EECS 3482

Introduction to Computer Security

Access Control

Instructor: N. Vlajic, Fall 2021

Learning Objectives

Upon completion of this material, you should be able to:

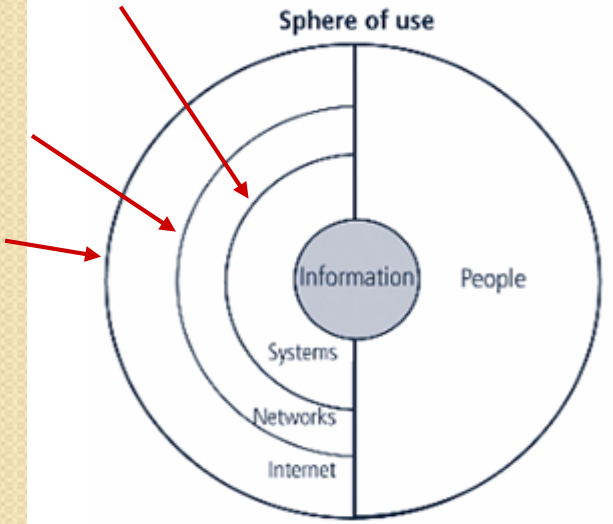
- Discuss three main processes/stages encompassing access control.
- Discuss the four general means of authenticating a user's identity.
- Outline the main pros and cons of various biometric authentication approaches.
- Distinguish between the major categories of access control policies.

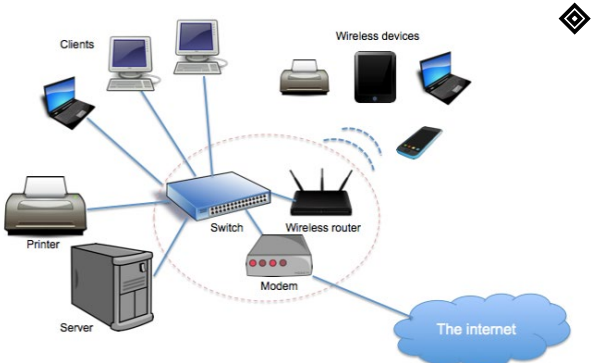
Required Reading

Computer Security, Stallings: **Chapter 3 & 4**

Introduction

- **Spheres of Information Use – information can accessed directly** (people accessing hard-copies) **and/or indirectly by means of computer systems** (if data in digital form)



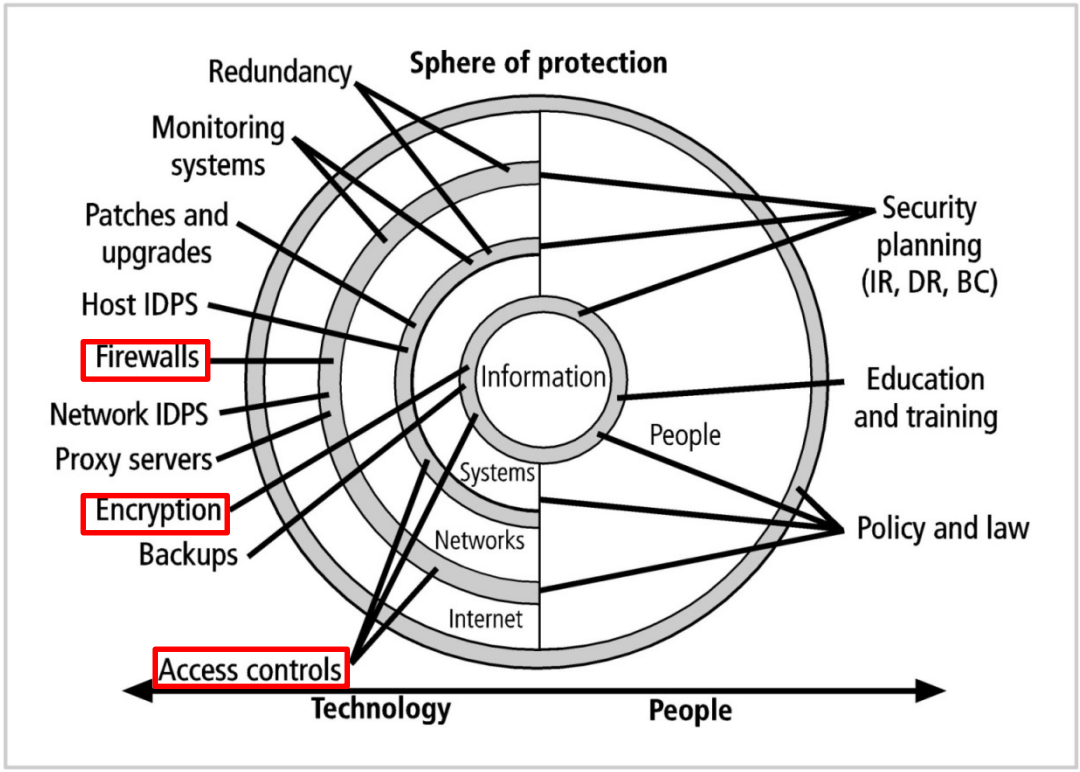


- multiple layers on 'technology' side of access sphere imply that one or more access stages may be required
- example: to access info stored on a system (database), the user must access / log-into the database-server
- example: to access info via Internet, the user must 'go through' local network (e.g., pass a firewall) and then access the system that hosts the info

Introduction (cont.)

- **Spheres of Protection** – **between each layer of use there must exist a layer of protection to prevent access to next inner layer**
  - shaded bands in the figure …

(Avoidance) **controls that can be applied to technology!**



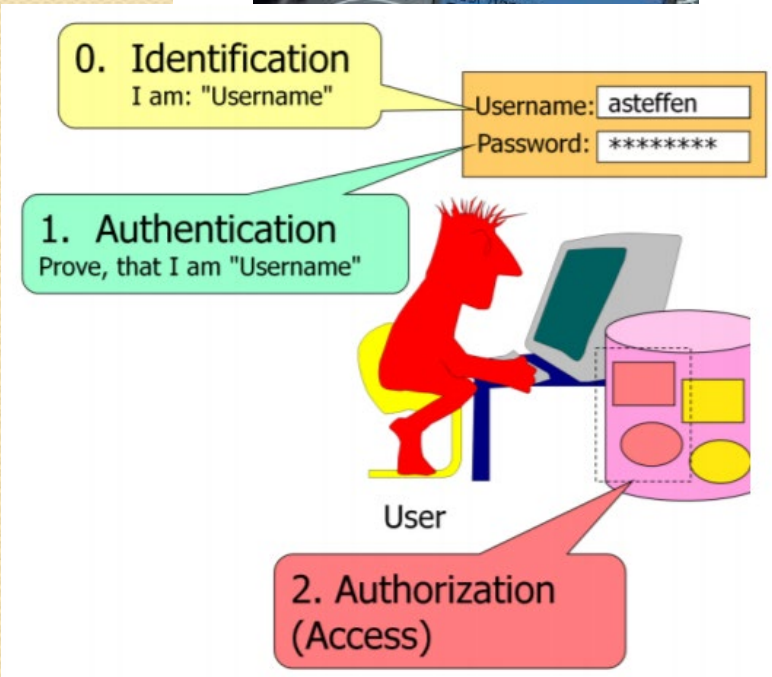
(Avoidance) **controls that can be applied to humans!**

Access Control

- **Access Controls** – selective restriction of access to a physical place, computer system or other resource
  - the act of 'accessing' may mean entering, using, consuming …

Access Control (cont.)

- **Stages of Access Controls = I / A / A**



- **identification** – obtain identity of an entity requesting access to a logical or physical area (obtain credentials)
- **authentication** – confirm identity of the entity seeking access …
  - making sure user's credentials are not false – the user 'is' who they claim to be
- **authorization** – determine whether the authenticated entity is permitted to access a particular system (e.g., OS, firewall, router, database, …) and its resources (e.g., system's files)
  - typically implemented by means of **access control lists / rules**

Access Control (cont.)

Example: Basic steps in access control

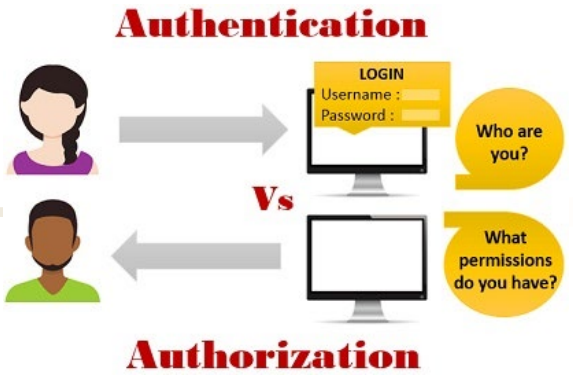
Action	Description	Scenario Example	Computer Process
Identification	Review of credentials	Delivery person shows employee badge	User enters username
Authentication	Validate credentials as genuine	Megan reads badge to determine it is real	User provides password
Authorization	Permission granted for admittance	Megan opens door to allow delivery person in	User authorized to log in
Access	Right given to access specific resources	Delivery person can only retrieve box by door	User allowed to access only specific data

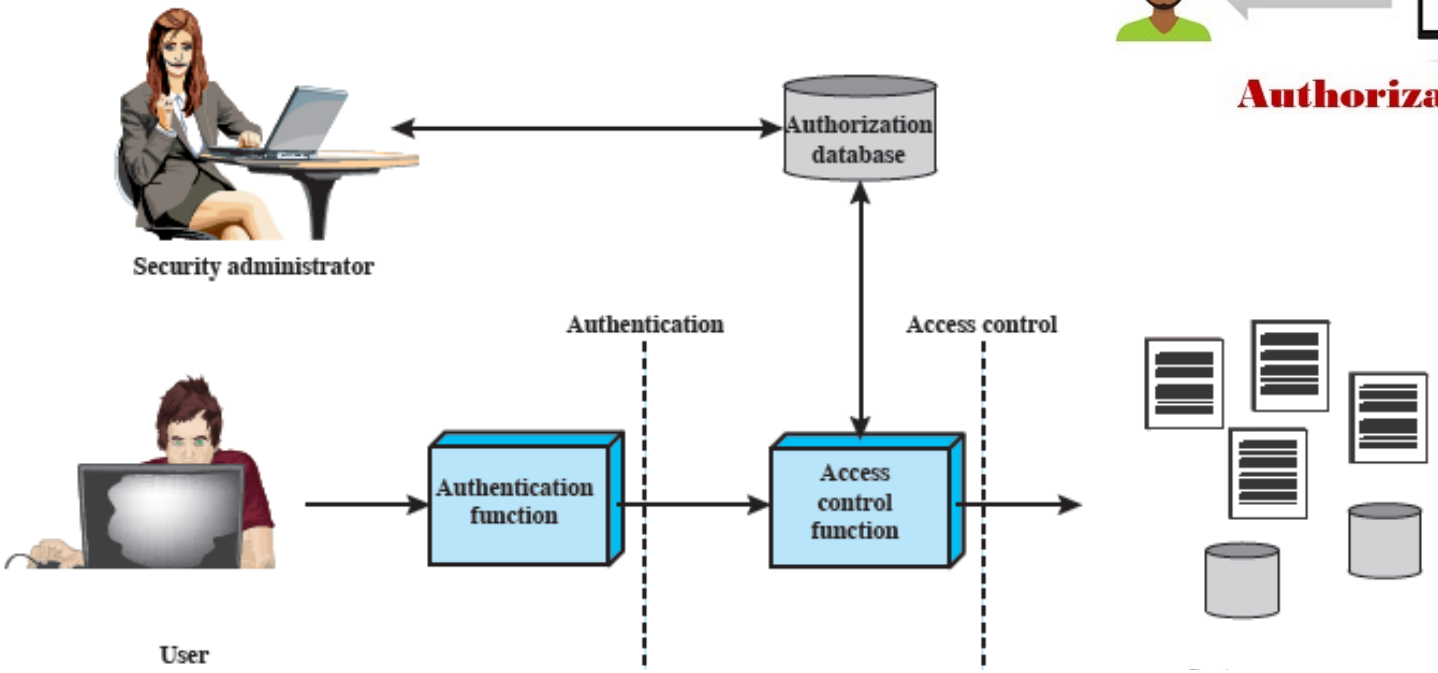
Table 7-1 Basic steps in access control

User is 'let' into the system with certain privileges.

'Authorization profile' of the user is matched against 'Access profile' of a specific/requested object.

Access Control (cont.)





Just because a user can authenticate to a system,
it does not mean they are given access to anything and everything.

Authorization ensues that the requested object or activity on an object is possible based on the privileges assigned to the subject.

