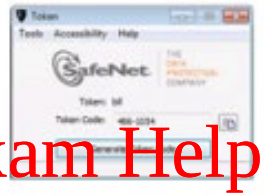
Authentication: Something you have …

Example: advanced tokens that produced password …

Smart Phone Tokens

SMS Tokens

USB Tokens



Software Tokens

Grid Tokens

Keyfob Tokens

Keypad Tokens

Credit Card Tokens

OATH

3rd Party Tokens

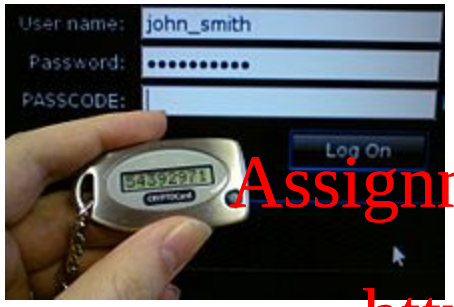
Tokens themselves are NOT presented to the system. Can be used 'remotely'.

Combine 'what you have' with 'what you know'!!!

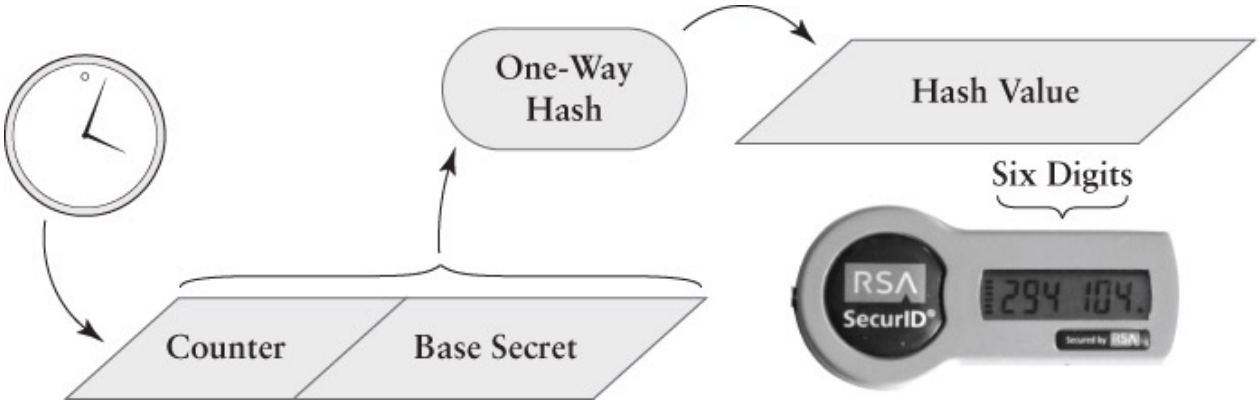
https://strom.wordpress.com/2013/05/28/two-factor-auth/

Authentication: Something you have …

2.2) Synchronous (One-Time Password) Tokens



- **small LCD device that generates a unique new password periodically** (e.g., every 60 seconds)
  - token combines '**base secret**' with a **clock** to generate new password
  - token and authentication server must have their clocks synchronized – which is often a challenge!



Authentication: Something you have …

Example: Synchronous (One-time Password) Token

Token

Time 12:16:03
Date 04/16/2014
Algorithm p19728

Algorithm and time create code

Code = 962991

May be a problem!

Time 12:16:03
Date 04/16/2014

Customer: Jean_Paul
Algorithm x11091

Customer: Adia_Umi
Algorithm r29071

Customer: Stacey_Harris
Algorithm p19728

1. User looks up code on token

Stacey Harris

2. User enters username and code

USERNAME: Stacey_Harris
PASSWORD: 962991

Codes match

3. Authentication server creates code

Algorithm and time create code

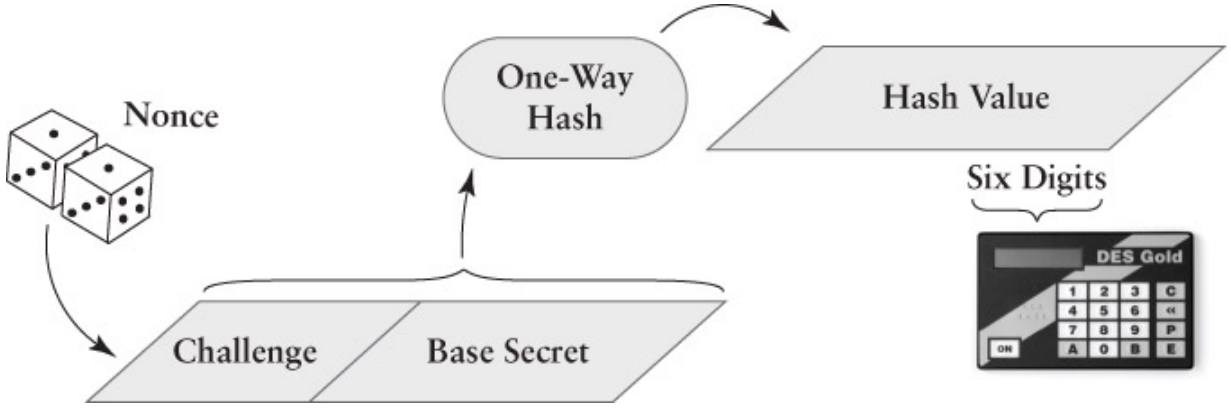
Code = 962991

Authentication server

Authentication: Something you have …

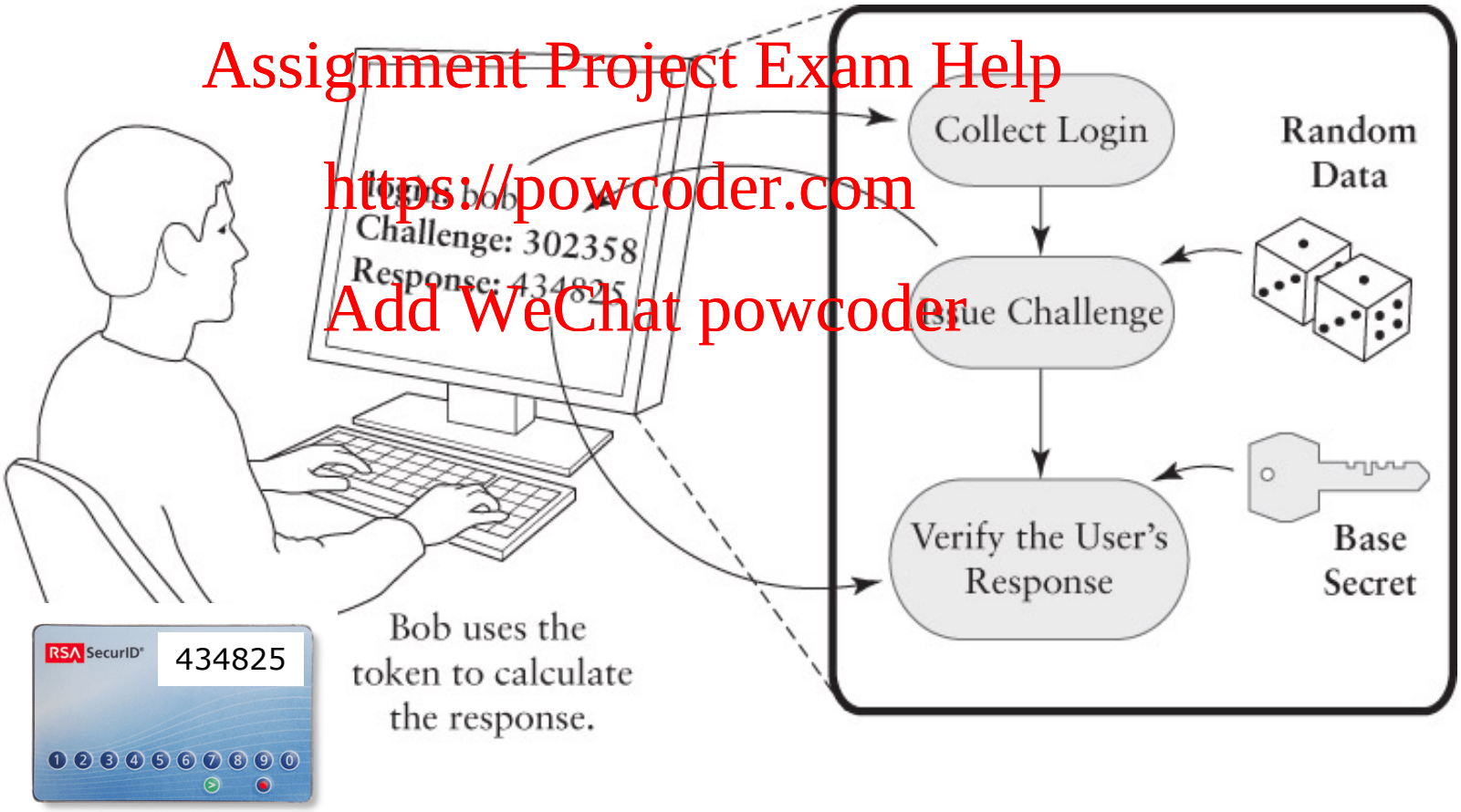
2.3) Asynchronous (Challenge-Response) Tokens

