CPSC 467b: Cryptography and Computer Security

Instructor: Michael Fischer
Lecture by Ewa Syta

Lecture 23
April 11, 2012

Biometrics

Security and Privacy of Biometric Authentication

Biometrics

Authentication factors

There are three kinds of factors used for authentication:

- Something you know: e.g., a password or a PIN number
- Something you have: e.g., a token or a cell phone
- Something you are: e.g., a fingerprint or an iris pattern

Using authentication factors

One, two, or even three factors can be required in order to authenticate a user.

Two–factor authentication is an approach which requires to present two different factors for authentication.

For example:

- A password and a USB token
- A fingerprint and a smart card
- A credit card and a signature


Someone discovered my
PASSWORD.
Now I have to rename my dog.
Use strong passwords. A simple password, such as your pet's name, is not sufficient protection. Hackers systematically check every possible word to decipher passwords in no time.
Watch for an online awareness program
PUBLIC JOBS: PRIVATE DATA
Minnesota

Biometrics

Biometrics[1] is the science of establishing the identity of an individual based on physical, chemical, or behavioral attributes of the person.

[1] A. K. Jain, P. Flynn, A. Ross, *Handbook of Biometrics* Springer, 2007

Biometric modes

Identification is a process of establishing subject's identity.

- "Who are you?"
- One to many comparison

Authentication is a process of verifying subject's identity.

- "Is that really you?"
- One to one comparison

We will focus on biometric authentication.

Pros & cons of biometric authentication

Pros:

- Biometric characteristics uniquely identify an individual
- Higher degree of security: biometric traits cannot be lost, forgotten, or shared
- Always available!

Cons:

- Biometric traits cannot be changed. If stolen, can be used to impersonate individual
- Usability and acceptability issues
- Privacy concerns

Basic biometric terms[2]

Biometric characteristic – physiological or behavioral property of an individual

Biometric sample – analog or digital representation of biometric characteristics before any processing is applied

Biometric feature – information extracted from a biometric sample

Biometric template – stored biometric features for the purpose of a comparison

[2] M. U. A. Bromba, `http://www.bromba.com/faq/biofaqe.htm`

Suitable biometric characteristics

A biometric characteristic suitable for authentication purposes should have the following properties:[3]

- *Universality* – everyone should have it
- *Uniqueness* – it should be different for every person
- *Permanence* – it should not change with time
- *Collectability* – it can be quantitatively measured

In practice, *acceptability* is also an important requirement.

[3] R. Clarke, *Human identification in information systems: Management challenges and public policy issues*, Information Technology & People, Vol. 7, No. 4, pp. 6-37, 1994

Types of biometric characteristics

Physiological:

- Fingerprint
- Face
- Iris
- Retina
- Hand
- Ear

Behavioral:

- Voiceprint
- Keystroke
- Signature
- Gait

Comparison of biometric characteristics[4]

Biometrics	Universality	Uniqueness	Permanence	Collectability	Acceptability
Face	High	Low	Medium	High	High
Fingerprint	Medium	High	High	Medium	Medium
Hand	Medium	Medium	Medium	High	Medium
Ear	Medium	Medium	High	Medium	High
Iris	High	High	High	Medium	Low
Retina	High	High	Low	Low	Low
Odor	High	High	High	Low	Medium
DNA	High	High	High	Low	Low
Voice	Medium	Low	Low	Medium	High
Gait	Medium	Low	Low	High	High
Keystrokes	Low	Low	Low	Medium	Medium
Signature	Low	Low	Low	High	High

