EXHIBIT B

https://web.archive.org/web/20241004043911/https://www.praetorian.com/wp-content/uploads/2024/06/Praetorian-DataSheet-Application-Penetration-Testing-new.pdf

praetorian

DATA SHEET

Application Penetration Testing

KEY BENEFITS

Assess the software technology stack, from the service mesh and managed services to proprietary application logic

Identify security risks associated with design, implementation, and configuration

Receive solutions to mitigate identified vulnerabilities

YOUR CHALLENGE

Your organization's applications rely on cloud-first technology stacks. That means the data and secrets you need to protect could be vulnerable to the full range of software- and cloud-based attacks that adversaries are continually expanding. You need assurance that your cybersecurity strategy is comprehensive, that your data and that of your clients is as secure as possible, and that your applications meet any applicable industry regulatory requirements.

OUR SOLUTION: CAPABILITIES OVERVIEW

Praetorian's Application Penetration Testing engagements provide clients with a timely, tailored, and thorough assessment of their product's cybersecurity from an adversarial perspective. Our assessments include a comprehensive analysis of the building blocks that make up modern applications, including the service mesh, managed services, and application-layer logic. We conduct assessments in one of the following two ways, depending on the client's needs:

- **Framework-based**

  What it does: benchmarks your application against industry standards such as OWASP ASVS or MASVS.

- **Goal-based**

  What it does: pursues attack paths that target specific critical assets based on a collaboratively-constructed custom threat model.

The application's deployment characteristics (and threat model, if applicable) determine whether we focus on externally facing attack surfaces or the security of private APIs, container breakout scenarios, and other secondary attack surfaces.

Using a combination of manual and automated techniques, we can identify vulnerabilities ranging from classical web application vulnerabilities on the OWASP Top 10 to complex attack paths that chain together multiple weaknesses. Manual techniques, such as code review, log analysis, and analyzing memory in a debugger provide depth of coverage. They also give us the right opportunities to emulate attackers in order to find subtle vulnerabilities. Automated techniques, such as fuzzers and custom enumeration scripts, provide breadth of coverage and ensure we are finding as much as possible.

Once we have identified the material risks in the application, Praetorian collaborates with your team to develop a pragmatic, actionable remediation plan. This is always a union of technical and business considerations that will meet the client's security needs without derailing the product roadmap.

SERVICES COMPARISON

	Foundational Application Penetration Test	Risk-Informed Security Assessment
TESTING REQUIREMENTS		
Authentication Credentials	✓	✓
Source Code Access	optional	✓
Design Documentation Access	optional	✓
Security & Engineering Interviews		✓
FEATURE COMPARISON		
DAST & Vulnerability Scanning	✓	✓
OWASP Top 10 Coverage	✓	✓
Business Logic testing	✓	✓
Code Assisted Testing	optional	✓
SAST & Manual Code Review		✓
Threat Modeling		✓
DELIVERABLES		
PDF Report	✓	✓
CSV/Excel Vulnerability Export	✓	✓
Engagement Summary Letter	✓	✓
Security Benchmark Comparison	✓	✓
Threat Model Diagram(s)		✓
Abuse and Test Case Matrices		✓
Strategic Recommendations		✓

WHY PRAETORIAN

Praetorian's clients gain maximum benefit from our decade of experience and deep technical expertise in application penetration testing. Our team is equally adept with cloud-first applications and on-premises deployments, and can assess server-side, desktop, and mobile applications. Praetorian's engineers bring a creative, adversarial mindset to every engagement.

We pair that expertise with a focus on the client experience, tailoring each engagement to the client's business needs in order to provide actionable findings. You can rely on us to ask deep questions, work closely with your teams, and provide direct, clear feedback on what we find. Our team keeps your bigger picture in mind so we can help your company understand both the ground truth about your security program and its implications for your company's future.

WHO NEEDS THIS SERVICE

- **Organizations** wanting to analyze risk to make security a central part of their business proposition. These engagements are highly productive, as Praetorian can help identify the best-in-class security controls needed to reach specific goals, then retest to verify those controls are implemented properly.
- **Security teams** requiring independent, trusted security reviews of their products to meet customer- or regulatory-driven requirements.

DELIVERABLES

Executive Summary

Concise explanation of engagement goals, significant findings, business impacts, and strategic recommendations

→ Upon request, a letter of attestation

Engagement Outbrief Presentation

Similar to the executive summary, presented to the audience of your choosing

Technical Findings Report

Detailed description of issues and the methodology used to identify them, as well as an impact assessment for each

Praetorian Security, Inc.
6001 W Parmer Ln, Ste 370, PMB 2923
Austin, TX 78727 USA
info@praetorian.com

To learn more about Praetorian, visit: www.praetorian.com

ABOUT PRAETORIAN

Praetorian is an offensive security engineering company whose mission is to make the digital world safer and more secure. Through expertise and engineering, Praetorian helps today's leading organizations solve complex cybersecurity problems across critical enterprise assets and product portfolios.

https://web.archive.org/web/20220126173822/https://facetec.com/ENISA_RFI_Remote_ID_Attacks_FaceTec_Countermeasures.pdf

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.*

Jumio EX1087 Page 7
Jumio v. FaceTec IPR2025-00107

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

https://web.archive.org/web/20220708092851/https://facetec.com/FaceTec_NIST_FRVT-PAD_Comments.pdf

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.

