Grant Agreement No. 675087

Vulnerability assessment in the use of biometrics in unsupervised environments

Anas Husseis

Carlos III University of Madrid

Motivation

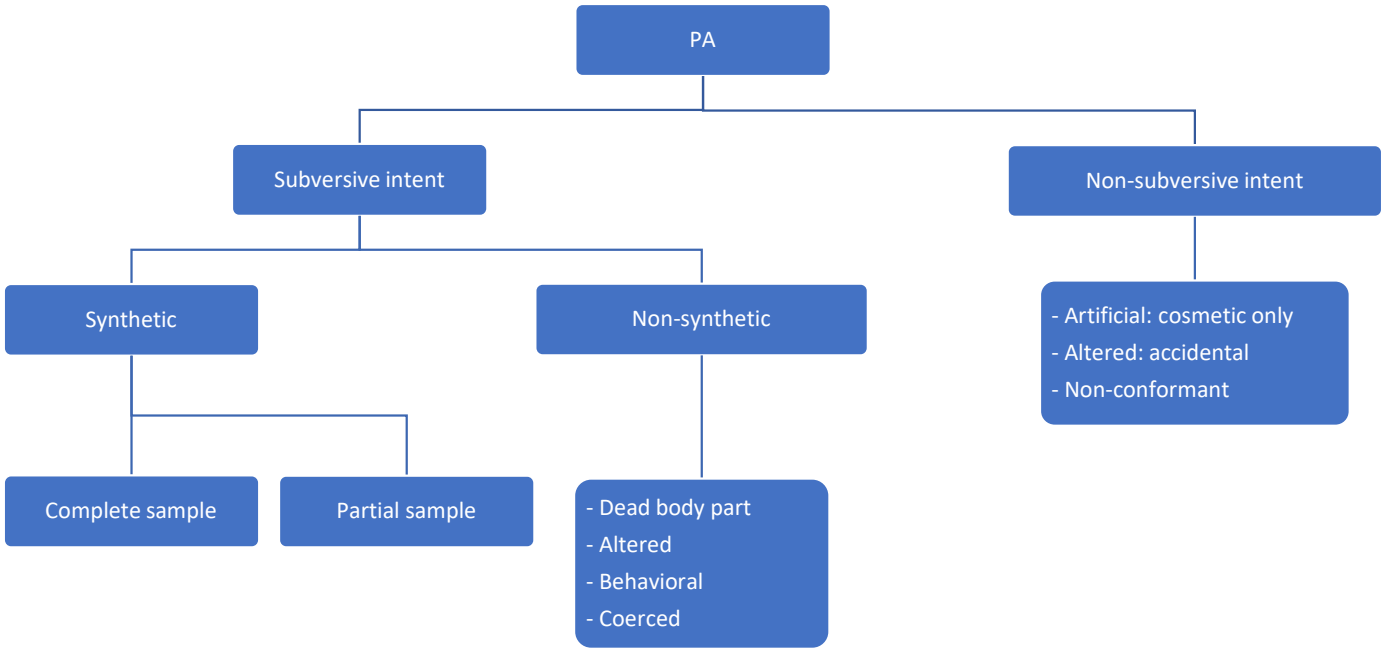
- Biometrics: Uniqueness vs. Security

- Why biometric systems are vulnerable?
  - ➢ Is it the user, sensor technology, algorithm, or biometric modality?

- How are we going to address this issue, and can we mitigate or eliminate potential attacks?

RESEARCH & INNOVATION
Marie Skłodowska-Curie actions

Presentation Attack (PA)

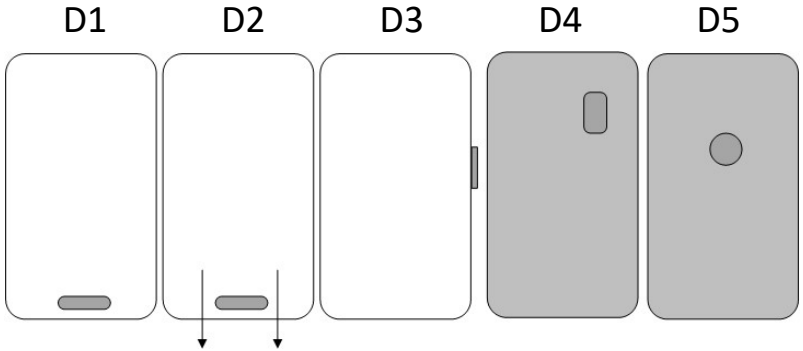


RESEARCH & INNOVATION
Marie Skłodowska-Curie actions

Attack Potential

- The required skills and tools to perform an attack can be characterized by:
  1. Elapsed time
  2. Expertise
  3. Knowledge of TOE
  4. Window of opportunity
  5. Software / hardware equipments

