

# RSA® Conference 2019

San Francisco | March 4–8 | Moscone Center



# BETTER.

SESSION ID: IDY-F03

## Are Spoof-Proof Biometrics Really Possible?

**Dr. Stephanie Schuckers**

Director, Center for Identification  
Technology Research (CITeR)

Paynter-Krigman Professor in Engineering  
Science

#RSAC

# RSA® Conference 2019

**Authentication Technology Landscape**

**Biometric Presentation Attacks**  
(Methods, Framework)

**Next Gen Technology**  
(The role of liveness in detection)

**Benchmarking** (Competitions, Datasets)

**Standards & Requirements** (ISO, platforms)

**Certification**  
(FIDO, Common Criteria)



# Before We Begin: Vocabulary

- Presentation Attacks
  - Presentation of an artefact or human characteristic to the biometric capture subsystem in a fashion that could interfere with the intended policy of the biometric system\*
  - Spoofs, artefacts, altered biometrics, non-conformance, obfuscation
- Presentation Attack Detection
  - Examples: liveness detection, altered fingerprint detection, anti-spoofing

\*ISO/IEC CD 30107-1, Information Technology — Biometrics -- Presentation Attack Detection

# THE WORLD HAS A PASSWORD PROBLEM

81%

Data breaches in 2016 that involved **weak, default, or stolen passwords**<sup>1</sup>

65%

Increase in **phishing attacks** over the number of attacks recorded in 2015<sup>2</sup>

1,579

Breaches in 2017, a **45% increase over 2016**<sup>3</sup>

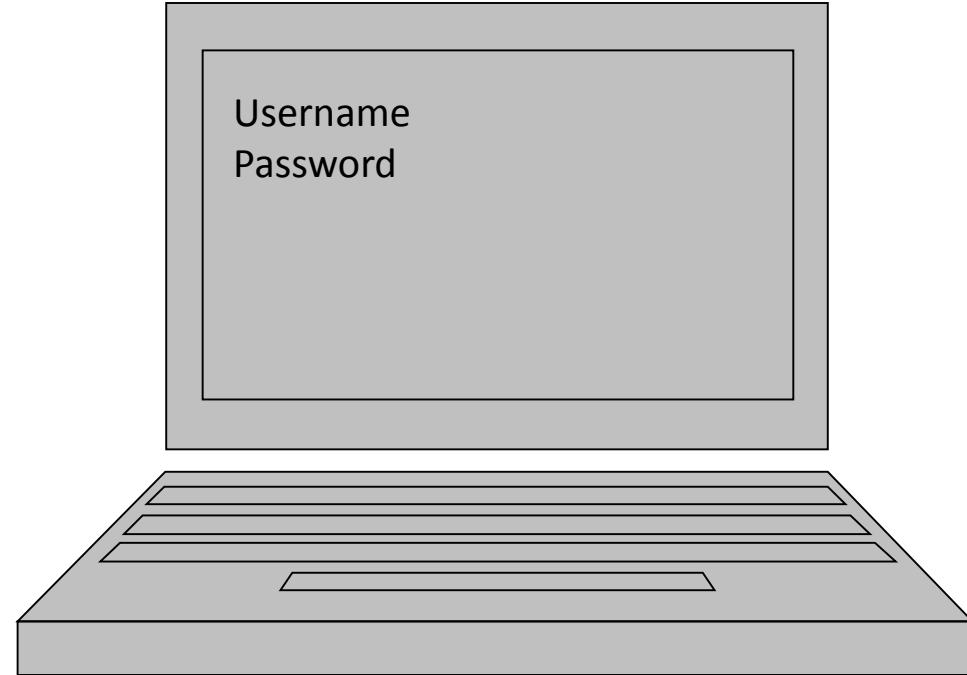


CLUMSY | HARD TO REMEMBER | NEED TO BE CHANGED ALL THE TIME

<sup>1</sup>Verizon 2017 Data Breach Report | <sup>2</sup>Anti-Phishing Working Group | <sup>3</sup>Identity Theft Resource Center 2017

# What Can You Do with a Stolen Password?

1. Find **any** computing device
2. Type in password

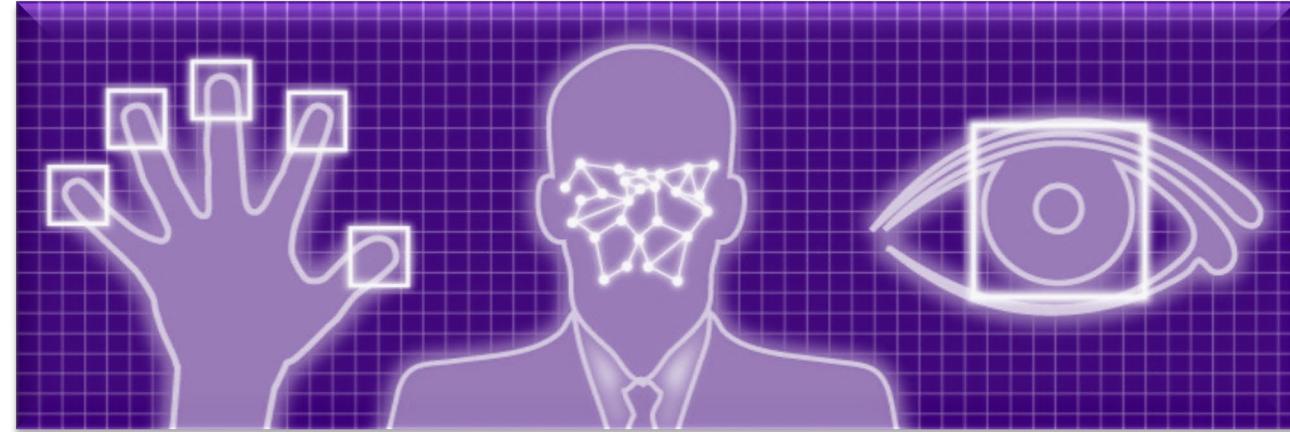


Traditional Username & Password

Easily  
Scalable

# The rise of biometrics

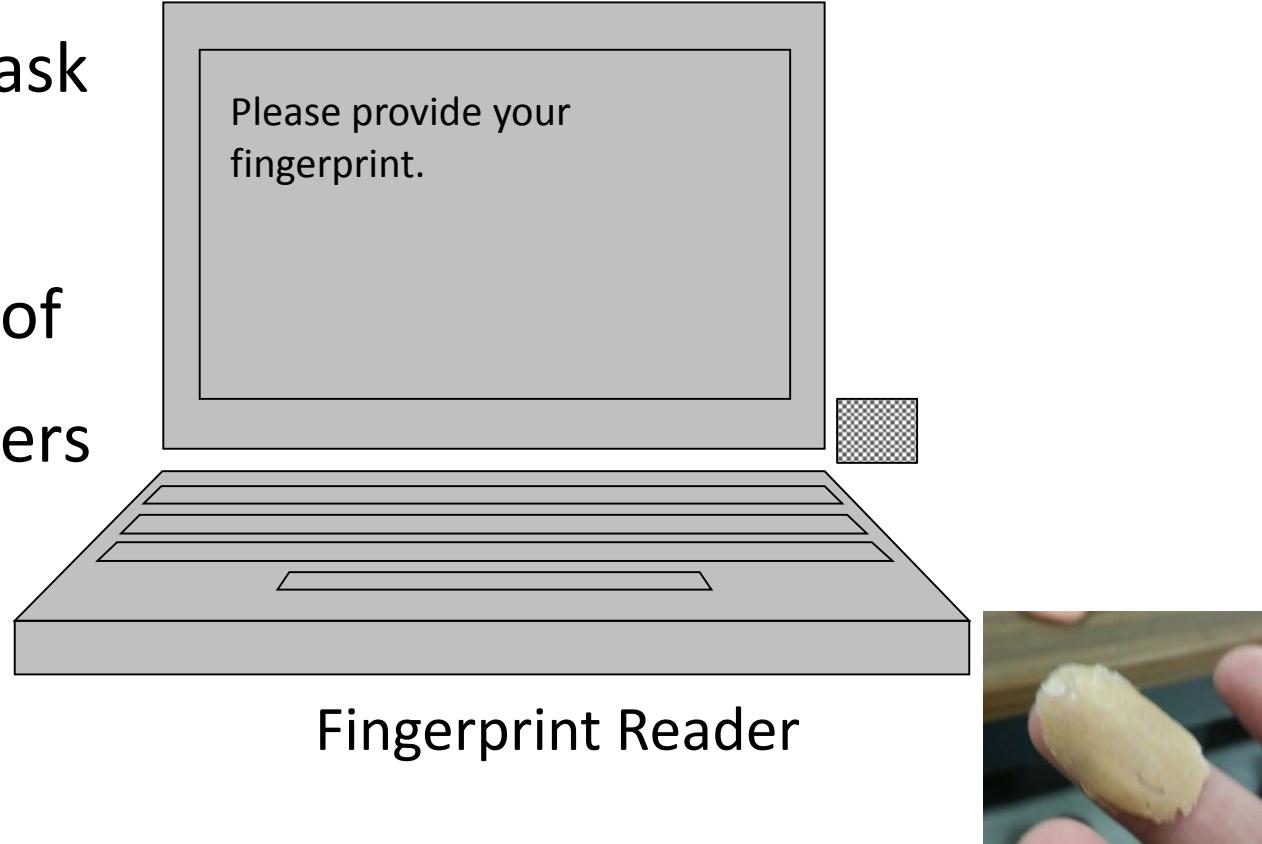
Biometrics can improve security and provide a positive user experience, but be conscious of potential weaknesses