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

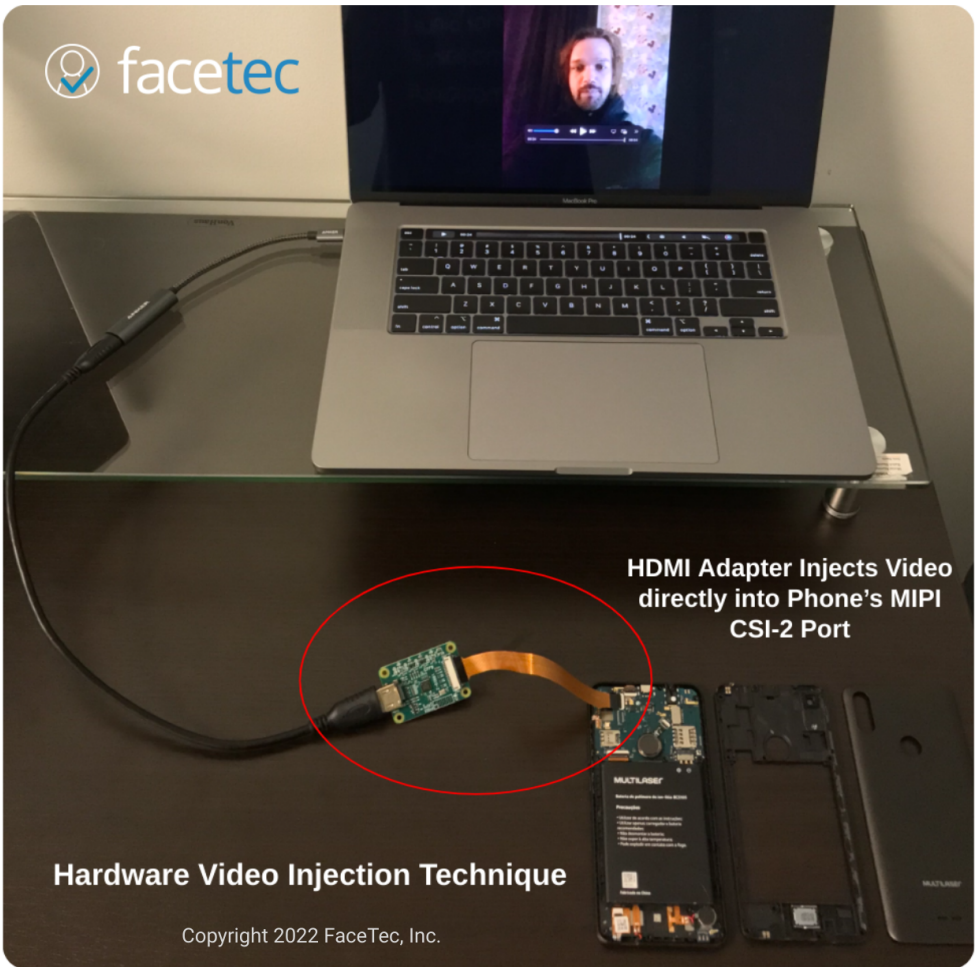
These topics are discussed further in FaceTec's **Liveness_Security_Report_Q2_2022**

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...."*

https://web.archive.org/web/20230206030934/https://www.facetec.com/FaceTec_Liveness_Security_Report_Q2_2022.pdf

LIVENESS DETECTION SECURITY REPORT - Q2 2022

Access to online accounts primarily relies on Knowledge-Based Authenticators (KBA), such as passwords, PINs, emails, and phone numbers, to attempt to prove that the person requesting access is actually the correct user. However, with passwords breached and PII data leaked, KBA is becoming ineffective since it cannot provide a high degree of confidence that the correct physical user is actually present. Compromised KBA systems open doors for fraudsters, and continuing to use KBA is exactly what bad actors want. Today, victims of social engineering attacks, such as phishing, where fraudsters capture an individual's credentials and gain their trust to commit fraud, can only make one simple mistake for their digital lives to be taken over by an attacker.

Biometric matching is now replacing legacy KBA, serving as a strong verifier of the user's unique biology that can provide the right to access their specific account. However, it is not enough to verify biometric data matches, as that data can be collected, stored, and then reused in most cases. To prevent such abuse, the new biometric data sample must be confirmed to be a first-generation capture from a living, 3D user just moments before it is matched to trusted enrolled data.

FaceTec Liveness Security Achievements:

- $200,000 Spoof Bounty program in place for 2.5 years.
- Performing over 600,000,000 Liveness Checks annually with no reports of fraud.
- iBeta Level 1&2 PAD Certifications for over three years.
- Over 85 FaceTec Partners have tested and chosen to resell FaceTec Liveness security.

The confirmation that the user is a real, 3D, physical human is called "Liveness Detection." FaceTec is a pioneer in Liveness Detection (more specifically, 3D Liveness Detection) and, for the past eight years, has developed and deployed a user-friendly, yet exceptionally secure Liveness AI, delivering the most accurate 3D face matching for smartphones and web browsers available.

Using only 2D face matching isn't sufficient for remote identity verification. Liveness Detection is required, but not all Liveness can actually stop attackers. In fact, most cannot and have become a mere nuisance for fraudsters to work around. Relying on outdated standards and testing criteria, such as iBeta/ISO 30107-3, creates a false sense of security. Attack vectors have evolved so quickly that standards released in 2017 were rendered obsolete within just a few years. ISO 30107-3 and iBeta testing does not include new attack vectors such as digital deepfakes or video injection, two of the most scalable types of attack vectors with the potential to cause widespread damage.