Identification

- **Identification** – mechanism that provides info about an unverified entity – aka supplicant – that wants to be granted access to a logical or physical area
  - must be a unique value that can be mapped to one and only one entity within the administered domain
  - in most organizations, identification = name OR (initial + surname)

Authentication

- **Authentication** – **process of validating a person's (supplicant's) purported identity**
  - **types of authentication mechanisms:**

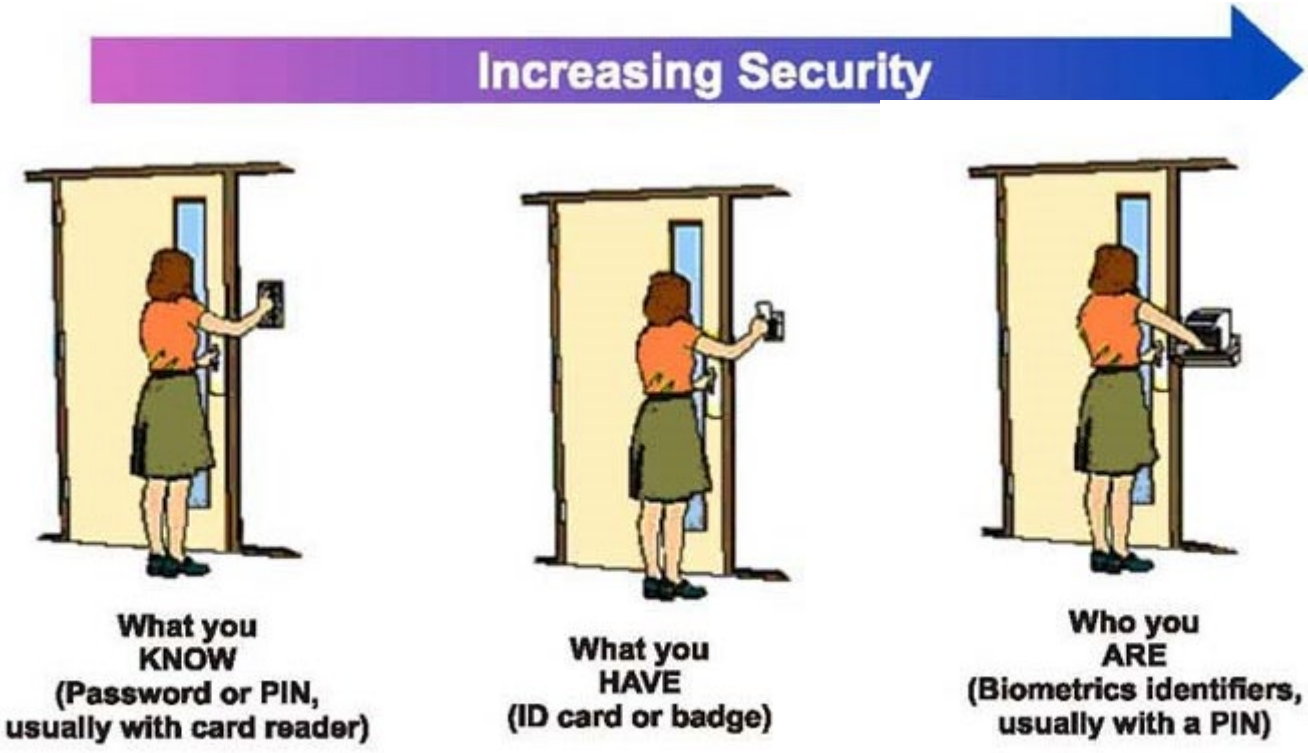
    1) **something you know**
       - password or passphrases

    2) **something you have**
       - cryptographic tokens or smart cards

    3) **something you are** - static biometrics
       - fingerprints, palm prints, iris scans, …

    4) **something you produce** - dynamic biometrics
       - pattern recognition of voice, signature / handwriting, typing rhythm

Authentication (cont.)



http://transit-safety.volpe.dot.gov/security/securityinitiatives/designconsiderations/CD/sec5.htm

If 'something you are' is so much better than 'something you have' or 'something you know' why do not we use biometrics all the time?!

Authentication (cont.)

TABLE 6.1 Examples of authentication techniques	
Example	Factor
Memorized password	Know
Memorized PIN	Know
Magnetic stripe card	Have
One-time password token	Have
SIM card or smart card	Have
USB password token	Have
Fingerprint	Are

Elementary Computer Security, R. E. Smith, pp. 232

Authentication: Something you know …

1) Something you know …

- authentication mechanisms based on use of passwords/pins and passphrases
- **password** – combination of characters that only the user should know
  - **challenge**: should be simple enough to remember, and complex enough for cracking
    - bad examples: name of spouse, child, pet
- **passphrase** – plain-language phrase typically longer but stronger than a password, from which a virtual password is derived
  - examples: Linksys, Windows 7 and up

CPIMFF = Cheese Pizza Is My Favorite Food

Password cracking speed

May 8, 2020 info@thesecurityfactory.be Passwords

Password Length	Numerical 0-9	Upper & Lower case a-Z	Numerical Upper & Lower case 0-9 a-Z	Numerical Upper & Lower case Special characters 0-9 a-Z %$
1	instantly	instantly	instantly	instantly
2	instantly	instantly	instantly	instantly
3	instantly	instantly	instantly	instantly
4	instantly	instantly	instantly	instantly
5	instantly	instantly	instantly	instantly
6	instantly	instantly	instantly	20 sec
7	instantly	2 sec	6 sec	49 min
8	instantly	1 min	6 min	5 days
9	instantly	1 hr	6 hr	2 years
10	instantly	3 days	15 days	330 years
11	instantly	138 days	3 years	50k years
12	2 sec	20 years	162 years	8m years
13	16 sec	1k years	10k years	1bn years
14	3 min	53k years	622k years	176bn years
15	26 min	3m years	39m years	27tn years
16	4 hr	143m years	2bn years	4qdn years
17	2 days	7bn years	148bn years	619qdn years
18	18 days	388bn years	9tn years	94qtn years
19	183 days	20tn years	570tn years	14sxn years
20	5 years	1qdn years	35qdn years	2sptn years

Password cracking is becoming very trivial with the vast amount of computing power readily available for anyone who desires so. At a current rate of 25$ per hour, an AWS p3.16xlarge nets you a cracking power of 632GH/s (assuming we're cracking NTLM hashes). This means we're capable of trying a whopping 632.000.000.000 different password combinations per second!

https://www.thesecurityfactory.be/password-cracking-speed/

Authentication: Something you know …

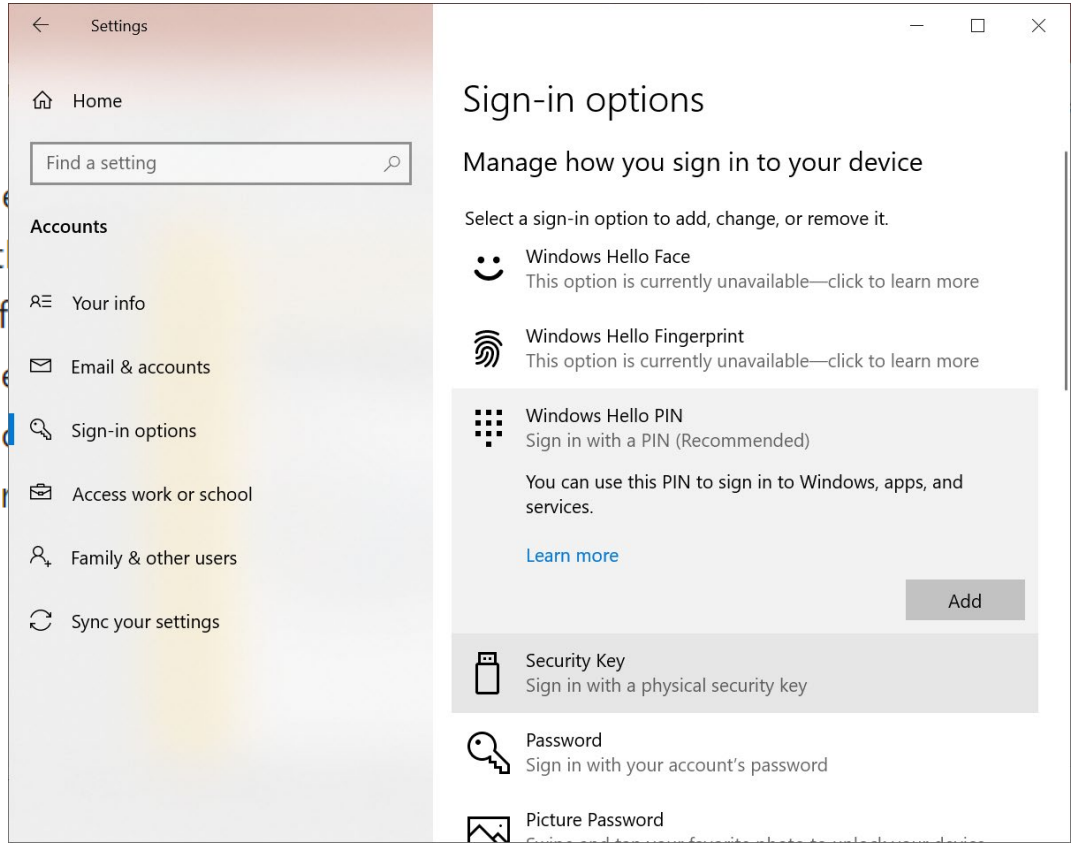
Why a PIN is better than a password

10/23/2017 • 4 minutes to read • +1

Applies to

- Windows 10

Windows Hello in Windows 10 e
PIN different from (and better t
password. A PIN can be a set of
include special characters and le
could be an account password d
complexity) that makes it better



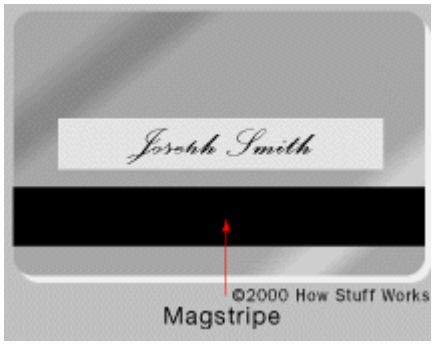
Authentication: Something you have …

2) Something you have …

- objects used for purpose of user authentication are called '**tokens**'
- token + PIN/password provides <u>significantly greater security than password alone</u>
  - **an adversary must gain physical possession of the token (or be able to duplicate it) in addition to 'cracking' the password**
- types of tokens:
  - **static tokens**
  - **dynamic synchronous** (one-time password) **tokens**
  - **dynamic asynchronous** (challenge-response) **tokens**

Authentication: Something you have …

2.1) Static Tokens



- e.g.: swipe card, smart card, RFID tags
- **swipe cards** - ID and ATM cards
  - aka 'dumb cards', transmit same credential every time – the credential (base secret) is impractical to memorize
  - PIN/password not on the card – ATM encrypts PIN provided by user and sends it to a data-base for verification …
- **smart card** - swipe cards with a chip
  - chip contains a CPU, memory blocks (RAM, ROM, …) and on-chip encryption module
  - stores 100x data stored on magnetic strip: encrypted PIN & other info about card holder
  - card checks user's PIN & generates a certificate to authorize transaction process …

Authentication: Something you have …

Example: advanced tokens that produce one-time password …

Smart Phone Tokens

SMS Tokens

USB Tokens

Software Tokens

8	4	5	9	1
9	5	4	0	2
0	2	8	3	7
3	3	7	9	6
7	6	8	1	7

Grid Tokens

Keyfob Tokens

Keypad Tokens

Credit Card Tokens

OATH

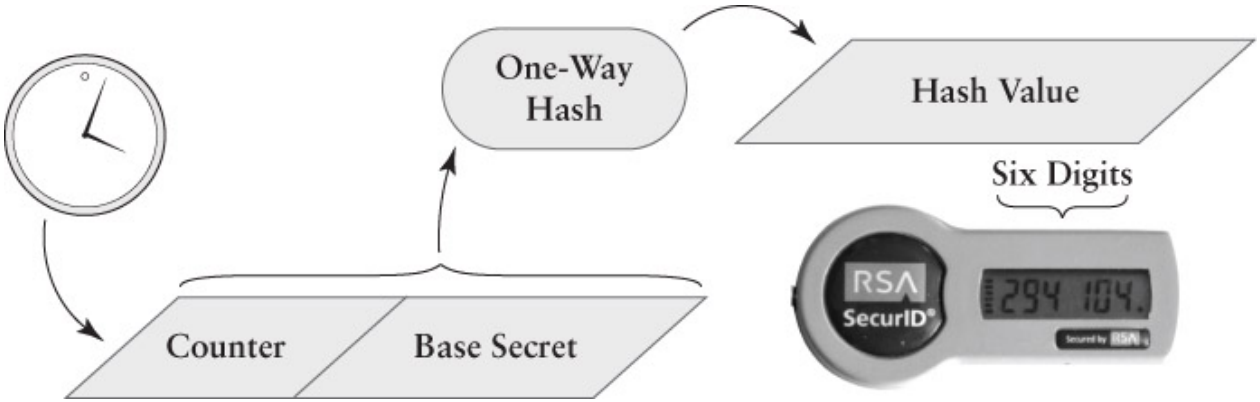
3rd Party Tokens

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

Authentication: Something you have …

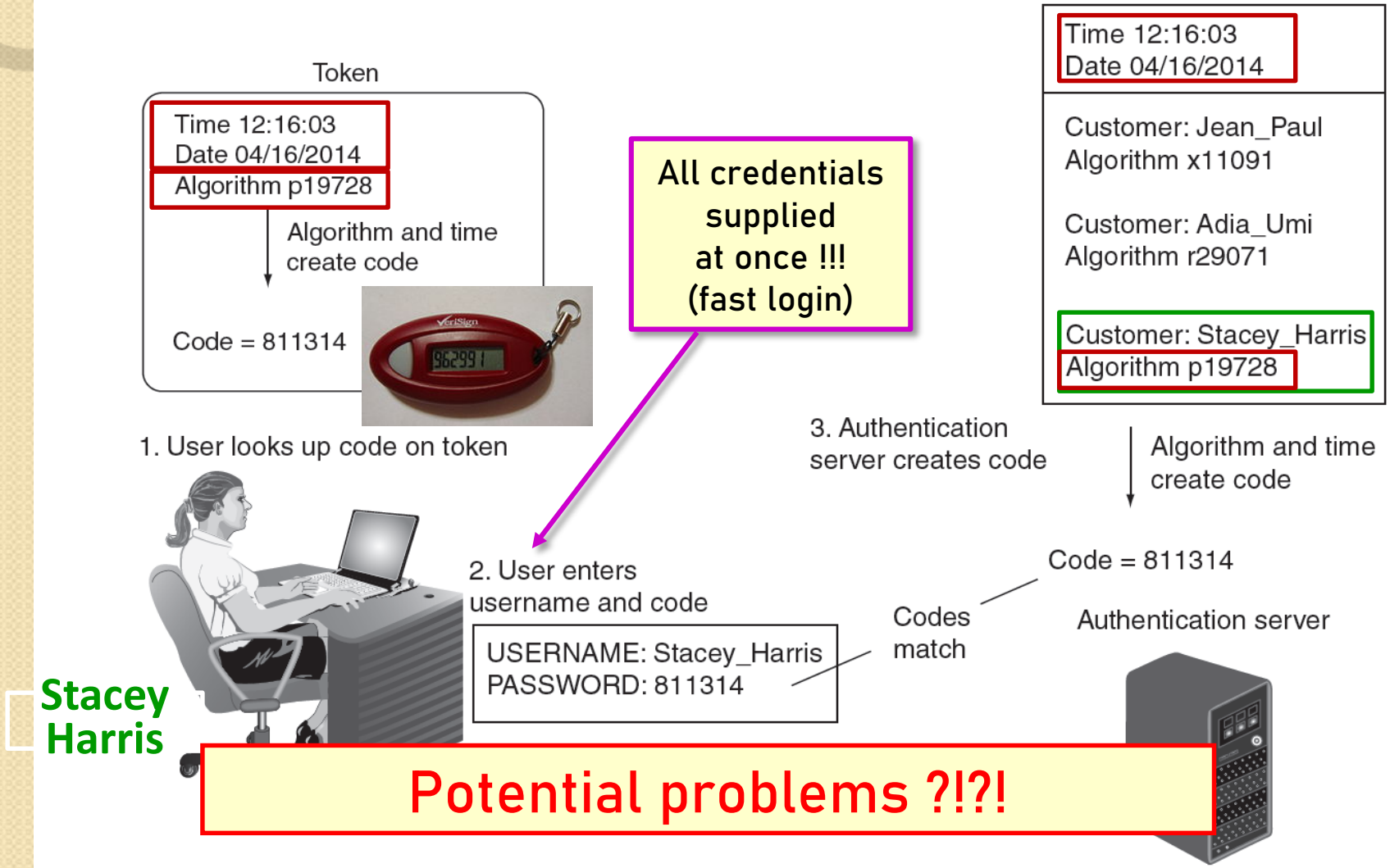
2.2) Synchronous (One-Time Password) Tokens