# What Can You Do with a Stolen Fingerprint?

1. Convert fingerprint to digital image
2. Clean and invert image to create mask
3. Etch or print 3D mold
4. Add material to create cast, i.e. spoof
5. (*If locally stored biometric*), steal users specific computing device associated with the stolen fingerprint

Not Easily Scalable



Fingerprint Reader

# Conventional Wisdom on the Weaknesses of Biometrics

- Biometrics cannot be changed
- Biometrics are not secret

# Mitigation of Weaknesses of Biometrics

*Ensure that biometric information cannot  
be inserted beyond the sensor*

*Locally Stored  
Biometric Templates,  
Security*

*Ensure that biometric was measured from  
the live, authorized individual at that  
time/place*

*Presentation  
Attack  
Detection*

# Spoofing: Don't Believe the Hype



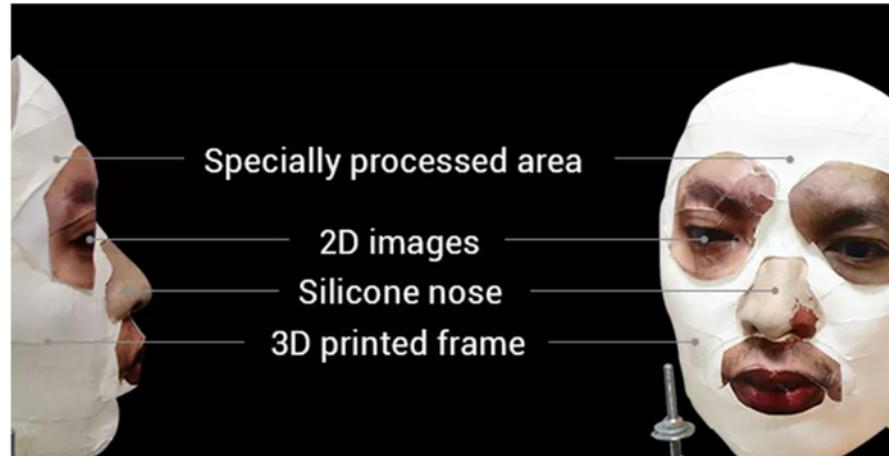
APPLE ▾ TECH ▾ CYBERSECURITY ▾

## This \$150 mask beat Face ID on the iPhone X

*It's just a proof of concept at the moment*

By Thuy Ong | @ThuyOng | Nov 13, 2017, 5:46am EST

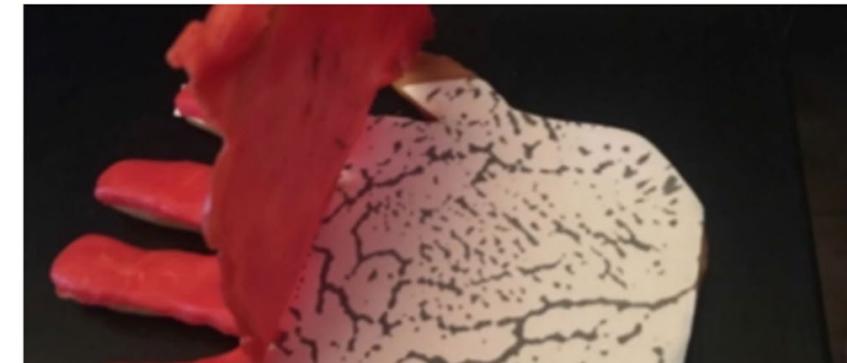
f t SHARE



MOTHERBOARD Moveable Hacking Environment Space Gaming He

Security researchers disclosed new work at the Chaos Communication Congress showing how hackers can bypass vein based authentication.

SHARE f TWEET t



PYMTS.com

SECTIONS TODAY'S NEWS RETAIL B2B OPINION STUDIES TRACKERS PODCASTS MASTERCLASS



AUTHENTICATION  
**TRENDING: Identical Twins Highlight Need To Double Up On Biometrics**

# Spoofing: But there are practical concerns

**The China Post** Since 1952

Home > Top News > Asia > South Korean fools finger printing system in Japan

**South Korean fools finger printing system in Japan**

January 2, 2009

AFP

TOKYO — A South Korean woman barred from entering Japan last year passed through its immigration screening system by using tape on her fingers to fool a fingerprint reading machine, reports said Thursday.

The biometric system was installed in 30 airports in 2007 to improve security and prevent terrorists from entering into Japan, the Yomiuri Shimbun said.

The woman, who has a deportation record, told investigators that she placed special tapes on her fingers to pass through a fingerprint reader, according to Kyodo News.

Japan spent more than four billion yen (US\$44 million) to install the system, which reads the index fingerprints of visitors and instantly cross checks them with a database of international fugitives

BBC NEWS

Home | UK | World | Business | Politics | Tech | Science | Health | Family & Education

World Africa Asia Australia Europe Latin America Middle East US & Canada

**Doctor 'used silicone fingers' to sign in for colleagues**

12 March 2013

A Brazilian doctor faces charges of fraud after being caught on camera using silicone fingers to sign in for work for absent colleagues, police say.

Thaune Nunes Ferreira, 29, was arrested on Sunday for using prosthetic fingers to fool the biometric employee attendance device used at the hospital where she works near Sao Paulo.

She is accused of covering up the absence of six colleagues.

Her lawyer says she was forced into the fraud as she faced losing her job.

The local public prosecutor's office opened an investigation on Monday.

The doctor was arrested by the local police following a two-week investigation in the town of Ferraz de Vasconcelos, and was released on Sunday.

Police said she had six silicone fingers with her at the time of her arrest, three of which have already been identified as bearing the fingerprints of co-workers.



Police said they recovered six silicone fingers at the time of the doctor's arrest

**MEDIANAMA**

HOME Aadhaar MOBILE ECOMMERCE PAYMENTS POLICY FUNDING REPORTS

Home > Aadhaar, Aadhaar fraud, Biometrics

**Cloned thumb prints used to spoof biometrics and allow proxies to answer online Rajasthan Police exam**

By  Viduy (@https://twitter.com/Viduy viduy@medianama.com) March 16, 2018

Share This:    Share via Email

New forms of fraud keep emerging but a gang arrested on Thursday managed to stun everyone with their ingenuity. The gang cloned the thumb prints of online examination candidates for the Constable admission exam in Rajasthan and used them to provide expert proxy examination solvers to answer examination papers on behalf of the real candidates. The SOG has arrested a village service worker and the mastermind along with 3 other members of this gang. Their revelations are even more astonishing. This same method is being used to clone thumb prints and provide proxies for 25 candidates in 7 examination centres.

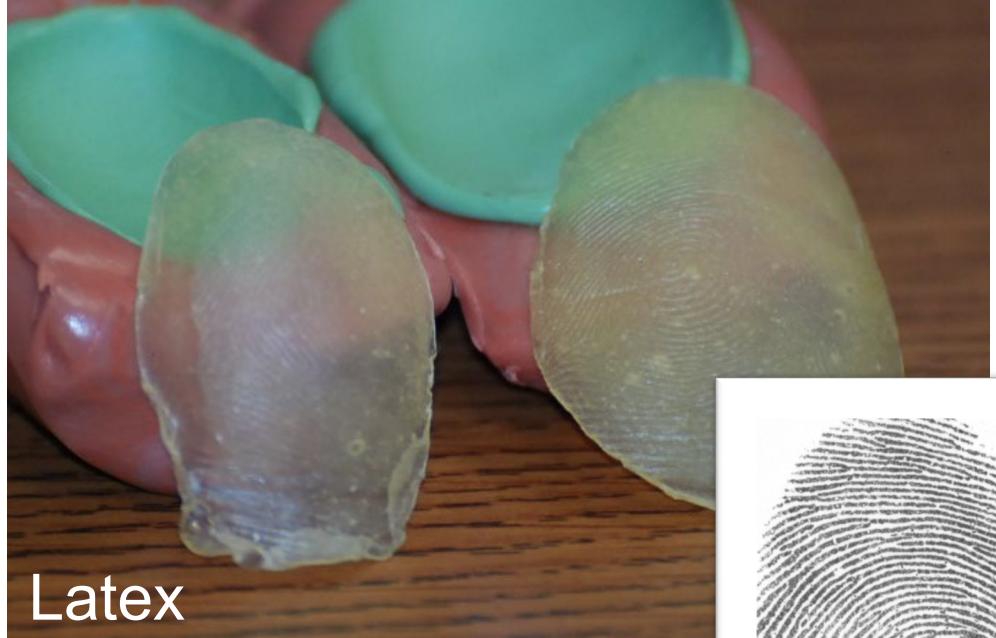
The methods used to bypass biometric checks for appearing for the exam.