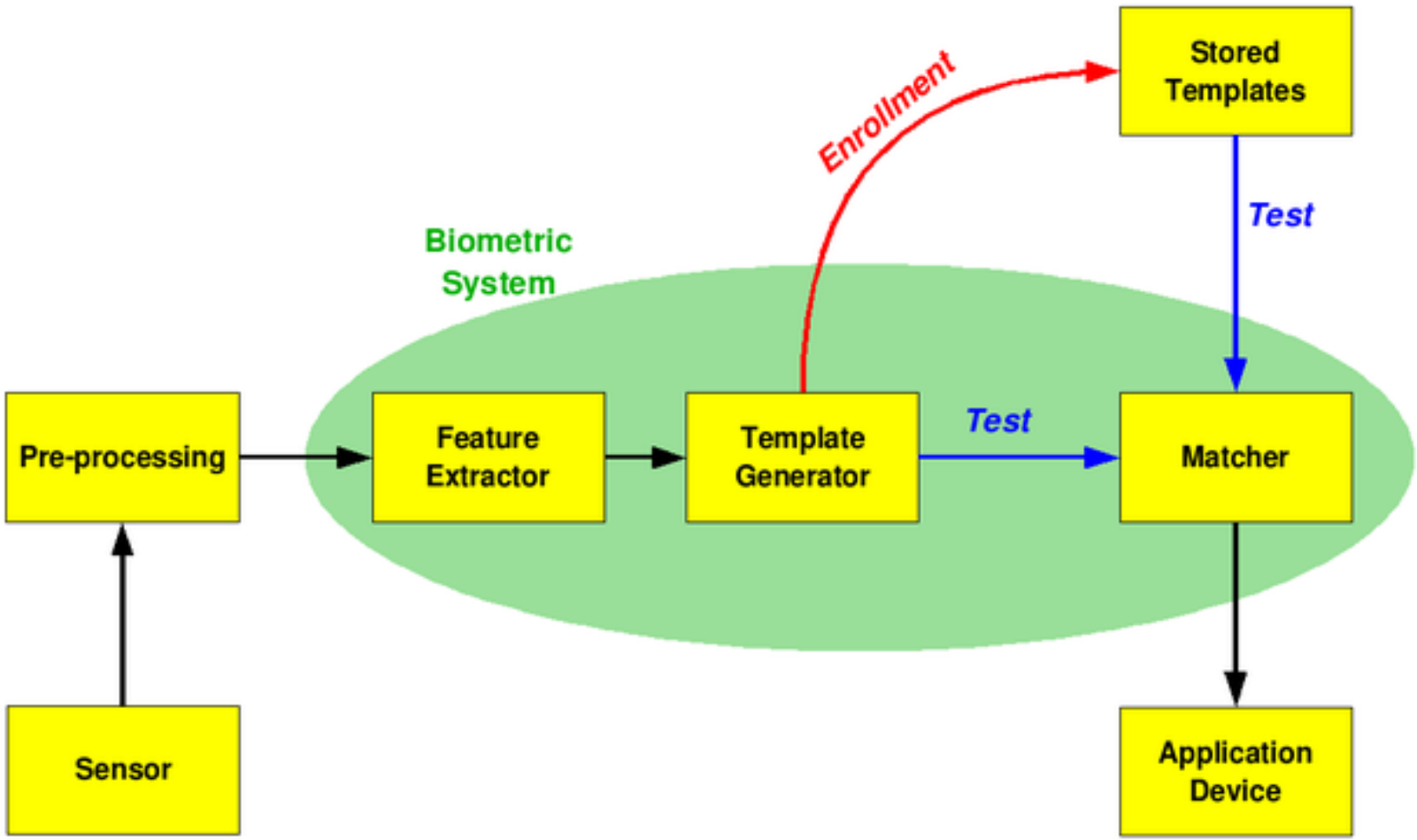
[4] A. Jain, R. Bolle, and S. Pankanti, *Introduction to Biometrics*
`http://www.cse.msu.edu/~cse891/Sect601/textbook/1.pdf`

Biometric protocol

A biometric-based protocol consists of two phases:

- *Enrollment phase*
  - Acquisition of biometric sample(s)
  - Creation of a biometric template
  - Storage of a biometric template
- *Verification phase*
  - Acquisition of biometric sample(s)
  - Comparison with a biometric template
  - Decision

Diagram of a biometric system[5]



[5]Image retrieved from `http://en.wikipedia.org/wiki/Biometrics`

Acquisition of a biometric sample[4]

It is a critical part of the enrollment process and will determine the performance of the entire system.

- *Quality assessment*: assessing the suitability of the input data

- *Segmentation*: separation of the input data into foreground (object of interest) and background (irrelevant information)

Creation of a biometric template

A biometric template is a representation of the features from a biometric sample.

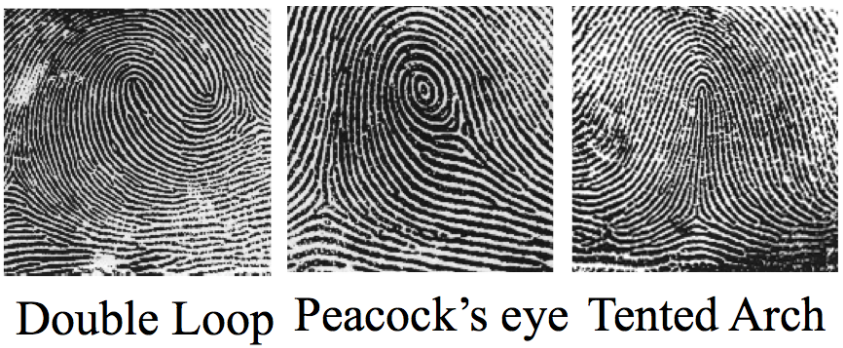
- *Feature extraction*: key features of the biometric sample are located, selected, measured and encoded.

