CITeR
Center for Identification Technology Research

PAD Categories defined in ISO 30107

1. Liveness not related to challenge-response (“passive”)*
2. Involuntary Challenge Response

   e.g. random colors of light; change in pupil dilation due to random input

3. Voluntary Challenge Response

   e.g. blinking/smiling at a specific time; saying specific words that are randomly given

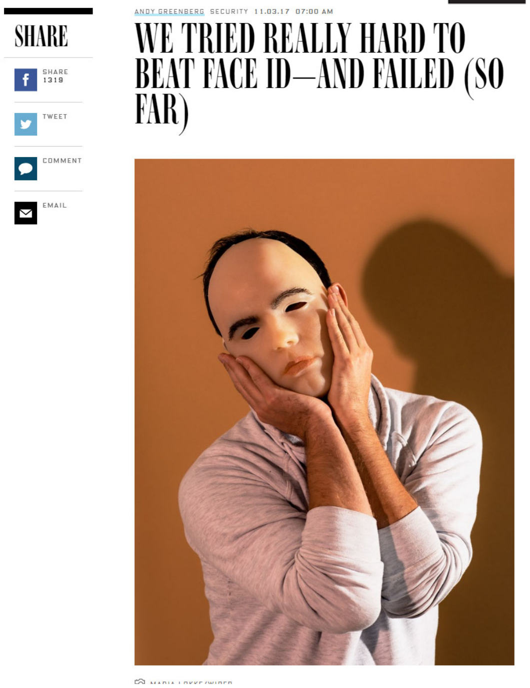
*Active PAD not defined in ISO

From: ISO/IEC 30107-1, Information Technology — Biometrics -- Presentation Attack Detection

Iphone X - Face

- “To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern.” *

WIRED



SHARE

SHARE 1319

TWEET

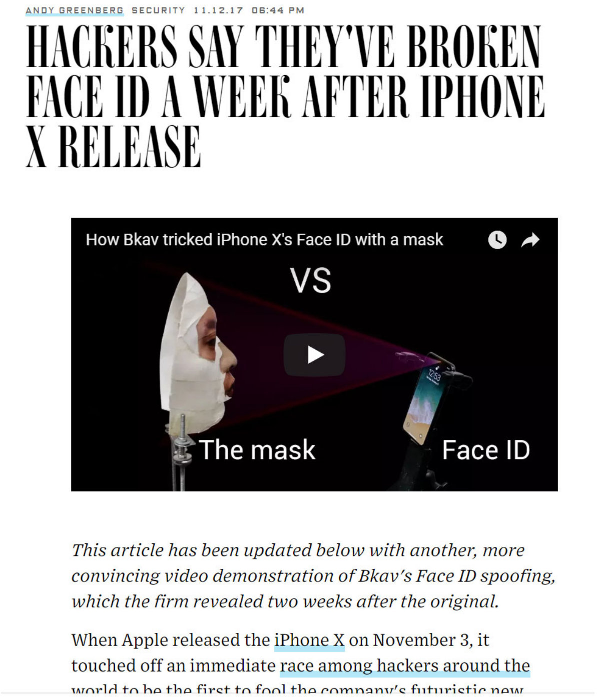
COMMENT

EMAIL

ANDY GREENBERG SECURITY 11.03.17 07:00 AM

WE TRIED REALLY HARD TO BEAT FACE ID—AND FAILED (SO FAR)

MARIA LOKKE/WIRED



ANDY GREENBERG SECURITY 11.12.17 06:44 PM

HACKERS SAY THEY'VE BROKEN FACE ID A WEEK AFTER IPHONE X RELEASE

How Bkav tricked iPhone X's Face ID with a mask

This article has been updated below with another, more convincing video demonstration of Bkav’s Face ID spoofing, which the firm revealed two weeks after the original.

When Apple released the iPhone X on November 3, it touched off an immediate race among hackers around the world to be the first to fool the company's futuristic new

*FaceID Security Guide, 2017, https://www.apple.com/business/site/docs/FaceID_Security_Guide.pdf

PAD - Technology and Scenario Evaluation

Technology

- Definition : offline evaluation of one or more algorithms for the same biometric modality using a pre-existing or especially-collected corpus of samples*

Scenario

- Definition: evaluation that measures end-to-end system performance in a prototype or simulated application with a test crew*

*ISO/IEC 19795-1:2021 Information technology — Biometric performance testing and reporting — Part 1: Principles and framework

PAD - Technology and Scenario Evaluation

Technology

- Easy to compare multiple algorithms based on a common datasets
- Does not reflect end-to-end system performance
  - such as user interface, dynamic PAD, challenge response, and quality checks
- Examples:
  - NIST FRVT PAD
  - LivDet - Algorithms