January 2, 2009

March 12, 2013

March 15, 2018

# LAB-CONTROLLED SPOOFING



Latex



Wood Glue



# RSA® Conference 2019

**Authentication Technology Landscape**

**Biometric Presentation Attacks**  
(Methods, Framework)

**Next Gen Technology**  
(The role of liveness in detection)

**Benchmarking** (Competitions, Datasets)

**Standards & Requirements** (ISO, platforms)

**Certification**  
(FIDO, Common Criteria)



# Production of Biometric Presentation Attack (Spoof)

- Production of spoof requires two things
  - (1) Source of biometric characteristic you are replicating
  - (2) Process for creating the spoof

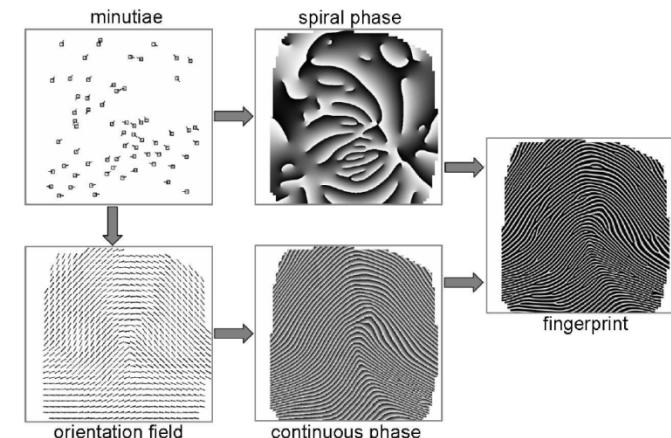
# Source of Biometric

- **Cooperative**—Captured directly from individual with assistance (e.g. finger mold, face mask)
- **Latent**—Captured indirectly through latent sample (e.g. latent fingerprint, hair, skin)
- **Recording**—Captured directly from individual onto media (e.g. photograph, video recording)
- **Template Regeneration**
- **Synthetic**—Not mapped to real person (e.g. synthetic fingerprint, iris, wolf sample)
- **Impersonation**—Conversion of natural characteristic to another individual's with artificial assistance (e.g. computer assisted voice)

ISO/IEC CD 30107, Information Technology — Biometrics -- Presentation Attack Detection, Part 3, Table A.1

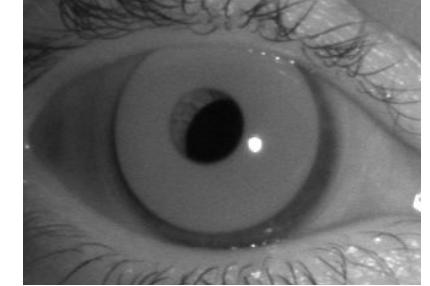


Feng and Jain, Advances in Biometrics article, 2009.



# PRODUCTION OF SPOOF

Molds, casts, masks, direct renderings and digital media



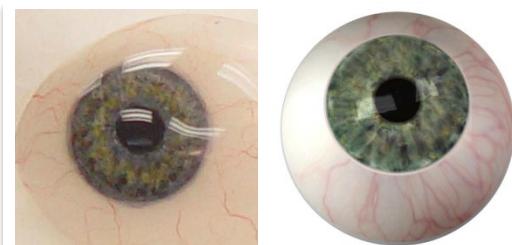
Seelen, "Countermeasures Against Iris Spoofing with Contact Lenses," Iridian Technologies Inc.



Thalheim, et al, C'T article, 2002.



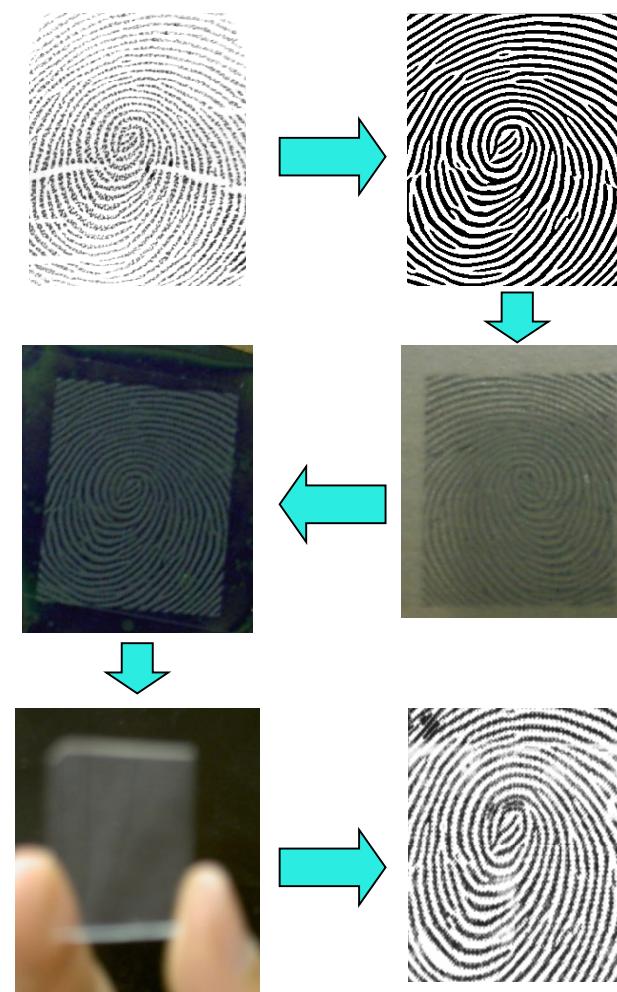
Schuckers, et al, 2002.



Lefohn, et al, IEEE Computer Graphics & Applications article, 2003.

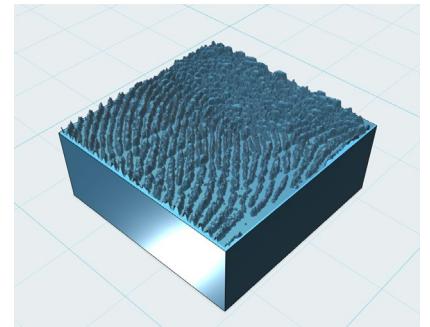
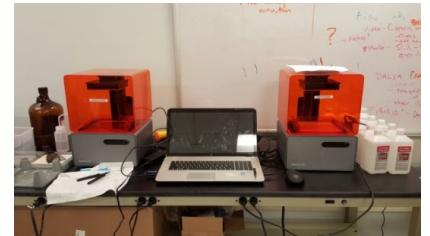
## Spoof Creation with Transparency

- Uncooperative
- Lifted latent print, stolen fingerprint image
- Fingerprint mask generation
- Print on transparent film
- Expose negative photosensitive silicon wafer
- Develop to form cast
- Pour silicone or other liquid material to form mold



## Spoof Creation with 3D Printer

- From fingerprint image, create 3D representation of fingerprint
- Since most 3D printers use rigid materials, print mold
- Create spoofs using mold with traditional materials (e.g. gelatin)



# RSA® Conference 2019

**Authentication Technology Landscape**

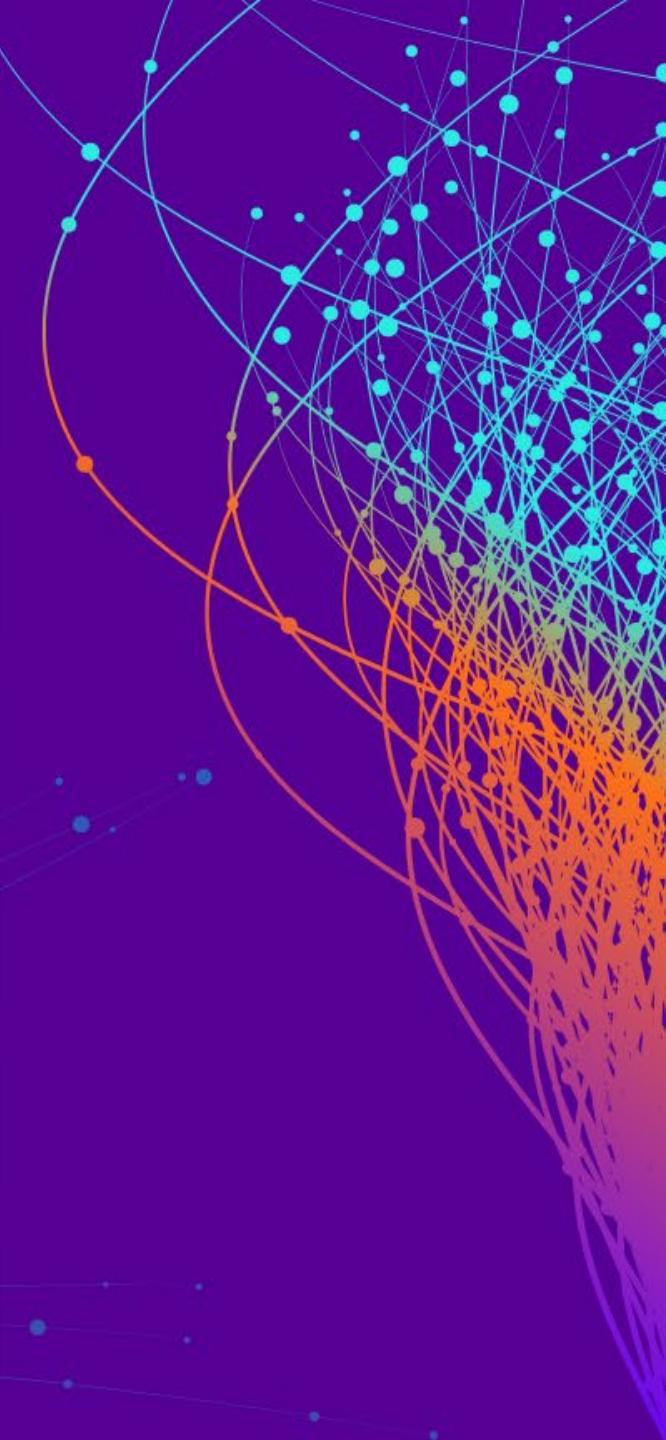
**Biometric Presentation Attacks**  
(Methods, Framework)