Characteristic	Features
Fingerprint	Finger lines, pore structure
Signature	Pressure and speed differentials
Facial geometry	Distance of specific facial features (eyes, nose, mouth)
Iris	Iris pattern
Hand geometry	Measurement of fingers and palm
Voice	Tone or timbre
Odor	Chemical composition of one's odor
Keyboard strokes	Rhythm of keyboard strokes

Example: Fingerprint features[7]

Common patterns

Less common patterns



Minutia are extracted from these features.

Example: Extracting fingerprint features[7]

1. Capture an image of a fingerprint
2. Enhance the image
3. Identify minutia

Storage of a biometric template[6]

The acceptance of biometric system depends on how secure the templates are.

There are four major locations for storing templates:

- Portable tokens
- Central databases
- Sensors
- Individual workstations

[6] A. Patrick and S. Mu, *Usability and Acceptability of Biometric Security Devices*, National Research Council of Canada

Comparison with a biometric template

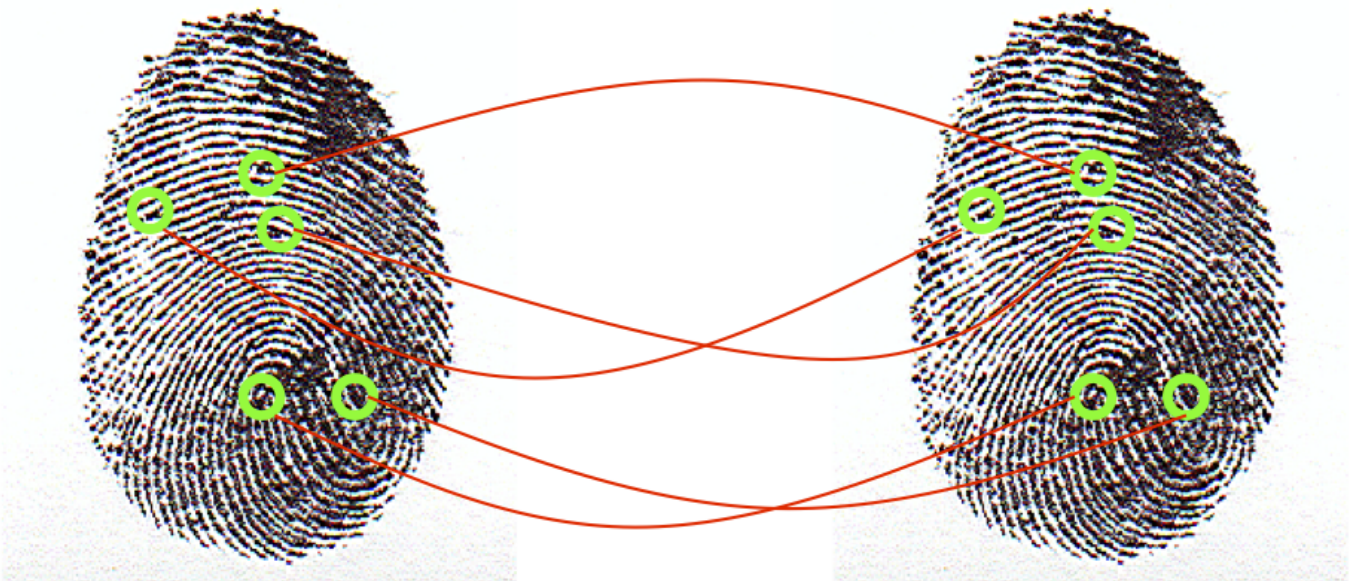
Each time a user wants to authenticate, the first two steps of the enrollment phase are repeated (acquisition and creation of template).

Freshly extracted features are compared with those saved in the reference template.

How similar the two samples should be to authenticate a user?

