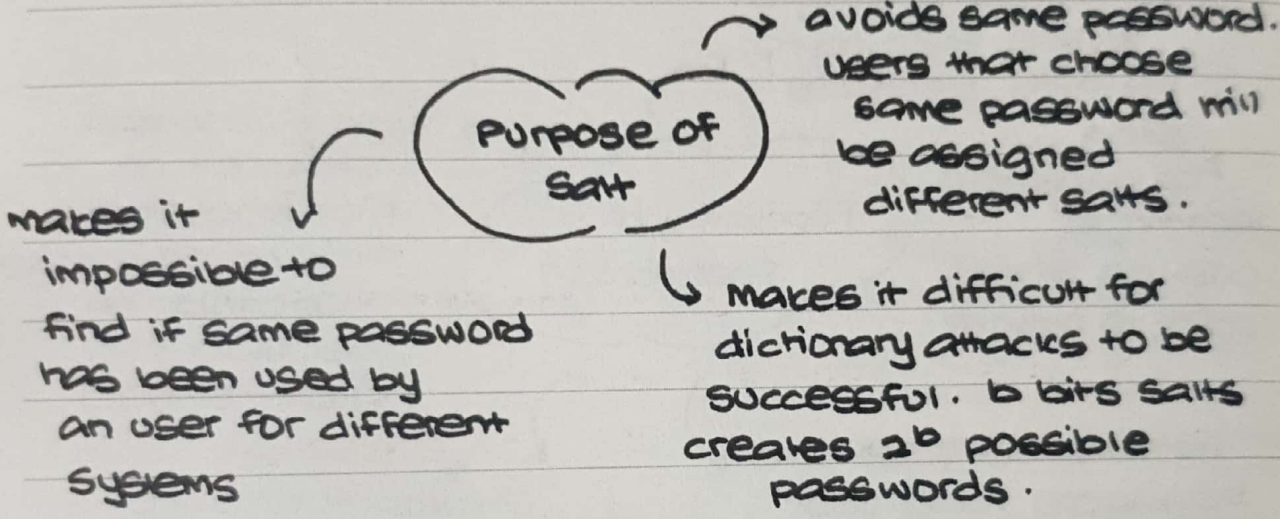
Date ____/____/____

MON TUE WED THU FRI SAT SUN

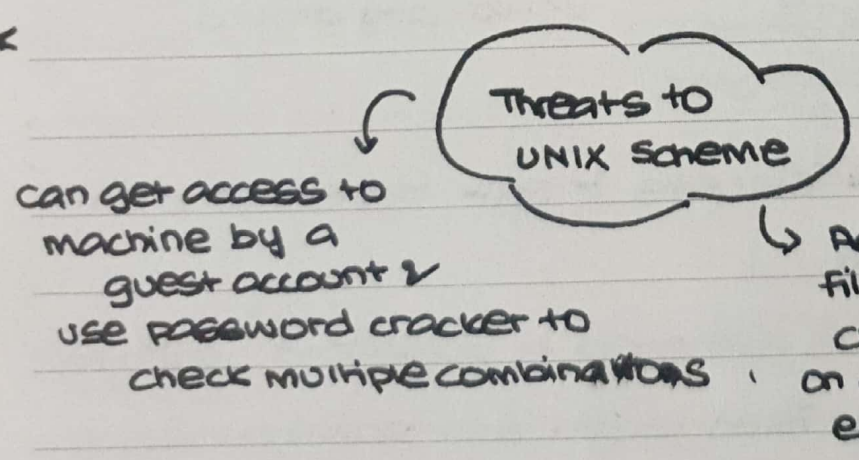
SANDEN
SANPAK ENGINEERING INDUSTRIES (PVT) LTD.

* Hash algorithm is designed to be slow to avoid attacks.
* Hash password is stored along with plaintext salt.
* On log-in the ~~encrypted~~ password and plaintext salt are inputted to an encryption routine. If result matches stored pass user allowed to log-in.

