Security of Biometric Systems

A Short Introduction

Kevin Atighehchi

Université Clermont Auvergne
kevin.atighehchi@uca.fr

February 20, 2020

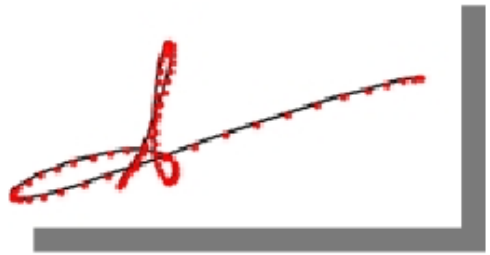
Automated Border Control

Authentication Factors

- **Something I know** (password, PIN code, ...)
- **Something I possess** (USB key, smart card, smartphone, ...)
- **Something I am** (morphological, behavioural, biological data)

Biometric Modalities

Keystroke dynamics

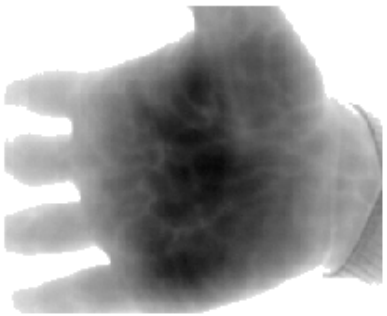


Signature dynamics

Finger knuckle print

Iris

Fingerprint

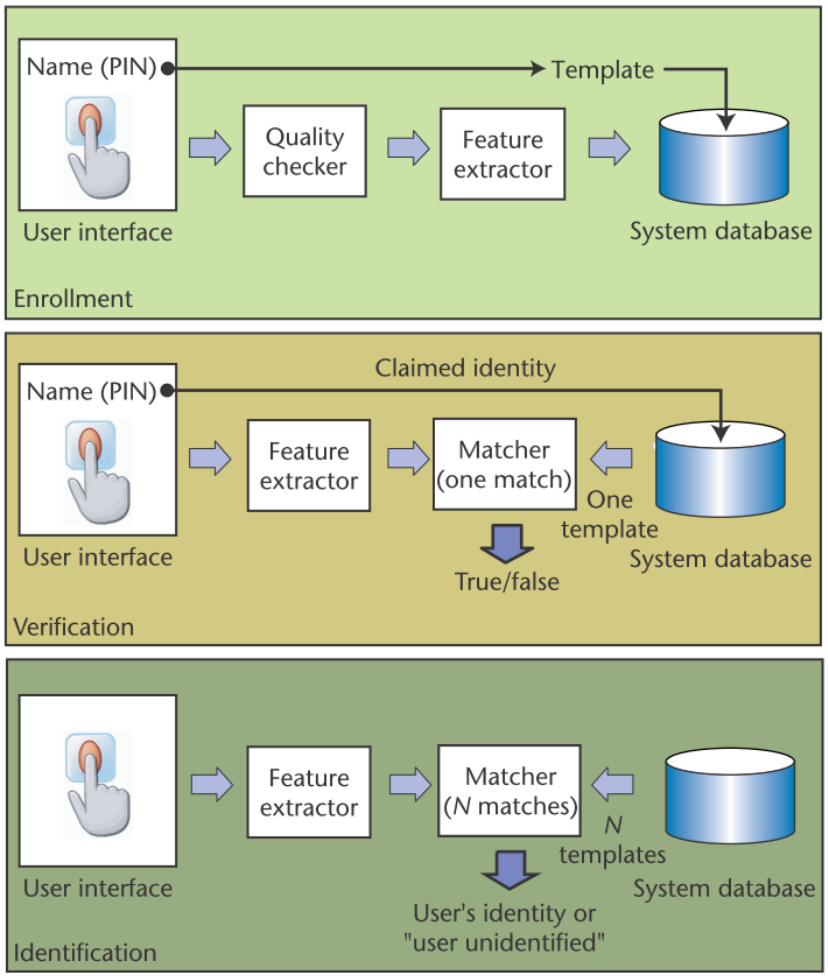


Palm vein, hand shape

Principle of a Biometric System

Two steps:

- Enrollment (sensing, processing, storage, at earlier time)
- Verification or identification (at later time)



Decision

How to decide if the claimed identity is correct?