To ensure real-world security in the face of emerging attack vectors, FaceTec's $200,000 Spoof Bounty Program has opened up the AI to attackers, inviting them to use their expertise to bypass FaceTec's Liveness Detection and providing up-to-the-minute proof that FaceTec's AI can defend against all known Level 1-5 Attacks. No other vendor in the world has Liveness AI capable of supporting such a transparent and dynamic program.

© 2022 FaceTec, Inc. All Rights Reserved. Visit www.FaceTec.com for additional information.

Spoof Bounty Program Details:

Threat	Description	Example	Bounty
Level 1	Hi-res paper & digital photos, hi-def videos exhibiting challenge/response and human-worn paper masks.		$30,000
Level 2	Commercially available lifelike dolls, and resin, latex & silicone 3D masks up to USD$300 in price.		$30,000
Level 3	Custom-made ultra-realistic 3D masks, sculptures, wax heads, etc. up to USD$3,000 in creation costs.		$40,000
Level 4	Successfully decrypt & edit the contents of a 3D FaceScan to contain synthetic data not collected from the session, have the Server SDK process it and respond with Liveness Success.	3D FaceScan Tampering	$60,000
Level 5	Successfully take over the camera feed & inject previously captured frames that result in the Server SDK responding with Liveness Success.	ManyCam Vcam vlc2Cam FakeWebcam	$40,000

More info at www.SpoofBounty.com & dev.facetec.com/spoof-bounty-program

The number of attacks on the Bounty Program broken out by Attack Level:

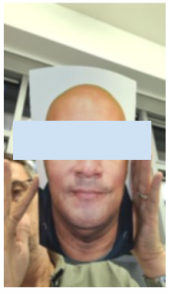
Attack Level	Current Bounty	Attacks	Bounties Paid	Attack Notes
Level 1	$30,000	>88,000	2*	PAD Paper & Digital Photos, Videos, 2D Masks
Level 2	$30,000	>2,000	-	3D Masks, Under $300
Level 3	$40,000	>1,000	-	Hollywood Masks, Madame Tussauds Wax, etc.
Level 4	$60,000	~5,000*	-	* ~5,000 est., but we cannot determine offline attempts to crack an already-encrypted 3D FaceScan
Level 5	$40,000	>14,000	-	Virtual-Cam & Video Injection attacks, as well as where attackers set breakpoints and fail to pass Liveness

* Two Level 1 PAD bounties were claimed in mid-2020. These attacks both used high quality video with slight blurs applied. The bounties were paid and the vulnerability was patched. There are no known vulnerabilities at this time.

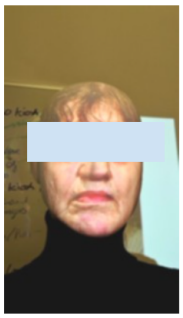
© 2022 FaceTec, Inc. All Rights Reserved. Visit www.FaceTec.com for additional information.

Rebuffed attacks with 2D & 3D artifacts:

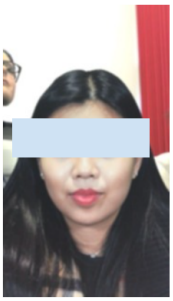
Customer	FaceTec Demo Apps
Application	Android Demo App
Created (UTC)	12/20/21 at 4:10pm
Email	90018@ibl.ibl
Action	Enrollment
Package/Domain	com.facetec.zoomlogin
Platform	android
Ip Address	
Model	SM-G988B
Version	9.4.4-dev-2021111903
Location	en_GB
3D Liveness	Not Proven
Response	• **success:** false • **livenessStatus:** 1 • **ageEstimateGroup:** -1 • **enrollmentIdentifier:** android_demo_93ad4b53ed17485994510fd90a7cf167



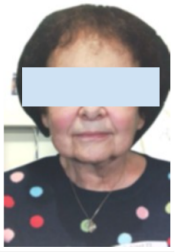
Customer	FaceTec Demo Apps
Application	Android Demo App
Created (UTC)	12/17/21 at 8:42pm
Action	3D Liveness
Package/Domain	com.facetec.zoomlogin
Platform	android
Ip Address	
Model	SM-G988B
Version	9.4.4-dev-2021111903
Location	en_GB
3D Liveness	Not Proven
Response	• **success:** false • **livenessStatus:** 1 • **ageEstimateGroup:** -1



Customer	FaceTec Demo Apps
Application	iOS Demo App
Created (UTC)	12/16/21 at 11:26am
Email	91260@ibl.ibl
Action	Enrollment
Package/Domain	com.facetec.identity.check2
Platform	ios
Ip Address	
Model	iPhone 7
Version	9.4.501-SNAPSHOT
Location	en_GB
3D Liveness	Not Proven
Response	• **success:** false • **livenessStatus:** 1 • **ageEstimateGroup:** -1 • **enrollmentIdentifier:** FaceTec_Identity_App_336232F0-DFE8-4B27-88D0-4C80CB78362A