*



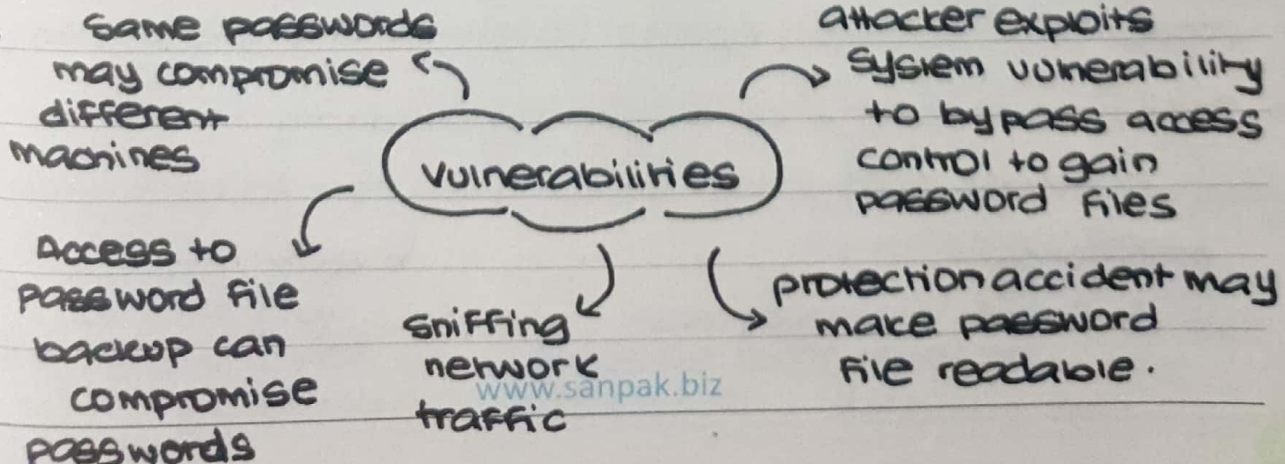
*



* Popular hash scheme used is MD5 hash algorithm.
* Bcrypt hash uses a cost variable to variate time required to

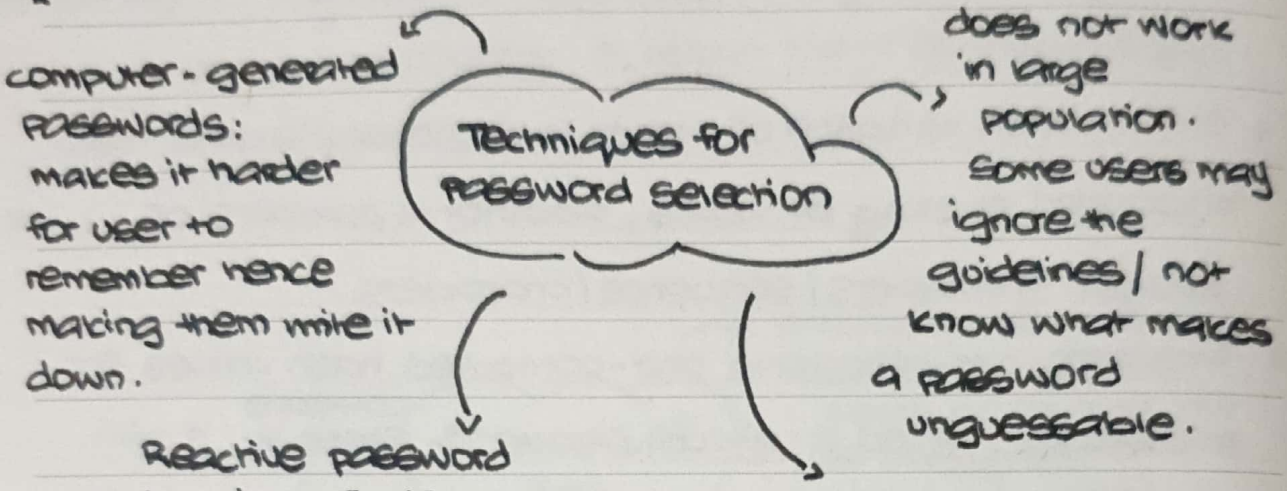
compute hash.

* Tradiontianal way of cracking passwords was to compare a large dictionary of passwords & compare it until a match was found.
* On no match variation of words in dictionary is done like backward spelling of words, additional numbers or special characters / sequence / characters.
* Attackers can also have pre-computed hash values for passwords called a rainbow table & compare it with password file. countermeasure large salt & hash length.
* complex password policy - organizations forcing users to build a complex password.
* Sophisticated models are trained on leaked password files which order guesses based on character-class structure, freq of digit & symbol substring.
* To avoid leaking of password files. Hash passwords are kept seperately from user ID files called shadow password file.
* Same passwords may compromise different machines



* Goal is to limit guessable passwords but also make it easier for user to remember.