- **instead of time, token uses a challenge/nonce provided by the system to generate the password**
  - e.g., token can generate the password by
    1) applying a unique hash function to (user's base secret + nonce)
    2) encrypting nonce using user's/token's public key



Authentication: Something you have …

Example: Asynchronous (Challenge-Response) Token



Authentication: Something you are …

3) Something you are (Static / Standard Biometrics)

Fingerprint scanner

- authentication mechanisms that takes advantage of users' unique **physical** characteristics, including
  - **fingerprints**
  - **facial characteristics**
  - **retina**
  - **Iris**

- in contrast to password/token authentic., biometric systems do not look for a 100% match – person's characteristics are inherently 'noisy'
  - **pattern recognition must be involved**
- very effective but costly if a large number of biometric readers need to be installed!

Authentication: Something you are …

- **Biometric Modality** = different types of biometric information / measurements that can be used to discriminate between different individuals

https://www.researchgate.net/publication/281659557_Soft_Biometrics_for_Keystroke_Dynamics/figures?lo=1

Authentication: Something you are …

- **an ideal biometric modality / information should have the following properties:**
  - **Universality** – all individuals must be characterized by this information
  - **Uniqueness / Distinctiveness** – this information must be as dissimilar as possible for two different individuals
  - **Permanency / Stability** – this information should be present during the whole life of an individual
  - **Collectability / Measurability** – this information should be measured in an easy manner
  - **Acceptability** – how willing individuals are to have this biometric information captured and assessed
  - **Performance** – this information can be used to build **accurate**, **fast** and **robust** biometric/authentication systems

Authentication: Something you are …

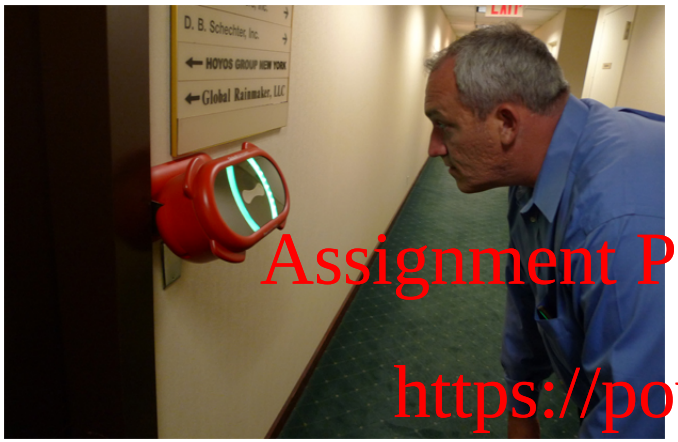
- an ideal biometric modality / information should have the following properties:
  - **Resistance to Attack** – how easy it is for this information to be forged

Information	U	N	P	C	A	E
DNA	Yes	Yes	Yes	Poor	Poor	*****
Gait	Yes	No	Poor	Yes	Yes	***
Keystroke dynamics	Yes	Yes	Poor	Yes	Yes	****
Voice	Yes	Yes	Poor	Yes	Yes	****
Iris	Yes	Yes	Yes	Yes	Poor	*****
Face	Yes	No	Poor	Yes	Yes	****
Hand geometry	Yes	No	Yes	Yes	Yes	****
Fingerprint	Yes	Yes	Yes	Yes	Fair	****

Table 1. Comparison study of biometric modalities in terms of universality (U), uniqueness (N), permanency (P), collectability (C), acceptability (A) and performance (E). For the performance, the number of stars is related to the modality's performance (i.e., EER) in the literature [3].

Authentication: Something you are …

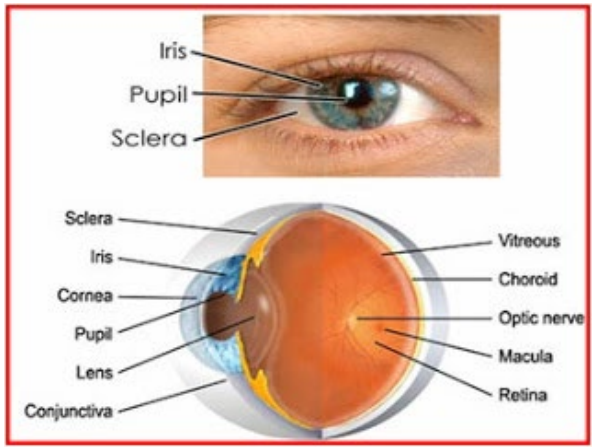
Iris scanner



Retina scanner

IRIS - colored section of an eye
scan = 2 seconds of near IR imaging ☺
subject can be at some distance ☺
alcohol consumption changes iris ☹

RETINA - cannot be seen by naked eye - the network of blood vessels
most reliable biometrics, aside from DNA ☺
scan = 15 seconds of low-energy IR scanning ☹
subject has to be close(er) to scanner ☹