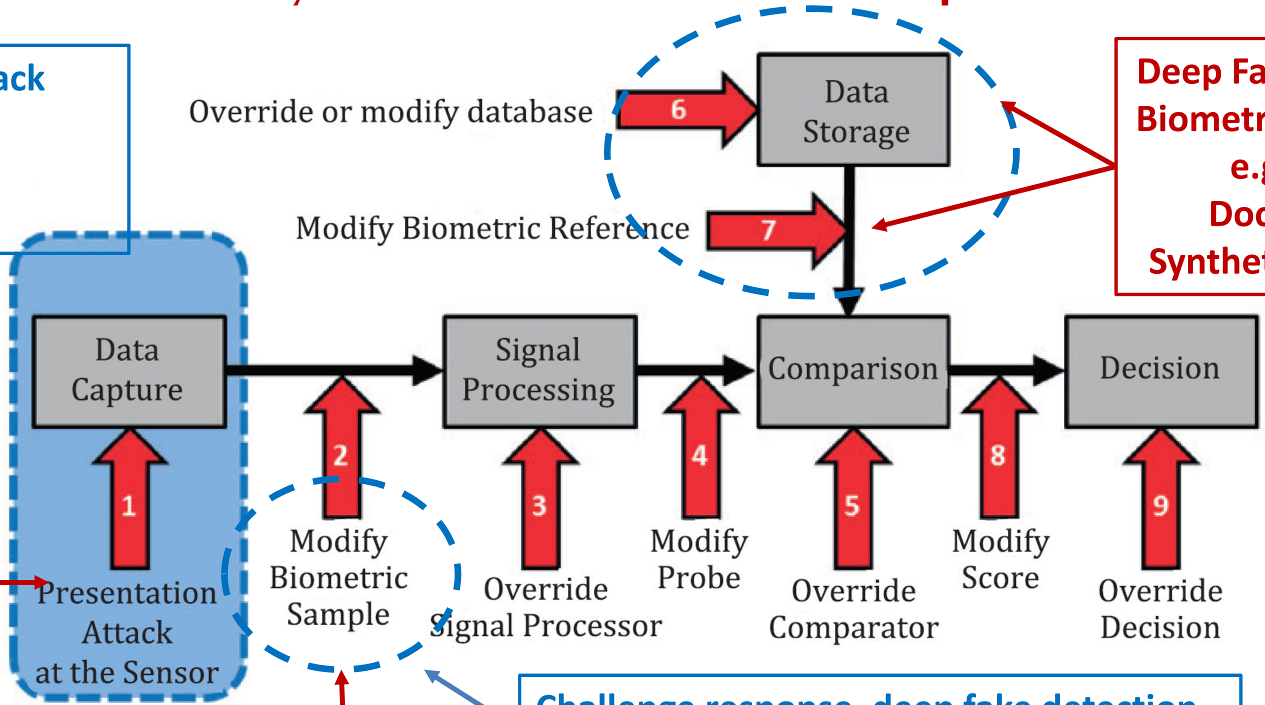
Scenario

- Live test subjects, incorporates user interface
- Able to test user interface, quality checks, and unique PAD systems, that include hardware, software, challenge response (both voluntary and involuntary)
- Examples:
  - LivDet – System
  - FIDO Biometric Component Certification (more later)

*ISO/IEC 19795-1:2021 Information technology — Biometric performance testing and reporting — Part 1: Principles and framework

Biometric Security—Attack Examples

Presentation Attack Detection
(spoof/liveness detection)

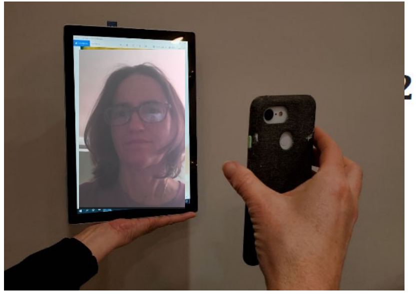


Deep Fake impacting Biometric Reference, e.g., Fake Documents, Synthetic Identities

Present Deep Fake to Biometric Sensor

Challenge response, deep fake detection
(e.g., random pattern on face)

2 — Examples of points of attack in a biometric system (from ISO/IEC 30107-1)



"Inject" Deep Fake Bypassing the Sensor

Deepfakes and Biometric Recognition

- Security, particularly between capture and processing
  - Detect virtual cameras, browser scripts
- Presentation attack detection
- Deep fake detection
- Challenge response (e.g. random challenge)
- Controlling camera from an app, rather than allowing people to upload their video/image
- Certification
  - Exists for PAD
  - Need certification for solutions that address bypassing camera that consider security and other detection methods

PAD and Injection Attacks

Presentation Attack Detection*

- Covered by ISO/IEC 30107
- Categories
  - Liveness not related to challenge-response (“passive”)
  - Involuntary Challenge Response
    - e.g. random colors of light; change in pupil dilation due to random input
  - Voluntary Challenge Response
    - e.g. blinking/smiling at a specific time; saying specific words that are randomly given

*Active PAD not defined in ISO

Injection Attack Detection

- Not covered by ISO/IEC 30107
- Possible similar solutions:
  - Deepfake detection not related to challenge-response (“passive”)
  - Involuntary Challenge Response
    - e.g. random colors of light; change in pupil dilation due to random input
  - Voluntary Challenge Response
    - e.g. blinking/smiling at a specific time; saying specific words that are randomly given
  - Best practices in IT security