# Multimodal Biometrics for Enhanced Mobile Device Security

By Mikhail Gofman

# Biometrics

- Science of identifying people based on what they are:
  - Physical Traits (e.g., face, fingerprint…)
  - Behavioral Traits (e.g., speech, gait, writing…)
- ***In theory strongest form of authentication***
  - *Faking biometrics is supposed to be difficult*

# Mobile Device Biometrics

- Practically in every modern smartphone
- A natural choice for mobile security:
  - **Passwords/PINs:** users pick easily guessable words
  - **Security Tokens/Smartwatches/etc:** not always convenient for unlocking a device
  - With biometrics users do not have to remember or carry anything!
- ***But how secure are current systems?***

# Mobile Biometrics…the facts of life

- We don’t really know…
- Manufacturers (e.g., iPhone, Samsung, etc) publish few details…:
    - What is verification accuracy? How was it measured?
    - What type of biometric data was it tested on (diverse individuals, different conditions etc)?
        - ‘’We tested it on some people in our office’’
    - How resistant is the system to faked (i.e., spoofed) biometrics?
    - Underlying matching algorithms? No details…

# Mobile Biometrics: Expectation vs Reality

- **Fingerprints:**
  - iPhone 5s TouchID bypassed within a week of release…similar issues with other iPhones
  - All Samsung Galaxy fingerprint readers bypassed with fake fingers

**Samsung S10 Expectation: "next generation vault-like security"**

**Samsung S10 Reality:**

**The Samsung Galaxy S10's ultrasonic fingerprint scanner is hacked**

Graham Cluley
11:38 pm, April 10, 2019

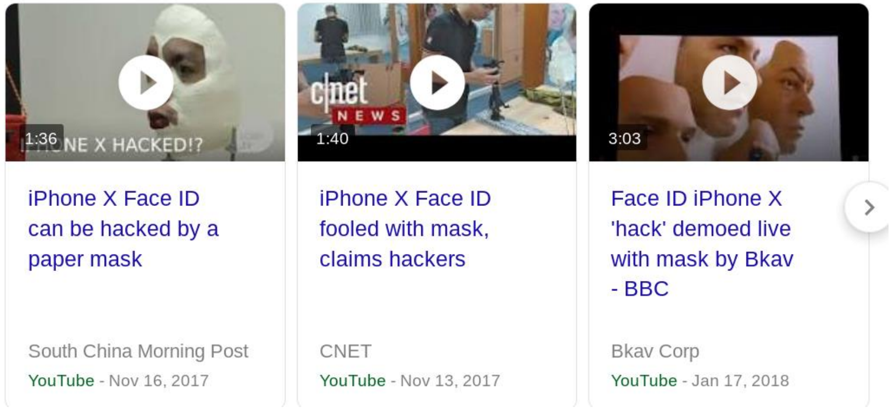
Source: https://www.grahamcluley.com

# Mobile Biometrics: Expectation vs Reality

- **Face Recognition:** iPhone’s FaceID

**Expectation:** **“ Face ID securely unlocks iPhone X. It provides intuitive and secure authentication enabled by the TrueDepth camera…” apple.com**