**Next Gen Technology**  
(The role of liveness in detection)

**Benchmarking** (Competitions, Datasets)

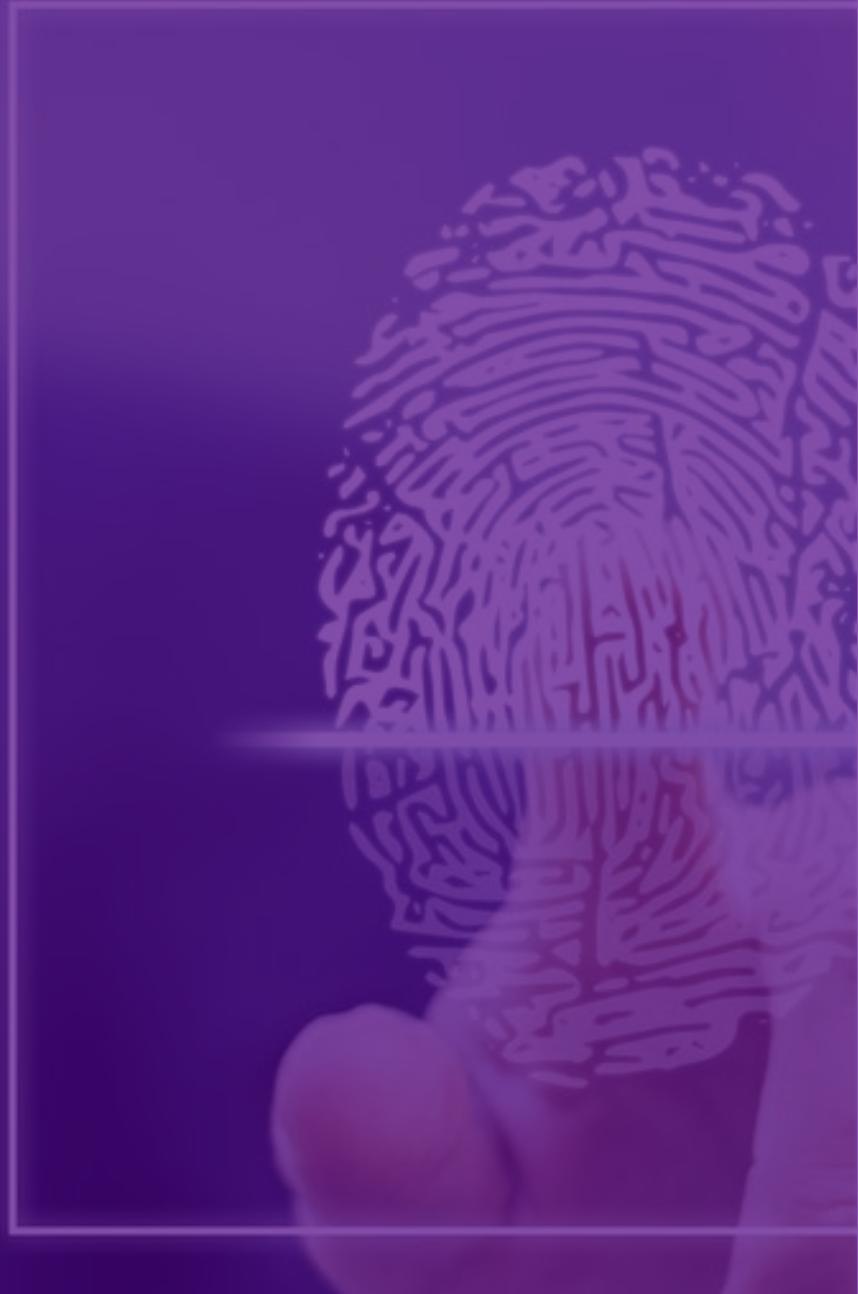
**Standards & Requirements** (ISO, platforms)

**Certification**  
(FIDO, Common Criteria)



**“It is ‘liveness’, not secrecy, that counts.”**

*Denning, Information Security Magazine, 2001*



# Fingerprint PAD

- Thousands of academic papers in this area!
- Hardware-based
  - Temperature, pulse, blood pressure, odor, electrocardiogram, multispectral imaging, spectroscopy, ultrasound, electrical characteristics
- Software-based
  - Skin deformation, elasticity, pores, perspiration pattern, power spectrum, noise residues in valleys



Qualcomm



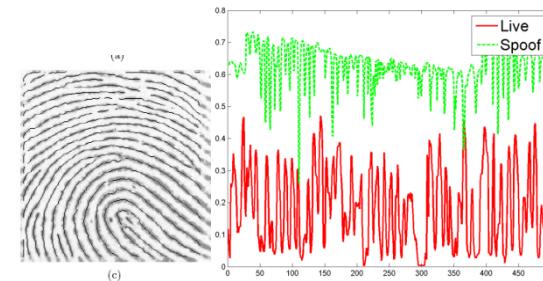
Morpho



Fingerprint Cards



Lumidigm



 **NexID** Biometrics

**PRECiSE** BIOMETRICS™



Dermalog

**RSA** Conference 2019

# Iris PAD

- Hardware-based:
  - Specular reflections, eye movements (e.g., saccades), spontaneous and stimulated pupil size changes, 3D properties (flat iris vs convex textured contact lens), thermal-based features, multi-spectral (melanin absorption as a function of the wavelength vs light absorption by artifacts)
- Software-based:
  - Texture patterns, pixelization, spatial frequency analysis, iris image quality features, deep-learning-based solutions



Iritech Mobile



IrisGuard AD100

# 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.” \*
- “An additional neural network that’s trained to spot and resist spoofing defends against attempts to unlock your phone with photos or masks.” \*

\*FaceID Security Guide, 2017, [https://www.apple.com/business/site/docs/FaceID\\_Security\\_Guide.pdf](https://www.apple.com/business/site/docs/FaceID_Security_Guide.pdf)

# W I R E D

ANDY GREENBERG SECURITY 11.12.17 06:44 PM

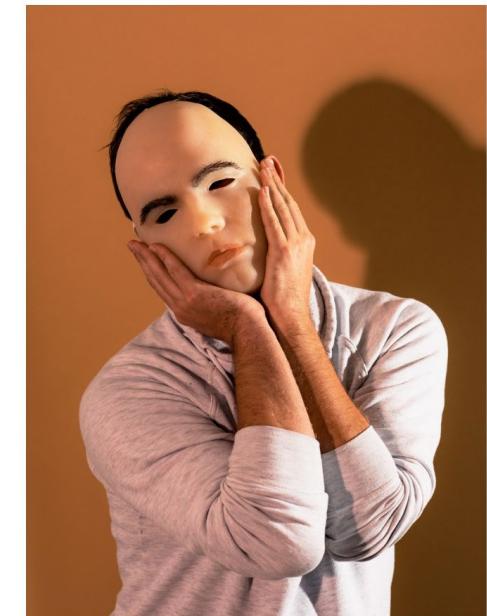
## HACKERS SAY THEY'VE BROKEN FACE ID A WEEK AFTER IPHONE X RELEASE



*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

ANDY GREENBERG SECURITY 11.03.17 07:00 AM  
WE TRIED REALLY HARD TO BEAT FACE ID—AND FAILED (SO FAR)