- **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 …

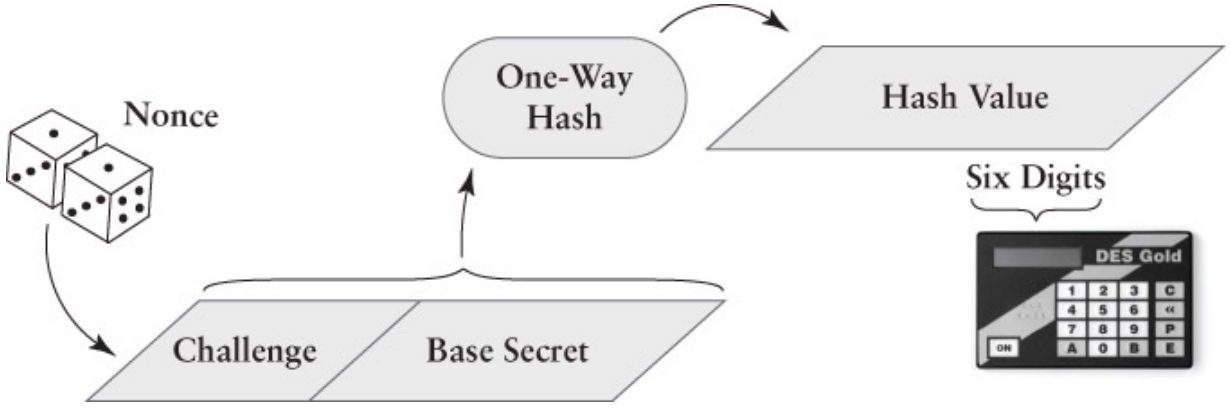
Example: Synchronous (One-time Password) Token



Authentication: Something you have …

2.3) Asynchronous (Challenge-Response) Tokens

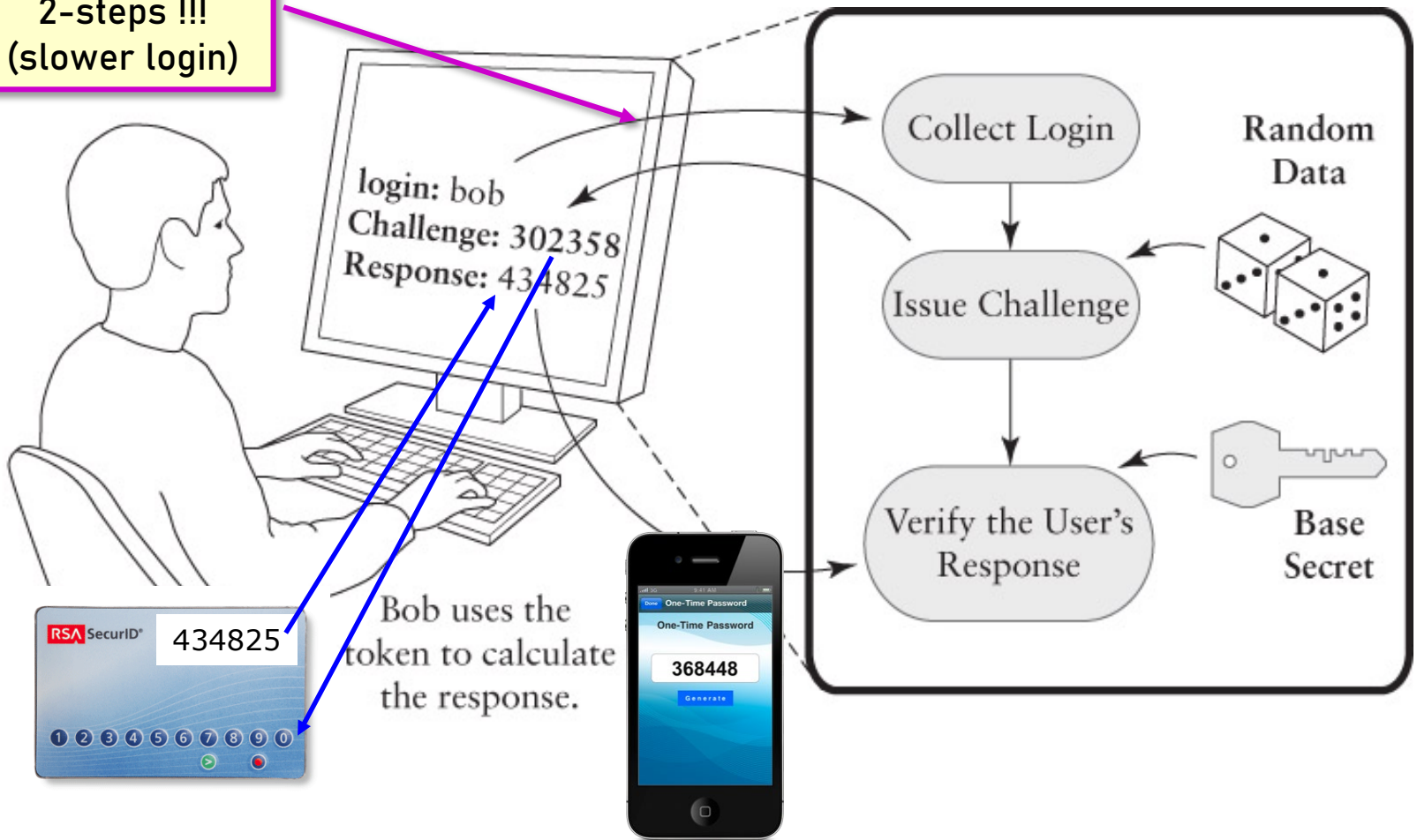
- **instead of time, token uses a challenge/nonce provided by the system to generate the password**
  - e.g., token can generate the password by
    1) applying a unique hash function to (user's base secret + nonce)
    2) encrypting nonce using user's/token's public key



Authentication: Something you have …

Example: Asynchronous (Challenge-Response) Token

Credentials supplied in 2-steps !!! (slower login)



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 …

Example: In password-based authentication, an exact (100%) match is required

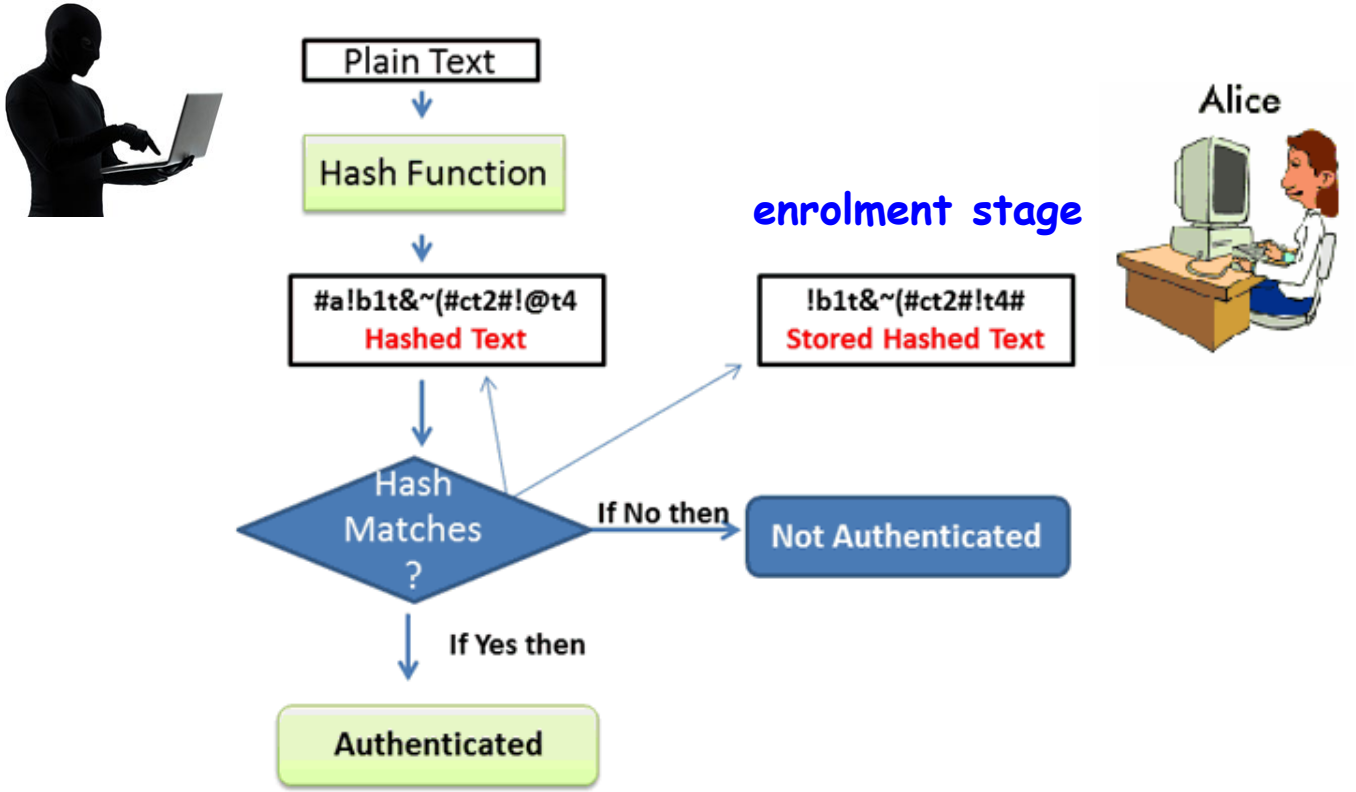


Fig : Flow Chart Example of Hash work

https://www.talwork.net/has-your-password-been-leaked

Authentication: Something you are ...

Example: enrollment & authentication in biometric syst.

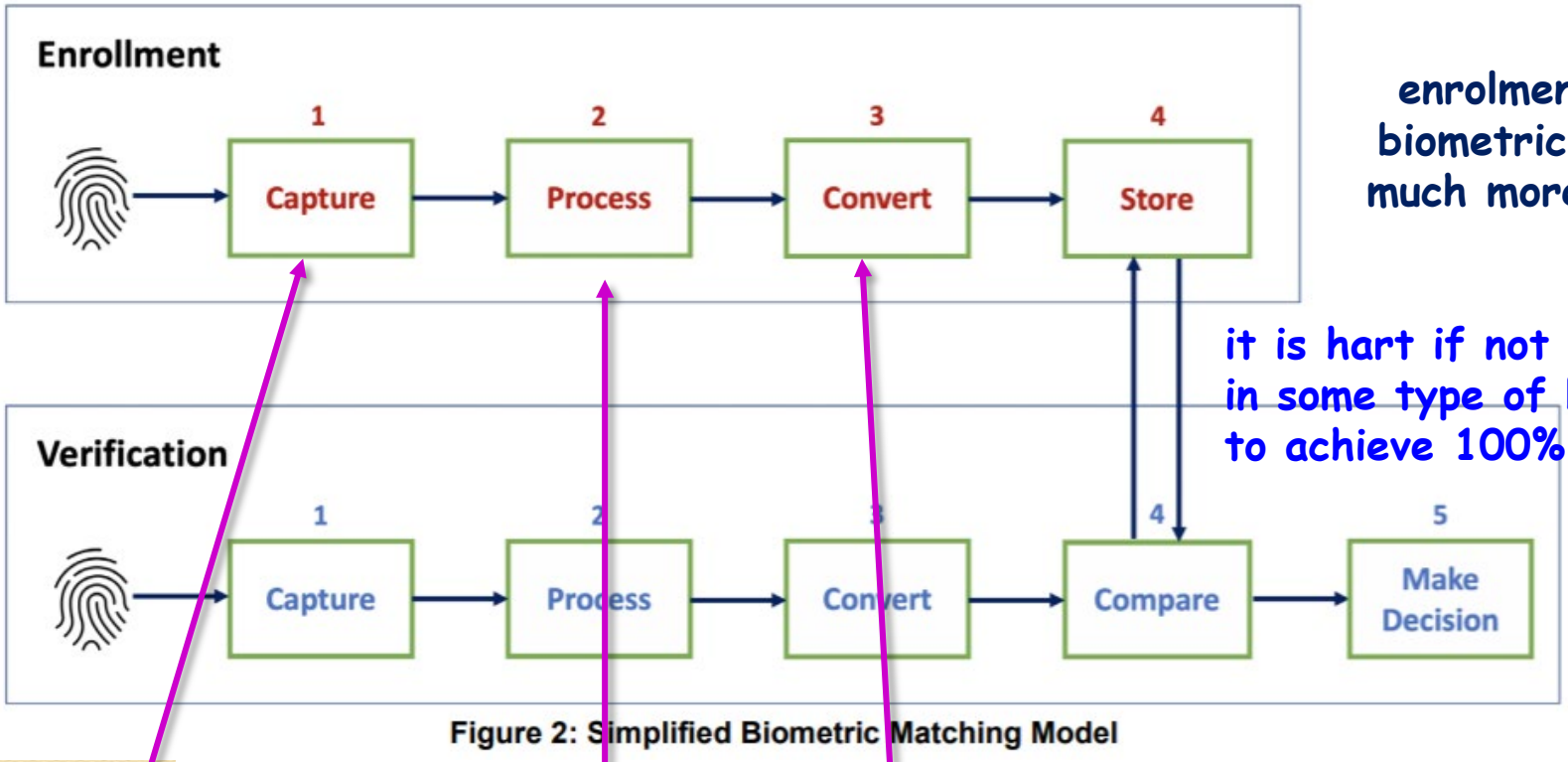


Figure 2: Simplified Biometric Matching Model

enrolment stage in biometric systems is much more involved !!!

it is hart if not impossible in some type of biometrics to achieve 100% match

A sample of biometric reading is captured.

