CLR Labs

La Ciotat

Digital Identities, Digital Wallets, Remote Identity Proofing. A not yet well understood vulnerability : Biometric Data Injection Attack

What are we talking about?

Digital Identities, Digital Wallets, Remote Identity Proofing

Remote Identity proofing solutions and all KYC (Know Your Customer) applications have emerged in order to secure sensitive services performed remotely, mainly since the COVID-19 pandemic. These sensitive services are concerning different domains such as:

- Banking
- Finance
- Governments
- Health

As these services are more and more used from distance and this is why remote identity proofing solutions were developed to securely identify the customer usually based on their ID documents and biometrics, and secure their data.

The awareness about the risks faced by such sensitive services has led to the deployment of regulations, such the AML5 (Anti Money Laundering 5), eIDAS V1 and the upcoming eIDAS V2 in Europe, to encourage industrials and governments to apply the same level of security concerning identity verification of their customers/citizens during a face-to-face transaction.

But even with the usage of remote identity proofing solutions, the upsurge of remote services such as opening a bank account or making a loan awoke the greed of fraudsters. The nascent nature of these security services can't always provide the level of security that these sensitive services require. This is why we have already seen important frauds.

Moreover, many countries have expressed the will to deploy their digital version of their ID documents on digital wallets. This is particularly the case in the United States where many States have already deployed their mobile driving license, or in the European Union where a project to deploy a European Digital Identity Wallet (EUDI Wallet), common for all Member States, is underway.

These wallets are particularly a new boon for fraudsters or criminal organizations to carry out large-scale and high-quality identity fraud. Indeed, we have already seen an example of fraud using a mobile driver's license in the United States, in the State of Louisiana. [1]

[1] https://www.biometricupdate.com/202303/banks-hit-with-biometric-fraud-fake-mobile-drivers-licenses

Biometrics in remote identity proofing

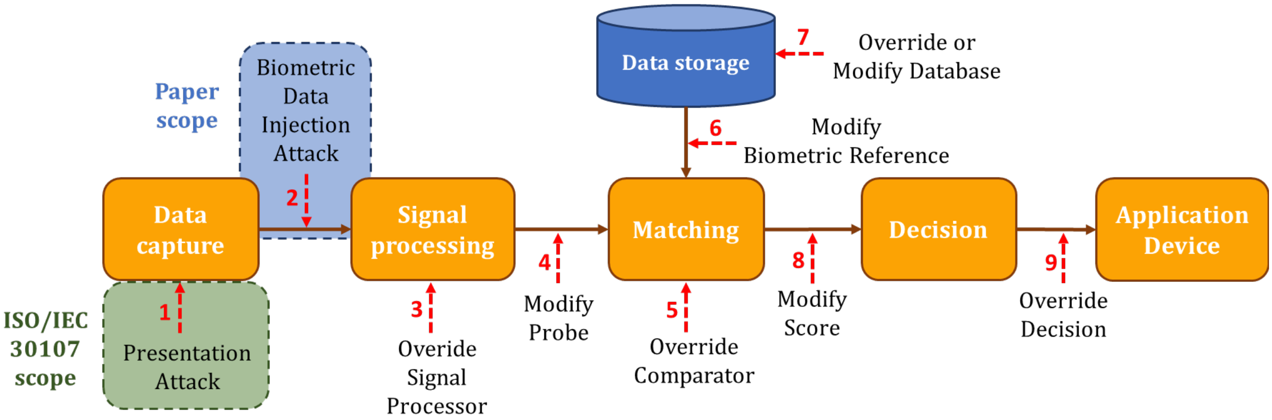
Remote identity proofing consists in verifying a user's identity at distance, based on its ID document, to get the ID information and biometrics, to check that its holder is the legitimate owner of the ID document. It is usually performed through three security verifications:

- The check of the authenticity of the ID document
- A face recognition between the photo on the ID document and the user's face
- The check of the authenticity of the person thanks to liveness detection

In most cases, these two phases are performed thanks to images (photos or videos): the user is filming its ID document and then its face. The remote identity proofing solution then performs all the security checks automatically, and some of them even add a human operator trained for fraud detection in the transactions. Note that solutions based on video offer greater data resources, and thus are more efficient to prevent fraud.

According to its definition, biometrics brings together all the computer techniques that make it possible to automatically recognize an individual based on their physical, biological or even behavioural characteristics. As all technologies, biometrics is vulnerable by default.