*



* Rule enforcement - password should be atleast 16 characters (basic 16) / should have 8 characters upper & lower case, symbol / digit. (comprehensive 16).

* Password checker - compile a long dictonary of dis-approved passwords. Do not allow user to keep those passwords.

↳ space: dictionary must be large to be effective

↳ time: takes a long time to search through the dictionary.

* Effective proactive password checker is based on bloom filter.
* Hash table of N bits is produced. Each password k hash values are calculated corresponding bits set to 1. If all values are one password rejected. Use a probality function to calculate false positives & decide how many hash functions to use.

3.3 : Token-based authentication.

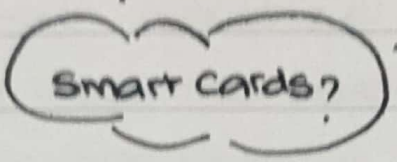
* Memory cards can store but not process data.
* Magneric strip stores a security code to be read/ reprogrammed by a card reader.
* Memory card combined with a PIN provides greater security than a password alone.
* Hackers need to know the PIN & have physical possesion of the card.
*

Date ____ / ____ / ____

MON TUE WED THU FRI SAT SUN

SANDEN
SANPAK ENGINEERING INDUSTRIES (PVT) LTD.

* Smart



Electronic interface: to communicate with the token reader

Contact - inserted into a card reader with a direct connection to a conductive plate.

Contactless - requires close proximity to a reader. communicate through radio Frequencies.

Physical characteristics: have embedded microprocessor

User interface: keypad & display for human/token interactions.

Authentication protocol: to provide a means for user authentication.

Static - user authenticates to token which authenticates to computer.

Dynamic password generator - computer generates unique password periodically, enter manually or via token. Must be kept synchronized.

challenge-response - system generates a challange & token generates response based on challange.

* Some smart cards can contain co-processing circuits to generate digital signatures.

* Smart card have 3 types of memorys.

ROM - read only, stores data that does not change card's no/ card holder's name.

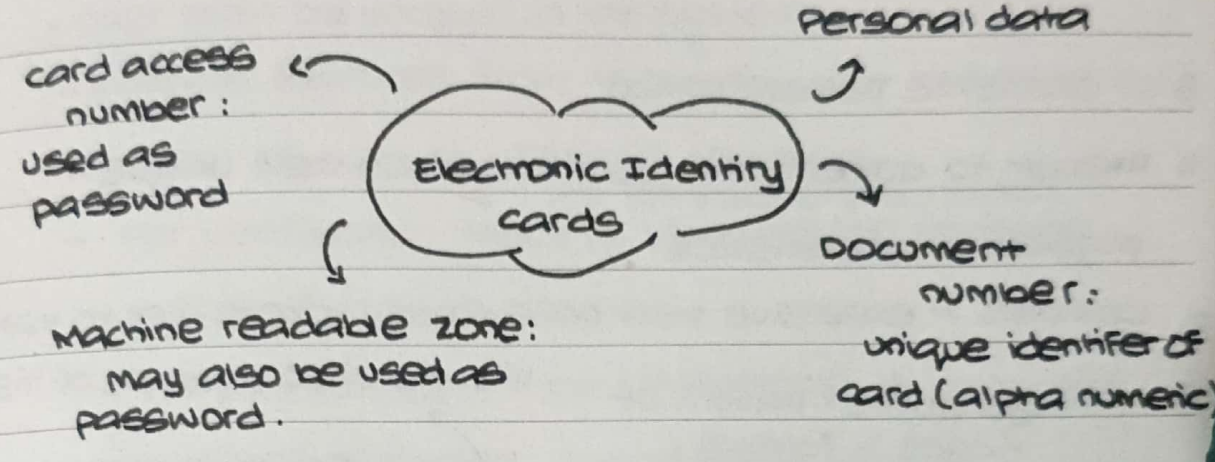
EEPROM - holds application data / programs like protocols to execute.

RAM - temporary data when application is executed.