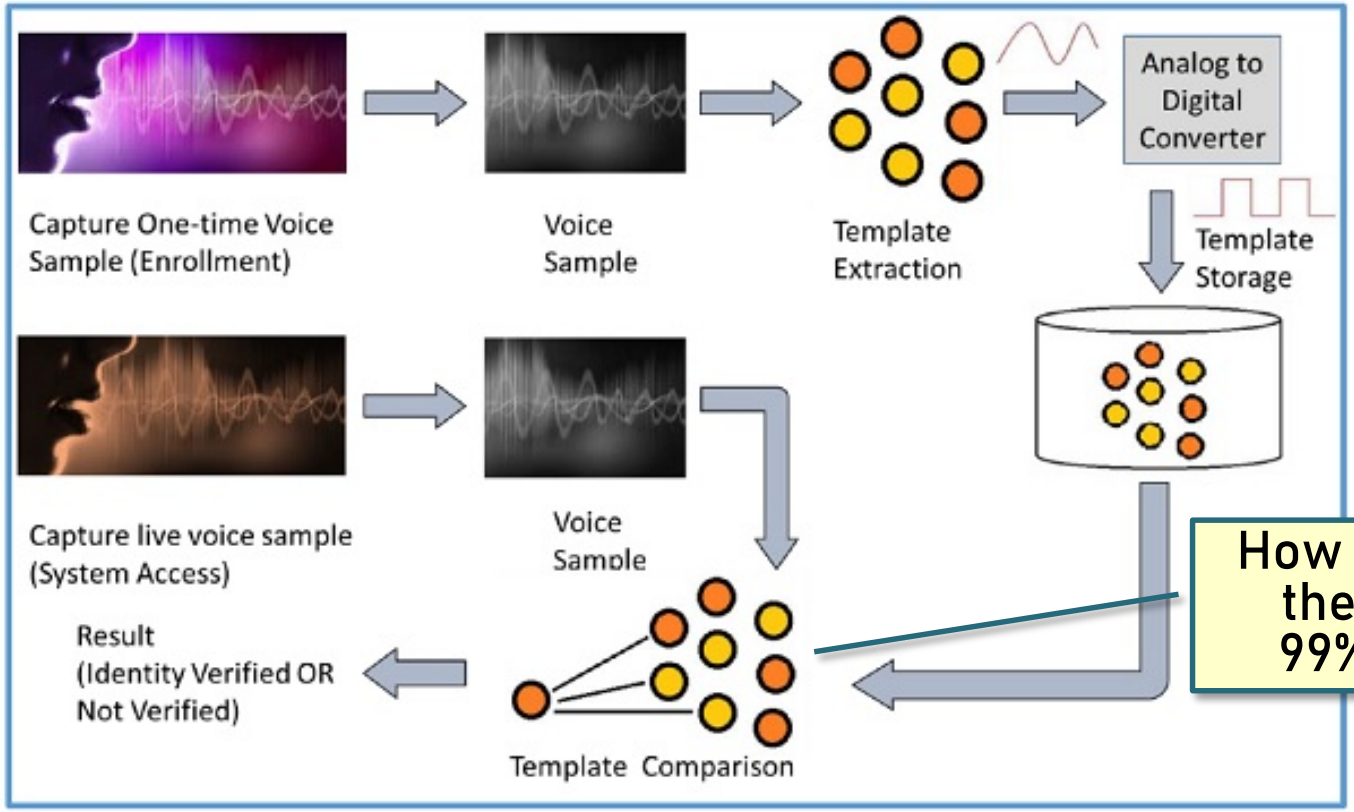
The sample is processed into feature set.

Feature set is converted into a template.

https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8334-draft.pdf

Authentication: Something you are …

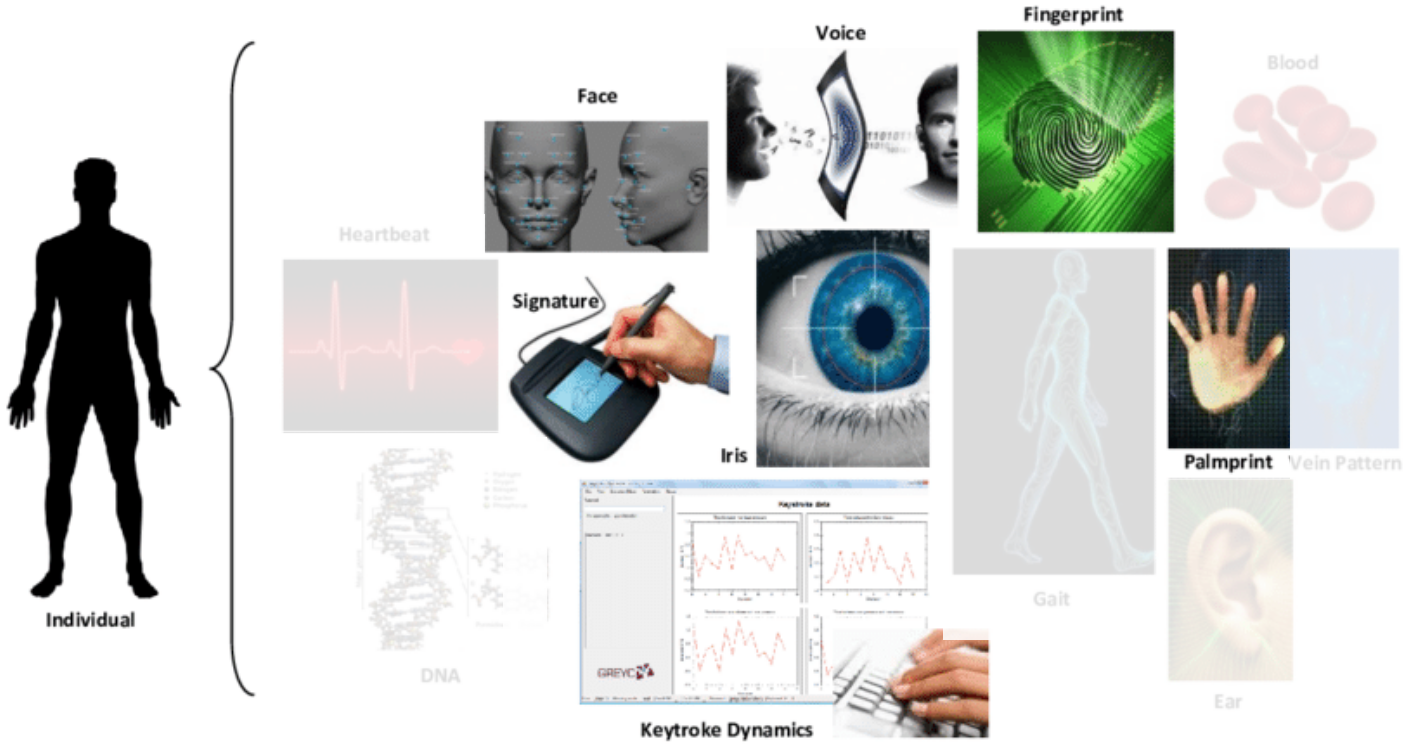
Example: In biometric-based authentication, an approximate match is required



https://www.tutorialspoint.com/biometrics/biometrics_quick_guide.htm

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

dental imprint

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

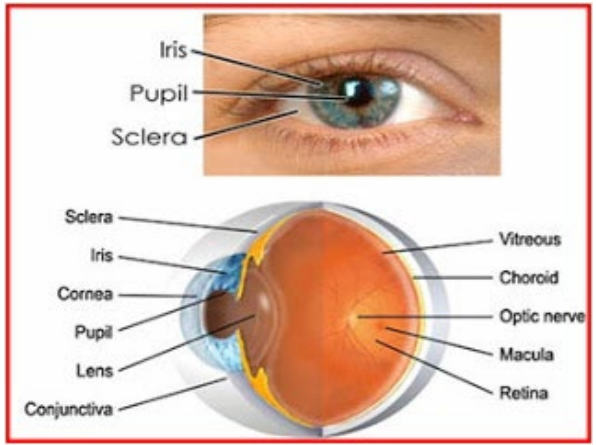
Information	U (universal)	N (unique)	P (permanent)	C (collectable)	A (acceptable)	E (performance/accuracy)
DNA	Yes	Yes	Yes	Poor	Poor	*****
Gait	Yes	No	Poor	Yes	Yes	***
Keystroke dynamics	Yes	Yes	Poor	Yes	Yes	****
Voice	Yes	Yes	Poor	Yes	Yes	****
Iris	Yes	Yes	Yes	Yes	Poor	*****
Face	Yes	No	Poor	Yes	Yes	****
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

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

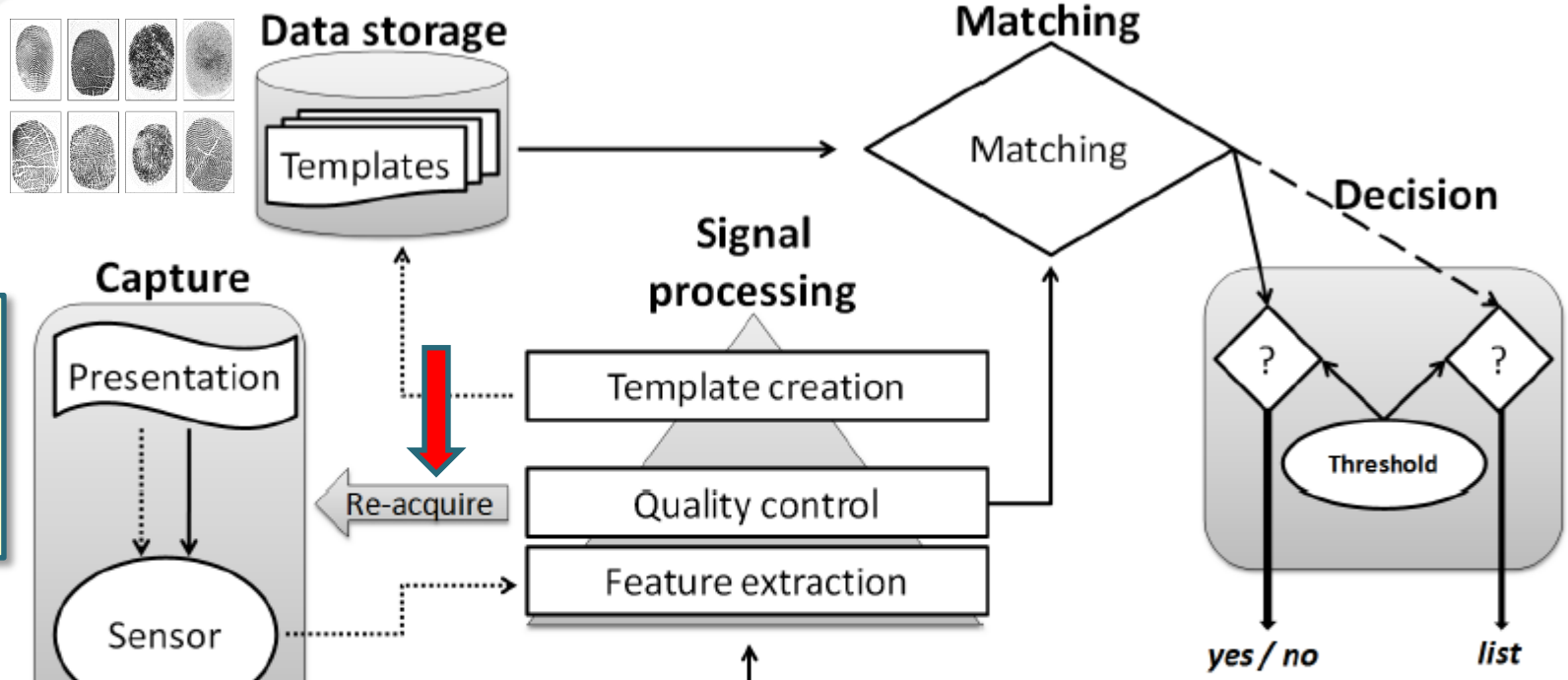


Retina scanner

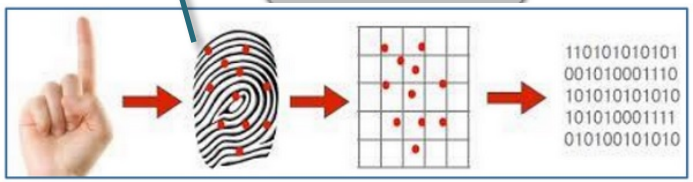
RETINA - cannot be seen by naked eye - the network of blood vessels
most reliable biometrics, aside from DNA ☺
but can be affected by eye-disease ☹
scan = 15 seconds of low-energy IR scanning ☹
subject has to be close to scanner ☹

Authentication: Something you are …

- **Biometric System** – architecture & operational stages



Should the entire scan (image) be stored ??