Customer	FaceTec Demo Apps
Application	iOS Demo App
Created (UTC)	12/16/21 at 11:01am
Email	91237@ibl.ibl
Action	Enrollment
Package/Domain	com.facetec.identity.check2
Platform	ios
Ip Address	
Model	iPhone 7
Version	9.4.501-SNAPSHOT
Location	en_GB
3D Liveness	Not Proven
Response	• **success:** false • **livenessStatus:** 1 • **ageEstimateGroup:** -1 • **enrollmentIdentifier:** FaceTec_Identity_App_FFF67551-9829-43AA-94BA-C37E8432B0D4



FaceTec's 3D Liveness proves to a very high level of confidence (+99.999%) that the physical user is present and the camera feed is not being tampered with. This is done by determining that the app is not running on an emulator, a virtual camera is not being used, and a camera hardware adapter bypass is not being attempted. Over the last two years, the FaceTec Spoof Bounty Program has rebuffed over 110,000 attacks, providing FaceTec with the data to closely examine the real-world attacks our software must defend against. The Spoof Bounty Program incentivizes attackers to employ their most effective methods to claim the bounty. All attacks are analyzed, and if a new potential spoof method is identified, the proper steps to mitigate the threat are taken immediately. This means that new threats are patched before they can be exploited by fraudsters in real-world applications. Security is about staying ahead of bad actors, and FaceTec is the only company that pays creative white-hat attackers to help uncover potential vulnerabilities *before* they can be maliciously used for actual fraud.

Many Liveness vendors cite outdated third-party testing conformances to get credibility, preferring lowest common denominator standards and methods that provide a false sense of security, rather than actively and successfully addressing attacks from deepfakes and video injection. The primary reason FaceTec's competitors do not provide spoof bounty programs is their AI would not be able to rebuff any sophisticated attacks and be quickly compromised, which would result in massive bounty payouts.

The European Union Agency for Cybersecurity's (ENISA) January 2022 [Remote Identity Proofing - Attacks & Countermeasures] report discusses the most recent threat vectors, highlighting the need for

© 2022 FaceTec, Inc. All Rights Reserved. Visit www.FaceTec.com for additional information.

3D data to be used in the Liveness assessment, as well as explains how spoof bounty programs are currently the most effective way to test known and unknown threats.

FaceTec Internal Security Self-Assessment

Over the last seven years, FaceTec's internal "Red Team" has attacked the FaceTec Liveness AI in hundreds of different ways and with 10's-of-millions of attacks. Over these years and millions of attacks, FaceTec has trained its AI to detect and reject attacks of all types.

These attacks are over and above the attacks in the iBeta Level 1 & 2 testing (total of 3,300+), and the 110,000+ attacks on the Spoof Bounty Program.

About FaceTec's 3D Liveness Detection AI

A user performs a 3D FaceScan™, which is the result of real-time processing on the video selfie. The 3D FaceScan is encrypted and sent to the organization running the FaceTec Server SDK. When the user's Liveness is deemed "true" by the AI, a 3D FaceMap™ (~170kb) is created, and the 3D FaceScan (and its Liveness data) can be deleted. In the future, the 3D FaceMap can be used to perform the most accurate face matching against 2D user photos that are on file, as a photo ID or in an NFC chip.

The 3D FaceScan (~350KB) is an encrypted byte blob that contains reverse engineered 3D data from 100-plus video frames captured during the two-second user selfie. FaceScans are always encrypted and are not human viewable. 3D FaceScans *do* contain Liveness data. However, 3D FaceMaps are always encrypted and are not human viewable. 3D FaceMaps do *not* contain Liveness data, and don't need to because new Liveness data is always recollected and reassessed each time there is a new access request.

FaceTec performs over 600,000,000 3D Liveness Checks annually and has ***never*** had any fraud reports from any customer using a properly deployed, up-to-date version of the FaceTec Liveness software.

