Meeting Minutes[1]

Interview	*Conference call, 2021 June 3 (17:00 – 18:30 CET)*

Remote Identity Proofing Practices: Attack Scenarios and Countermeasures

Location:	Conference call
Attendees:	*ENISA* Viktor PAGGIO *PwC* Piero DE SIMONE Federica MAGNA Jody MAGANUCO Fabio GALASSI Enrico Manuel DE WAURE *FaceTec* Alberto LIMA Jay MEIER Kevin Alan TUSSY

Summary of the interview

Premise and Topics

The interview was focused on the understandings of the ENISA study, *"Remote identity proofing Practices: Attack Scenarios"*. The goal was to collect FaceTec's experience and perspective on:

- methods of remote identification against government-issued ID documents and on government servers with access to the source 2D ID photos;
- attacks on these methods, from changes of physical appearance to deep-fakes;
- practical countermeasures using liveness detection and anti-spoofing AI.

The content of the interview, including this document, is confidential and will not be disclosed to third parties without FaceTec's authorization.

[1] *For clarity, the items discussed are not presented chronologically but grouped by theme.*

Main points

Please find below a high-level summary of the main topics discussed:

- FaceTec is a world-leading provider of 3D Face Liveness & Matching software.
- FaceTec is not an identity proofing platform provider for end users, but supplies its 3D Face Liveness & Matching technology to its customers and partners, intermediaries, and 3rd party platform providers, including the Department of Homeland Security, Canadian Parliament, and other high-profile institutions.
- FaceTec technology uses 3D FaceScans and derived 3D FaceMaps, which are superior in matching and liveness confidence over classic 2D photos/videos. They enable stronger Liveness Checks and much more accurate matching, as well as providing additional security because 3D FaceMaps can't be phished, and are not stored on sites like Facebook, Google or LinkedIn, unlike ubiquitous 2D photos.
- FaceTec's 3D capture of the user collects both liveness and matching data concurrently while the camera is zooming in on the face. FaceTec AI measures depth by observing perspective distortion, and uses those metrics to reverse-engineer the 3D FaceMap. Typically variations in pose, capture distance and lighting hurt matching performance and accuracy in 2D systems, but they actually provide more information to make FaceTec 3D AI stronger.
- In particular, FaceTec states that validation through 3D FaceMaps utilizes more than 100-times more data than classic 2D photos, which necessarily increases match confidence significantly.
- FaceTec's technology works, first by ensuring camera feed integrity, and second, by acquiring the highest quality video data possible from the device at the maximum camera resolution and frame-rate. The video frames are then processed on the device itself, producing a small file containing 3D FaceScan data. This 3D FaceScan file (~350kb) is then encrypted and sent to the server for analysis. Once liveness is confirmed on the server, the one-time use liveness data is deleted, leaving only 3D matching data, called a 3D FaceMap, which cannot be resubmitted or reused, eliminating "Honeypot" risk. All remaining video data is deleted from the device itself, making the process secure as well as inclusive for clients on low bandwidth/data plans.
- FaceTec allows both 3D-to-3D FaceMap matching (for example, when implemented to authenticate returning users) and 3D FaceMap-to-2D image matching (for example, when matching 3D face data captured from a live user against a photo obtained from an ID document, passport chip, or government ID photo database).
- The False Acceptance Rate (FAR) for 3D-to-3D FaceMap matching is accurate to 1/12.8 million @ <1% FRR. 3D FaceMap-to-2D portrait photo accuracy is up to 1-in-950,000 @ 1% FRR. 3D FaceMap-to-photo ID is accurate up to 1-in-500,000/1% FRR, and

a 3D FaceMap -to-profile photo match is accurate at up to 1-in-100,000/1% FRR.

- FaceTec systems require a minimum camera resolution of .3 megapixel, significantly lower than typical 2D systems, and does not need to utilize data from unrelated phone sensors (accelerometer, gyroscopes, microphone, etc.), providing extraordinary liveness and matching accuracy, while enabling backward compatibility for lower economic demographics and geographies.
- The data is processed on the server by neural network models that have been trained by over a half-a-million volunteers from 180 countries all over the world for greater precision, and to avoid any age, gender, or skin-tone bias.
- FaceTec provides passive liveness via involuntary human signal measured by deep neural networks, which validate up to 60 human traits. All of the algorithms agree for a "Liveness Confirmed" decision to be rendered. Examples include, reflections in the user's eyes, reactions in the user's eye focus, and much more.
- FaceTec does not employ unsupervised learning algorithms leveraging untagged data; all data is ground-truthed by trained human evaluators.
- FaceTec contributes to ongoing education using the five-level attack threat vector categorization from www.liveness.com:
    - Level 1 - digital videos/photos, paper photos.
    - Level 2 - cheap (<$300) 3D masks.
    - Level 3 - high quality (Hollywood-level) 3D masks.
    - Level 4 - tampering with the biometric data in the payload.
    - Level 5 - virtual camera attacks and video injection camera sensor bypasses.
- FaceTec has offered a $100,000 spoof bounty program for the last 18 months. Two bounties have been paid during the first six months, both for Level 1 attacks. There have been no successful attacks on the Bounty Program in the last year. To date, there have been more than 80,000 attacks to the bounty program, which have revealed the categories of attacks used most frequently have been Level 1 and Level 5. FaceTec believes no system can be 100% "spoof-proof," but FaceTec systems have proven to be extremely robust.
- FaceTec believes that the most difficult to defend attacks are video attacks utilizing video injection and virtual cameras, and lower resolution cameras pointed at higher resolution screens against using 2D face matching as the biometric modality, but considers deep-fake attacks (controllable real-time 3D puppets) the #1 threat to be concerned about in the future.
- FaceTec highlighted the danger of deep-fake attacks in conjunction with methods aimed at bypassing the device camera (e.g. video injection, running the app in an emulator, etc.). These attacks can

bypass most presentation attack detection (PAD) methods that look for skew, glare or other "dead" giveaways and hope to catch a hint they're dealing with pre-captured biometric data being replayed on a monitor, and not a live video feed.

- Regarding countermeasures, FaceTec believes 3D Liveness and matching combined with camera feed security checks are by far the strongest defense against modern threats, like presentation attacks, deep-fake puppets and camera bypasses.
- As an example, FaceTec pointed out an attack that targeted a Chinese government facial verification online ID system, which utilized deepfake puppets controlled in real time using a mouse/keyboard to trick the active liveness detection requiring the user to turn their head or move their eyes.
- FaceTec participates in and contributes to major standards and specification development, including AAMVA, NIST, US DHS, ISO and ENISA requests.
- FaceTec pointed out it is very important for the next generation of tools/frameworks to understand the importance of Level 5 attacks. ISO/IEC 30107-3, for example, did not consider these attacks since they were not well known at the time it was drafted (2017), and consequently testing labs had not taken them into consideration.

Resources shared:

NIST 800-63: Request For Information-Reply:
https://facetec.com/NIST_800-63_RFI_FaceTec_Reply.pdf

FaceTec's Remote Verification Architecture for Identity Verifiers:
https://www.facetec.com/Legal_Identity_Issuers_The_New_Verifiers_FaceTec.pdf

$100,000 Spoof Bounty Program:
https://spoofbounty.com/

FaceTec 3D Face Matching Whitepaper:
https://www.facetec.com/FaceTec_3D_Face_Matching_Whitepaper.pdf

FaceTec's Security Best Practices:
https://dev.facetec.com/security-best-practices

Large scale deepfake's attack in China:
https://www.biometricupdate.com/202103/hackers-spoofed-biometric-authentication-videos-to-steal-millions-in-china