STAGE 1:

STAGE 2:

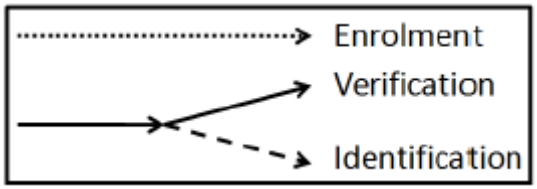
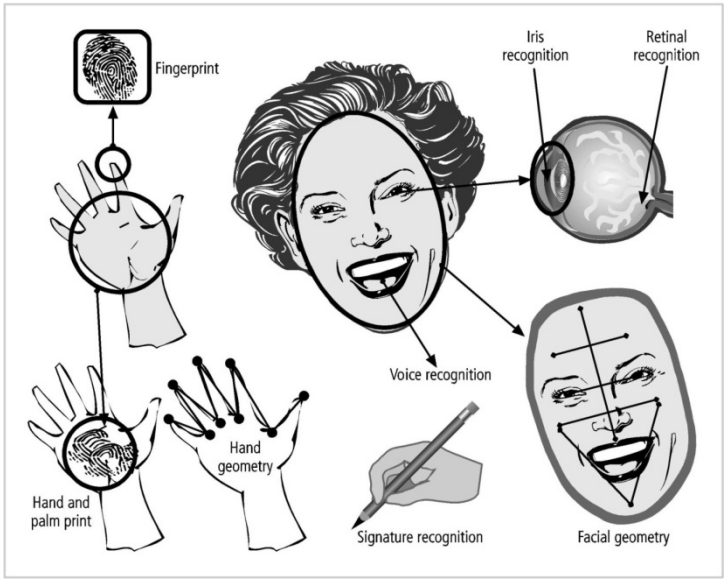


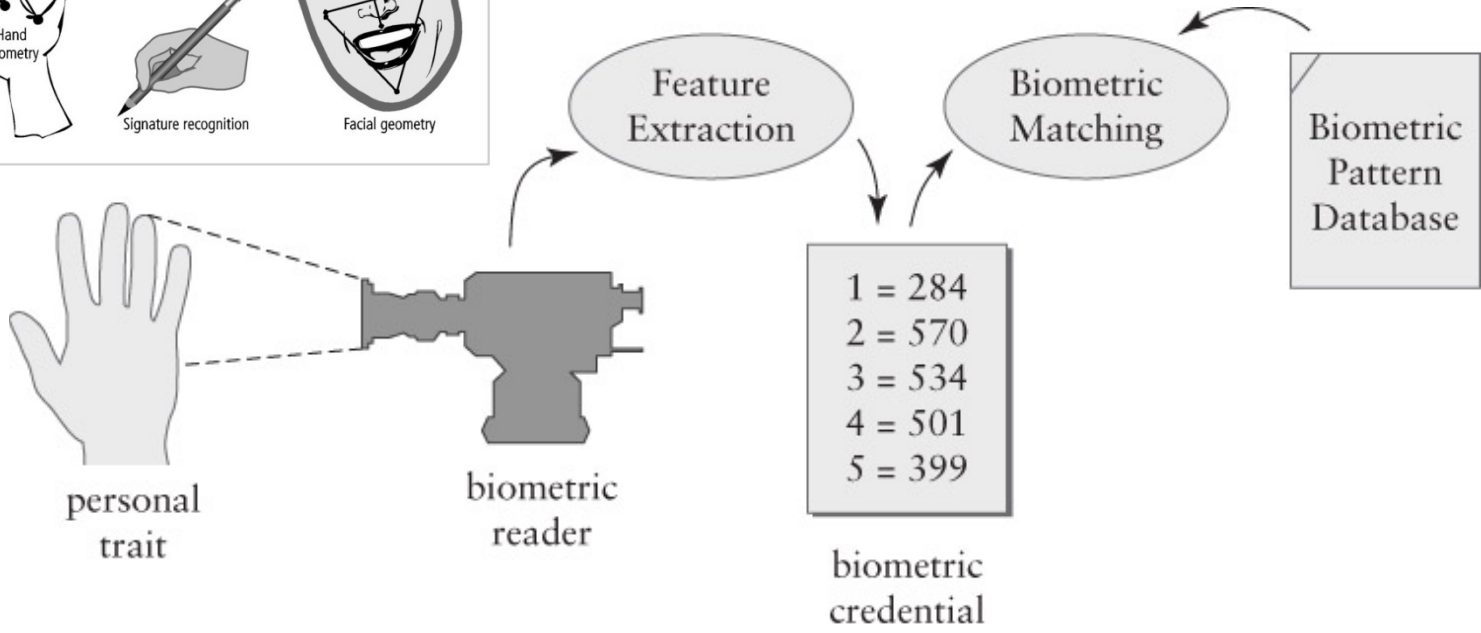
Figure 4. Generic architecture of a biometric system (source [4]).

Authentication: Something you are …

Example: Extraction of biometrics features



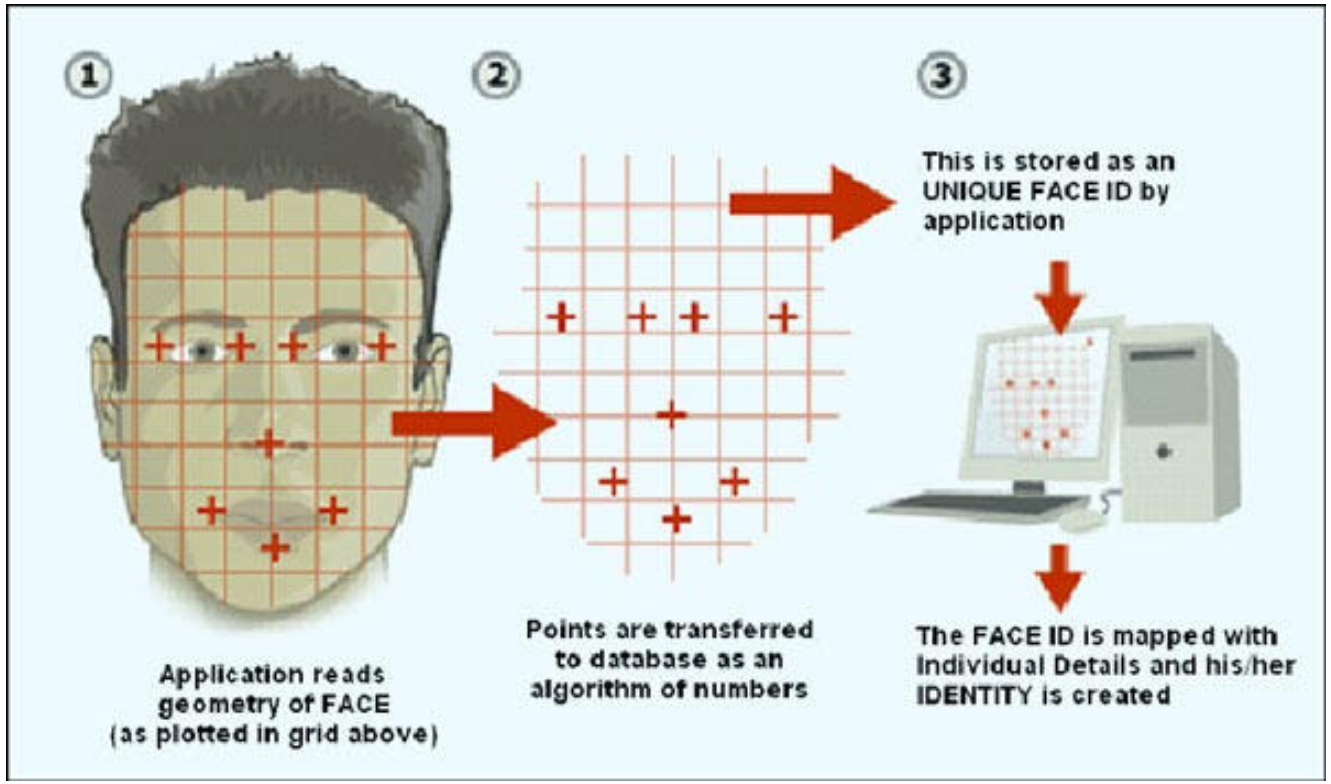
many biometric systems are based on image processing



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

Authentication: Something you are …

Example: Extraction of biometrics features



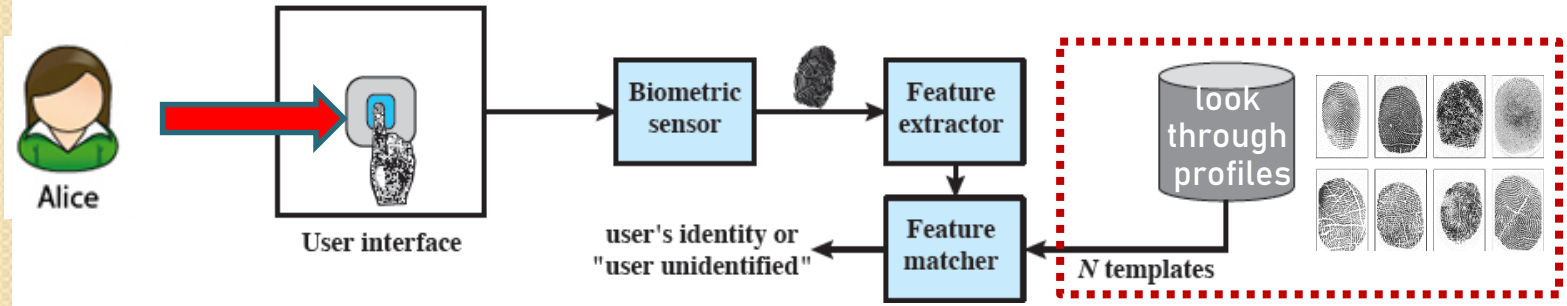
https://creativentechno.wordpress.com/2012/02/18/face-recognition/

Authentication: Something you are …

- **Types of Biometric Systems**

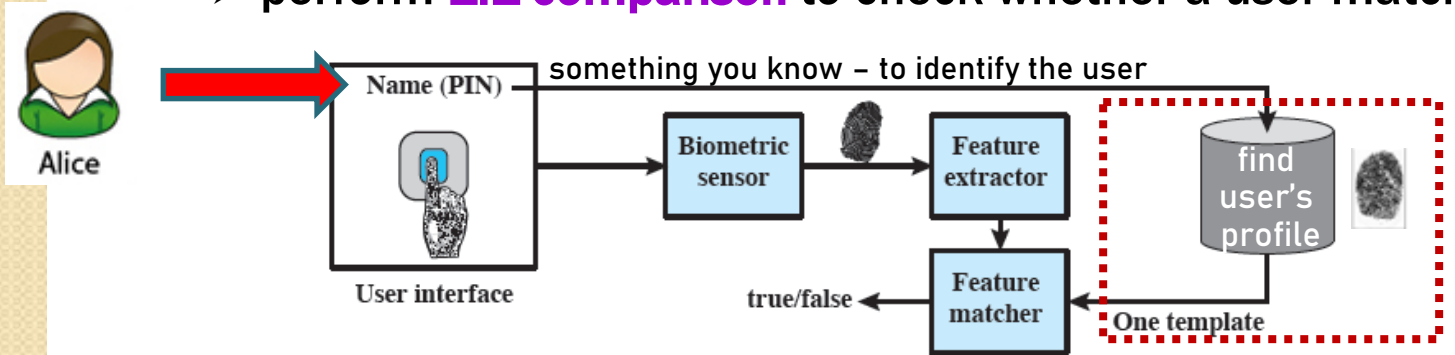
1) systems for **IDENTIFICATION**

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



2) systems for **AUTHENTICATION**

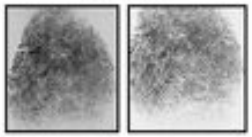
- perform **1:1 comparison** to check whether a user matches his profile



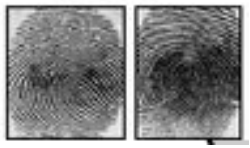
Authentication: Something you are …

- **Biometric Accuracy / Performance**
  - 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, …
    - the results of fingerprint scan may vary as a function of: finger placement, finger swelling and skin dryness …

user 1:



user 2:

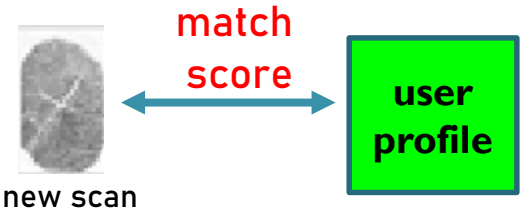


  - multiple mappings may have to be taken in order to create a (statistically) useful biometric **representation / profile**
  - a biometric sensor must be able to adapt to a broad range of appearances

Authentication: Something you are …

Biometric Accuracy

statistical distribution of 'match score' between user's new scan and user's stored profile/record