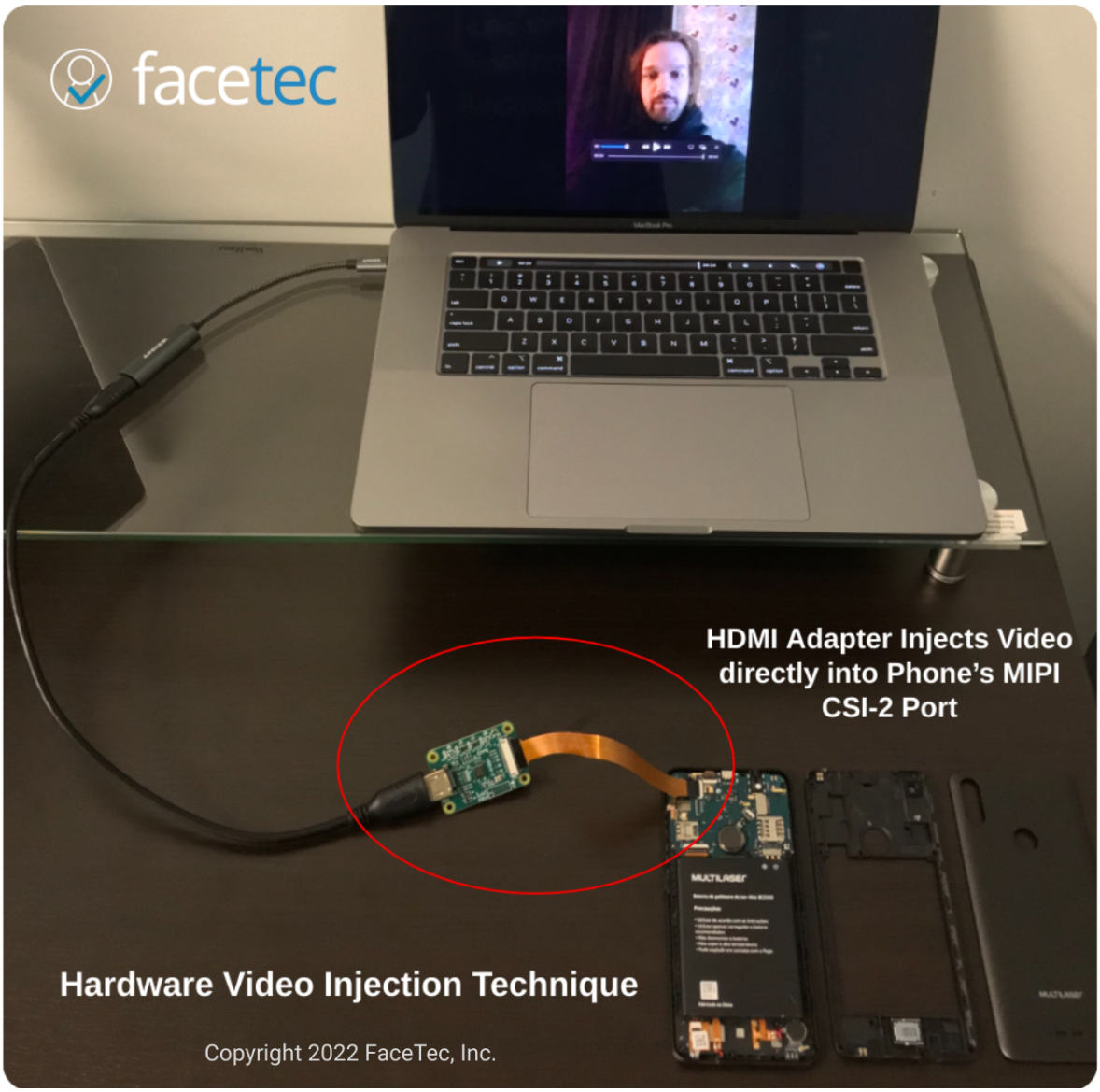
Understanding Video Injection Threat Vectors

There are two types of video injection attacks that can defeat most Liveness Detection systems, either software or hardware-based.

The software-based attack vector uses breakpoints in the Device SDK code or a virtual camera program to fool the system into thinking it is seeing data that was collected from a real camera.

Hardware video injection attacks use adapters to connect to the camera port of a device, and then video is played from another device. This simulates live video that is captured by a physical camera, but it is just receiving the incoming recorded video or synthetic deepfake video feed.

© 2022 FaceTec, Inc. All Rights Reserved. Visit www.FaceTec.com for additional information.



© 2022 FaceTec, Inc. All Rights Reserved. Visit www.FaceTec.com for additional information.

Resources
Educational Wiki-style site - www.Liveness.com
ENISA 2022 - Identity Proofing Guidelines Report
NIST 800-63 RFI - Liveness Security Report Letter
Deepfake vs. 2D Liveness Paper - Seeing is Living?
Deepfake Spoof Article - Unite.ai

Properties of 3D FaceScans & 3D FaceMaps:

- **Encrypted:** This is required and enforced by the FaceTec SDK APIs.
- **Proprietary:** 3D FaceMaps cannot be used by anything other than the FaceTec Server SDK.
- **Created via a patented process:** Users performing user sessions from any device are using FaceTec's patented interface to create 3D FaceMaps.
- **Cross-platform:** FaceMaps from iOS, Android, or Browser can be used interchangeably.
- **Data-rich:** FaceTec 3D FaceMaps are created by processing (in most cases) upwards of 100 frames of data from the raw camera data.
- **Future-proof & forward-compatible:** All FaceTec 3D FaceMaps are guaranteed to be compatible with all future FaceTec Matching Algorithm improvements.
- **No Honeypot Risk:** The 3D Liveness data used for Liveness Detection is deleted from 3D FaceScans after the session is processed; 3D FaceMaps do not contain Liveness data.
- **Flexible:** FaceTec 3D FaceMaps can be stored as files, in databases, in blocks, on a server, or on a device. Customer-specific encryption schemes can be applied in addition to FaceTec SDK built-in security mechanisms.

© 2022 FaceTec, Inc. All Rights Reserved. Visit www.FaceTec.com for additional information.

https://web.archive.org/web/20200426172133/https://www.facetec.com/FaceTec_Case_Study_ZenGo.pdf

CASE STUDY

KZen Networks, Tel Aviv, 2020

Cryptocurrency wallet user authentication and biometric backup

facetec

At a Glance

Technology Need
Biometric Account Recovery

Requirements
- Certified Liveness Detection
- Universal device support
- User-friendly interface
- Straightforward integration
- Ongoing monitoring & updates

Solution
Outperforming all other secure authentication solutions, FaceTec's NIST/iBeta-certified, 100% software, 3D Face Authentication solution, met or exceeded all KZen's user re-authentication process requirements on mobile devices and PC's with webcams. FaceTec 3D Face Authentication has been rigorously tested by KZen's security team who also performed multiple security audits on the implementation of the architecture. Robust, Certified Liveness Detection was recognized as the most critical component of an unsupervised user re-verification process enabling biometric account recovery.