Authentication: Something you are …

- **Biometric System** – generic architecture

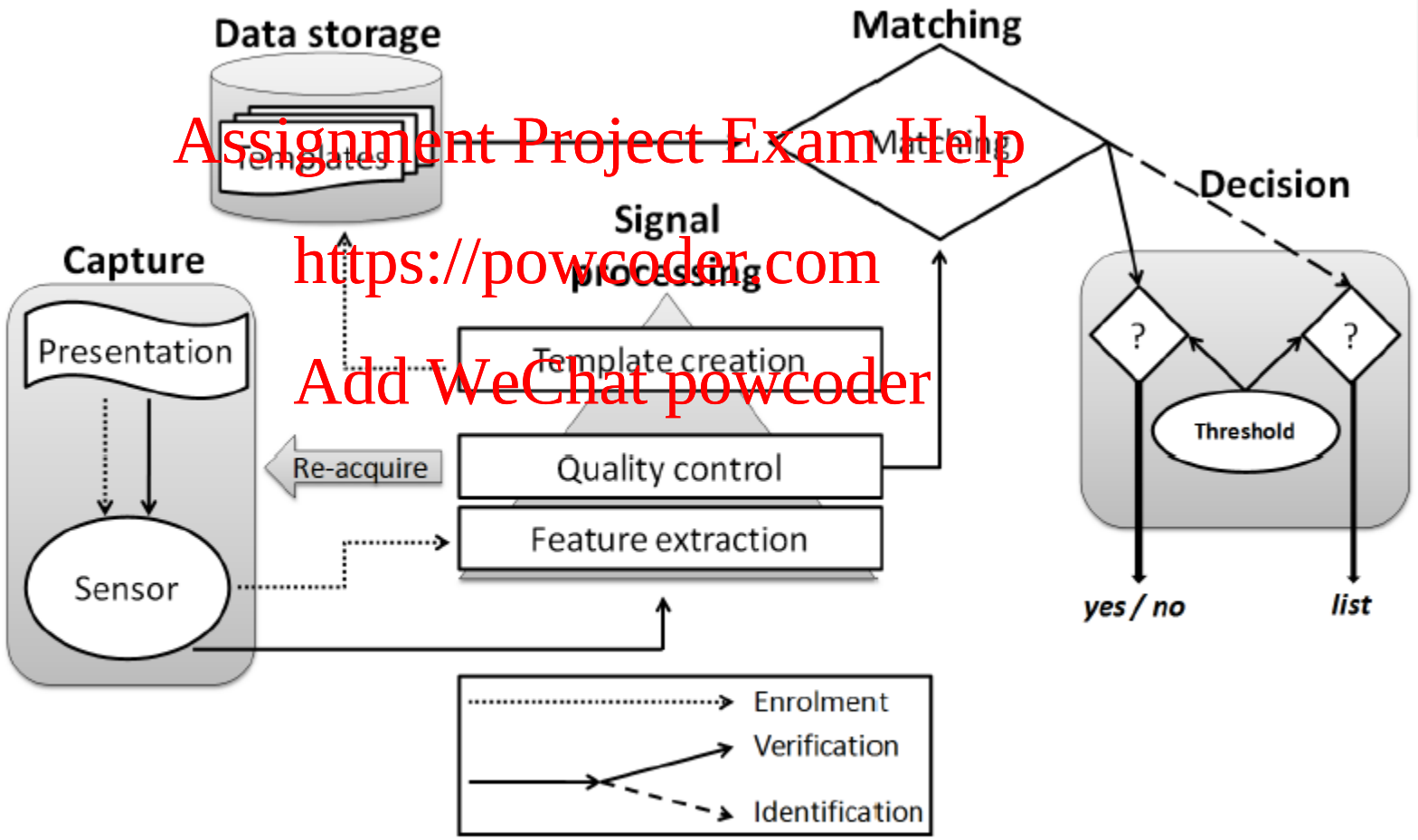
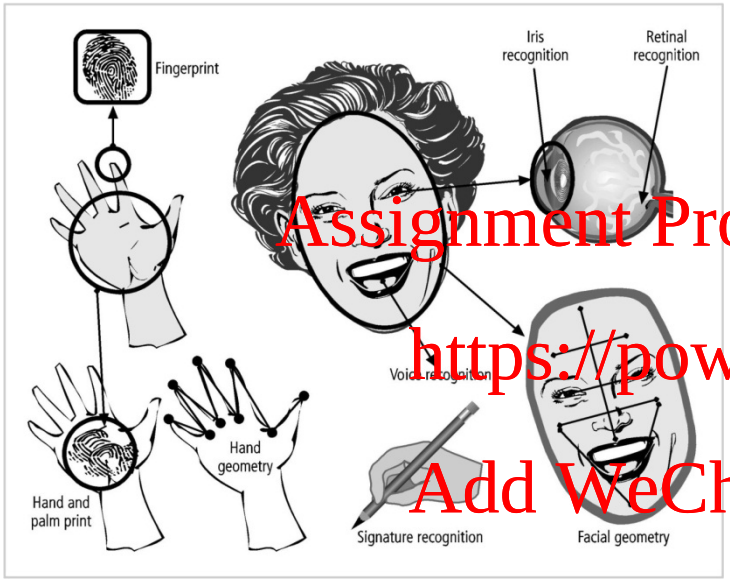
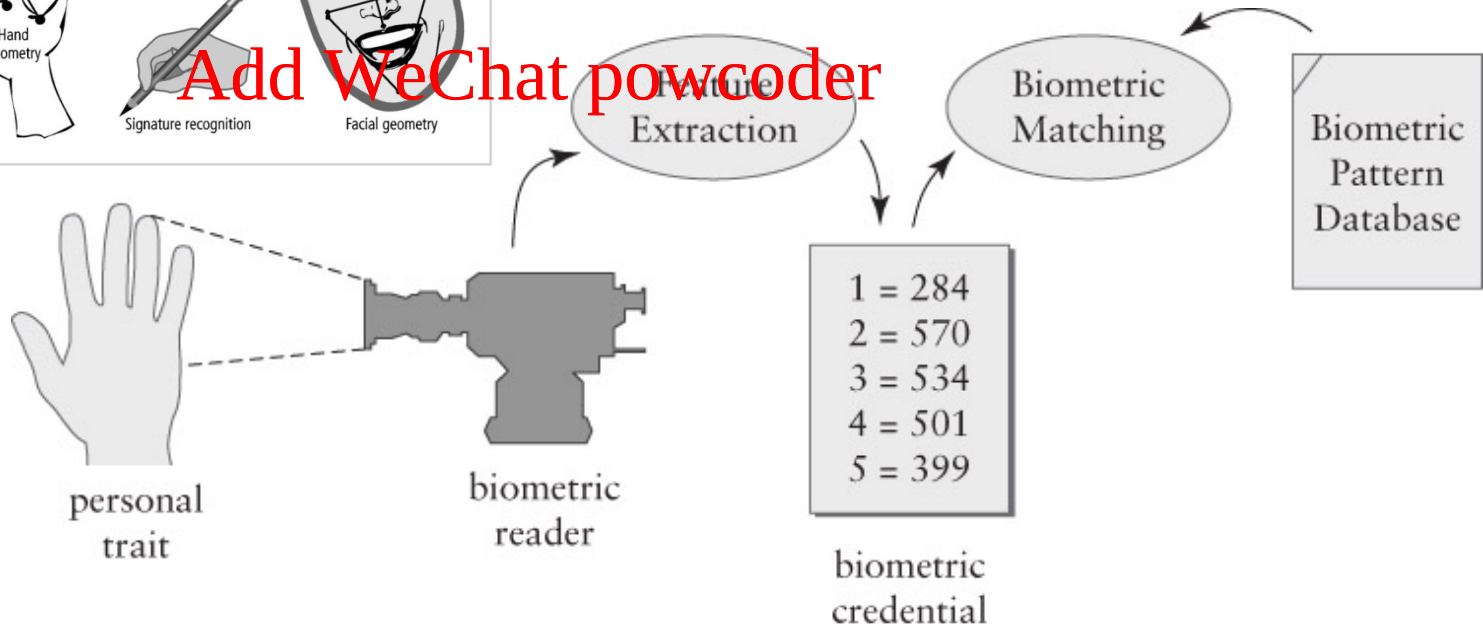


Figure 4. Generic architecture of a biometric system (source [4]).