According to a study made by scientists of IBM in 2001 [2], 9 different attack paths exist on a biometric system (see the following diagram). The most famous attack is called presentation attack (classified as type 1 attack in the following diagram) and is focusing on the data capture system (i.e., the sensor). As presentation attacks do not require any knowledge about the targeted product from the attacker, this attack has captured the main interest from researchers, while other attacks were considered inherently prevented by their security-by-design.

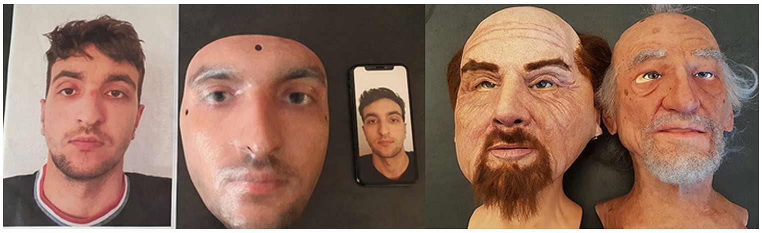


[2] https://ieeexplore.ieee.org/document/5386935

Liveness Detection (PAD) & ISO/IEC 30107

A presentation attack consists in presenting a falsified biometric trait to the biometric capture module. These attacks have attracted the attention of biometric experts and have even given birth to a specific international standard series called ISO/IEC 30107. Presentation attacks on biometric systems are made with artifacts, also called Presentation Attack Instrument (PAI). For face recognition, the PAI usually belongs to one of these categories:

- Face printed
- Face displayed on a screen
- Paper face mask
- 3D face mask



Because of this threat, the development of Presentation Attack Detection (PAD), also called Liveness Detection, has been a prior topic for the biometric community. The improvement of Artificial Intelligence (AI) and many years of research have given rise to the emergence of plenty of methodologies to detect presentation attacks.

These solutions allow to detect the presence of an artifact in front of the data capture system, and/or to identify a living characteristic from the user in order to ensure that it is not a fake representation of someone else.

ANSSI has noticed that the only usage of PAD systems was not sufficient to provide the requested level of security. Indeed, the Agency was the first protagonist to identify the risk of biometric data injection attack against such system. The fact that the device used to capture the ID document and the user's face was under the control of the attacker allows him to get an attack's surface more important that only presentation attacks.

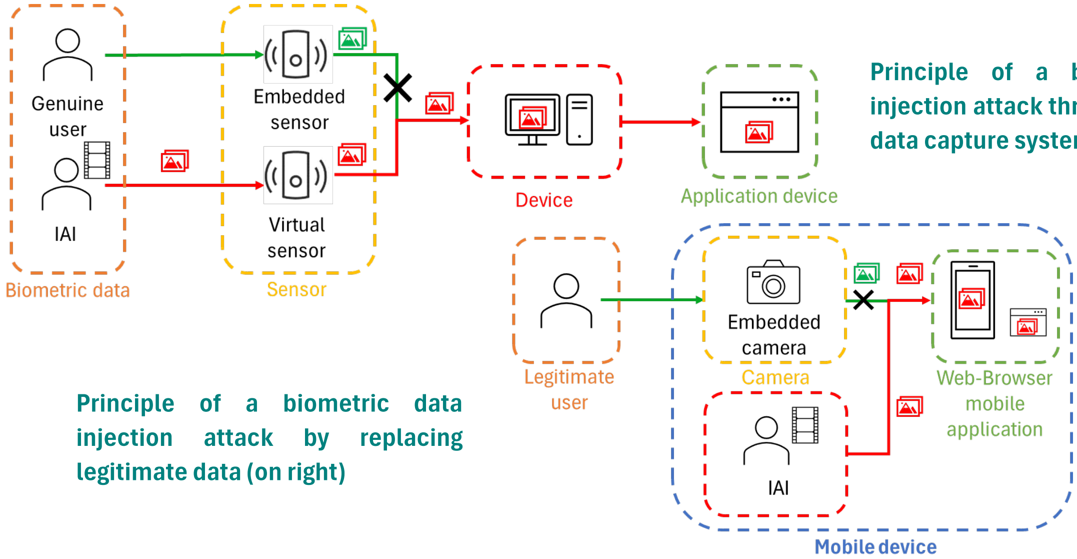
The Agency also noticed that the security level of the current biometric security components on the market were not sufficient to obtain a fully automatic remote identity verification solution. This is why the PVID certification scheme obliges remote identity proofing solution providers to have a human operator trained for fraud detection checking each transaction classified as an attack by the automatic system.

What is a Biometric Data Injection Attack?