Overview

KZen Networks, the Tel Aviv-based developer of the ZenGo crypto wallet, decided from the start to make the "perfect" cryptocurrency management solution. Their technology has been called a game changer and a revolution in crypto storage that can bring bitcoin, etherium and many other digital assets to the masses.

KZen knew that for mass adoption the next generation crypto wallets had to be trusted as more than just vaults to store an asset, and they needed to address the significant problem of lost or stolen keys. The news is filled with stories of missing or damaged hard drives containing the only method users could employ to access their wallets again.

KZen's definition of a what a successful crypto wallet should be must include the following:

1. Prime security and security
2. Diverse asset and token support
3. Privacy
4. Superior, simple user experience

Given ZenGo's primary mission, it was imperative that security remained the top priority, and they focused on solving two long-standing challenges: problematic private keys and difficult - or *impossible* - account recovery.

We are well aware that replacing a recovery phrase with a password will not ultimately solve the problem of lost or stolen keys, as either can leave funds locked in wallets and abandoned forever. A business-critical issue, not solving this important matter could easily prevent mass adoption of crypto assets.

ZenGo's keyless security model removes the single point of failure of traditional cryptocurrency management solutions and frees the user from concern about their private keys being lost or stolen. Their unique approach replaces traditional private keys with two independently created "mathematical secret shares." One share is stored on a personal smart device or webcam-enabled system, the other on the ZenGo server.

Using a distributed key generation protocol (based on open source multi-party computation) to generate each secret key separately, no party has access to the other's secret. They also created a distributed signing protocol so both shares are always required to sign transactions on the blockchain. The user's shares never leave the device that created them, and with no single point of failure, even if something happens to one of the shares, the assets remain safe.

© 2020 FaceTec, Inc. All rights reserved.

"

We encourage you to test the system for yourself by trying to restore your account with a picture or video of your face. It will fail, and you can rest assured those pictures of you on Facebook won't unlock your ZenGo account.

"

-- Tal Be'ery, Co-founder and Security Research Manager, KZen

If users lose a device, delete an app, or want ZenGo on a new device, they can recover their account with a simple face scan to match the 3D FaceMap created during the initial backup process. This allows the encrypted device share to be decrypted on the new device and the wallet quickly restored. With a simple, intuitive, fast interface, the ZenGo wallet is easier to use than any other option.

The Business Problem

According to research firm Statista, by the end of 2019, there were over 44 million crypto wallet users, a five-fold increase over a three-year period. It is expected when cryptocurrencies become more stable and the security questions are substantially answered, the rate of wallet use will skyrocket. Several factors for usage include a rise in crypto currency offerings and value; addressing security concerns from unintended use, device damage and theft; heightened user expectations; and continued global increases in general mobile use. But without robust access security, the advancement of the crypto industry would suffer. To mitigate security concerns in KZen's use case, effective authentication safeguards will ensure that only legitimate users are allowed access.

In addition, to create a commercially viable product, costs to KZen, and the user and business experiences must clearly benefit from authentication solutions, providing clear, positive impact on a company's image and bottom line.

Authenticating a user – verifying they are legitimate, and alive and physically present at the time of the login request – is a key requirement. However, unless the specific problem of recovering lost access through misplaced or stolen keys was fully resolved, all other issues and benefits would be of no consequence, and wallet acceptance could easily flounder.

KZen recently released the Android version of ZenGo, their highly anticipated crypto currency wallet with 3D Face Authentication and account recovery powered by FaceTec.

Choosing the Authenticator

To safeguard the highly sensitive, valuable assets cryptocurrency wallets manage, a truly secure access method must meet the following criteria:

- Ensure the user requesting access is verified as authorized *and* - to prevent spoofing – verify they are alive and present *at the time of account login*
- Be fast, easy and intuitive enough for anyone to use daily
- Perform in a broad range of physical environments and circumstances
- Work for all users of standard smart devices and webcams
- Be simple for customers to integrate and manage

After rigorous internal testing, and recognizing the value of the iBeta certifications and a history of millions of users on six continents, the Facetec's 3D Face Authentication solution met or exceeded KZen's demanding usability and security requirements when tested in a wide variety of common environmental and situational circumstances with a diverse user base.

© 2020 FaceTec, Inc. All rights reserved.

KZen considered and tested numerous purported face authenticators from several vendors, many claiming capable liveness detection, including a solution that flashed random colors at the user's face. By after testing, the choice was clear.

FaceTec's patented, NIST/NVLAP iBeta-certified 3D face authentication software increases security and convenience with the most secure and intuitive biometric on the market. Available for all smart devices and webcam-enabled systems, FaceTec leverages decades of computer vision and artificial intelligence experience to ensure positive identification verification, three-dimensionality and human liveness.

> *"We encourage you to test the system for yourself by trying to restore your account with a picture or video of your face," said ZenGo Co-founder and Security Research Manager, Tal Be'ery. "It will fail, and you can rest assured those pictures of you on Facebook won't unlock your ZenGo account."*

Having funds secured by a face scan can be unnerving, especially knowing that technologies like Apple's Face ID have been defeated before. But as ZenGo CEO Ouriel Ohayon says, they use FaceTec authentication because it's been "battle tested over millions of users including banks", and it "cannot" be gamed.