Suppose SCORE is a similarity matcher of biometric templates.

```
IF SCORE(REFERENCE TEMPLATE,
         CAPTURED TEMPLATE) > THRESHOLD
    ACCEPT
ELSE
    REJECT
```

THRESHOLD value is set according to the application

Protection des données biométriques

Motivation

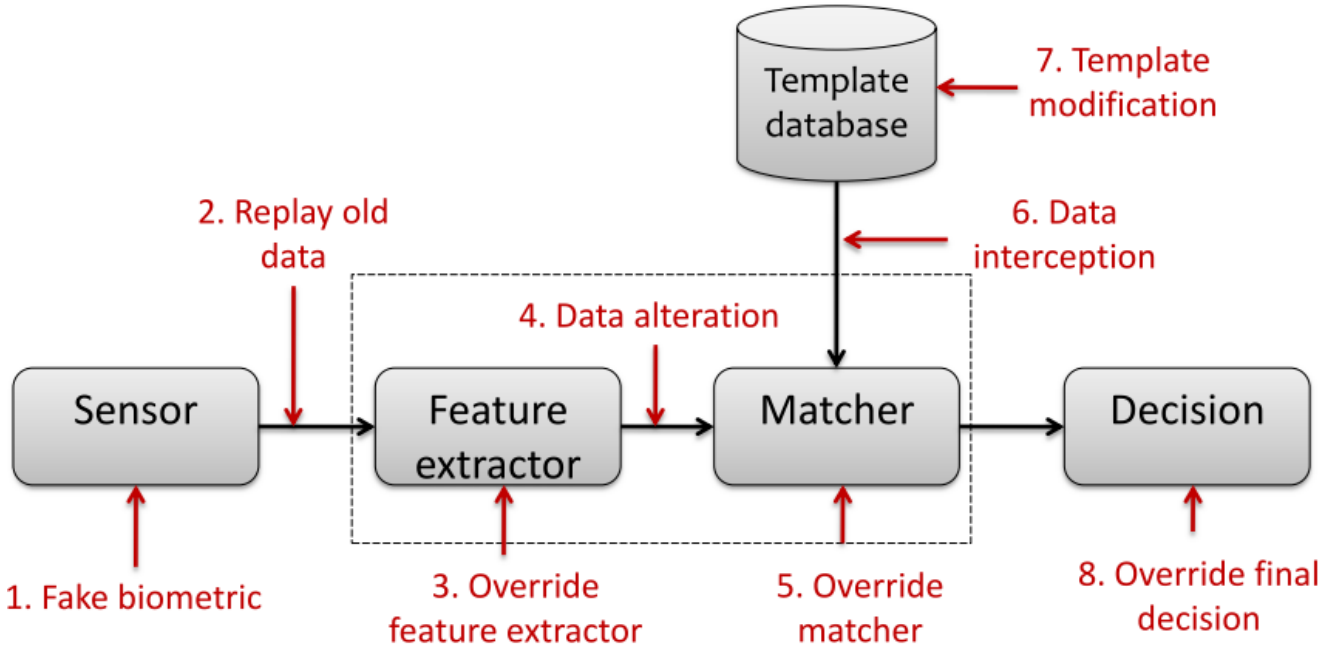
Legislative and regulatory context:

- GDPR
- Loi Informatique et Libertés (update for compliance with GDPR)
- *Privacy-by-design*, *privacy-by-default*

Biometric data:

- A long-term and unique personal identifier
- A non-revocable data
- Whence categorized as a highly sensitive and private data

