NIST FRVT-PAD Commentary

April 26, 2022

Introduction - FaceTec, Inc. (a Delaware Corp.) is the leading global provider of 3D Liveness and 3D Face Matching software for remote identity verification. U.S. federal and state governments, numerous foreign governments, and hundreds of commercial entities use FaceTec software to authenticate, verify, and reverify customers and users. Examples include the Colorado Mobile Driver License (mDL), the Utah mDL, the coming Virginia mDL, the U.S. Department of Homeland Security Mobile Trusted Traveler program, the Canadian Parliament Remote Voting Verification System, and the Digital Dubai project.

Over 550 million people on six continents have proven their Liveness remotely with FaceTec software using smart devices and webcams. FaceTec's user interface is intuitive and accessible, requiring only a 2-3 second "video selfie". FaceTec's data collection SDKs are designed to work effectively on low-cost devices with low camera resolutions, and have no observable age, gender, or skin tone bias when tested with billions of face match pairs.

FaceTec provides software that runs inside its customers' firewalls, and FaceTec never receives *any* of the end-users' PII or biometric data. In 2022, FaceTec will enable over 600 million distinct 3D Liveness checks globally.

ENISA recognized FaceTec's contributions to its 2022 Remote ID Proofing Report - which states, "*During the identity verification session, the "liveness" of the applicant's facial image is verified. Presentation attack detection (PAD) and face matching controls are used. The technology addresses various presentation attacks (e.g., still or video imagery submission, usage of high-quality masks, a replay of a previous video capture). "*

To ensure real-world security, FaceTec operates the world's first-and-only persistent $200,000 Spoof Bounty Program, incentivizing hackers to attempt to beat its biometric security platform. It has successfully defended over 110,000 bounty program attacks over the last 28 months, providing unmatched insight into the modern methods required to rebuff the most sophisticated new threats to remote access management, identity proofing, and biometric verification systems.

We are grateful for the opportunity to contribute our insights to NIST regarding face Liveness in the upcoming FRVT-PAD project, and the following is our general commentary and recommendations regarding the announced framework for FRVT-PAD.

Thank you.

Jumio EX1064 Page 1
Jumio v. FaceTec IPR2025-00108

Our reliance on remote access to our private digital information creates a treasure trove of data that cybercriminals can now steal by attacking inadequate user "identity" verification systems, including the naive belief that a code, device, or token proves that the correct person is using it. We must add true human verification and authentication to stop the waves of digital identity theft and data breaches that are crashing daily. Biometrics, and specifically face biometrics, are being used more than ever before, but most lack sufficient Liveness capabilities, and users are again forced to rely on inadequate identity verification systems. Bad actors exploit the vulnerabilities in poorly designed biometric liveness systems just as those that rely on "something you know." Today, biometric spoof attacks, presentation attacks, video injection attacks, deep fake puppets, etc., easily render most biometric verification and authentication systems ineffective.

To see sobering examples of the scalable spoof and bypass methods that have defeated some well-known biometrics vendors, visit this channel: YouTube.com

We commend the National Institute of Standards & Technology for proposing and addressing the need for biometrics and, more specifically, face biometrics in Special Publication (SP) 800-63-4. FaceTec submitted extensive commentary and recommendations to respond to that Request for Information, which can be viewed here. We also commend NIST for officially proposing the establishment of a NIST-controlled and managed testbed (FRVT-PAD) for face biometric liveness Presentation Attack Detection (PAD) systems.

However, we are concerned that the current framework for FRVT-PAD is not comprehensive enough to actually defend against modern spoof and bypass attacks. Not testing to the level of sophistication that attackers already use will serve no purpose except to build over-confidence in systems that complete the FRVT-PAD test, which will likely be leaving significant vulnerabilities unaddressed. At the heart of the matter is FRVT-PAD's narrow focus on pre-collected face images and video, and the reliance on nothing more than ISO/IEC 30107, which fails to include many modern attack vectors. Notably, that standard was first published in 2016, when relatively little was known about biometric liveness and related attack defenses. Moreover, ISO/IEC 30107-4 was published in 2020, almost two years ago, and was not a particularly comprehensive nor robust evolution from 30107-3 which was published in 2017. Modern biometric liveness attack vectors have evolved substantially and beyond the scope of 30107, rendering this standard largely ineffective against many current related attacks.

We fear FRVT-PAD will only test biometric PAD systems to a standard that has been outdated for years, and success in the FRVT-PAD test will be irrelevant to today's primary, digital, and scalable attack vectors. NIST will come to realize, as FaceTec has, that 2D image/video evidence of Liveness is insufficient to block these new attacks and that new ideas must be considered. Therefore, we strongly encourage NIST to expand the scope of the test to address modern attack vectors and to use live-captured image data in each test so that unique user interfaces may be tested. For example, enrollment into Apple's Face ID requires the user to roll their head in a circular motion, and FaceTec's user interface requires the user to move closer to the camera, both of these implementations of Liveness heavily leverage 3D data from the user's face. But unless NIST is willing to collect specific

data and create attack species for these data collection requirements, two of the most used Face Authentication systems will be unable to participate in the FRVT-PAD.