# RSA® Conference 2019

**Authentication Technology Landscape**

**Biometric Presentation Attacks**  
(Methods, Framework)

**Next Gen Technology**  
(The role of liveness in detection)

**Benchmarking** (Competitions, Datasets)

**Standards & Requirements** (ISO, platforms)

**Certification**  
(FIDO, Common Criteria)



# Competitions for Benchmarking

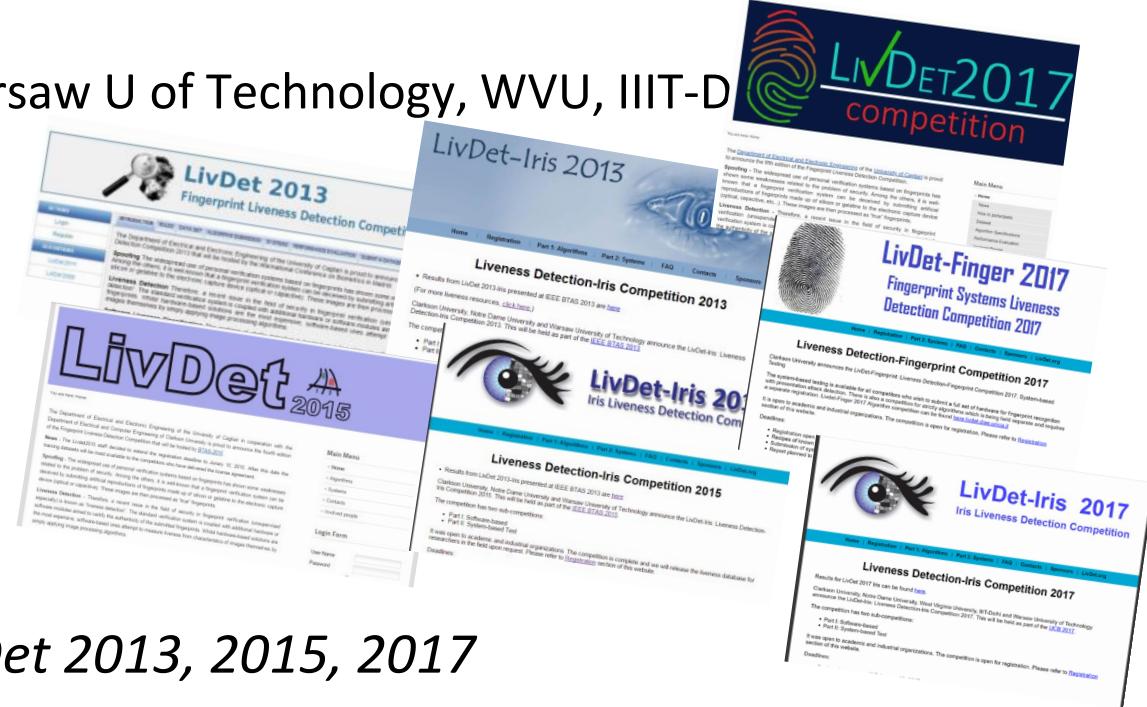
- Liveness Detection Competitions
  - Sense of the State of the Art in the Field
  - Publically available databases to support R&D (even after competitions)
  - Co-host: Fingerprint—Clarkson U & U of Cagliari;
  - Iris—Clarkson U, Notre Dame University & Warsaw U of Technology, WVU, IIIT-D



- *LivDet 2009*
  - Fingerprint Algorithms



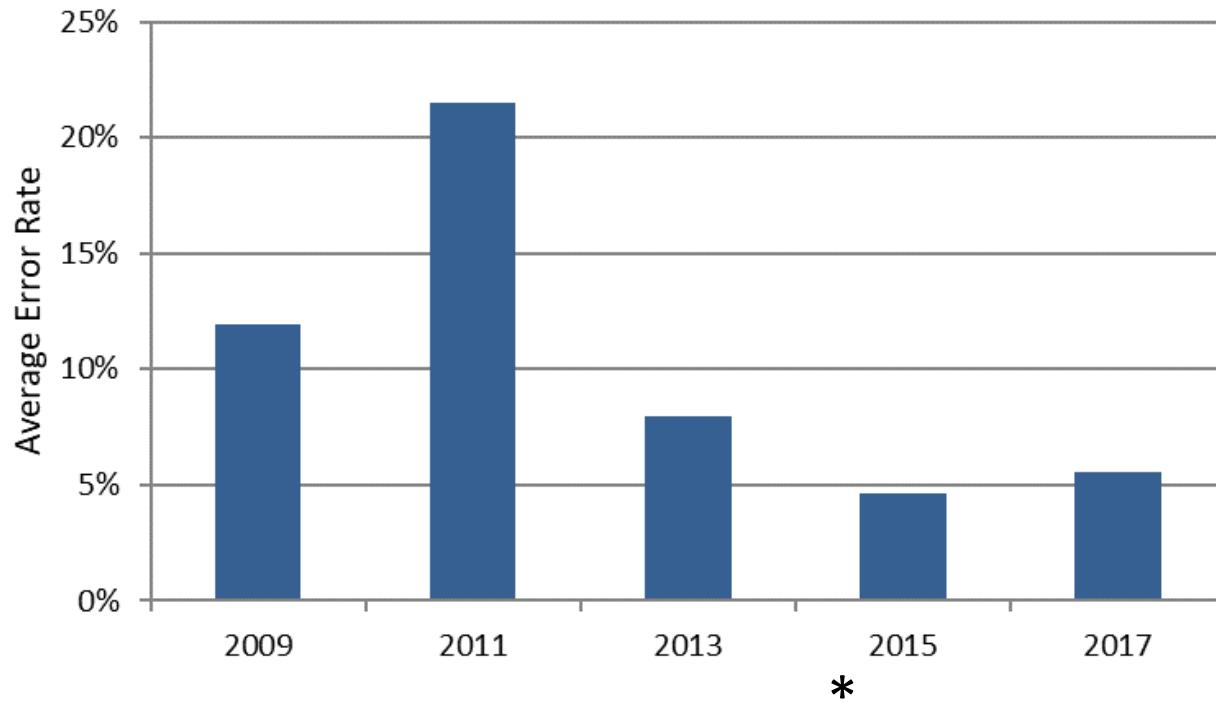
- *LivDet 2011*
  - Fingerprint Algorithms
  - Fingerprint Systems



- *LivDet 2013, 2015, 2017*
  - Fingerprint Algorithms
  - Fingerprint Systems
  - Iris Algorithms

<http://livdet.org>

# LivDet over the years (Fingerprint)



Average of APCER and BPCER for top two performers across all databases tested in LivDet competitions hosted 2009, 2011, 2013, 2015, 2017.

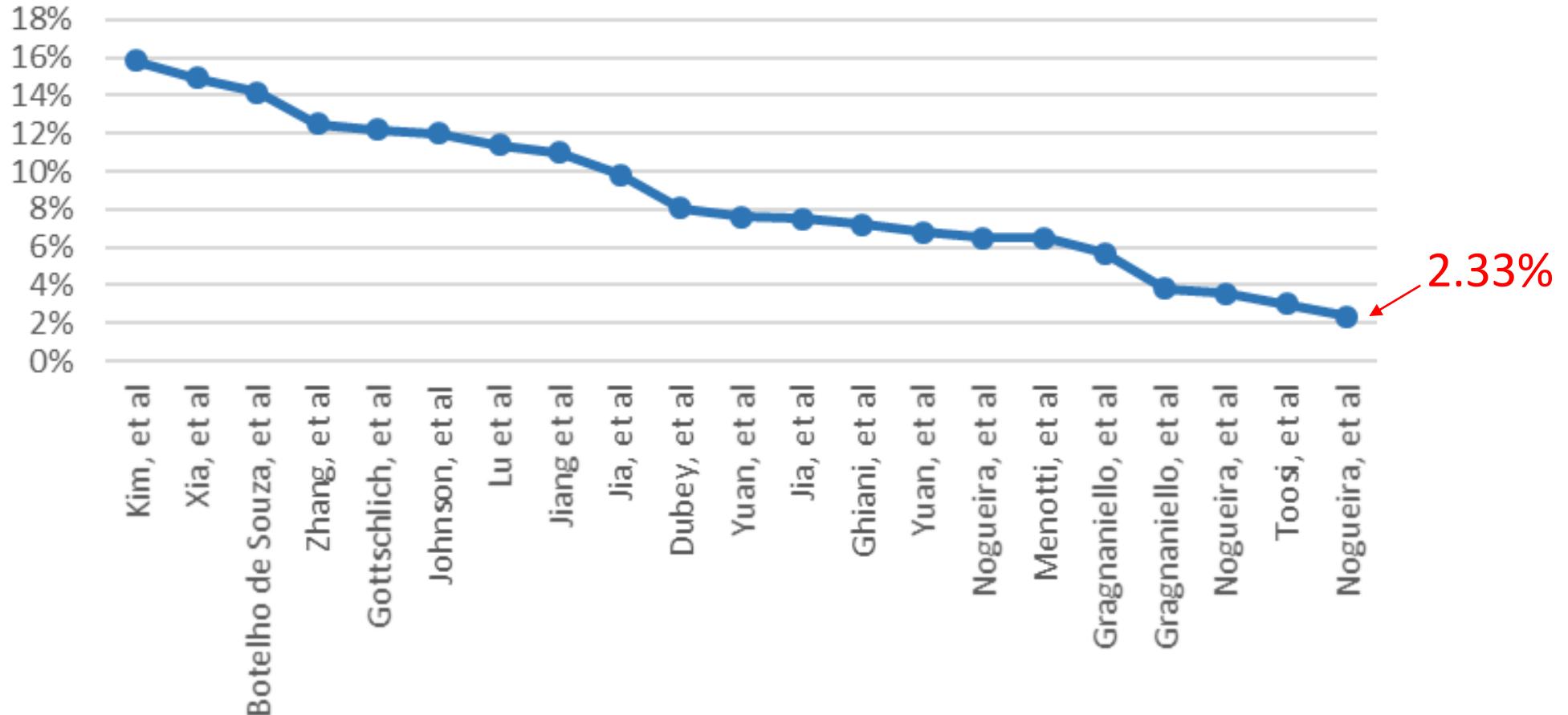
Ghiani, L., Yambay, D.A., Mura, V., Marcialis, G.L., Roli, F. and Schuckers, S.A., 2017. Review of the Fingerprint Liveness Detection (LivDet) competition series: 2009 to 2015. *Image and Vision Computing*, 58, pp.110-128.