Authentication: Something you are …

Example: Extraction of biometrics features

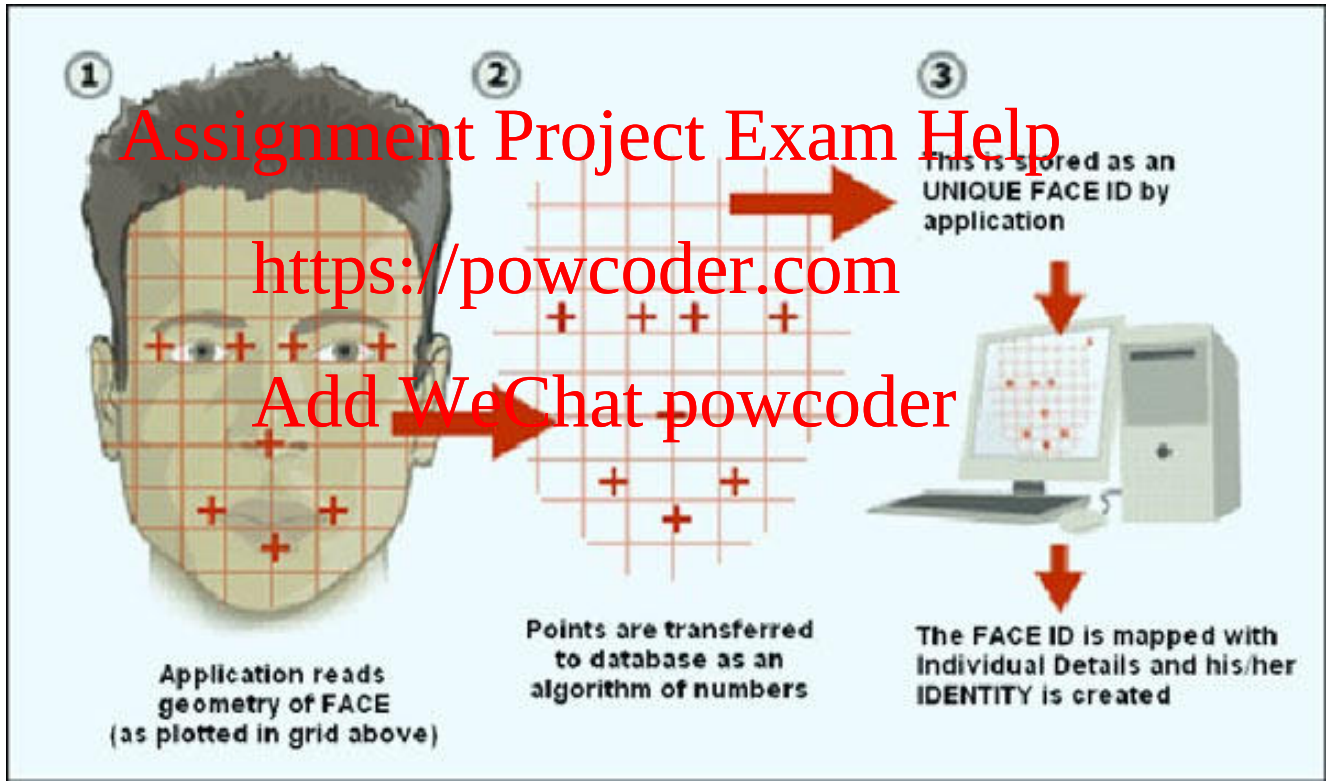




Also see: http://computer.howstuffworks.com/biometrics-privacy.htm

Authentication: Something you are …

Example: Extraction of biometrics features



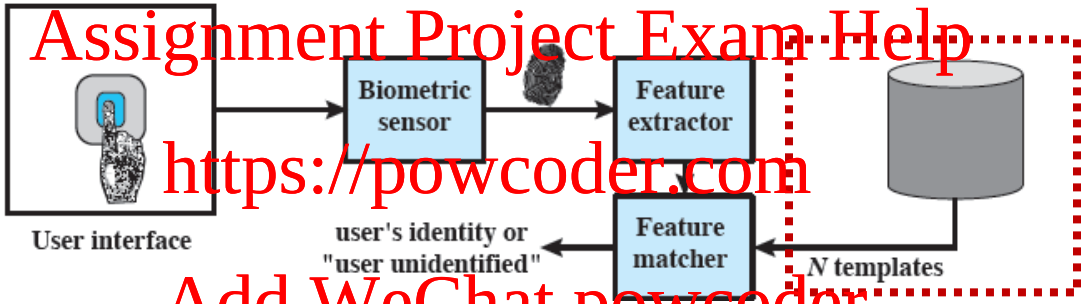
https://creativentechno.wordpress.com/2012/02/18/face-recognition/

Authentication: Something you are …

- **Types of Biometric Systems**

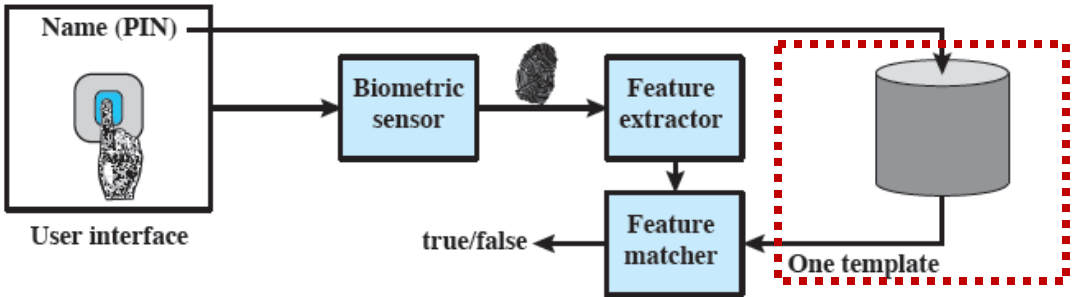
  1) systems for **IDENTIFICATION**

  - perform **1:n comparison** to identify a user from a database of n users



  2) systems for **AUTHENTICATION**

  - perform **1:1 comparison** to check whether a user matches his profile



Authentication: Something you are …

- **Biometric Accuracy**
  - in all biometrics schemes, some physical characteristic of the individual is mapped into digital representation
  - however, physical characteristics may change
    - facial contours and color may be influenced by clothing, hairstyle, facial hair, makeup …
    - the results of fingerprint scan may vary as a function of: finger placement, finger swelling and skin dryness …
  - multiple mappings may have to be taken in order to obtain a (statistically) useful biometric representation
  - a biometric sensor must be able to adapt to a broad range of appearances