FRVT-PAD proposes to test for photo and video presentation attacks only. However, modern biometric system attack vectors include various forms of data substitution, including deepfake video injections. **It is imperative to understand that such attacks are not defendable by PAD alone**.

Please note that SP800-63-3 includes the following reference to biometric spoof and bypass attacks; ***"While presentation attack detection (PAD) technologies (e.g., liveness detection) can mitigate the risk of these types of attacks, additional trust in the sensor or biometric processing is required to ensure that PAD is operating in accordance with the needs of the CSP and the subscriber…. An authenticated protected channel between sensor (or an endpoint containing a sensor that resists sensor replacement) and verifier SHALL be established and the sensor or endpoint SHALL be authenticated prior to capturing the biometric sample from the claimant."***

It is critical to establish the integrity of the biometric capture sensor (the camera), along with any related data flow, prior to and during the biometric capture of the data itself which cannot be trusted.

Liveness.com defines Level 5 Attacks as those that: **"Take over the camera feed and inject previously captured video frames or a deepfake puppet that results in the FaceTec AI responding with "Liveness Success."**

In order to successfully defend against camera bypass attacks, there must be software running on the user's device, and significant checks must be done to ensure that the image capture application is receiving a real-time video feed, is not running on an emulator, having had video injected, or is accepting a deepfake puppet that is synthesized in real-time. **www.unite.ai/deepfakes-can-effectively-fool-many-major-facial-liveness-apis/**

Therefore, failing to test for real-time data collection by the camera and related data flows could effectively enable the most scalable biometric system attacks to be successful against FRVT-PAD-tested vendors. In effect, biometric liveness systems are symbiotic with cybersecurity systems and should be tested as such. We strongly encourage NIST to broaden the FRVT-PAD test to include sufficiently validating the sensor's integrity, and the integrity of all related components and the data flow.

It is also imperative to the security of Liveness detection systems **not** to return any information about why an artifact was rejected **or** how close that artifact came to being accepted. With "zero trust" in mind, no one outside the developers of the algorithm should know how it works, and developers should not provide a Liveness rating, Risk Score, or PAD Score. The result should be binary for every session: Either "Liveness Proven" or "Liveness Not Proven," then no user, customer, tester, or anyone else will be able to hill-climb the AI. We ask you to carefully consider the following before testing biometric liveness:

Presentation Attack & Camera Bypass Threat Vectors

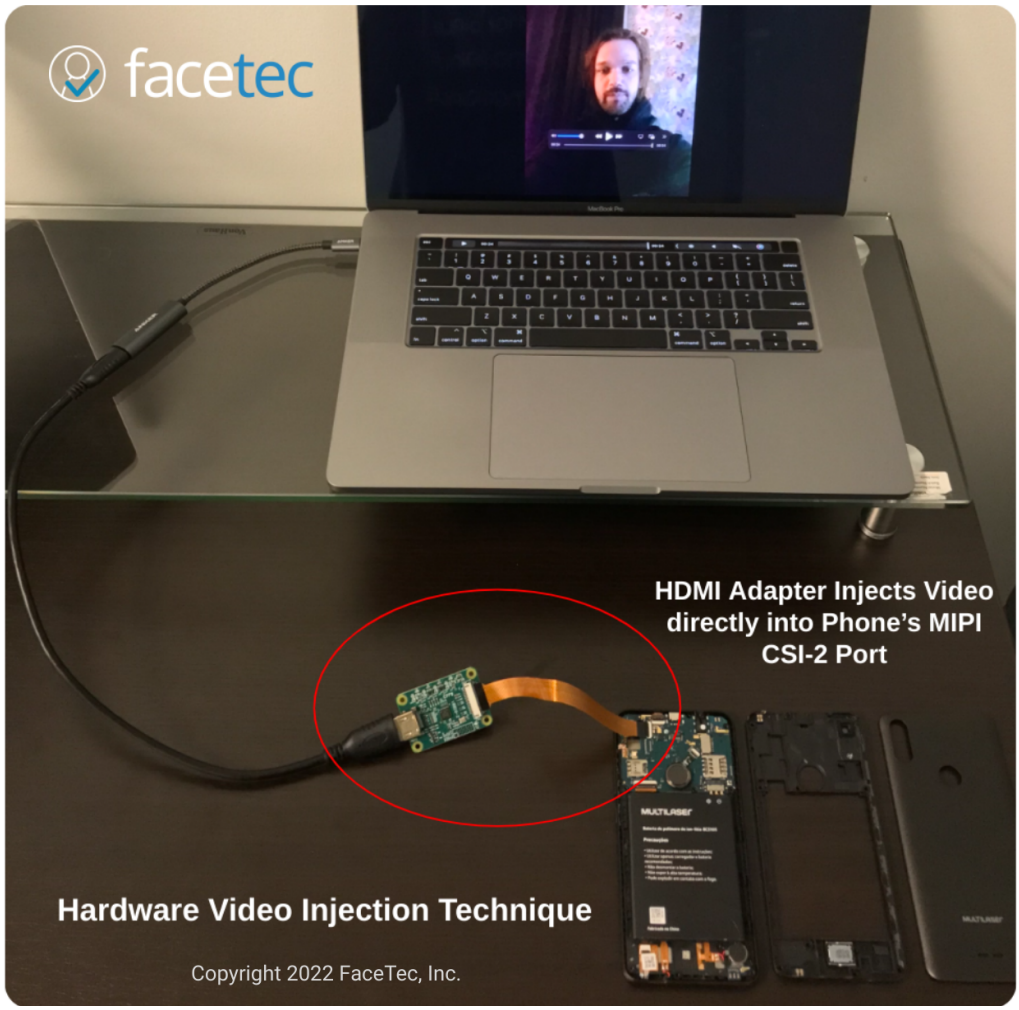
These topics are discussed further in FaceTec's **Liveness_Security_Report_Q2_2022**