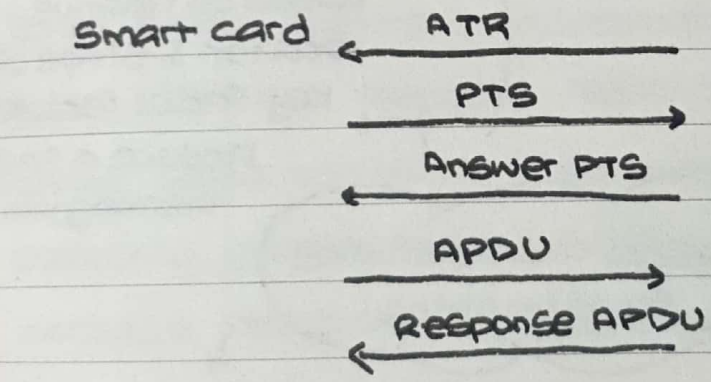
* When card entered into reader reset (ATR) performed. card responses to ATR message defining parameters &

protocols. Terminal may be able to change these through PTS command. cards PTS response confirms parameters & protocols.

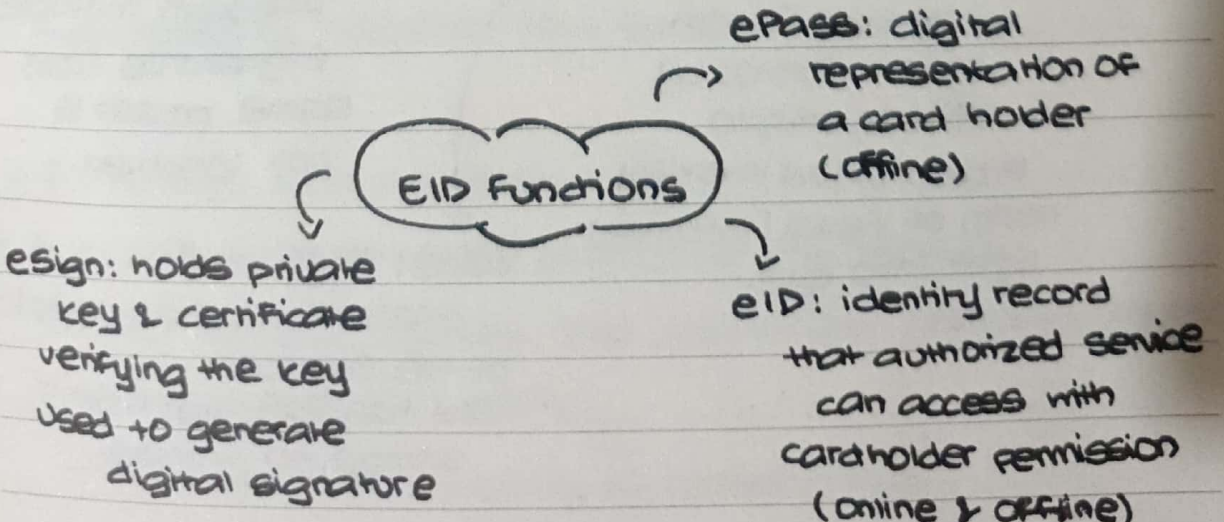
*



*



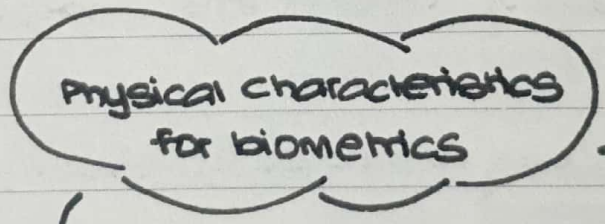
*



* PACE ensures RF chip cannot be accessed without explicit access contrl. Online user enters 6-digit PIN. Offline use MRZ / CAN.

3.4: Biometric Authentication

* Attempt to authenticate user based on their unique physical characteristics.
* complex & expensive than passwords / tokens, yet to mature.
* Fingerprints: Pattern of ridges & furrows. Are unique for each human
* Iris: detailed structure of iris
* Facial characteristics: based on relative location & shape of key facial features. Produce a face thermogram.
* Hand-geometry: features of hand like shape, length, width of fingers
* Retinal Pattern: Pattern formed by veins is unique. Project a low intensity beam of visual / infrared light into eye.
* Signature: Although multiple signatures from same person is not identical.
* Voice: Physical & anatomical characteristics of the speaker. Still has variation from sample to sample.



