facetec

NIST 800-63-4.2pd: Request For Information - Reply

Introduction—FaceTec, Inc. (a Delaware Corp.) is the leading global 3D face liveness and matching software provider for Remote Identity platforms. U.S. Federal Agencies, states, numerous foreign governments, and hundreds of commercial entities use FaceTec's technology to verify and authenticate citizens, customers, and users. For example, Utah, Louisiana, Virginia, and Colorado incorporated FaceTec in their mDL programs, while the U.S. Department of Homeland Security incorporated FaceTec's technology into The Electronic System for Travel Authorization (ESTA).

Hundreds of millions of users worldwide have proven their liveness remotely with FaceTec on tens of thousands of different smartphone, tablet, and webcam models (mostly low-end & low-resolution), and with no observable age, gender, or skin-tone bias. **FaceTecs Device SDK has been downloaded over 1.8 billion times, and FaceTec will conduct roughly 2.9 billion 3D Liveness checks in the next twelve months.** In addition, **FaceTec is the only biometric Liveness vendor that operates a persistent Spoof Bounty Program,** offering as much as a $600,000 incentive to hackers to attempt to bypass the biometric cybersecurity platform. FaceTec software has successfully defended against over 150,000 Bounty Program attacks, providing unmatched experience rebuffing today's most sophisticated threats.

We are pleased with the broader yet more specified application of biometric Liveness, binding, and matching within NIST SP 800-63-4.2pd., as well as Best Practices to mitigate Deep Fake Injection attacks and traditional PAD. With that, however, we have specific comments regarding biometric Liveness. We have identified and quoted the relevant section and listed our comments numerically per section.

Thank you for the opportunity to contribute FaceTecs knowledge to NIST 800-63.

FaceTec's Recommendations to SP 800-63A-4.2pd:

Sect. 3.1.11- 2 -1273-1276 - "When collecting and comparing biometrics remotely, the CSP SHALL implement presentation attack detection (PAD) capabilities, which meet IAPAR performance metric <0.15, to confirm the genuine presence of a live human being and to mitigate spoofing and impersonation attempts."

1. We commend allowing biometric verification. We further commend requiring PAD capabilities for biometric verification, as well as maximum IAPAR thresholds. However, this requirement does not include complying with appropriate PAD standards, like ISO 30107-3. Further, a maximum 0.15 IAPAR threshold is effectively meaningless. Once the attacker successfully defeats the PAD, it will utilize that specific vector from that point forward, increasing its successful use as a percentage

of all attacks. Thus, the IAPAR will increase substantially over time and beyond the 0.15 recommendation. We strongly encourage NIST to **require** PAD testing compliant with ISO 30107-3. We strongly encourage NIST to **require** an IAPAR of 0.0 to randomize potential spoof vectors and mitigate such attacks as much as possible.

2. As noted below, SP 800-63B-4.2pd does NOT require PAD for biometric authentication. This is inconsistent with SP 800-63A-4.2pd, which DOES require PAD for biometric verification. We encourage NIST to consistently require PAD for biometrics used in both verification and authentication.

FaceTec's Recommendations to SP 800-63B-4.2pd:

Sect. 3.2.3-1275-1279 - "The biometric system SHOULD implement PAD. Testing the biometric system for deployment SHOULD demonstrate an impostor attack presentation accept rate (IAPAR) of less than 0.15. Presentation attack resistance SHALL be tested in accordance with Clause 13 of [ISO/IEC30107-3]. The PAD decision MAY be made either locally on the claimant's device or by a central verifier."

1. We commend allowing biometric authenticators. However, making PAD and IAPAR thresholds optional substantially increases the risk of their use. Further, a maximum 0.15 IAPAR threshold is effectively meaningless. Once the attacker successfully defeats the PAD, the attacker will utilize that specific vector from that point forward, increasing its successful use as a percentage of all attacks. Thus, the IAPAR will increase substantially over time and certainly beyond the 0.15 recommendation. We strongly encourage NIST to **require** PAD testing and Deep Fake Injection attack mitigation certification. We strongly encourage NIST to **require** an IAPAR of 0.0 to mitigate such attacks as much as possible.

Sect. 3.2.3-1290-1295 - "The verifier SHOULD determine the performance and integrity of the sensor and its associated endpoint. Acceptable methods for making this determination include but are not limited to:

• Use of a known sensor, as determined by sensor authentication

• First- or third-party testing against biometric performance standards

• Runtime interrogation of signed metadata (e.g., attestation), as described in Sec. 3.2.4."

1. We commend the suggestion to verify biometric sensors and endpoints to mitigate Injection attacks. However, making this determination optional substantially increases the risk of such attacks. We strongly encourage NIST to **require** biometric sensor and endpoint determination to mitigate Deep Fake Injection attacks.