Assessing 2D Facial Recognition: Two-dimensional facial recognition can be very effective at matching the face a device's camera sees to a stored photo taken at a similar angle and lighting conditions, and it is necessary in making a positive ID. However, 2D face matching cannot provide enough image data (signal) to distinguish between a photo or video spoof and a live person. Without robust Liveness Detection and 3D depth detection, it is not possible to anchor a human identity to an account for digital verification. Some 2D face matchers require users to blink, wink or nod randomly, but are easily fooled by simple spoof attempts like, "Photoshopping" eyelids on a copy of a photo and toggling between the two. Further, 2D photos can even be made to smile, talk, nod and look around using simple deepfake programs like CrazyTalk.

FaceTec 3D Face Authentication is trusted to stop fraud and identity theft by organizations of all sizes on six continents in banking, government, IAM, connected transportation and more.

Assessing 3D Face Authentication: A 3D face biometric contains at least 100-times more data than a 2D photo or a video and can verify both identity and three-dimensionality using the same data. Some 3D face authentication methods are based on proprietary hardware, and some require several seconds to authenticate. Intense, direct lighting can also overwhelm smart device cameras regardless of how good they are, preventing authentication.

The two primary 3D face authentication approaches are either hardware- or software-based. Hardware-based 3D face authentication is accomplished using specialized cameras, and expensive AI chips, sensor arrays and IR dot projectors that beam invisible dots onto a user to model a 3D face. While this approach can be effective in discerning three-dimensional from two-dimensional objects, there is one key issue: a 3D object is not necessarily a real person. Dolls, masks, 3D prints and wax figures are all 3D, but not alive. Every 3D face verification hardware solution released can be fooled by at least one of these artifacts.

© 2020 FaceTec, Inc. All rights reserved.

FaceTec's software measures perspective distortion to prove the user's face is 3D and measures several dozen uniquely human traits. It converts a two-second video selfie into a proprietary biometric 3D FaceMap that contains the data to make an exceptionally accurate face-matching decision *and* a highly trusted liveness decision. AI-driven continuous learning makes authentication more effective over time, and FaceTec continually updates algorithms to guard against new threats. The FaceMaps are encrypted and securely stored in the cloud, the liveness data – half the required login data – is deleted immediately, preventing theft and fraud, and allowing users to securely authenticate across operating systems and multiple devices, ideal for large scale deployments.

For more information about FaceTec 3D Face Authentication can solve your most challenging authentication problems, please visit FaceTec.com.

The ZenGo Biometric Account Recovery Solution

In an industry-first, biometric-based ZenGo Account Recovery can now re-establish the digital identities of their users through the simple act of taking a selfie. Advanced 3D FaceMap technology quickly and securely authenticates users and unlocks their digital identities to allow them to easily regain access to their accounts after the loss or theft of their devices.

In addition to providing this critical service and a superior user experience, the verification process must also catch fake IDs, meet compliance mandates and work across a wide range of operating systems and device hardware. Given the complexity and the importance of verifying identities digitally in real-time, FaceTec's authentication solution ensured the correct user is present and alive.

For a primer on the critical importance of Liveness Detection, please visit Liveness.com

Put Your Bitcoin Where Your Mouth Is!

ZenGo showed the skeptics that their system was secure enough to protect users crypto wallets by issuing a challenge on their blog:

© 2020 FaceTec, Inc. All rights reserved.

"We're all about putting our money where our mouth is. We've designed ZenGo to be super convenient and super secure against attacks or errors of all forms and we have completed two security audits to prove it (1 and 2). Since we launched, we've received many questions about our innovative security model. "Where's the private key?" and "What happens if someone gets my email or a photo of my face?" are just a few of the questions we've received. We've written lots about these questions in our blog posts.

For the latest company and industry news and announcements, please visit FaceTec and KZen.

"Since we feel pretty confident in ZenGo's security, we figured we'd show you just how secure it is. And to prove it we've put 1 BTC in a wallet just waiting for you. All you need to do is break into the wallet and take it. If you can, the bitcoin is yours. Bitcoin just broke $11,000 so get to work ☺."

FaceTec's 3D Face Authentication exceeded the security and usability requirements for KZen's use case, ensuring the account recovery experience provided real users a superior user experience, and allowing them to very quickly and simply regain control over their high value crypto accounts.

FaceTec's 3D Face Authentication:

- Is iBeta Level 1 & Level 2 certified against presentation attacks
- Matched 3D face images with extreme accuracy
- Used standard 2D device cameras and webcams to create encrypted 3D FaceMaps on all modern Android and iOS smart devices and webcam-enabled systems (omnichannel support)
- Enrolled users consistently and reliably
- Enrollment took only 10-15 total seconds

For business inquiries, please visit: https://dev.zoomlogin.com/zoomsdk/#/quote.

Further leveraging FaceTec's advanced technology, KZen recently announced a proof-of-concept of the first Threshold Signatures wallet for Facebook's proposed disruptive Libra blockchain digital currency testnet. Libra, with this technology, has the potential to reshape the financial landscape.

FaceTec, itself, had upped the ante when it introduced the world's first spoof bounty program in October of 2019. The goal of the $75,000 global, ongoing bounty program is to uncover potentially unknown vulnerabilities in the Liveness AI and security layers so any issues can be patched and the anti-spoofing capabilities and overall platform security elevated even further. To date, more than 13,000 spoof attempts by experts from around the world have been unsuccessful.