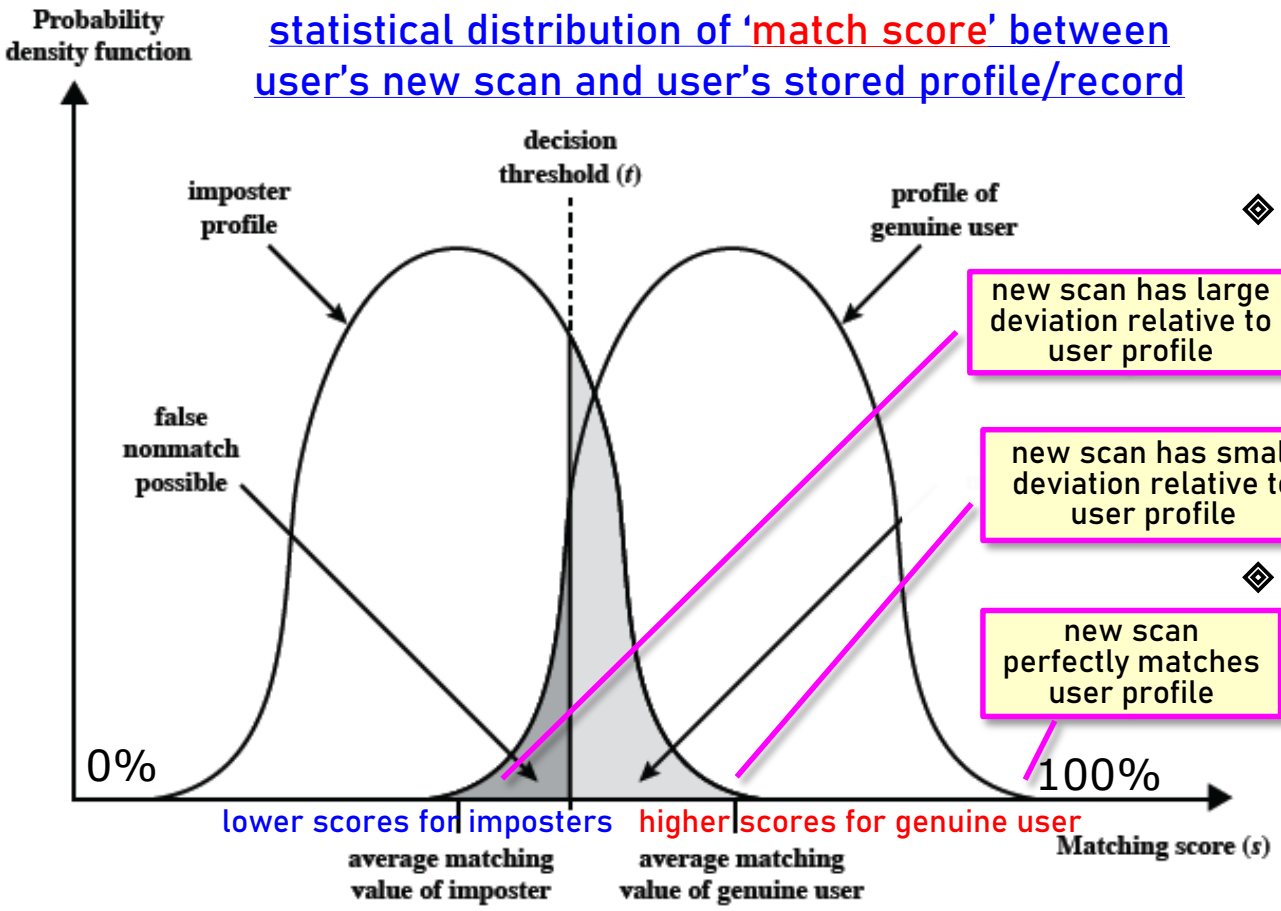


Figure 3.7 Profiles of a Biometric Characteristic of an Imposter and an Authorized Users In this depiction, the comparison between presented feature and a reference feature is reduced to a single numeric value. If the input value (s) is greater than a preassigned threshold (t), a match is declared.

- 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

move *t* to left ⇒

system more tolerant to noise 👍, but also

system more likely to accept wrong person 👎

Authentication: Something you are ...

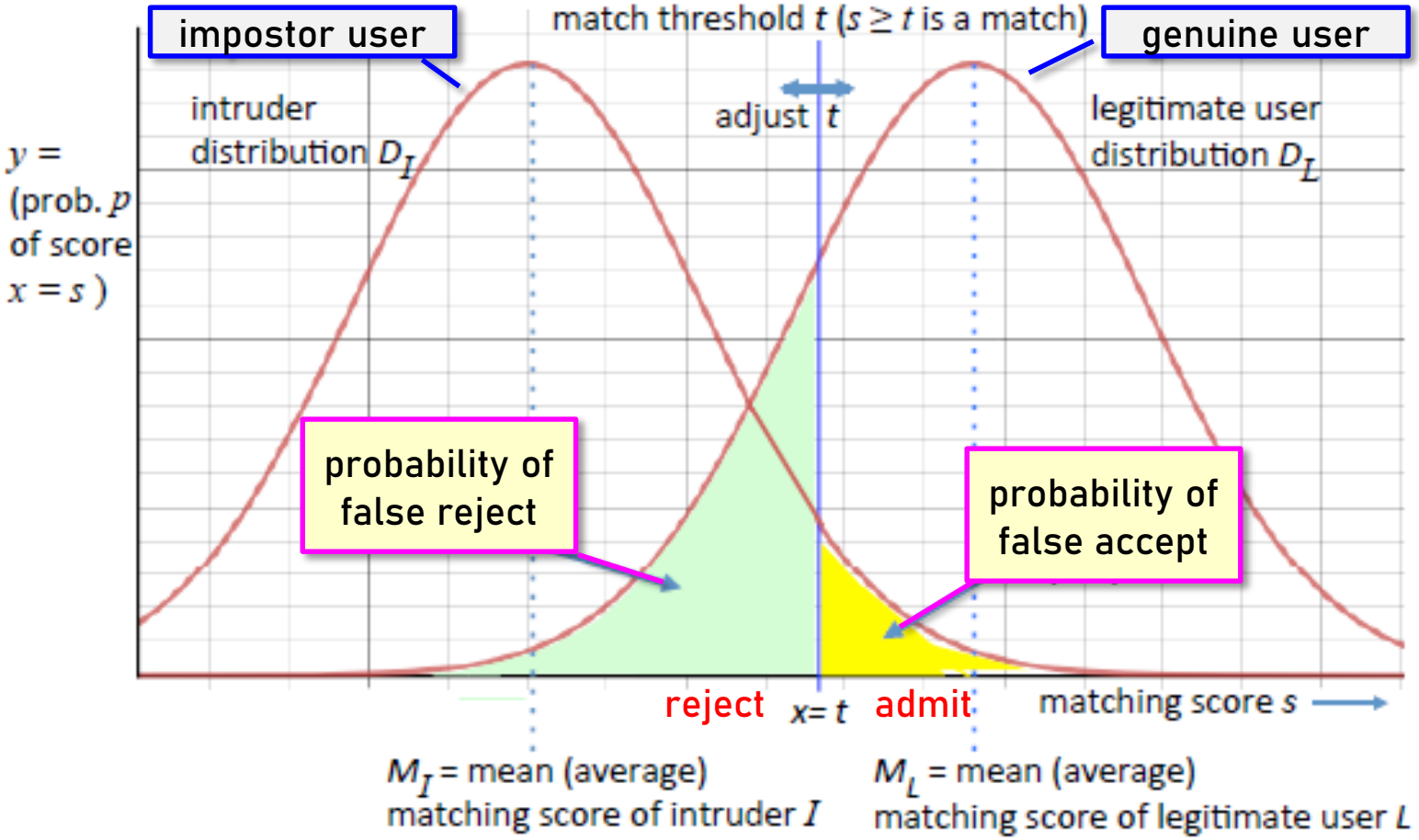


Figure 3.6: Biometric system tradeoffs. Curves model probability distributions for an intruder and legitimate user's matching scores; higher scores match the user's biometric template better. The y axis reflects how many biometric samples get matching score $x = s$.

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

Authentication: Something you are …

- Biometric Accuracy (cont.)

Biometric systems are typically described in terms of their probability of FR & FA across all user profiles !

values across the whole system !!!

- **False Reject Rate (FRR), aka False Negative**
  - **% 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**
  - **% of unauthorized / fraudulent users who are allowed access to system**
  - represent serious security breach

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

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

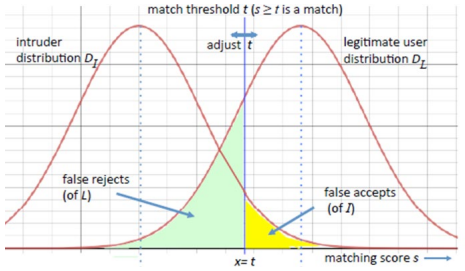
$$\text{"Security"} = (1 - \text{FA})$$
against impostors

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

Authentication: Something you are …

Example: biometric accuracy

If you are offered a system with a small FAR, do not assume a small FRR !!!



	False reject / (FN)	False accept / (FP)
Fingerprint	3-7 in 100 (3-7%)	1-100 in 100K (0.001-0.1%)
Face	10-20 in 100 (10-20%)	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%)	$\geq 10^{-5}$ ($\geq 0.001\%$)
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

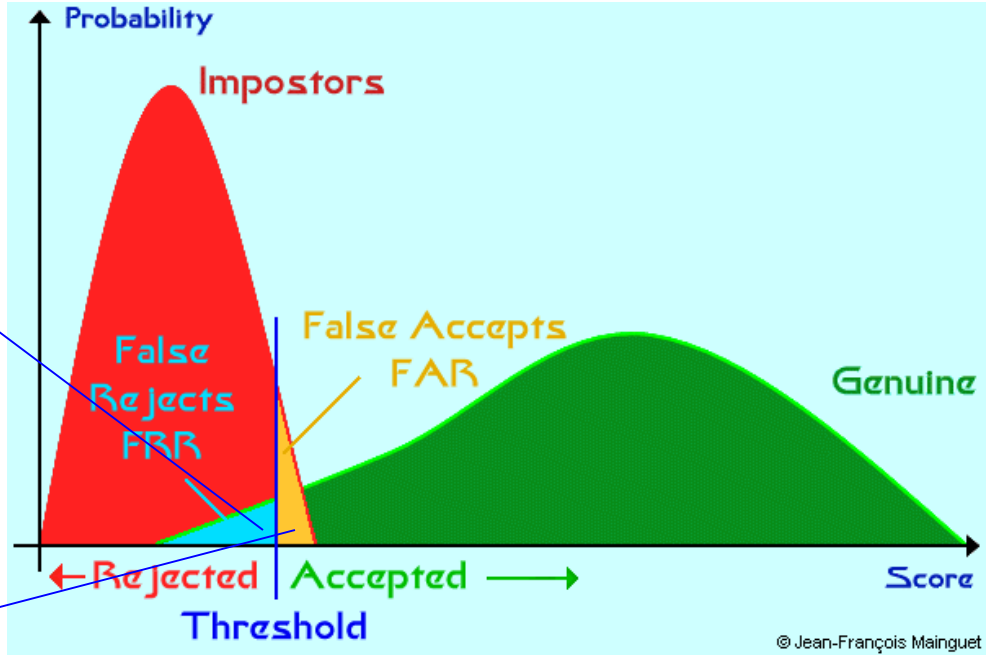
Authentication: Something you are …

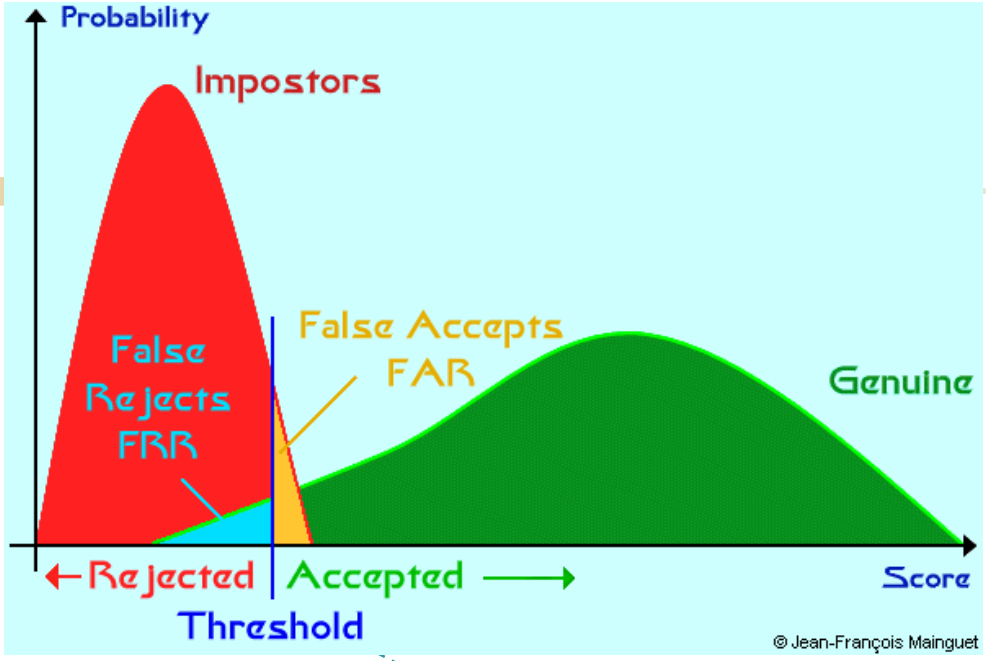
trade-off point !!!

- **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

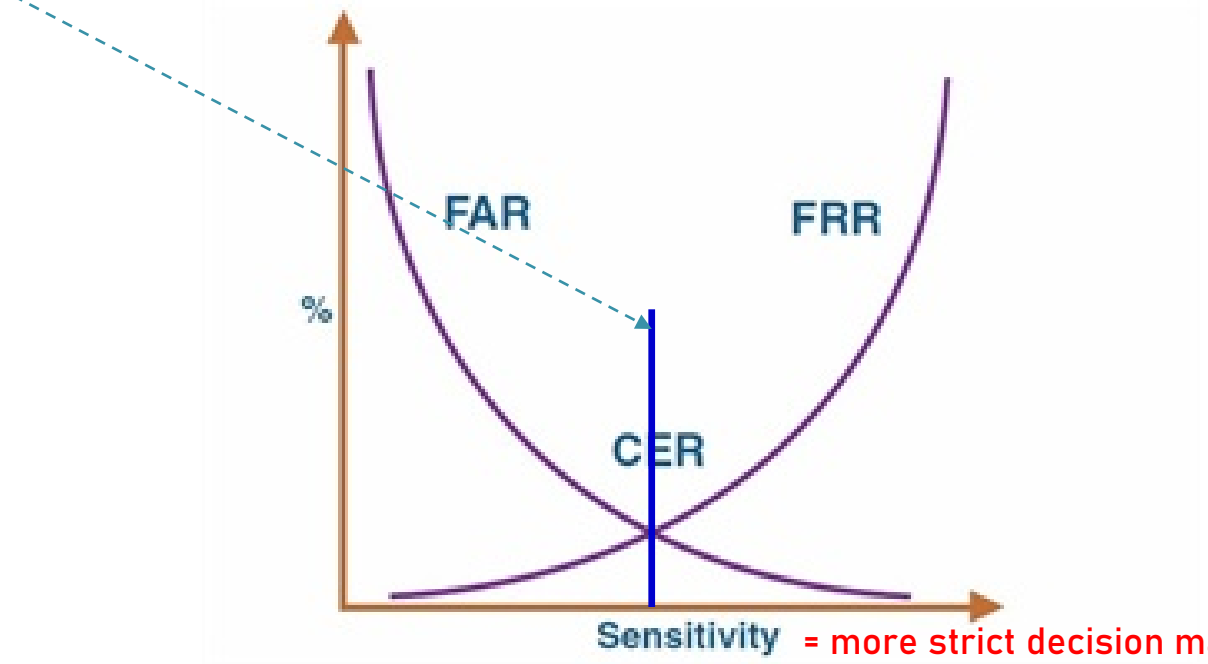
as threshold moves to the left, system becomes '**less sensitive**' and the value of FRR decreases but the value of FAR increases