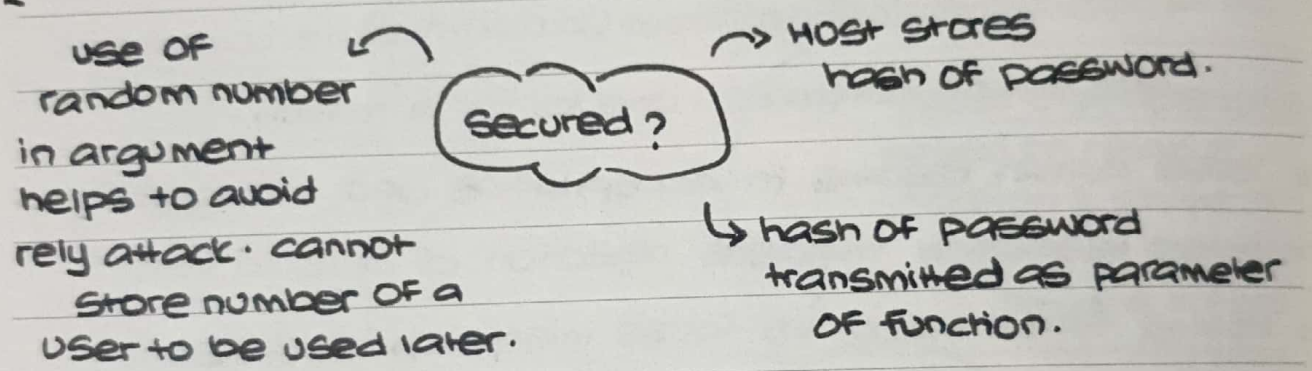
* In biometrics we check how closely related the input is to stored data.
* Working of biometrics system:
  - User must be enrolled in the system.
  - Extracts features from biometric input and store it as a set of number. Termed template.
  - For verification input (→ PIN, biometrics, token) is compared to template. checks if their is a match.
  - For identification input (biometrics) is compared with set of templates. checks for a match.
* False match results in acceptance of a wrong user.
* False mismatch triggers rejection of a valid user.
* Plotting false match vs false mismatch is called operating characteristics curve.
* Increase threshold increases security but reduces convience and vice versa.
* High security requires low false match rate.

3.5: Remote user authentication

* Authentication that takes place over the network.
* Counter threats systems use challange-response protocol.
* Password protocol (PP)
  - User transmits identity to remote hosts.

- Host generate random no (r) called nonce, send to the user.
- Host specifies h() & f() to be used in response.
- User responses f(r', h(P')), r' = r & P' = password.
- Host stores hash function of each registered user's password as h(P(U)), U = user
- Host compares f(r', h(P')) with f(r, h(P(U))) to match.

*



* Token Protocol
  - User transmits identity to host.
  - Host returns r, f(), h().
  - User's token provide W' = passcode. Can be static/ one time generation.
    ↳ Needs to be synchronized with host.
  - Passcode activated by user through P' = password only between token & user.
  - Token sends f(r', h(W'))
  - Host for static stores h(W(U)) for dynamic generates a one time passcode & its hash.
  - Same as PP.

* Static Biometric Protocol
  - A user transmits identity to host
  - Host responds with r , E() → encryption.
  - Biometric template BT' from biometrics B' returns E(r', D', BT') , D' = biometric device. Send to host.
  - Host decrypt parameters & compare to stored values. Must find r'=r , score of BT' > threshold & D' in registered devices list.

* Dynamic Biometric Protocol
  - Host provides random sequence & random no as challange.
  - Human must vocalize / type / write to generate a biometric signal BS'(x') . Encrypt BS'(x') & random no.
  - Host decrypts r'=r , generates comparison based on BS'(x'), BT(U) & original signal x.
  - comparison > threshold for user to match.

3.6: Security issues for user authentication.

* Host attacks: password file under attack
  one time passcode for token. use challange-response protocol for dynamic biometrics

Attacks

Client attack: adversary tries to attack as a legitimate user.
increase password size, limit no of attacks.
use PIN with token
require both to grant access.

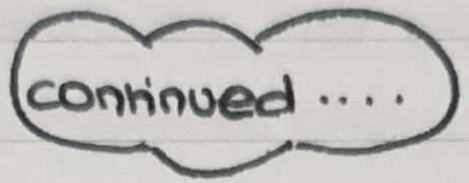
Date ____/____/____

MON TUE WED THU FRI SAT SUN

SANDEN
SANPAK ENGINEERING INDUSTRIES (PVT) LTD.

Replay: use previously captured user response
use challange-response protocol

eavesdropping:
gain password by observing user / read written password / keystroke logging.
use multiple factors
Static biometrics,
use device auth.



Trojan Horse:
device pretends to be auth device to gain password

Denial of service: disable user auth by flooding host with requests
can be done to a selective user by exceeding log-in limit.
use multiple auth factors.