Vulnerabilities of a Biometric System

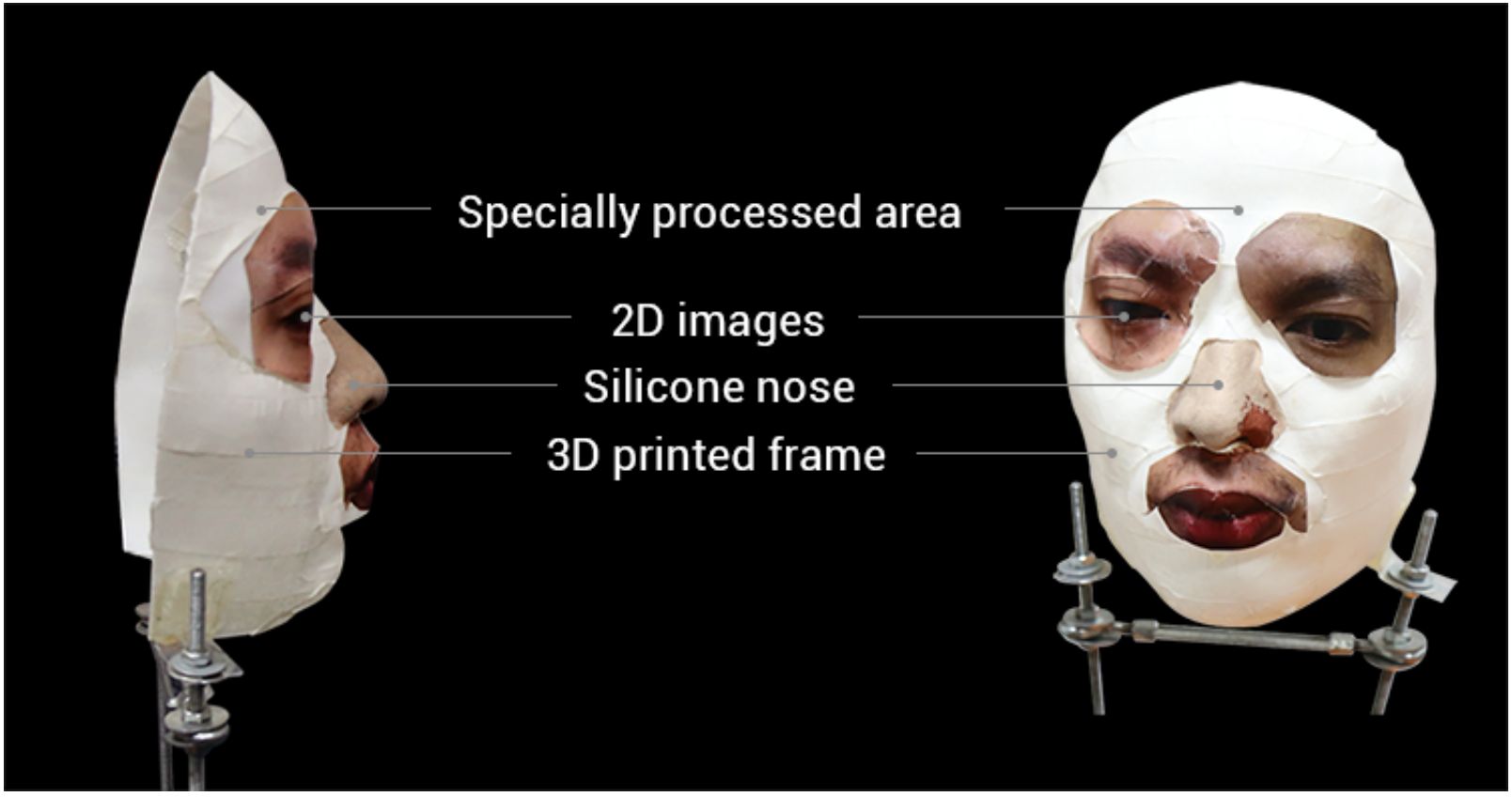


Attack points (Model of Ratha *et al.*, 2001)