Example: Comparing fingerprint features[7]

1. Obtain a fresh fingerprint
2. Extract minutia and create a template
3. Compare with the minutia from the stored template



[7] M. Stamp, *Information Security Principles and Practice*, Wiley, 2006

Matching fingerprints[8]

- United Kingdom employs a 16-point minimum match
- Australia mandates a 12-point minimum match
- Canada uses no minimum point standard
- In the US, state jurisdictions set their own minimum point standards
- FBI has no minimum number that must be identified to declare an "absolutely him" match, but does rely on a 12-point "quality assurance" standard

Following the ruling of Judge Louis H. Pollak, experts cannot tell juries that two fingerprints are a "match", they can only can testify about how the prints were obtained and the similarities and differences between them.

[8] S. P. Duffy, *Experts May No Longer Testify That Fingerprints "Match"* The Legal Intelligencer, January 9, 2002

Authentication decision

Unlike other authentication methods, biometric authentication does not yield a definitive authentication decision.

A decision is made based on how close (similar) is the biometric template obtained in the enrollment phase to the one obtained in the verification phase.

If the system is too lenient, it will result in a high number of false acceptances; if too strict, there will be a high number of false rejections. Both are bad!

Biometric errors

False Acceptance Rate (FAR)

- Frequency that a user A is authenticated as user B
- Security relevant measure
- Target rate: $\leq 0.5\%$

False Rejection Rate (FRR)

- Frequency that an authorized user is denied access
- Usability relevant measure
- Target rate: $\leq 5.0\%$

False to Enroll Rate (FER)

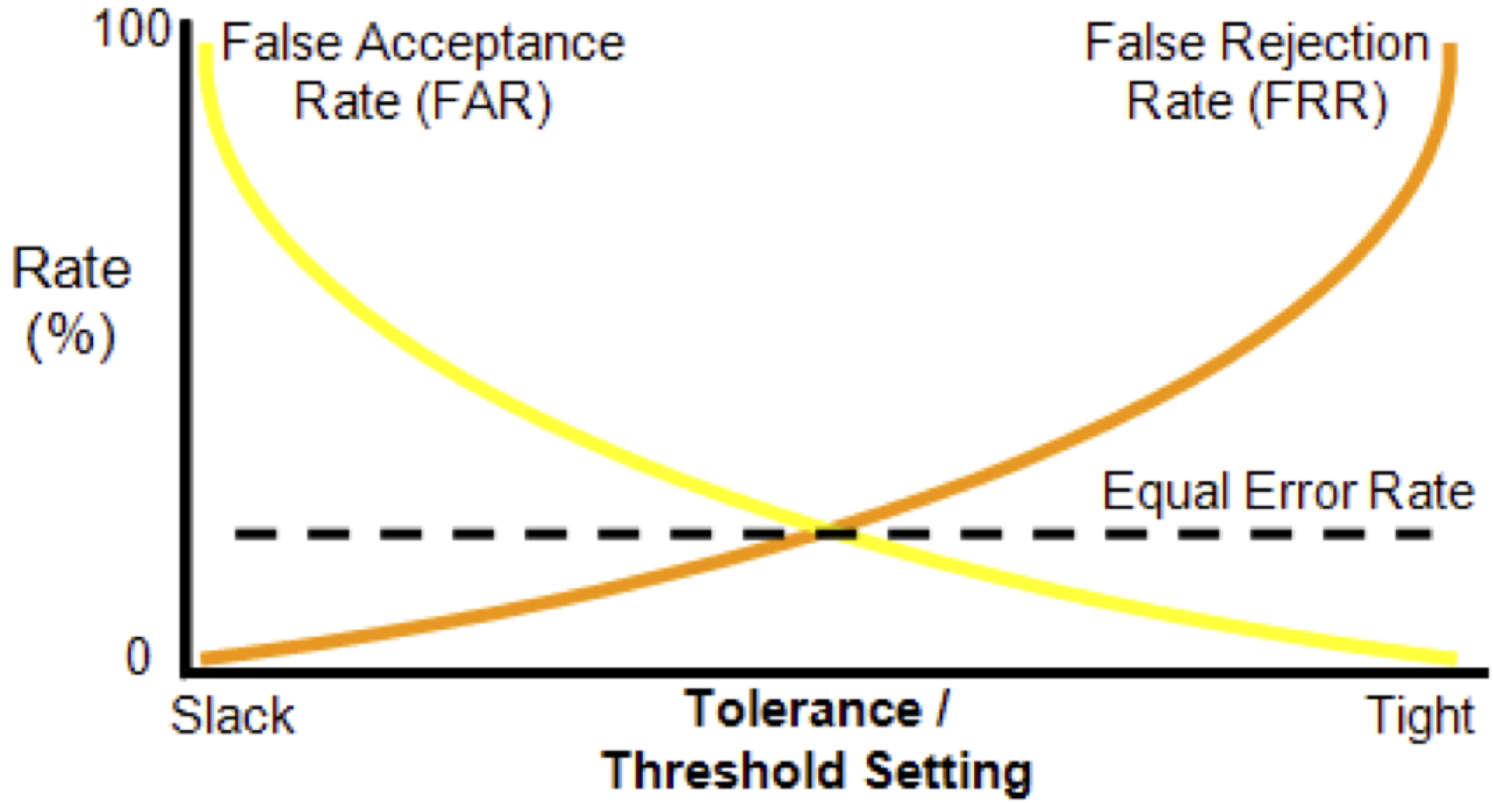
- Frequency that a user cannot enroll into the system
- Usability relevant measure
- Target rate: $\leq 5.0\%$