Authentication: Something you are …

- **Biometric Accuracy**

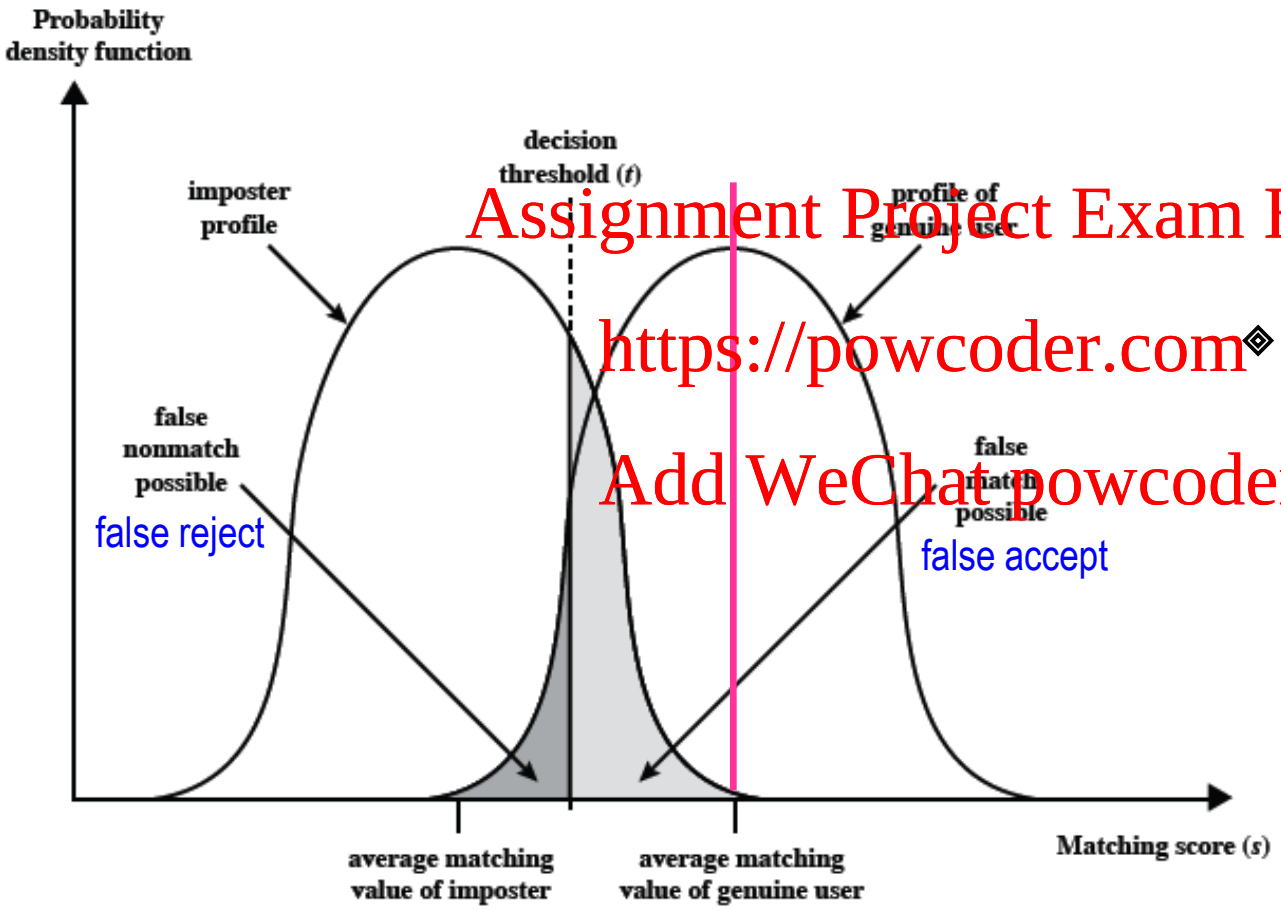


Figure 3.7 Profiles of a Biometric Characteristic of an Imposter and an Authorized Users In this depiction, the comparison between presented feature and a reference feature is reduced to a single numeric value. If the input value (s) is greater than a preassigned threshold (t), a match is declared.

- unfortunately, range of scores/features for any particular user is likely to overlap with scores/features of other users
- by moving the '**decision threshold**', sensitivity of biomet. system changes

Where should we put the Threshold?!

move *t* to left ⇒

system more tolerant to noise 👍, but also

system more likely to accept wrong person 👎

Authentication: Something you are ...

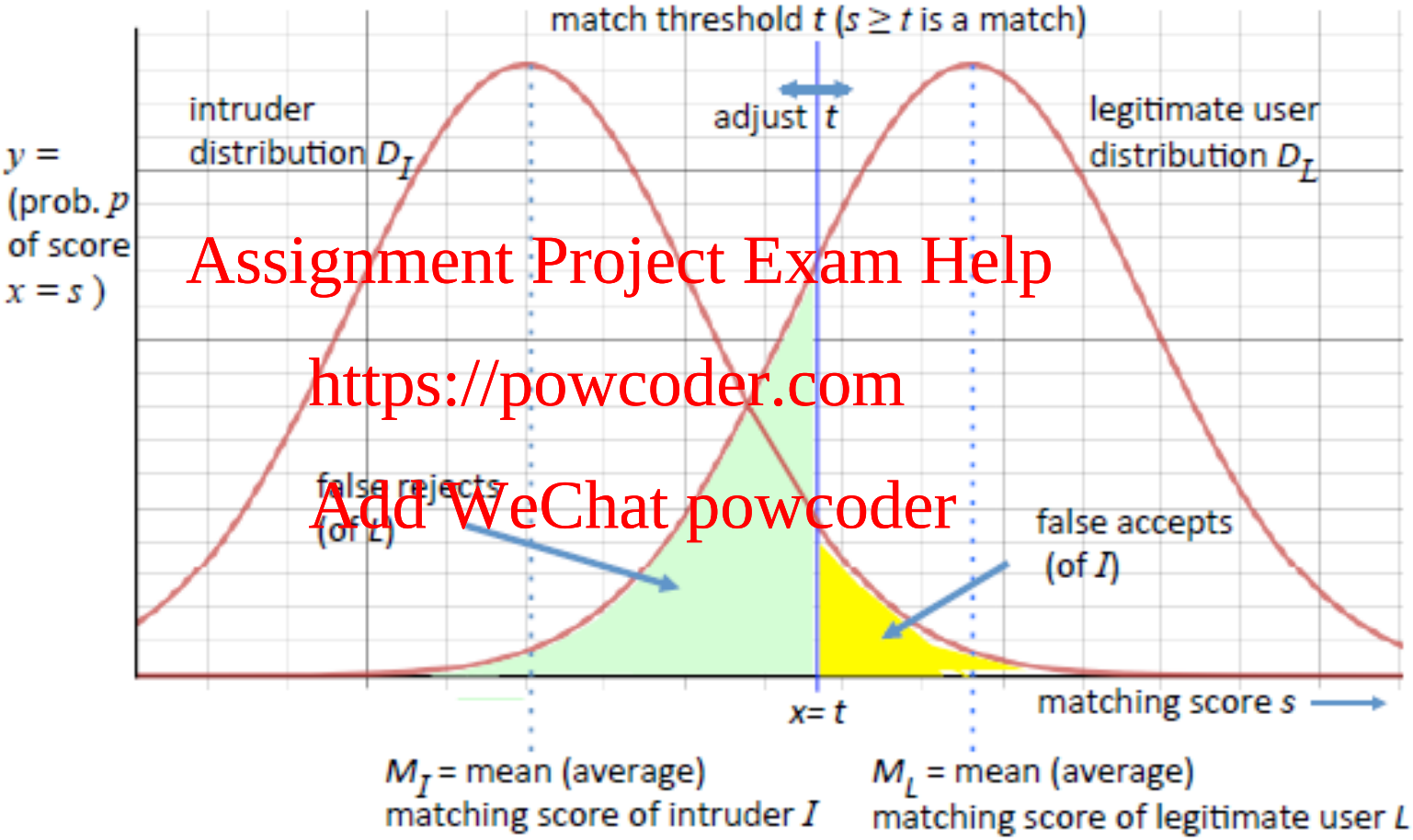


Figure 3.6: Biometric system tradeoffs. Curves model probability distributions for an intruder and legitimate user's matching scores; higher scores match the user's biometric template better. The y axis reflects how many biometric samples get matching score $x = s$.