\*Crossmatch removed

# Results on LivDet data (after test set release)

\*Sampling of papers

ACE for LivDet 2013 Dataset (After Test Set Release)



*ACE: Average Classification Error Rate*

# RSA® Conference 2019

**Authentication Technology Landscape**

**Biometric Presentation Attacks**  
(Methods, Framework)

**Next Gen Technology**  
(The role of liveness in detection)

**Benchmarking** (Competitions, Datasets)

**Standards & Requirements** (ISO, platforms)

**Certification**  
(FIDO, Common Criteria)



# ISO Standards for PAD

- ISO/IEC CD 30107, Information Technology — Biometrics -- Presentation Attack Detection
  - Part 1 2016
  - Part 2 2016
  - Part 3 2017
- PAD sub-system metrics:
  - Attack Presentation Classification Error Rate (APCER) – Spoof
  - Bonafide Presentation Classification Error Rate (BPCER) - Live
- Performance metrics
  - False non-match rate, false match rate
  - AND **imposter attack presentation match rate**
- Tradeoff between the three

# Industry Requirements

- Microsoft Windows Hello biometric requirements
  - FAR < 0.002%.
  - Effective, real world FRR with antispoofing or liveness detection <10%.
- Google
  - “MUST have a false acceptance rate not higher than 0.002%.
  - [SR] Are STRONGLY RECOMMENDED to have a spoof and imposter acceptance rate not higher than 7%.
  - [C-1-5] MUST rate limit attempts for at least 30 seconds after five false trials for fingerprint verification.”

Windows Hello biometrics requirements, 05/01/2017, Accessed 9/26/2018.

<https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/windows-hello-biometric-requirements>

Compatibility Definition, Android 9, August 8, 2018, Google, Accessed 9/26/2018.

<https://source.android.com/compatibility/android-cdd.pdf>

# RSA® Conference 2019

**Authentication Technology Landscape**

**Biometric Presentation Attacks**  
(Methods, Framework)

**Next Gen Technology**  
(The role of liveness in detection)

**Benchmarking** (Competitions, Datasets)

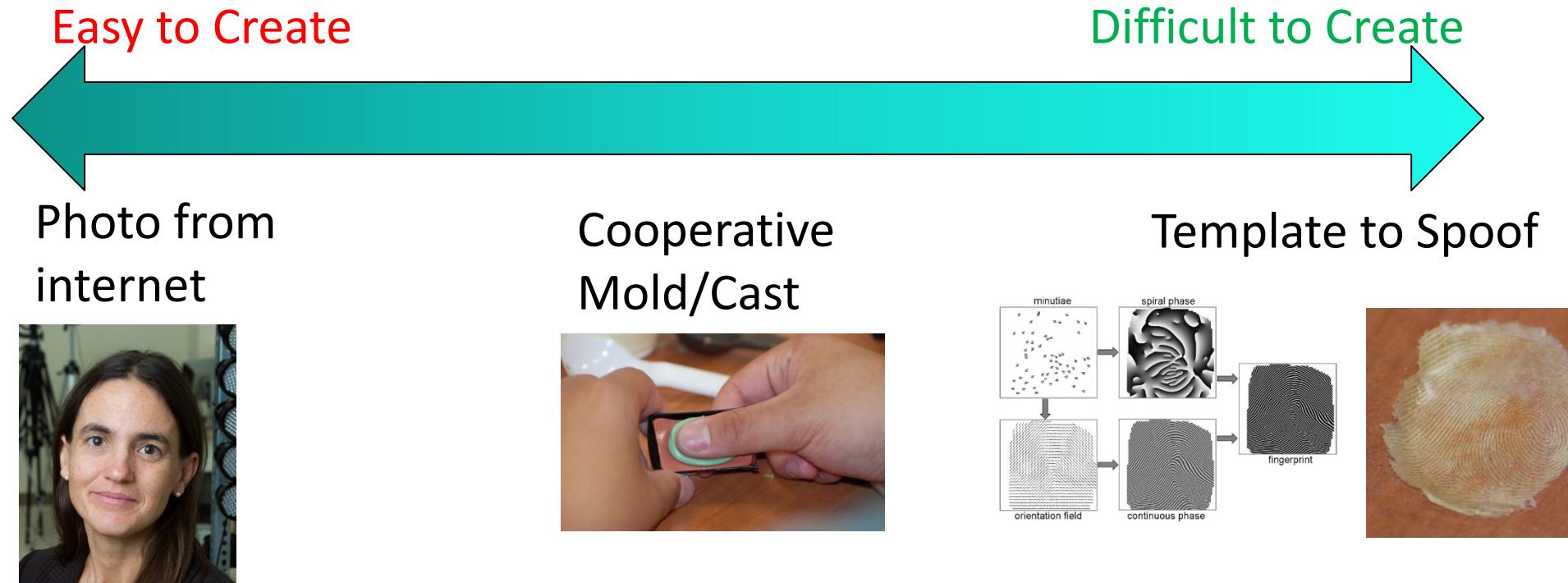
**Standards & Requirements** (ISO, platforms)

**Certification**  
(FIDO, Common Criteria)



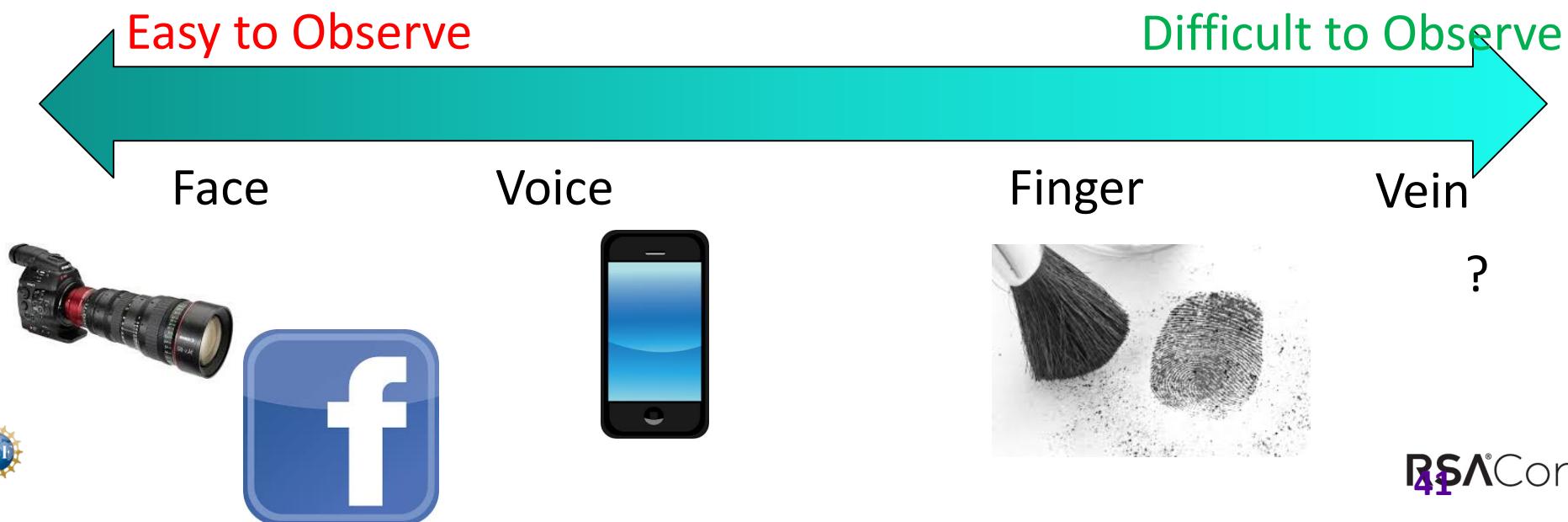
# Spoofing and Relative “Difficulty”

- How difficult is create a spoof?
- How much time/money? How much expertise/skill?