ISO 30107-3 did not contemplate deepfake videos, puppets, or camera bypasses, and in 2022 any Liveness testing that *only* considers threats outlined in ISO-30107 is no longer adequate to ensure any level of Liveness security.

Artifact Level	Description	Example
Level 1 (A) (Spoof Bounty Avail)	Hi-res paper & digital photos, hi-def challenge/response videos and paper masks. Beware: iBeta Lab Tests DO NOT include digital deepfake puppets, but FaceTec's Spoof Bounty DOES include deepfake puppets.	
Level 2 (B) (Spoof Bounty Avail)	Commercially available lifelike dolls, and human-worn resin, latex & silicone 3D masks under $300 in price.	
Level 3 (C) (Spoof Bounty Avail)	Custom-made ultra-realistic 3D masks, wax heads, etc., up to $3,000 in creation cost. *No Lab Testing Avail	

Bypass Level	Description	Example
Level 4 (Spoof Bounty Avail)	Decrypt & edit the contents of a 3D FaceMap to contain synthetic data not collected from the session, have the Server process and respond with Liveness Success.	
Level 5 (Spoof Bounty Avail)	Successfully take over the camera feed & inject previously captured frames that result in the Server responding with Liveness Success.	

This video injection method was used **in a massive fraud against the Chinese Govt**.



Recommendation: FaceTec believes the best way to learn which threat vectors Liveness detection must thwart is to stand up a Spoof & Bypass Bounty Program. FaceTec encourages NIST to change its FRVT-PAD from an internal test to an external one, and allow the most knowledgeable white-hat hackers in the world to attack the Liveness systems that vendors provide to NIST. This approach has been very successful with the recent "Hack DHS" Program Bug Bounty Program.

- **Explicit Threats Against Today's Remote Identity Proofing Processes**
    - **Presentation Attacks** performed by a bad actor showing a mask, mannequin, video, digital, or paper photo (synthetic artifact) in place of a real, 3D human's face. These attacks can affect initial Identity Verification *and* future Authentication sessions. Presentation Attacks are among the easiest to attempt and are pervasive, with an estimated 2% of all current Remote ID Verification attempts being PAD attacks. While often simple to procure and perform, Presentation Attacks can be very difficult to detect and are considered Levels 1-3 on the Liveness.com Attack Vector Scale.
    - **Biometric Template Tampering Attacks** are performed on the device. The subject's biometric data is replaced within the legitimate user data with imposter data and then matched against trusted data and man-in-the-middle attacks. These attacks are considered Level 4 on the Liveness.com Attack Vector Scale.
    - **Camera Bypass Attacks** include processes whereby the bad actor bypasses the camera hardware and injects previously collected data into the video feed. Common Bypass techniques include using virtual camera software (e.g., ManyCam) or leveraging vulnerabilities in WebRTC by setting injection points or running the application on an emulator. These attacks are considered Level 5 on the Liveness.com Attack Vector Scale.
    - **"Imposter" Attacks** are perpetrated by presenting a live human to the camera who looks similar to the legitimate user. These attacks are more often successful against 2D or otherwise weak face matching algorithms incapable of compensating for image capture perspective distortions. In addition, 2D "Selfie-to-ID Card" systems are particularly vulnerable to perspective distortions resulting in lower match confidence.
    - **In-Device Authentication Spoof Risk** - Remote Identity Proofing and Authentication systems relying on biometric matching on a mobile device (like Apple and FIDO) are vulnerable to imposter attacks. First, the enrolled biometric data on the device is anonymous and cannot be bound to a subscriber account. Second, the enrolled data cannot be moved from the device to a server, limiting match data size to accommodate fixed and limited in-device processing capability, impacting potential accuracy. Further, in-device biometric processors do not provide any opportunity to scan for duplicate or fraudulent identity profiles (i.e., "de-dup") within an identity profile database. As a result, in-device biometric sensors are particularly vulnerable to Level 1-5 attacks on the Liveness.com Attack Vector Scale.