https://people.scs.carleton.ca/~paulv/toolsjewels/ch3-long.pdf

Authentication: Something you are …

- Biometric Accuracy (cont.)
  - **False Reject Rate (FRR), aka False Negative**
    - % (fraction) of authorized users who are denied access
    - false negatives do not represent a threat to security but an annoyance to legitimate users
  - **False Accept Rate (FAR), aka False Positive**
    - % (fraction) of unauthorized / fraudulent users who are allowed access to system
    - represent serious security breach

$$\text{"Convenience"} = (1 - \text{FR})$$

the higher the FR rate, the less convenient an application is because more subjects are incorrectly rejected …

$$\text{"Security"} = (1 - \text{FA})$$

the lower the FA rate, the fewer imposter users (adversaries) are incorrectly accepted into the system

Authentication: Something you are …

Example: biometric accuracy

	False reject / (FN)	False accept / (FP)
Fingerprint	3-7 in 100 (3-7%)	1-100 in 100K (0.001-0.1%)
Face	1-20 in 100 (1-20%)	100-10K in 100K (0.1-10%)
Voice	10-20 in 100 (10-20%)	2K-5K in 100K (2-5%)
Iris	2-10 in 100 (2-10%)	$\leq 10^{-5}$ ($\leq 0.001\%$)
Hand	1-2 in 100 (1-2%)	10-20 in 1000 (1-2%)
Signature	10-20 in 100 (10-20%)	2-5 in 100 (2-5%)

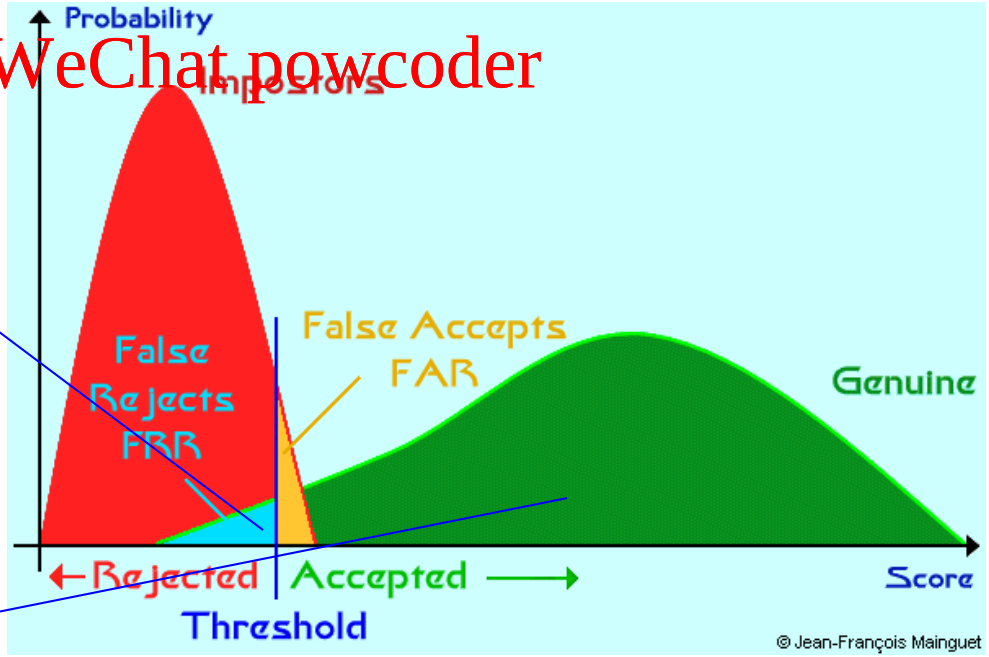
Table 15: Roughly the error rates that can be found in the literature, based on scenario and technology evaluation.

http://www.cse.lehigh.edu/prr/Biometrics/Archive/Papers/rc22481.pdf

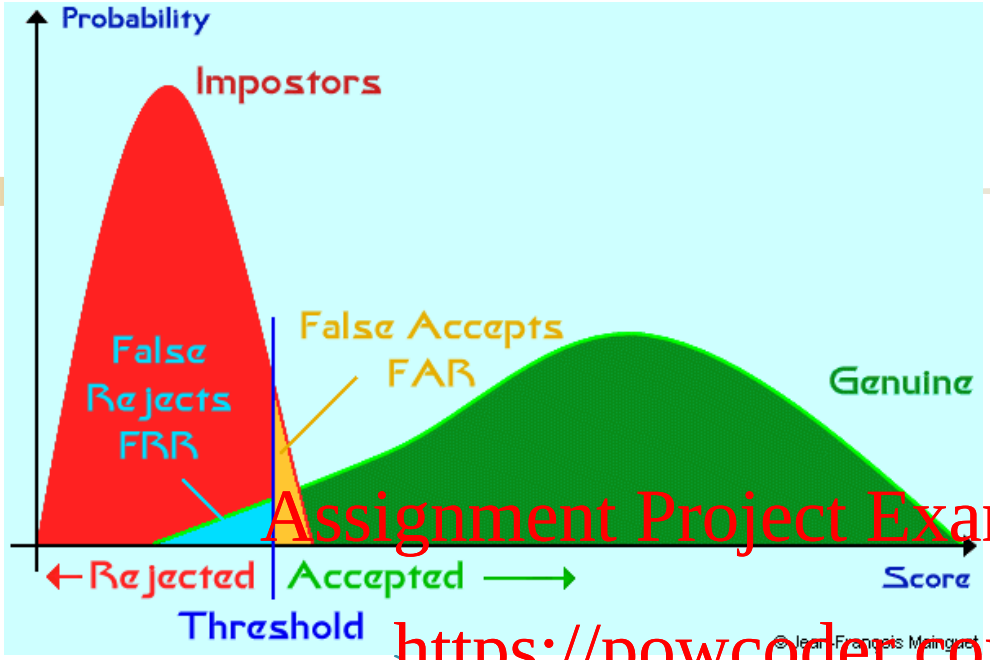
Authentication: Something you are …

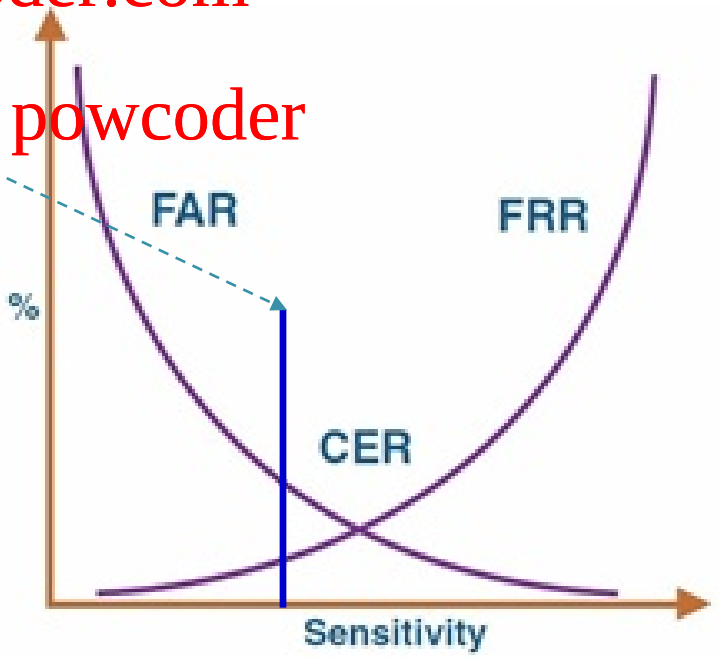
- **Crossover Error Rate (CER)**, aka Equal Error Rate
  - point at which FRR = FAR – Operating Point of choice for most biometric systems – provides balance between sensitivity & performance (i.e., convenience & security)
  - techniques with 1% CER superior to 5% CER

as threshold moves to the left, system becomes '**less sensitive**' and the value of FRR decreases but the value of FAR increases