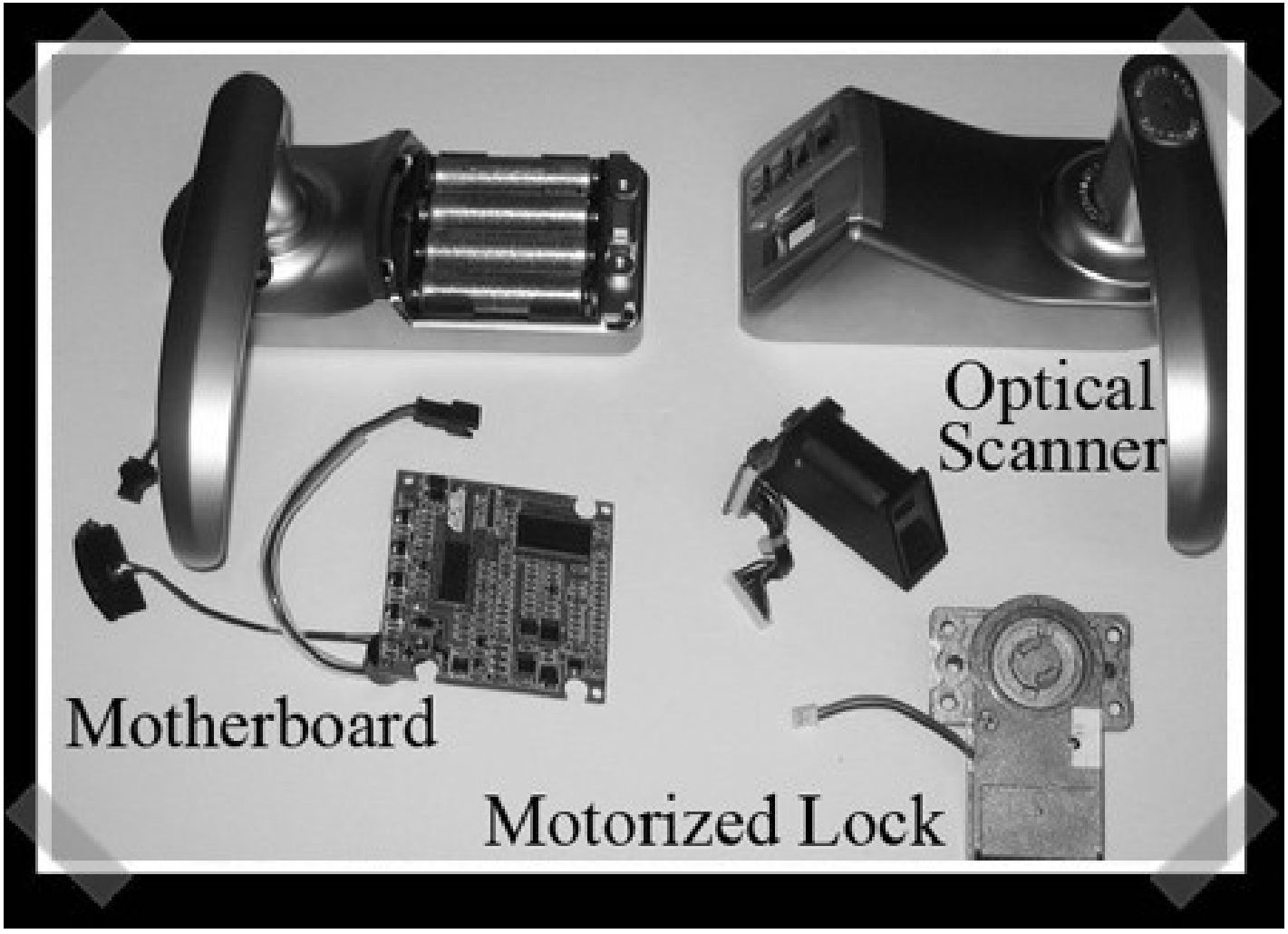
- 1: Sensor attacks
- 2, 4, 6: Communication channel attacks (eavesdropping, interruption, modification, replay)
- 3, 5, 8: Attacks on the processing modules (malware injection to control the initial module)
- 7: Attacks on the templates (compromise of the database)

Sensor Attack: Make-up

Sensor Attack: FaceID Spoofing



Attack on the Decision Module



The matcher result (accept or reject) can be overridden by the attacker.

Attacks on the Matcher: Hill-Climbing

The reference template T is compared with the fresh template T', using a metric distance d and a threshold τ. If $d(T, T') \leq \tau$, access to the system is granted.

Assumption: The distance is leaked.

Let T, $T' \in \mathbb{F}_2^n$ and d the Hamming distance. If each time an authentication attempt the adversary makes he learns the resulting score, then he can recover the template T with **only $\mathbf{n+1}$ attempts**.

To compare with the $\sim 2^{n-t}$ attempts that require a brute-force attack when the distance is not leaked.

Biometrics with standard cryptography

Assumption: the reference biometric template is encrypted with a standard algorithm (AES), by the user (or by the server after a secure transmission), prior its storage on the server.

1. Enrolment phase: The server encrypts the biometric reference template T, sent by the user (variant: the user encrypts his template T and sends it to the server).
2. Verification phase: The user sends a fresh template T' to the server. The server decrypts the reference template T and compares it with T'.

Insights:

- Biometric templates are not protected during the verification. If the server is compromised, the biometric template is compromised.
- Standard cryptography does not preserve distances.

Template Database Integrity

Assumptions:

- The templates of the database are separately protected in integrity, *i.e.* a MAC or a digital signature is computed on each template (along with the user ID).
- The adversary is a user of the system.

Insights:

- The adversary could swap its own pair of template/MAC with the pair of another user.
- The data structure should be authenticated as well.

PET and Security Criteria

Crypto-biometric schemes are used to protect biometric templates and are included in the Privacy Enhancing Techonologies, standardized in ISO 24745 (2011).

Required criteria in ISO 24745:

- **Performances**
- **Irreversibility**
- **Unlinkability/diversity (Indistinguishability)**
- **Revocability/renewability**

Protection of biometric data

Motivation and examples of primitives

Biometric data require special treatments adapted to their level of sensitivity:

- Protection against a passive attacker
- Protection against an active attacker
- With a variety of assumptions regarding the communicating systems:
  - Honest-but-curious server
  - Server compromise
  - Authentication device stolen (*e.g.* smartphone)

Some mechanisms:

- Fuzzy {Commitment, Vault, Extractor}
- Computations in the encrypted domain
- Secure Multi-Party Computation
- Cancelable biometric transformations

Thanks for your attention...

Questions?