- **Liveness Methods in Use by Identity Proofing and Technology Providers**

  - **Active Liveness Detection** commands the user to perform a movement successfully, or action like blinking, smiling, tilting the head, and track-following a bouncing image on the device screen. Defeated by Deepfake Puppets or masks.
  - **Passive Liveness** relies on involuntary user cues like pupil dilation, reducing user friction and session abandonment. Additionally, passive Liveness can be undisclosed, randomizing attack vector approaches. Alone, it can determine if captured image data is first-generation and not a replica presentation, eliminating Levels 4-5 Attacks.
  - **Device & Server-Side Liveness** - Significantly higher Liveness and biometric match confidence can be gained if device camera data is captured securely with a verified camera feed. For example, the image data is verified to be captured by a device SDK in real-time. Under these circumstances, both Liveness and Match confidence can be determined concurrently from the same data, mitigating several vulnerabilities.
  - **Multimodal Liveness** allows the user to choose between liveness check modalities to increase user uptake and increase the number of devices supported. This often requires the user to “jump through hoops'' of numerous Active Liveness tests and increases friction. But when one Liveness check is weaker than the others, the fraudsters will simply attack the weakest one.
  - **Liveness & 3D Depth Data Dependence** - A human must be 3D to be alive, while a mask-style artifact may be 3D without being alive. Thus, while 3D face depth measurements alone do not prove the subject is a live human, observing 2-dimensionality proves the subject is not alive. Furthermore, regardless of camera resolution, 3-dimensionality provides substantially more usable and consistent data than 2D, dramatically increasing accuracy. Therefore, 3D depth detection is a critical component of more robust Liveness Detection, and in general, deleting used Liveness data is an effective means of mitigating Honeypot risk.

    1. Specialized In-Device 3D Camera Hardware (i.e., Apple's Face ID) can collect 3D Face Data almost instantaneously by projecting invisible dots on the face and analyzing derived depth data. However, it requires special hardware.

    2. FaceTec’s 3D Face Data Collection Software utilizes video frame data captured from the X & Y axes from numerous 2D video frames over a few seconds and processes observed changes in the facial appearance to "reverse-engineer" the 3D Face. In addition, 3D Face Liveness software systems can securely deliver interdependent, concurrent Liveness and face

data to a server for matching 1:1 to the trusted user data and (1:N) for de-duplication and other anti-fraud tactics.

- **Relevant Standards & Testing/Certification Programs**

  - ENISA Remote ID Proofing Report - Published: March 2021 - "*1. During the identity verification session, the "liveness" of the applicant's facial image is verified. Presentation attack detection (PAD) and face matching controls are used. The technology addresses various presentation attacks (e.g., still or video imagery submission, usage of high-quality masks, a replay of a previous video capture). The system is continually monitored and reacts to evolving threats. The face matching algorithm uses the latest advances in deep neural networks to deliver matching performance with the highest level of assurance. It is optimized for 'selfies' taken on smartphones and PCs in a huge variety of lighting conditions, poses, and facial features."*
  - *ETSI "Survey of technologies and regulatory requirements for identity proofing"* Published: March 2021 - *"...the applicant to take and send a mobile phone video or photo with other liveness checks; compare the applicant's submitted photo to the photos on the passport identity evidence or the photo on file in the government's passport or license database;."*
  - Liveness.com - Published: September 2020 - Threat Vector Scale: PAD Levels 1-3, Level 4 = Payload Tampering Prevention & Level 5 = Camera Feed Bypass Prevention
  - ISO 30107-3 - Published: 2017- Purely Presentation Attack Detection Levels 1-3, no cybersecurity aspects or bypasses addressed.
  - US Presidential Memorandum M-19-17 - *"DHS is responsible for the following actions: 2. Lead research and development (R&D) coordination with the interagency, private sector, and international partner stakeholders to identify ICAM mission needs with related technology capability gaps, including in particular those that cannot be solved with currently fielded technologies and that may require additional R&D investment to reach operational deployment maturity...."*