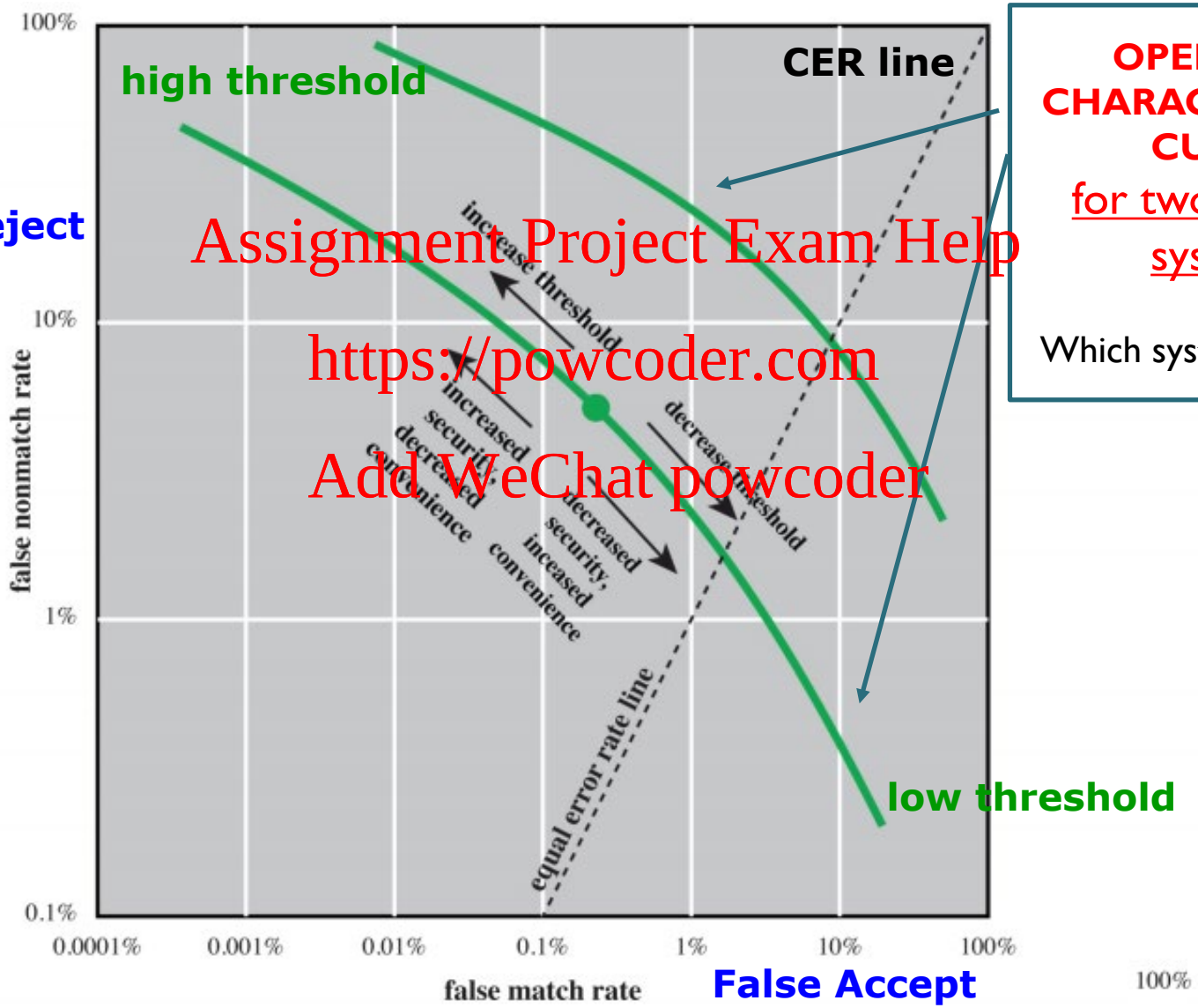
as threshold moves to the right, system becomes '**less sensitive**' and the value of FRR decreases but the value of FAR increases





http://fingerchip.pagesperso-orange.fr/biometrics/accuracy.htm

Authentication: Something you are …



False Reject

False Accept

OPERATING CHARACTERISTICS CURVES

for two different systems.

Which system is better?!

Authentication: Something you are …

Example: biometric accuracy

Assume a system where each airport passenger is identified with a unique frequent flyer number and then verified with a finger print sample.

The systems false reject (FR) rate for finger is: 0.03 (= 3%).

5000 people / hour are requesting access to the airport during a 14 hour day.

How many people will fail to be verified in a day?

rejected passengers =
= (5000 * 0.03) [rejects / hour] * 14 [hours] =
= 150 [rejects / hour] * 14 [hours] =
= 2100 [rejects]

Authentication: Something you produce …

4) Something you produce: Dynamic Biometrics

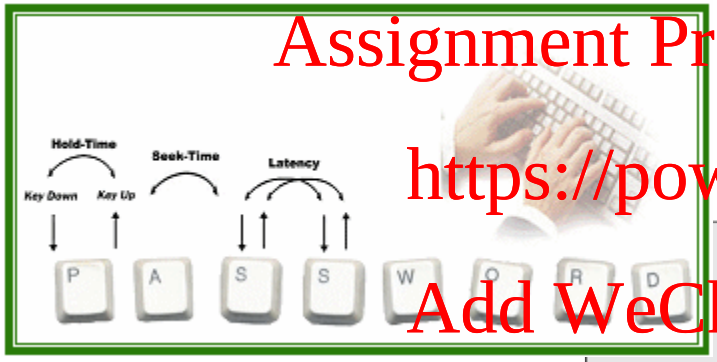
- authentication mechanisms that makes use of something the user performs or produces
  - signature recognition
  - voice recognition
  - keystroke pattern recognition

- less costly than 'what you are' systems, but not as reliable
  - signature, voice, keystroke pattern may change significantly with time and under different circumstances

Authentication: Something you produce …

Example: Dynamic / behavioral biometrics

Authentication that examines normal actions performed by the user, e.g. keystroke dynamics.