But what is a biometric data injection attack, the new threat highlighted by ANSSI ?

Biometric data injection attack consists in the replacement of a biometric sample by an impostor. It exists two families of injection attack methods (i.e., the way to inject the malicious data in the system):

- Using a malicious data capture system (e.g., a virtual camera)
- Intercepting the legitimate biometric data and replace them by malicious data (e.g., through a hooking process)



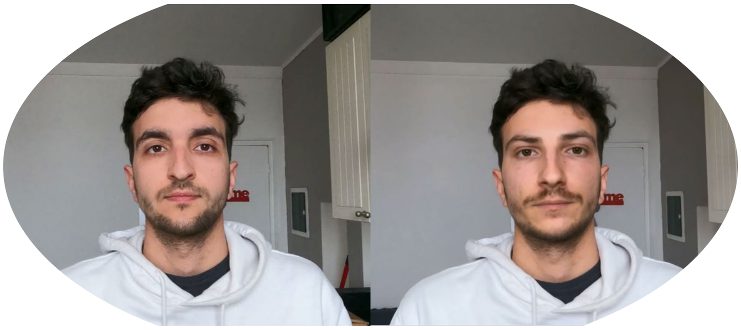
Principle of a biometric data injection attack through malicious data capture system (on left)

Principle of a biometric data injection attack by replacing legitimate data (on right)

The purpose of the attack is to inject a malicious biometric sample in order to get recognised by the biometric system as a specific victim thanks to one of these methods.

These methods can be performed by using plenty of different tools (non-exhaustive list), usually freely available on the web:

- Software virtual capture device
- Hardware malicious capture device
- Device emulator
- Hooking toolkit



ORIGINAL **DEEPFAKE**

The injection attack methods allow the attacker to inject malicious data, also called Injection Attack Instruments (IAI). The most known IAI is the deepfake video, where the face of the attacker is replaced by the one from the victim inside the video. The deepfakes are quite famous on the web and have already attracted the interest from researchers in order to detect them.

Biometric data injection attacks are not only deepfakes !

But injection attacks are not only deepfakes and most of the times researchers don't take into account the injection in the scenario. A French team of researchers have released the first research paper on injection attacks on face recognition system and have shown that even state-of-the-art liveness detection systems can be fooled with a simple selfie, but also with face videos, video montages, photo animations and deepfakes [3].

Injection attacks are possible because the data capture system is under the control of the attacker (in its smartphone or computer) and usually divided from the other parts of the biometric system which are present on the server. In most Operating Systems (OS), camera and microphones have a public access for developers, which means that the devices are easily targetable by attackers.

This is why, if injection attacks are getting more and more famous for face recognition, these attacks are also a threat for other biometrics like **iris recognition, voice recognition or even remote fingerprint recognition.**

This threat highlights the real need of certification scheme and standards in order to help the biometric market to improve its level of security against injection attacks and gain confidence from customers.

	FIDO Alliance	International Payment Schemes	ANSSI	LSTI-CLR Labs	Other Biometrics Confomity Evaluation Laboratories
	ISO/IEC 30107	ISO/IEC 30107	PVID referential	ISO/IEC 30107 and ETSI TS 119 461	ISO/IEC 30107
Presentation Attack Detection testing	✓	✓	✓	✓	✓
Injection Attack Detection testing	✗	✗	✓	✓	✗
Falsified ID document detection testing	✗	✗	✓	✗	✗
Certification	✓	✓	✓	✓	✗

[3] *https://www.iiis.org/CDs2023/CD2023Spring/papers/ZA474HC.pdf*

Europe leads this urgent topic

Europe has taken the lead on the subject. Indeed, some Member States have already set up their National Certification Scheme for remote identity proofing with a particular attention on testing the detection of injection attacks. Moreover, CEN CENELEC, a European standardisation organisation, is developing the first standard on biometric data injection attack detection.

Eventually, CLR Labs is proud to be the first laboratory in the world to provide security audit services and certification services (through the LSTI-CLR ISO/IEC 30107 certification scheme and through the LSTI-CLR ETSI TS 119 461 certification scheme) on biometric data injection attacks detection [4].

If injection attacks are a threat for the biometric component, this is also the case for the ID document component in a remote identity proofing solution. Indeed, an attacker could use the same injection attack methods to inject video of digitally falsified ID documents. Thus, the next challenge will be to find a legal framework to authorize independent laboratories to test the security of the ID document authenticity check components of remote identity verification solutions.

[4] *https://www.biometricupdate.com/202305/first-european-certificate-program-for-presentation-attack-detection*