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





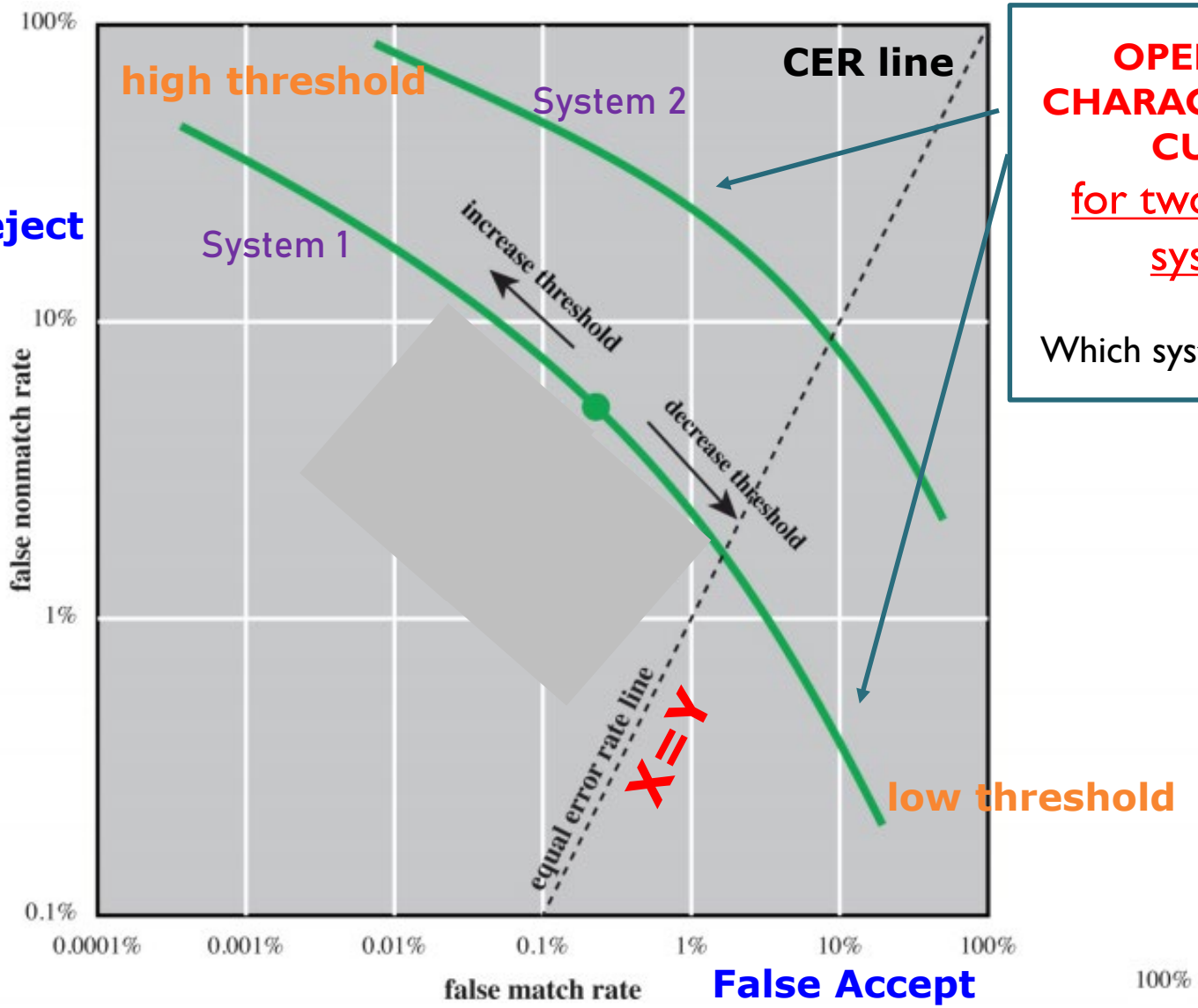
How do we find the CER operating point ??



= more strict decision making (threshold)

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 fingerprint 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

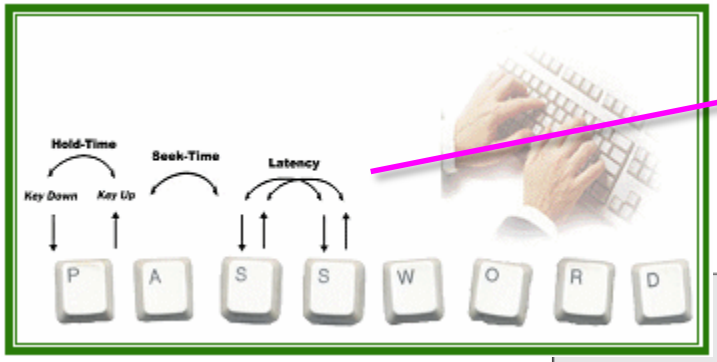
- authentication mechanisms that makes use of something the user performs or produces:
  - **signature recognition**
  - **voice recognition**
  - **keystroke recognition**

- 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.



measure/observe various time-related parameters during a user's interaction with a keyboard

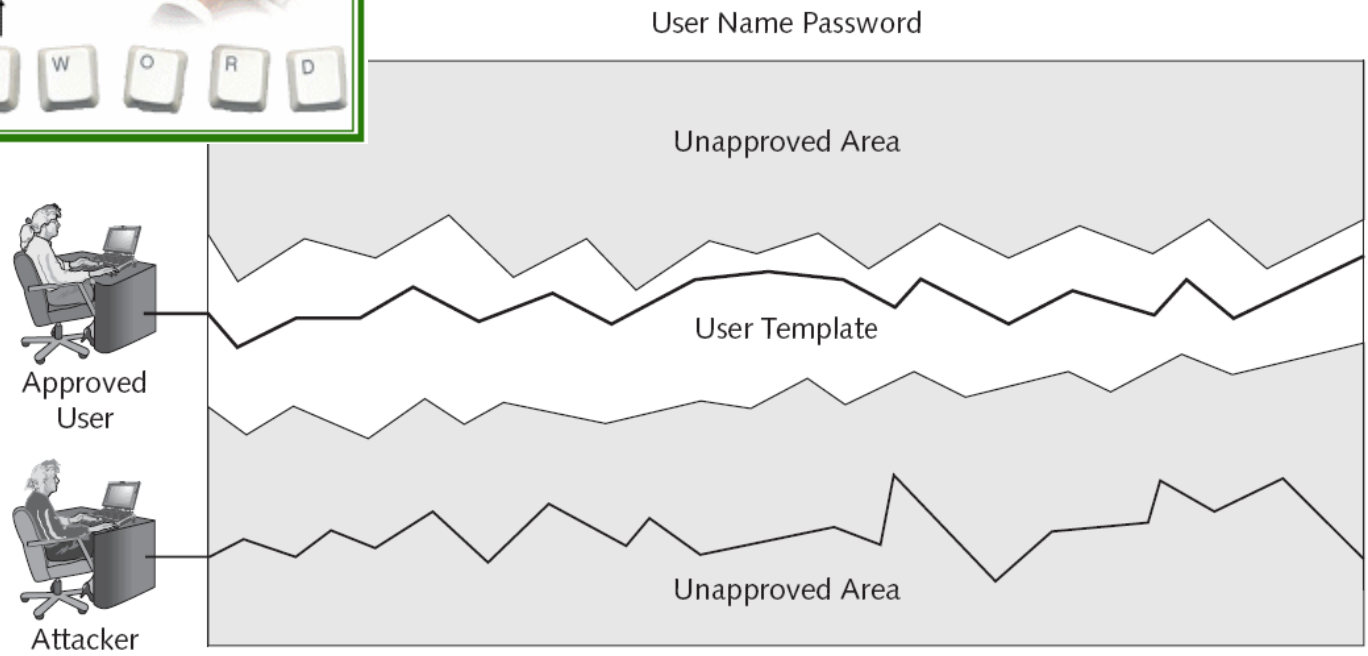
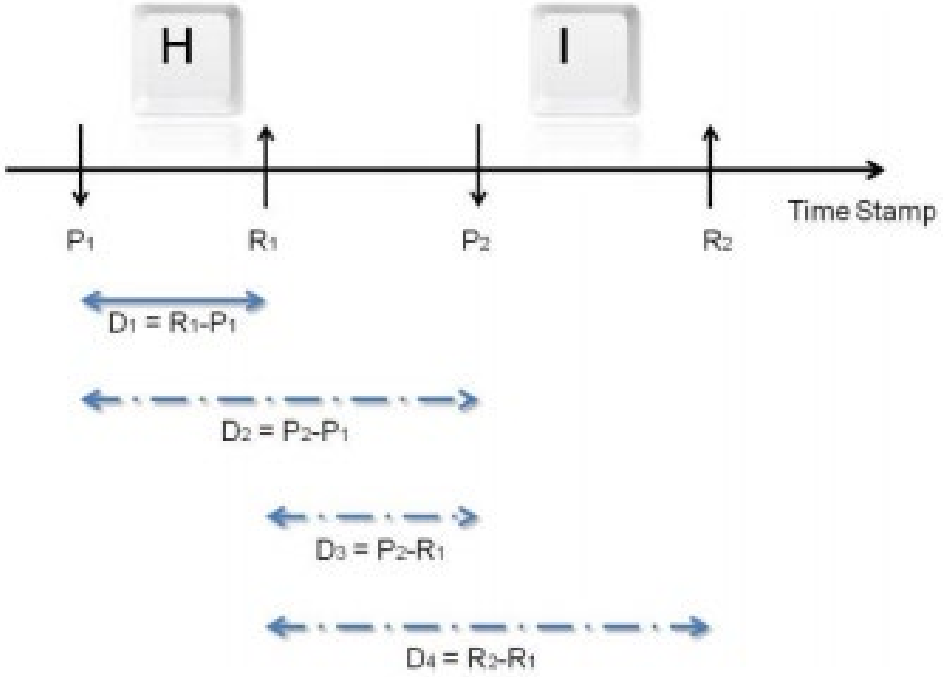


Figure 8-5 Authentication by keystroke dynamics

Authentication: Something you produce ...



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

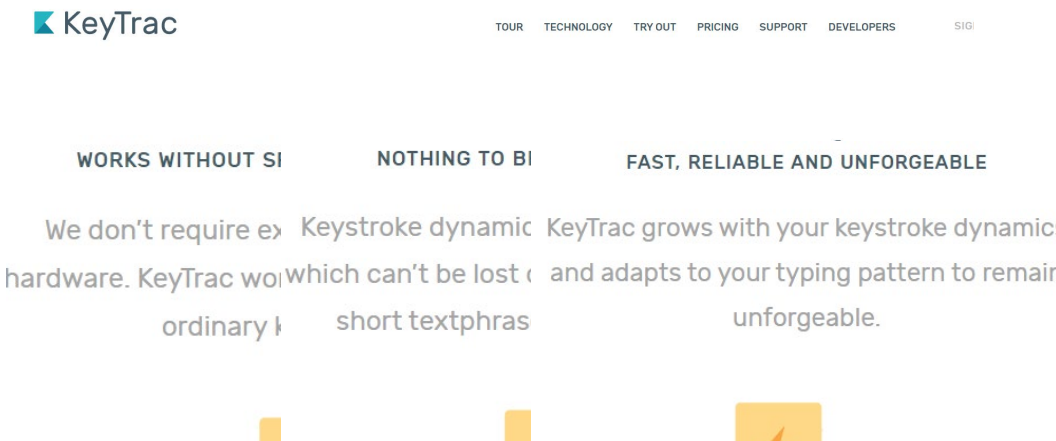
Flight Time (D_2): The time interval between a key press and the next key press.

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.