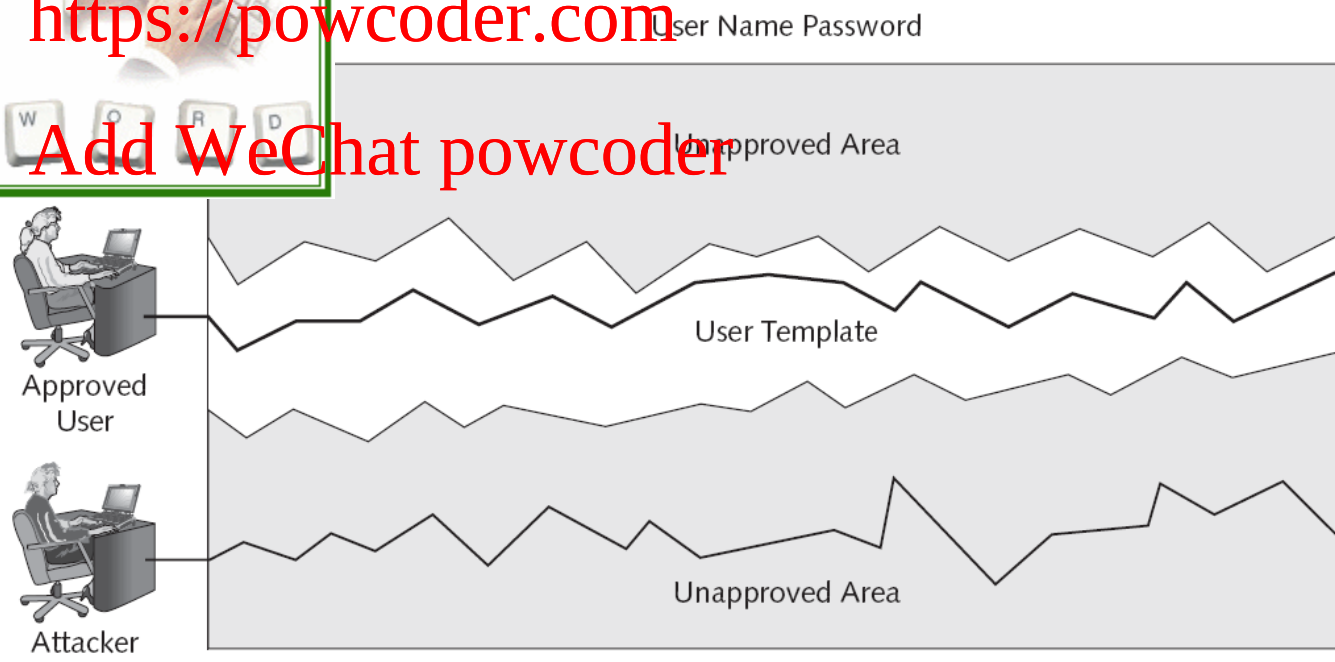
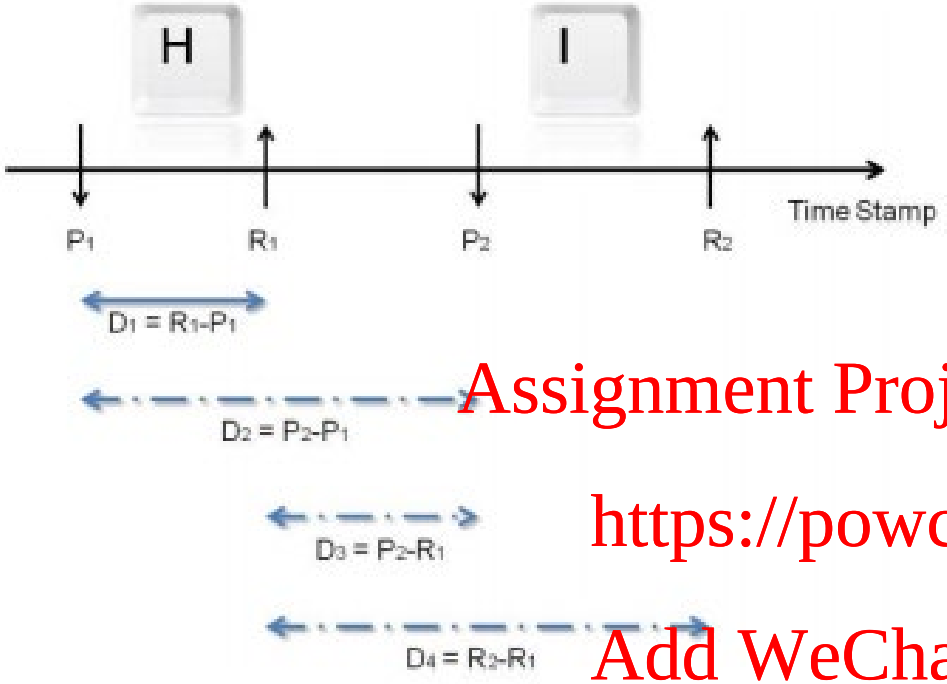


Figure 8-5 Authentication by keystroke dynamics

Authentication: Something you produce ...



Dwell Time (D_1): The time interval between a key pressed until the key is released.

Flight Time (D_2): The time interval between a key press and the next key press.

Flight Time (D_3): The time interval between a key release and the next key press. Negative value may occur if the next key is pressed before the previous key release.

Flight Time (D_4): The time interval between a key release and the next key release.

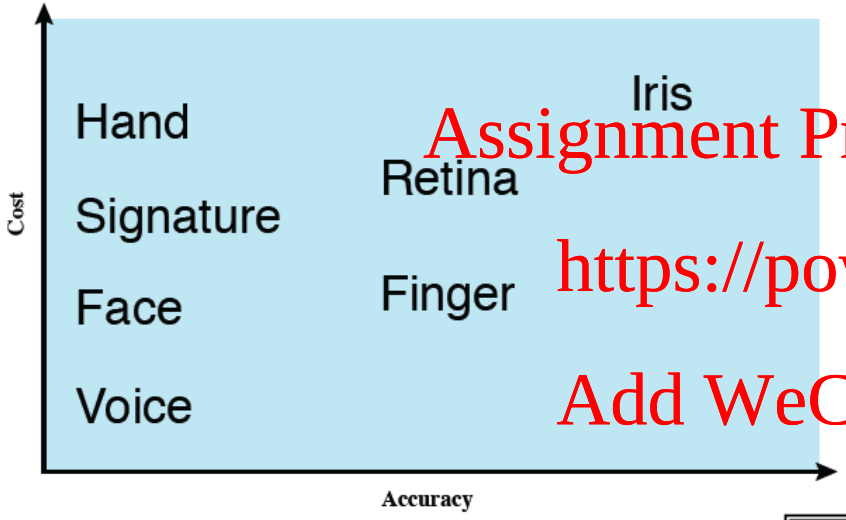
Keystroke features can be extracted in terms of:

- Dwell Time (DT) [13],[14],[15],[16],[17],[18]
- Flight Time (FT) [19],[20],[21],[22],[23],[24]
- Difficulties of typing phrase [4]
- Pressure of keystroke [25],[26],[27],[28],[29]
- Typing rate [30],[31],[32]
- Linguistic style [33]
- Sound of typing [34]
- Frequency of word errors [30],[14]

What makes your keystroke unique!?

Authentication (cont.)

Example: Cost vs. accuracy of various biometric characteristics



Biometric Technology	Accuracy	Cost	Devices required	Social acceptability
ADN	High	High	Test equipment	Low
Iris recognition	High	High	Camera	Medium-low
Retinal Scan	High	High	Camera	Low
Facial recognition	Medium-low	Medium	Camera	High
Voice recognition	Medium	Medium	Microphone, telephone	High
Hand Geometry	Medium-low	Low	Scanner	High
Fingerprint	High	Medium	Scanner	Medium
Signature recognition	Low	Medium	Optic pen, touch panel	High

Authentication (cont.)

Example: Biometrics accuracy vs. acceptance

Organizations implementing biometrics must carefully balance a system's effectiveness against its perceived intrusiveness and acceptability to users...

Effectiveness of Biometric Authentication Systems Ranking from Most Secure to Least Secure	Acceptance of Biometric Authentication Systems Ranking from Most Accepted to Least Accepted
• Retina pattern recognition	• Keystroke pattern recognition
• Fingerprint recognition	• Signature recognition
• Handprint recognition	• Voice pattern recognition
• Voice pattern recognition	• Handprint recognition
• Keystroke pattern recognition	• Fingerprint recognition
• Signature recognition	• Retina pattern recognition