Comparing biometric systems

Equal Error Rate (EER) – the rate at which both FAR and FRR are equal.

It is a quick to compare the performance of biometric systems. In general, the system with the lowest EER is most accurate.

Equal Error Rate[7]



Comparison of biometric systems[9]

	Finger	Voice	Iris	Face
EER	$2-3.3\%$	$<1\%$	$4.1-4.6\%$	4.1%
FER	4%	2%	7%	1%
FAR	2.5%	$<1\%$	6%	4%
FRR	0.1%	$<1\%$	0.001%	10%

[9] G. Huntington, Huntington Ventures Ltd.
http://www.authenticationworld.com/Authentication-Biometrics/index.html

Comparison of biometric systems[10]

	Face	Fingerprint	Hand	Iris	Keystrokes	Voice
EER	*N/A*	2%	1%	0.01%	1.8%	6%
FAR	1%	2%	2%	0.94%	7%	2%
FRR	10%	2%	2%	0.99%	0.1%	10%
Subjects	37437	25000	129	1224	15	30

Face: varied light, indoor /outdoor
Fingerprint: rotation and exaggerated skin distortion
Hand: with rings and improper placement
Iris: indoor environment
Keystrokes: during 6 months period
Voice: text dependent and multilingual

[10] D. Bhattacharyya, R. Ranjan, F. Alisherov, and M. Choi, *Biometric Authentication: A Review*, International Journal of u- and e- Service, Science and Technology, 2009

Security and Privacy of Biometric Authentication

Privacy & security concerns

Concerns with biometrics:[11]

- Unauthorized access to biometric data
- Unauthorized disclosure of biometric data to third parties
- Use of biometric data for other than intended purpose
- Collection of biometric data without the knowledge of the individual

[11] B. Wirtz, *Biometric Systems 101 and Beyond*, Secure - The Silicon Trust Quarterly Report, Fall 2000

Source of the privacy & security issues

Recall, that biometric characteristics uniquely identify an individual and cannot be changed.

If Eve obtains Alice's biometric data, she can convince Bob that she's her and there is not much Alice can do.[12]