# Spoofing and Relative “Observability”

- How difficult is it to capture the biometric from an individual without their knowledge?
- From a distance? Over the internet?
- Requirements for liveness detection higher if biometric is more “observable”



# Certification

- BSI Certification based on Common Criteria
  - Morpho 2013
  - Dermalog 2018



e.g., "Morpho, Common Criteria Certification for Fake Finger Detection", July 2013

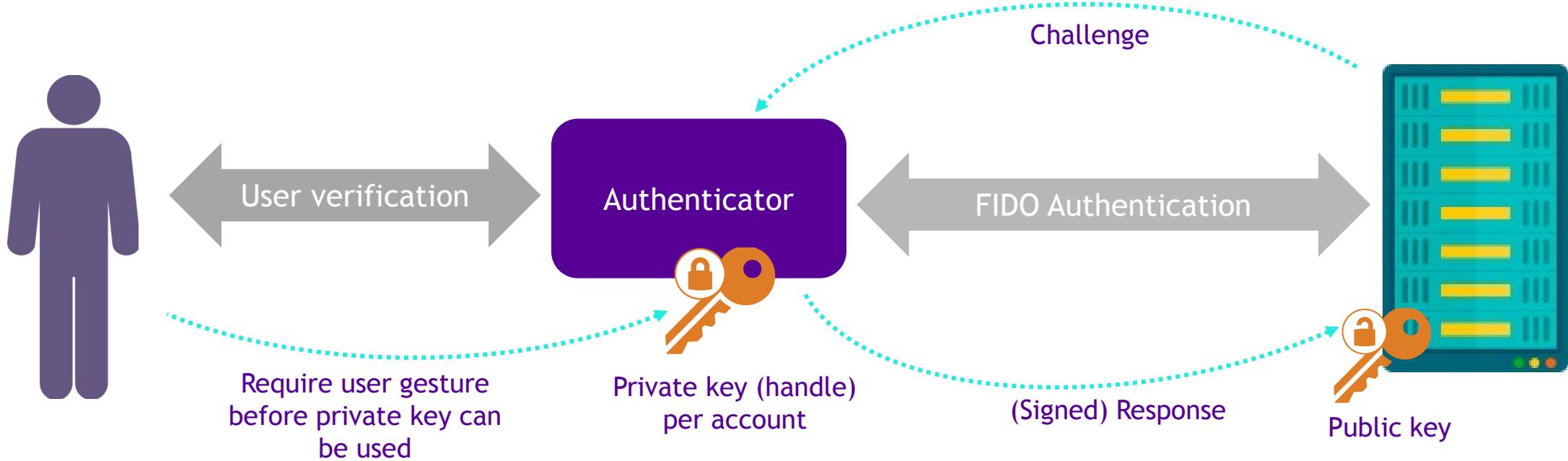
Fingerprint Spoof Detection Protection Profile based on Organizational Security Policies (FSDPP\_OSP),  
Version 1.7, 27 November 2009, BSI-CC-PP-0062-2010

BSI issues Common Criteria certificate for DERMALOG fingerprint scanner, Aug 23, 2018  
<https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/CC-Zertifikat-Dermalog-220818.html>



## FIDO Alliance Biometric Certification Program (Mobile)

# HOW DOES FIDO WORK?



# FIDO IS “HIGH-ASSURANCE STRONG AUTHENTICATION”

High-assurance strong authentication =

- ✓ Use of two + factors 
- ✓ At least one leverages public key cryptography 
- ✓ Not susceptible to phishing, man-in-the-middle and/or other attacks targeting credentials

# FIDO Certification Purpose

The FIDO Biometric Certification Program is intended to certify biometric components and/or subsystems and is independent from Authenticator Certification Program.



**fido**  
ALLIANCE simpler stronger authentication

简体中文 English 日本語

What is FIDO? Blog Get Involved  Search...

ABOUT TECHNOLOGY ADOPTION PARTICIPATE FIDO CERTIFICATION NEWS & EVENTS RESOURCES

## FIDO Alliance Launches Biometrics Certification Program

September 6, 2018

Program certifies that biometric recognition systems meet globally recognized performance standards and are fit for commercial use

MOUNTAIN VIEW, Calif., September 6, 2018 – Biometric user verification has become a popular way to replace passwords and PINs, but the lack of an industry-defined program to validate performance claims has led to concerns over variances in the accuracy and reliability of these solutions. To fill this gap, the [FIDO Alliance](#) today announced its [Biometric Component Certification Program](#) – the first such program for the industry at large. The program utilizes accredited independent labs to certify that biometric subcomponents meet globally recognized performance standards<sup>[i]</sup> for biometric recognition performance and Presentation Attack Detection (PAD)<sup>[ii]</sup> and are fit for commercial use.

The FIDO Alliance aims to deliver several benefits to providers and users of biometric recognition systems through the new Biometric Component Certification Program. Until now, due diligence was performed by enterprise customers who had the capacity to conduct such reviews. This required biometric vendors to repeatedly prove performance for each customer. The FIDO Alliance program allows vendors to test and certify only once to validate their system's performance and re-use that third-party validation across their potential and existing customer base, resulting in substantial time and cost savings. For customers, such as regulated online service providers, OEMs and enterprises, it provides a standardized way to trust that the biometric systems they are relying upon for fingerprint, iris, face and/or voice recognition can reliably identify users and detect presentation attacks.

"The lack of standards has long been an issue in biometrics, forcing security professionals to 'get deep in the weeds' to not only understand the attributes that are important but subsequently evaluate vendors on those attributes. An unbiased Alliance-based certification program expedites solution evaluation for companies but also eases adoption by providing assurances to the C-suite of proper choice," said Frank Dickson, research vice president, IDC.

"With biometrics being a popular option for mobile and web applications implementing FIDO Authentication, there is a growing need for those service providers to appropriately assess the risk of fraud from lost or stolen devices. While border control and law enforcement markets have mature assessment programs for their biometric systems, we were surprised that no such program existed for this rapidly growing consumer market," said Brett McDowell, executive director of the FIDO Alliance. "As an organization that is driven by our members' real-world business requirements, and already experienced at delivering globally scalable high-quality certification programs, the FIDO Alliance was the organization our members chose to fill this gap in the market."

# BIOMETRIC PERFORMANCE REQUIREMENTS

- Evaluation framework and certification program – Independent Laboratory Verification of Vendor Claims
- References ISO Standards
  - 19795 Biometric performance testing and reporting
  - 30107 Presentation attack detection
- Testing plan focuses on:
  - Consistent set of tests for different implementations under test submitted by vendors
  - Supporting different modalities of biometrics
  - False accept rate (FAR)
  - False reject rate (FRR)
  - Imposter attack presentation match rate (IAPMR) (*artefact success rate*)
- Testing program will be implemented by approved third party testing laboratories (accredited by FIDO Alliance)

# PAD Requirements

“PAD Light”...

Provide guidelines for testing low level spoof attacks (those which require minimal expertise)

Testing performed on biometric sub-system provided by vendor

Measures Imposter Attack Presentation Match Rate (IAPMR)

- ▶ IAPMR: Proportion of presentation attacks in which the target reference is matched. From ISO 30107 Part 3
- ▶ Each spoof type measured separately

Attacks triaged into levels

- ▶ Low level attacks require less time/knowledge/equipment
- ▶ Testing will only include “known” attacks
- ▶ “Unknown” attacks reserved for future certification

Evaluation Process

- ▶ Each subject enrolled as non-artifact
- ▶ Testing with at least 10 PAI species\* per enrolled subject
- ▶ “Unknown” attacks reserved for future certification

.

