enhAnced Mobile BiomEtRics

THESIS Deliverable Number: D34 D4.19
Submission of PhD Thesis ESR 9
Vulnerability Assessment in the Use of Biometrics in Unsupervised Environments

Contract number:	675087
Project acronym:	AMBER
Project title:	Enhanced Mobile Biometrics
Project duration:	1 January 2017 – 31 December 2020
Supervisors:	Professor Raul Sanchez-Reillo

Deliverable Number:	D4.19
Type:	Thesis
Dissemination level:	Public
Expected submission date:	February 2021
Expected defence date:	April 2021

Authors / contributors:	Anas Husseis
Place:	Universidad Carlos III de Madrid

RESEARCH & INNOVATION
Marie Skłodowska-Curie actions

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675087

Thesis full text

Abstract

In the last few decades, we have witnessed a large-scale deployment of biometric systems in different life applications replacing the traditional recognition methods such as passwords and tokens. We approached a time where we use biometric systems in our daily life. On a personal scale, the authentication to our electronic devices (smartphones, tablets, laptops, etc.) utilizes biometric characteristics to provide access permission. Moreover, we access our bank accounts, perform various types of payments and transactions using the biometric sensors integrated into our devices. On the other hand, different organizations, companies, and institutions use biometric-based solutions for access control. On the national scale, police authorities and border control measures use biometric recognition devices for individual identification and verification purposes.

Therefore, biometric systems are relied upon to provide a secured recognition where only the genuine user can be recognized as being himself. Moreover, the biometric system should ensure that an individual cannot be identified as someone else. In the literature, there are a surprising number of experiments that show the possibility of stealing someone's biometric characteristics and use it to create an artificial biometric trait that can be used by an attacker to claim the identity of the genuine user. There were also real cases of people who successfully fooled the biometric recognition system in airports and smartphones [1]–[3]. That urges the necessity to investigate the potential threats and propose countermeasures that ensure high levels of security and user convenience.

Consequently, performing security evaluations is vital to identify: (1) the security flaws in biometric systems, (2) the possible threats that may target the defined flaws, and (3) measurements that describe the technical competence of the biometric system security. Identifying the system vulnerabilities leads to proposing adequate security solutions that assist in achieving higher integrity.

This thesis aims to investigate the vulnerability of fingerprint modality to presentation attacks in unsupervised environments, then implement mechanisms to detect those attacks and avoid the misuse of the system. To achieve these objectives, the thesis is carried out in the following three phases.

In the first phase, the generic biometric system scheme is studied by analyzing the vulnerable points with special attention to the vulnerability to presentation attacks. The study reviews the literature in presentation attack and the corresponding solutions, i.e. presentation attack detection mechanisms, for six biometric modalities: fingerprint, face, iris, vascular, handwritten signature, and voice. Moreover, it provides a new taxonomy for presentation attack detection mechanisms. The proposed taxonomy helps to comprehend the issue of presentation attacks and how the literature tried to address it. The taxonomy represents a starting point to initialize new investigations that propose novel presentation attack detection mechanisms.

In the second phase, an evaluation methodology is developed from two sources: (1) the ISO/IEC 30107 standard, and (2) the Common Evaluation Methodology by the Common Criteria. The developed methodology characterizes two main aspects of the presentation attack

RESEARCH & INNOVATION
Marie Skłodowska-Curie actions

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675087

detection mechanism: (1) the resistance of the mechanism to presentation attacks, and (2) the corresponding threat of the studied attack. The first part is conducted by showing the mechanism's technical capabilities and how it influences the security and ease-of-use of the biometric system. The second part is done by performing a vulnerability assessment considering all the factors that affect the attack potential. Finally, a data collection is carried out, including 7128 fingerprint videos of bona fide and attack presentation. The data is collected using two sensing technologies, two presentation scenarios, and considering seven attack species. The database is used to develop dynamic presentation attack detection mechanisms that exploit the fingerprint spatio-temporal features.

In the final phase, a set of novel presentation attack detection mechanisms is developed exploiting the dynamic features caused by the natural fingerprint phenomena such as perspiration and elasticity. The evaluation results show an efficient capability to detect attacks where, in some configurations, the mechanisms are capable of eliminating some attack species and mitigating the rest of the species while keeping the user convenience at a high level.

References

[1] "Amsterdam airport's facial ID fooled by simple photo," *Biometric Technol. Today*, vol. 2020, no. 1, pp. 11–12, Jan. 2020.

[2] "Man boards plane disguised as old man then arrested on arrival in Canada | Daily Mail Online." [Online]. Available: https://www.dailymail.co.uk/news/article-1326885/Man-boards-plane-disguised-old-man-arrested-arrival-Canada.html. [Accessed: 02-Nov-2020].

[3] "How Bkav tricked iPhone X's Face ID with a mask - YouTube." [Online]. Available: https://www.youtube.com/watch?v=i4YQRLQVixM&feature=emb_logo. [Accessed: 02-Nov-2020].

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675087