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 Relying on outdated standards and testing criteria, such as iBeta/ISO 30107-3, creates a false sense of security.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:

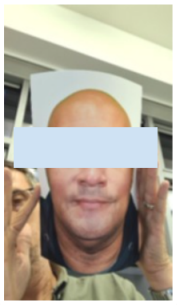
Attack Level	Current Bounty	Attacks	Bounties Paid	Attack Notes
Level 1	$30,000	>88,000	2*	PAD Paper & Digital Photos, Videos, 2D Masks
Level 2	$30,000	>2,000	-	3D Masks, Under $300
Level 3	$40,000	>1,000	-	Hollywood Masks, Madame Tussauds Wax, etc.
Level 4	$60,000	~5,000*	-	* ~5,000 est., but we cannot 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.

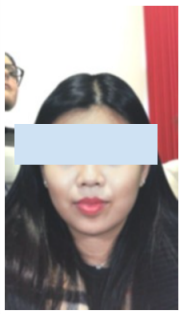
Rebuffed attacks with 2D & 3D artifacts:

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.

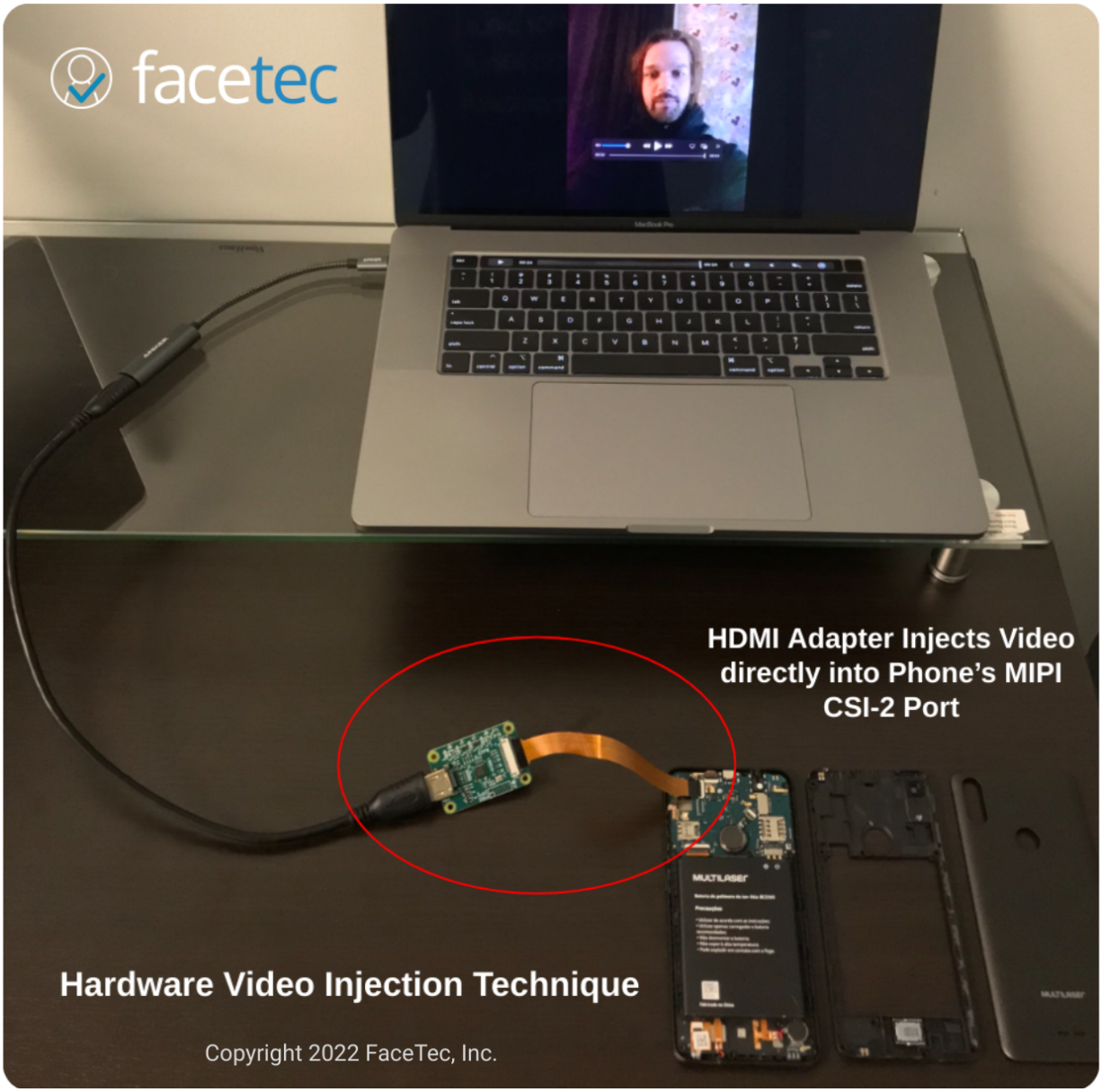
Understanding Video Injection Threat Vectors

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.