**\*Presentation Attack Instrument (PAI) -Biometric characteristic or object used in a presentation attack**

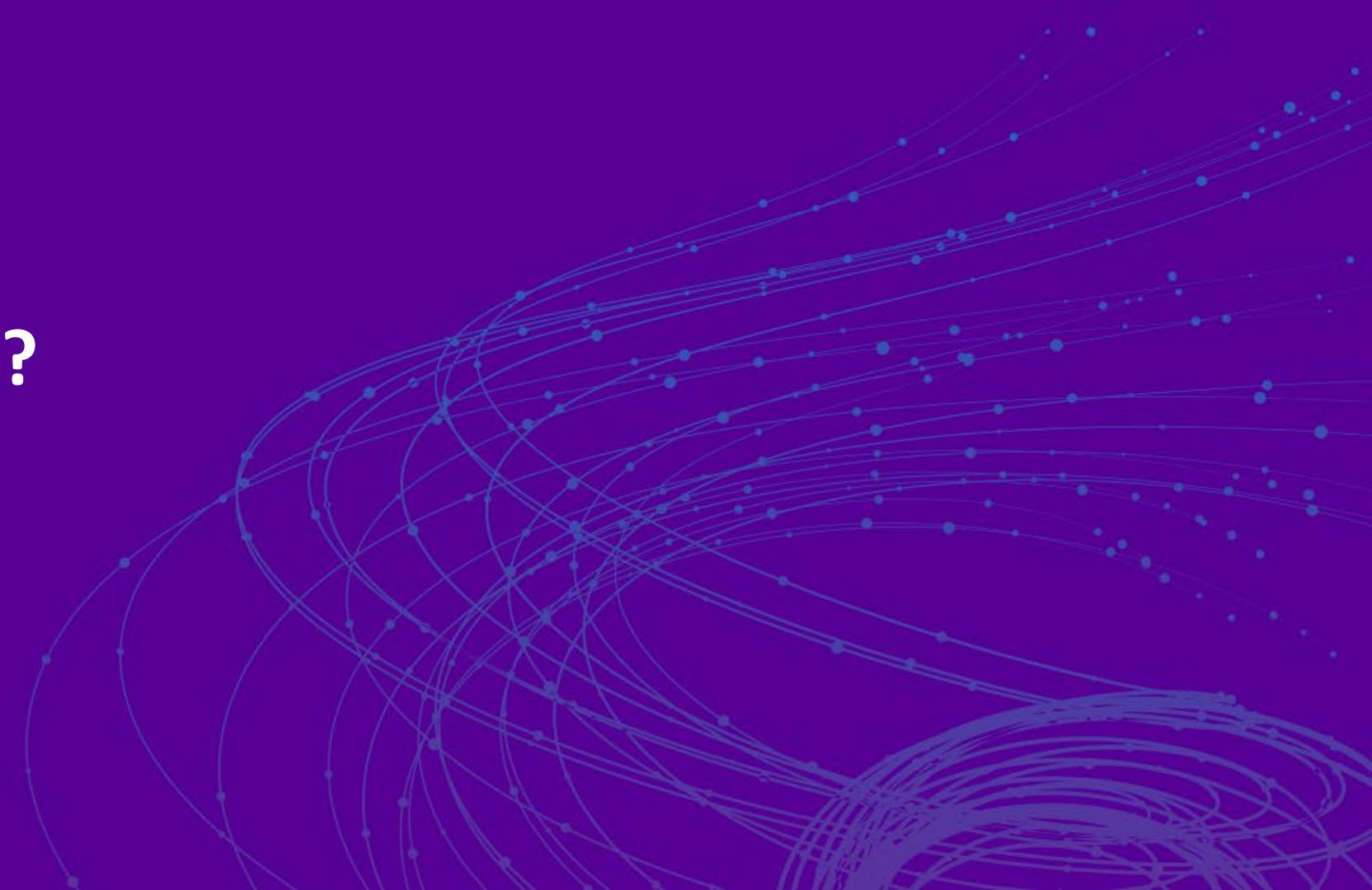
**PAI Species - Class of presentation attack instruments created using a common production method and based on different biometric characteristics (ISO/IEC 30107-3)**

## Spoof Type Triaged by Attack Potential

		Fingerprint	Face	Iris/Eye	Voice
<b>Level A</b>	<p><b>Time:</b> &lt;1 day  <b>Expertise:</b> layman  <b>Equipment:</b> standard</p> <p><b>Source of biometric characteristic:</b> easy to obtain</p>	paper printout, direct use of latent print on the scanner	paper printout of face image, mobile phone display of face photo	paper printout of iris image, mobile phone display of iris photo	replay of audio recording
<b>Level B</b>	<p><b>Time:</b> &lt;7 days  <b>Expertise:</b> proficient  <b>Equipment:</b> standard, specialized</p> <p><b>Source of biometric characteristic:</b> moderate</p>	<p>fingerprints made from artificial materials such as gelatin, silicon.</p> <p>Lift of latent print from elsewhere, stolen fingerprint image</p> <p>Cooperative molds - out of scope</p>	<p>paper masks, video display of face (with movement and blinking)</p>	<p>video display of an iris (with movement /blinking); paper printout w/ contact lens/doll eye</p>	<p>replay of audio recording of specific passphrase, voice mimicry</p>
<b>Level C</b>	<p><b>Time:</b> &gt;7days  <b>Expertise:</b> expert(s)  <b>Equipment:</b> specialized, bespoke</p> <p><b>Source of biometric characteristic:</b> difficult</p>	3D printed spoofs	<p>silicon masks, theatrical masks,</p>	<p>contacts lens or prosthetic with a specific pattern</p>	<p>voice synthesizer</p>
		3D fingerprint information from subject	3D face information from subject	high quality photo in Near IR	<p>multiple recordings of voice to train synthesizer</p>

# RSA® Conference 2019

## What's Next?



# Challenges

- Adoption of Biometric Certification
  - Certification program is relatively new (Fall 2018)
  - Need to drive adoption
  - Ask if biometric products are certified
- Address Zero-Day Attacks (“Unknown” attacks)
  - Part of LivDet evaluations
  - Focus of USA IARPA Odin effort
  - Expected to become part of future FIDO biometric certification

## IARPA LAUNCHES "ODIN" PROGRAM TO HARDEN BIOMETRIC TECHNOLOGY AGAINST ATTACKS

[Recent News](#)

Thursday, 19 October 2017 17:23

[Print](#)

[Reports & Publications](#)

[Press Releases](#)

[Speeches & Interviews](#)

[Congressional Testimonies](#)

[IC in the News](#)

[CTIIC Newsroom](#)

[NCSC Newsroom](#)

[NCPC Newsroom](#)

[NCTC Newsroom](#)

[Photos](#)

[Seals & Graphics](#)



NEWS RELEASE

FOR IMMEDIATE RELEASE  
ODNI News Release No. 22-17  
October 19, 2017

IARPA Launches "Odin" Program to Harden Biometric Technology Against Attacks

WASHINGTON – The Intelligence Advanced Research Projects Activity, within the Office of the Director of National Intelligence, announces today a multi-year research effort to develop and evaluate biometric presentation attack detection technologies to ensure the integrity of biometric security systems. If successful, the Odin program will provide solutions to the Intelligence Community and its partners to remediate critical vulnerabilities in today's biometric recognition

USA, IARPA Odin Program, <https://www.iarpa.gov/index.php/research-programs/odin>

# Apply what you have learned today

- Next week you should:
  - Identify applications of biometric recognition in your organization
  - Determine if biometric templates are locally stored
  - Explore authentication based on locally stored biometrics (e.g. FIDO)
- In the first three months following this presentation you should:
  - Understand security risks associated with presentation attacks for your organization
  - Define appropriate biometric requirements for organization or product
- Within six months you should:
  - Adopt authentication based on locally stored biometrics which your organization's requirements
  - Require vendors to have completed biometric certification

# 1993



*"On the Internet, nobody knows you're a dog."*

Peter Steiner, The New Yorker, July 5, 1993

# 2015

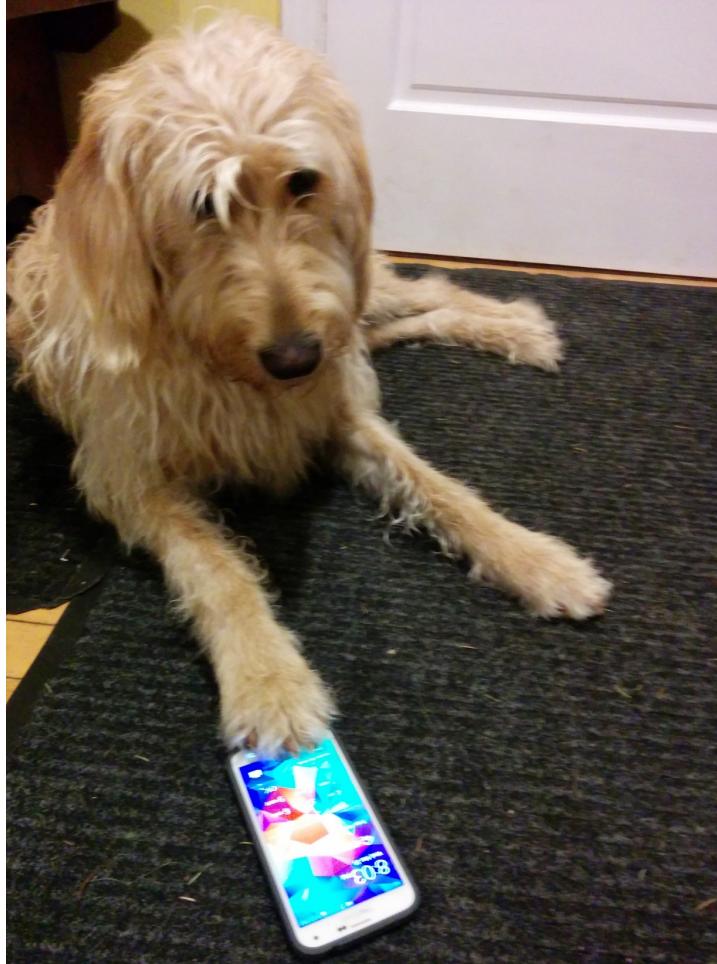


Kaanran Hafeez, The New Yorker, February 23, 2015

# 20??

*Can we have it all?*

Identity  
technologies  
without revealing  
private data



# RSA® Conference 2019

## Questions?

Thank you!