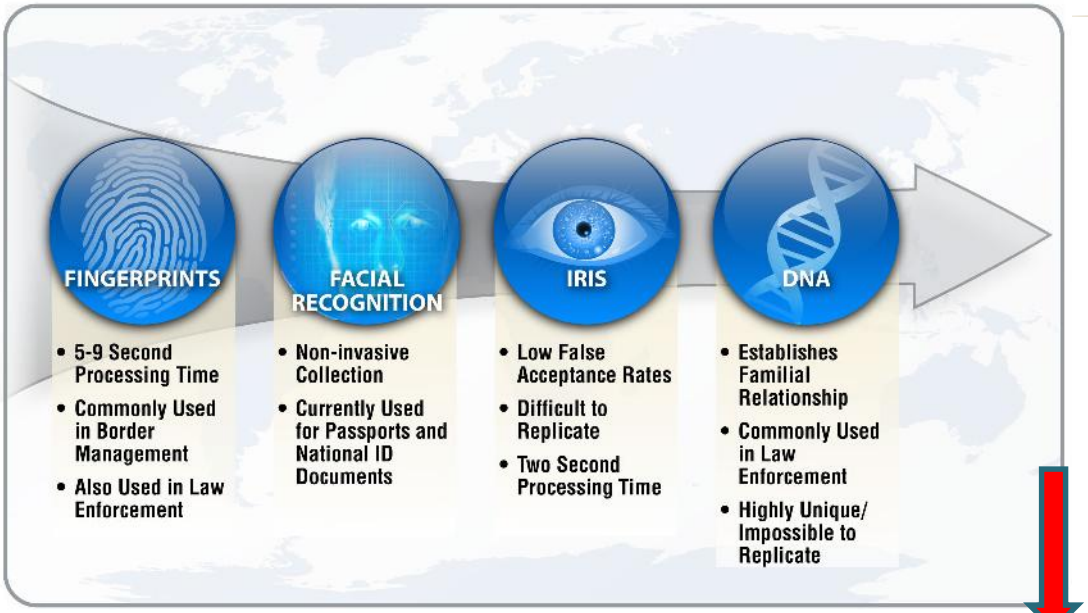
Keystroke features can be extracted in terms of:

- 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]



https://www.keytrac.net/en/

Example: Cost vs. accuracy of various biometric characteristics



Biometric Technology	Accuracy	Cost	Devices required	Social acceptability
DNA	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

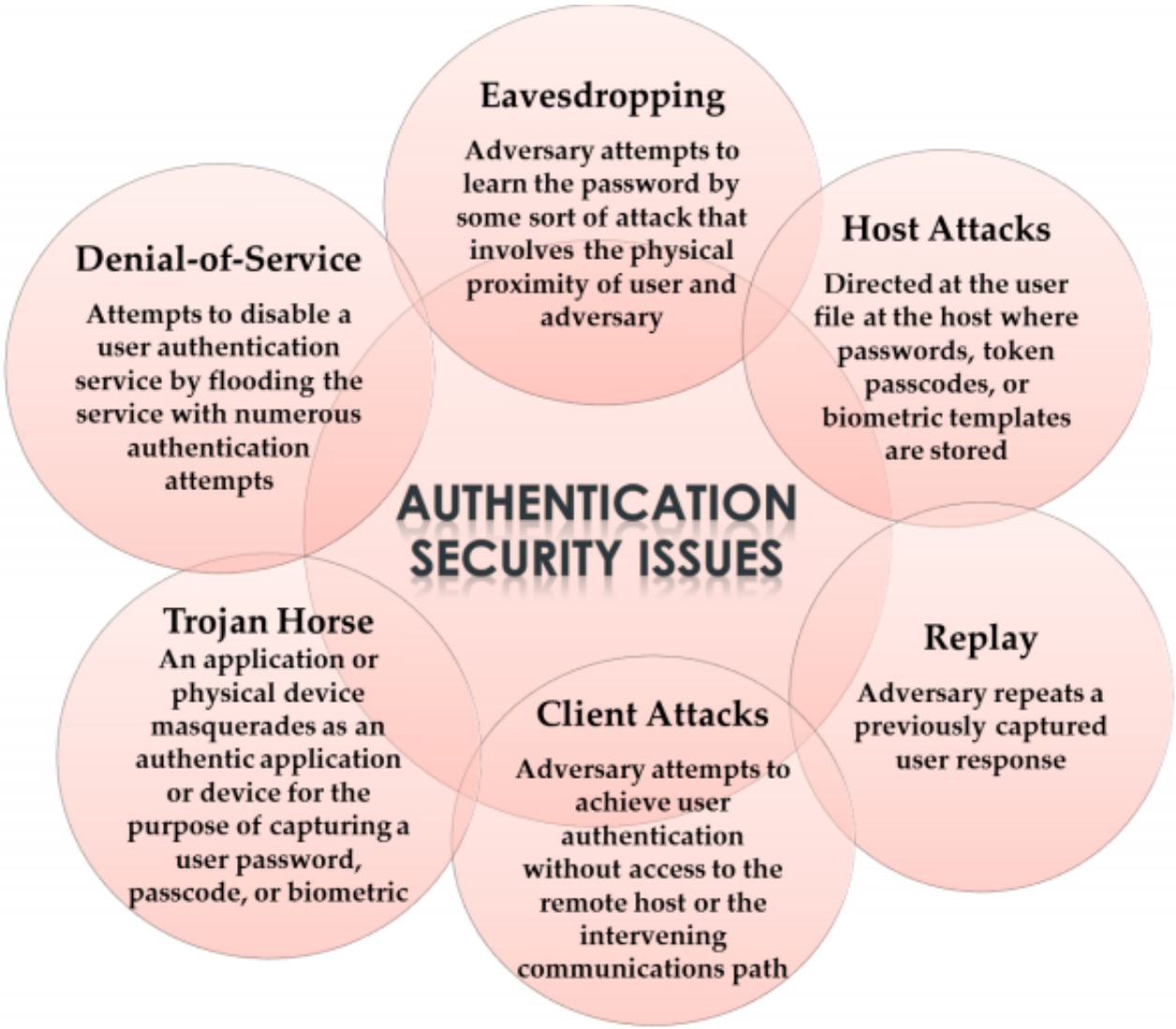
Authentication (cont.)

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

Authentication (cont.)



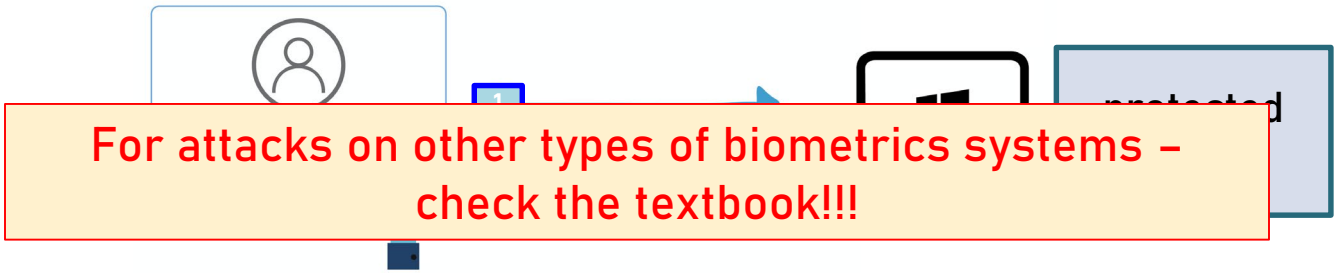
Authentication (cont.)

Example: Attacks on password-based authenticat. systems

breaking (try to 'get into' the system by using a legitimate password)

disabling (prevent legitimate user from getting into the system)

Attacks	Authenticators	Examples
Client attack	Password	Guessing, exhaustive search
Host attack	Password	Plaintext theft, dictionary/exhaustive search
Eavesdropping	Password	"Shoulder surfing"
Replay	Password	Replay stolen password response
Trojan horse	Password	Installation of rogue client or capture device
Denial of service	Password	Lockout by multiple failed authentications



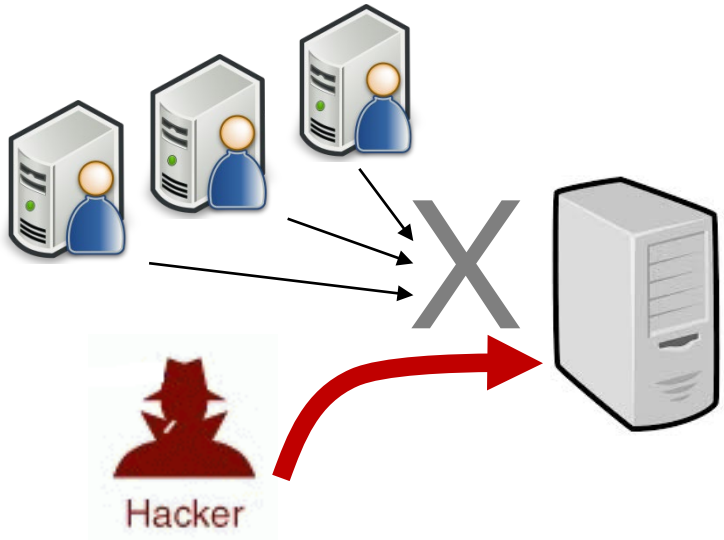
For attacks on other types of biometrics systems – check the textbook!!!

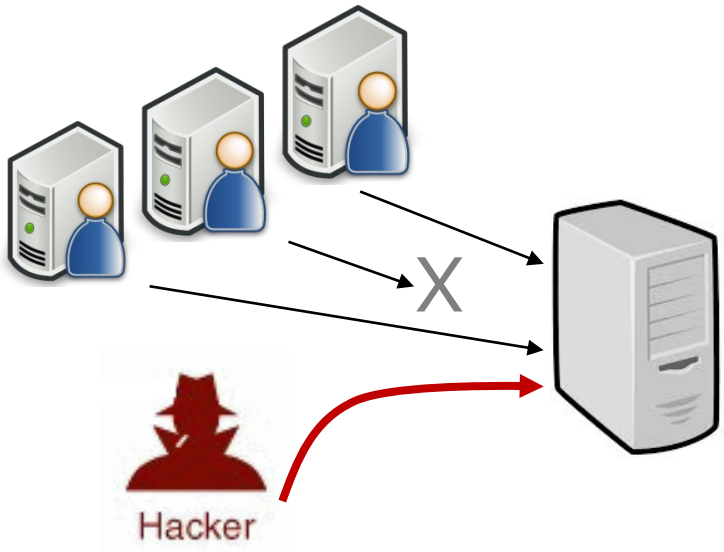
Authentication (cont.)

Example: Standard vs. Targeted DoS Attacks

Standard DoS Attack

Attacker's goal is to prevent victim-server from providing access/service to all legitimate user.





Targeted DoS Attack

Attacker's goal is to prevent one particular victim-user from obtaining access/service from a server.

Most systems 'lock-out' a user after multiple login attempts using false password ....

Authentication (cont.)

Example: **Single- and multi- factor authentication**

Systems that use one authentication credential (e.g. something you know) are known as **one-factor authentication systems**.

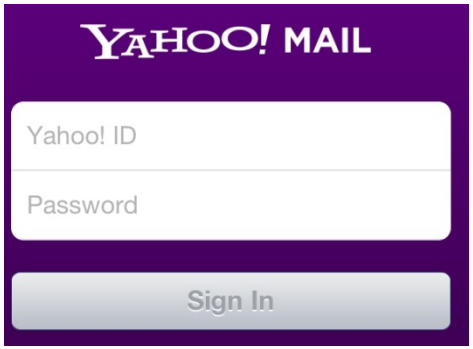
Most computer systems / applications are one-factor authentication systems – they rely on passwords only.

Systems that require strong protection typically combine multiple authentication mechanisms – e.g. something you have and something you know. They are known as **two-factor authentication systems**.

For example, access to a bank's ATM requires a banking card + a personal identification number (PIN).

Authentication (cont.)

Example: Gmail, Hotmail, York-mail as 2- factor authentication systems …



Signing in to your account will work a little differently

1 **Enter your password**

Whenever you sign in to Google, you'll enter your password as usual.

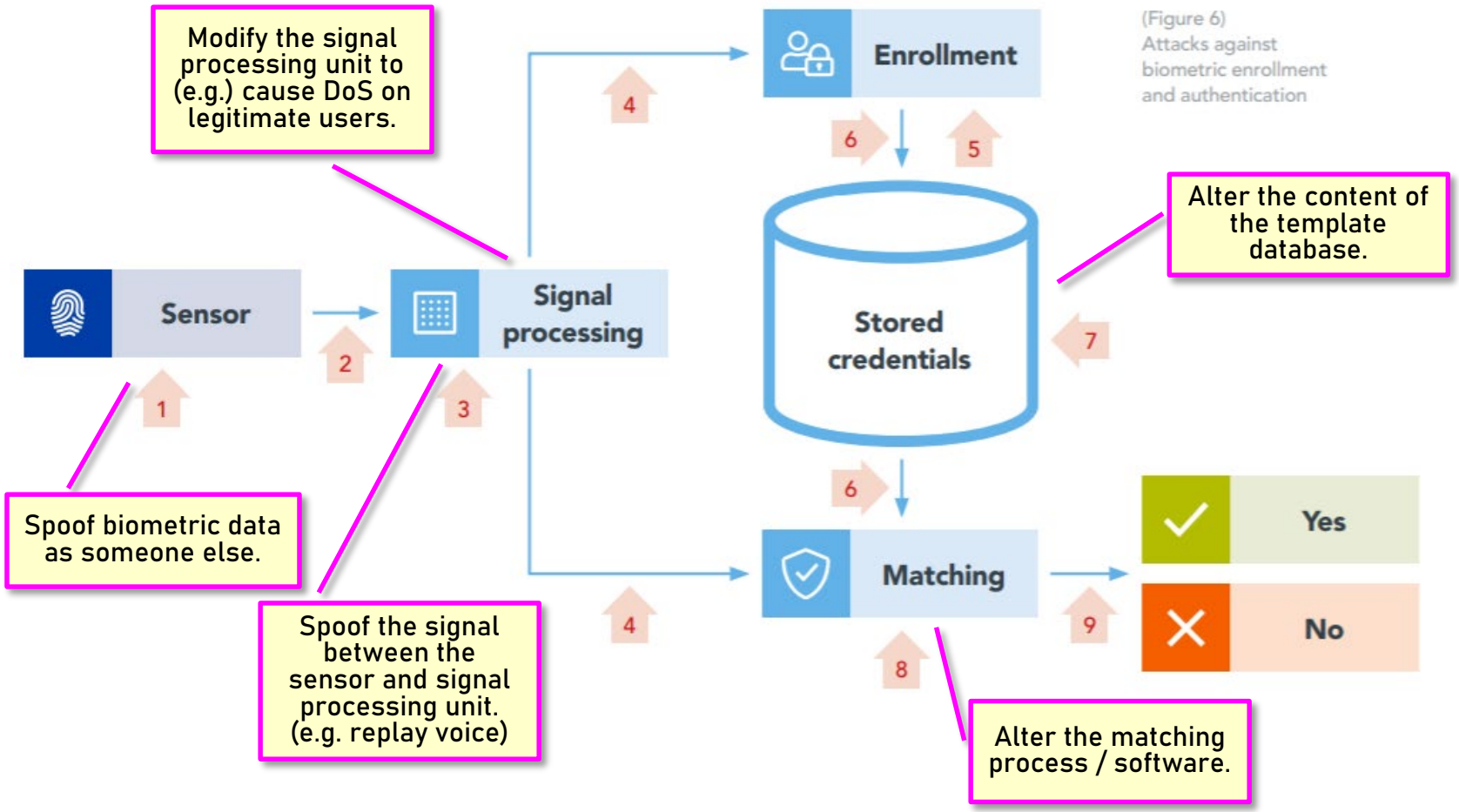
2 **Enter a verification code**

Then, you'll be asked for a code that will be sent to your phone via text, voice call, or our mobile app.

http://www.google.ca/landing/2step/

Authentication (cont.)

Example: Attacks on biometrics-based authenticat. systems



https://www.nxp.com/docs/en/white-paper/SECBIOAUTHWP.pdf