Recommendations

When deciding on a biometric authenticator, several factors must be considered. Security, usability, cost and future flexibility must be evaluated together.

© 2020 FaceTec, Inc. All rights reserved.

1. *Security*: Unauthorized account or document access can be dangerous and costly, and require strong security measures. For true user authentication, the method must accomplish five things during login:

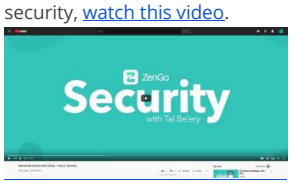
1) Verify human liveness traits
2) Verify three-dimensionality
3) Match images captured by device to enrolled users' FaceMaps
4) Encrypt unique 3D FaceMap data for secure storage and transmission
5) Properly manage acquired and saved data

To learn more about ZenGo and KZen Networks, please visit zengo.com.

For the application to avoid spoofs by non-human representations of the authorized user (photos, videos, image projections, masks, etc.), the steps listed above must happen in real-time at login. Other face biometrics tested met one or two of the required authentication attributes. FaceTec's solution managed all steps seamlessly and consistently.

An important note: All biometric solutions *must* be 3rd-party certified by a sanctioned lab to verify the performance claims made by the vendor, and *must also* offer an open spoof bounty program to provide the very highest level of real-world vulnerability testing.

To learn more about Zengo's security, watch this video.



2. *Usability*: User authentication will occur in a wide variety of circumstances and environments, and the experience needs to be consistent, fast and reliable. Authentication processes that take more than a few seconds, require special hardware, or are not easily accessible in inclement weather will be quickly rejected by typical users. The interface must be quick, and easy to understand and access. FaceTec's fast, simple selfie interface proved easy to use, even for the least tech savvy.

Usability must also be considered for IT management. FaceTec's 3D Face Authentication can perform user authentication without IT intervention: a liveness determination allows or blocks account access and sends a pass-fail decision to the customer application. No additional processing is required, except when an organization requires additional steps, such as document verification.

3. *Total Cost*: Overall costs must consider all direct and indirect expenses, as well as any projected savings from reductions in support overhead, breach mitigations and damage to hard-won branding.

Use licenses, subscriptions, in-house development or outright purchase costs are just the beginning of a realistic cost assessment. Support requirements must also include server setup and maintenance, additional hardware and

© 2020 FaceTec, Inc. All rights reserved.

personnel, coding and interface customization, vendor support agreements, upgrades, bug fixes and internal customer support representatives.

A secure solution also offsets significant costs by preventing breaches, avoiding internal IT and post-breach mitigation costs, and preventing potentially very expensive brand damage.

4. *Future-Proofing*: Security technology and threats change rapidly. It is of strategic importance to select a 100% software security solution that is constantly improved and third-party tested. Updates must be developed and deployed quickly, and the solution must react rapidly to market needs. It must be cross-platform compatible, and work on any popular mobile or stationary device, even devices the user does not own. An AI-driven software solution is the only real-world approach to meeting all these demands.

For press inquiries and additional information about FaceTec and Liveness.com, please contact John Wojewidka, VP of Communications, at johnw@facetec.com.

Summary

By anchoring a user's human identity to their digital identity through robust liveness detection, ZenGo users can - for the first time ever - now securely access their accounts even after losing or damaging their devices without remembering their keys, PINs or passwords. In this demanding environment, where fraud is a troubling constant, yet users cannot be inconvenienced, FaceTec was considered the perfect security solution for ZenGo. Every aspect of FaceTec's 3D Face Authentication, from security to usability to costs, validated the solution as the best cross-platform biometric access method, exceeding KZen's user's expectations and requirements.

- *Security*: Seamlessly, consistently allows fast enrollment and authentication of real, registered users with valid IDs while rejecting fraudsters
- *Usability*: Fast and simple for users, works in nearly all lighting conditions, no special hardware required; quickly deploys for POC trials with easy app SDK integration, plus extensive visual customization options
- *Total Cost*: Insignificant integration costs, near-zero management/maintenance costs, straightforward pricing, dramatically reduced password-reset related costs, increased usage and customer loyalty
- *Future flexibility*: Fast, seamless, timely updates; quick, thoroughly tested deployments; future-threat and customer-integration-needs ready

© 2020 FaceTec, Inc. All rights reserved.

Additional Resources

White Papers

- FaceTec – 3D Matching: 1/4.2M FAR@<1%
- Liveness, Biometrics' Final Frontier?
- PAD Testing, There's a New Sheriff in Town
- Anchoring Identity, From KYC to Finish
- FaceTec – 3D Liveness Methodology
- FaceTec – Internal Testing Guidance

Case Studies

- FaceTec – Jumio: Partner Case Study
- FaceTec – Turbi Car Sharing Case Study
- FaceTec – IAV Connected-Car Case Study

ZoOm Documentation

- FaceTec – Authentication Configurations
- FaceTec – Server & Cloud Architecture
- FaceTec – Frequently Asked Questions
- FaceTec – Frequently Asked Questions
- FaceTec – Passport Morphing Prevention

Latest FaceTec News

- FaceTec in the Media

FaceTec Spoof Bounty Program

- FaceTec $75,000 Spoof Bounty

© 2020 FaceTec, Inc. All rights reserved.