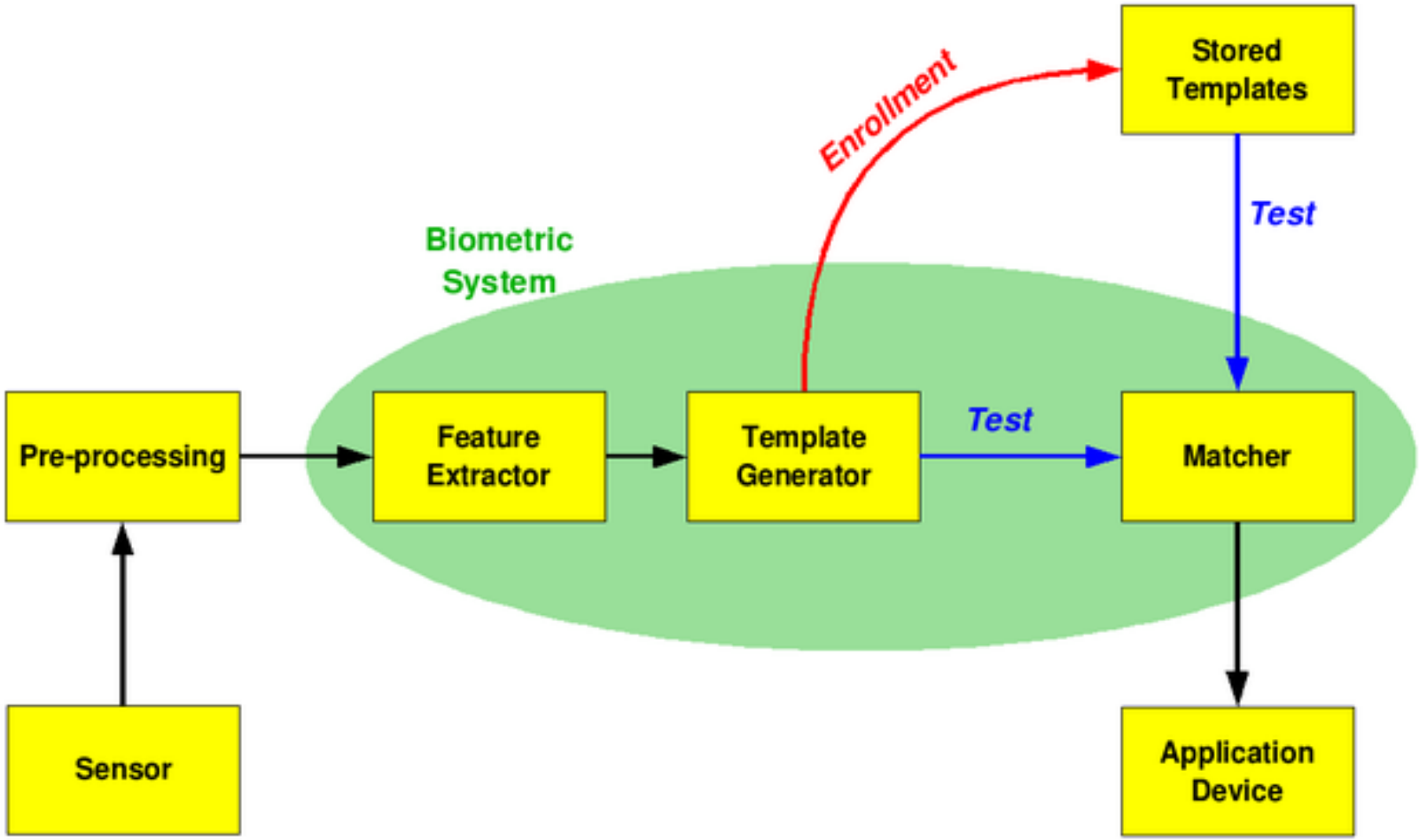
Therefore, security of biometric data is extremely important.

[12] Intentional oversimplification

"If McDonald's offered a free Big Mac in exchange for a DNA sample, there'd be lines around the block."

Bruce Schneier

Security issues in a biometric system



Biometric security

Recall, that authentication is done by comparing a freshly obtained biometric sample with a biometric template created during enrollment. This approach implies that both biometric data must be made available to a verifying party.

Securing biometric data is much easier if a sample is obtained and verified on a stand-alone system.

Remote biometric authentication is very challenging – biometric data can be intercepted during transmission or stolen from the verifying party.

New approach to remote biometric authentication[13]

Based on two-factor authentication: combination of possession-based authentication and biometrics.

A new way to handle biometric data: users identity is created with respect to a special blinding factor, not the biometric data itself. The verifying party has access only to the blinding factor.

Identity verification is based on the difference between biometric data obtained in the enrollment phase and data provided in the verification phrase.

Suitable for authentication based on any biometric characteristic.

[13] E. Syta, G. Gallegos García, M. Fischer, A. Silberschatz, *Strong, Theft-proof, and Privacy-preserving Biometric Authentication*, unpublished work

Protocol properties

It is secure against a loss of a smart card.

The smart card stores only the blinded biometric sample. If an attacker steals Peggy's card, he does not learn anything about her biometric data.

It is secure against eavesdroppers.

A passive attack will see a stream of blinded differences between two readings of Peggy's biometric data.

Protocol properties

It is secure against a dishonest server.

An authentication server does not store or receive any biometric data. Users identity is first linked to a blinding factor seed and then to the next state of pseudo-random number generator used to verify the difference between two biometric readings.

If the server is compromised, then all that is learned is the PRNG sequence. But even with that information, the sequence of messages sent by the legitimate user does not contain the biometric data but only their difference.

Additional Resources

More information on biometrics:

- NIST, ITL, Introduction to Biometrics, `http://biometrics.nist.gov`
- NIST, ITL, Fingerprint Biometrics, `http://fingerprint.nist.gov`
- NIST, ITL, Face Biometrics, `http://face.nist.gov`
- NIST, ITL, Iris Biometrics, `http://iris.nist.gov`