Presentation Attack on Smartphones

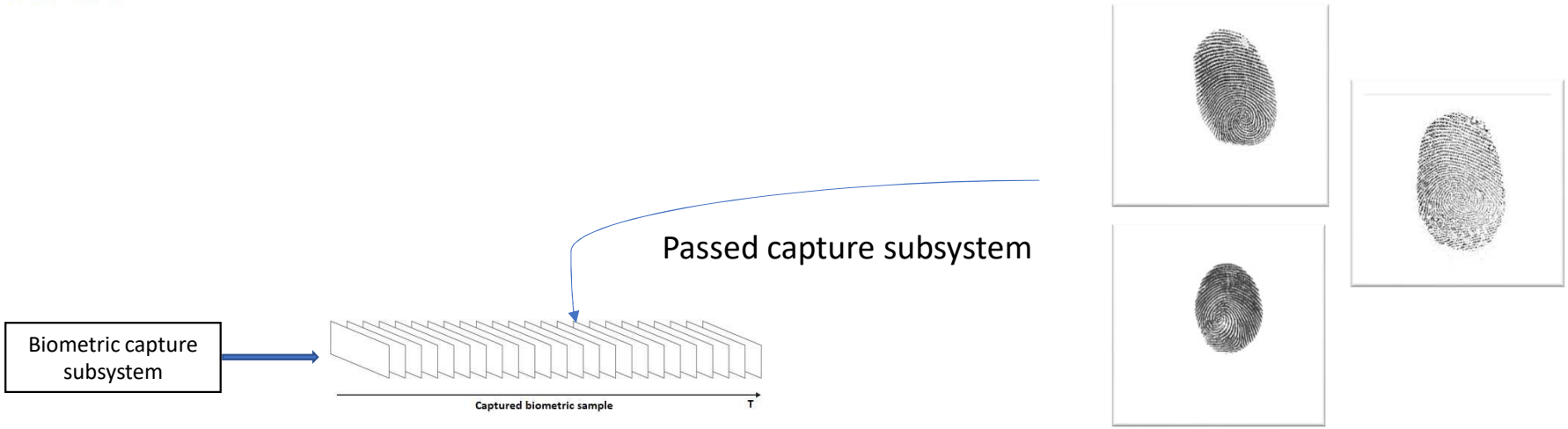


- 10 participants tries to attack smartphones for the first time
- Only 24 hours time is given to finish the experiment
- All required materials are available on Amazon.com

Device	Number of Experiments	Number of Detections	Number of Presentations	Number of Successful Attacks	Successful attacks (%)
D1	15	8	115	23	20.0%
D2	4	4	50	3	6.0%
D3	4	4	52	39	75.0%
D4	2	0	0	0	0.0%
D5	10	9	142	25	17.6%

R. B. Gonzalo *et al.*, "Attacking a Smartphone Biometric Fingerprint System: A Novice's Approach," in *2018 International Carnahan Conference on Security Technology (ICCST)*, 2018, pp. 1–5

Presentation Attack on Fingerprint Systems

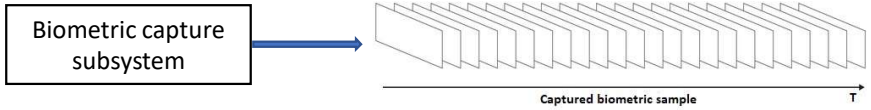


- How to distinguish attack presentations?

RESEARCH & INNOVATION
Marie Skłodowska-Curie actions

Dynamic Fingerprint Acquisition

- How to distinguish attack presentations?



Dynamic capturing

RESEARCH & INNOVATION
Marie Skłodowska-Curie actions

Thank you for your attention

- For further details: ahusseis@ing.uc3m.es

- Further details on the AMBER project can be found here: https://www.amber-biometrics.eu