**Reality:** **3D Masks, kids unlocking parents’ phones, etc**



iPhone X Face ID can be hacked by a paper mask

South China Morning Post

YouTube - Nov 16, 2017

iPhone X Face ID fooled with mask, claims hackers

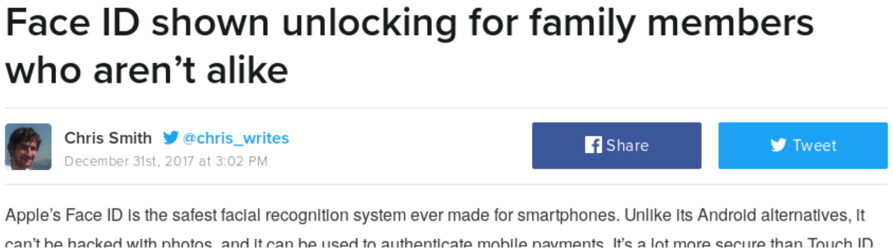
CNET

YouTube - Nov 13, 2017

Face ID iPhone X 'hack' demoed live with mask by Bkav - BBC

Bkav Corp

YouTube - Jan 17, 2018



## Face ID shown unlocking for family members who aren’t alike

Chris Smith @chris_writes
December 31st, 2017 at 3:02 PM

Share Tweet

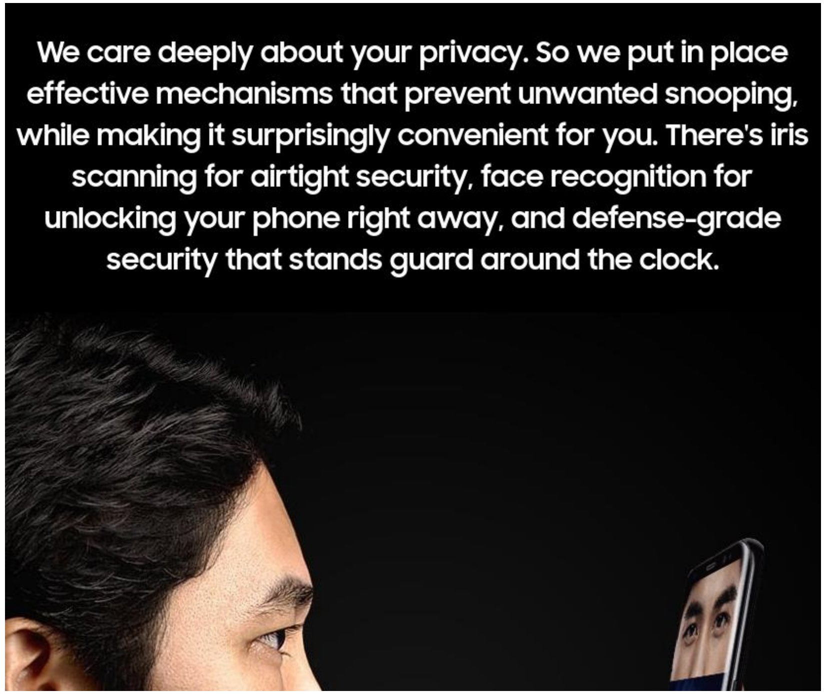
Apple’s Face ID is the safest facial recognition system ever made for smartphones. Unlike its Android alternatives, it can’t be hacked with photos, and it can be used to authenticate mobile payments. It’s a lot more secure than Touch ID

Source: https://bgr.com

# Mobile Biometrics: Expectation vs Reality

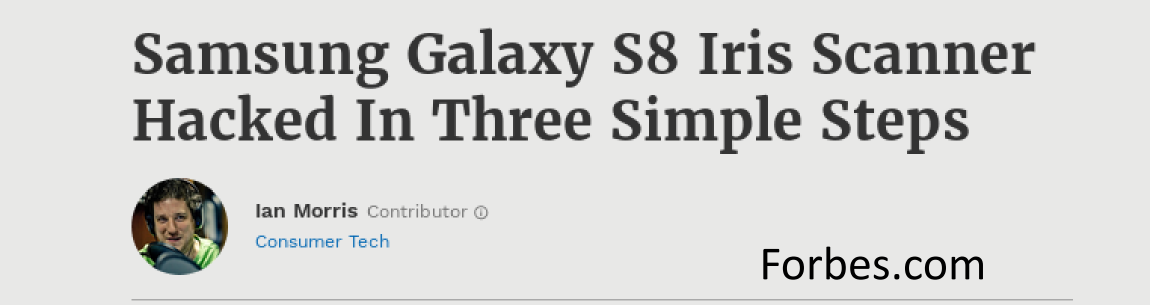
- Iris Recognition: a feature in Samsung Galaxy S8/S8+ and S9/S9+:

**Expectation: Samsung:**



We care deeply about your privacy. So we put in place effective mechanisms that prevent unwanted snooping, while making it surprisingly convenient for you. There's iris scanning for airtight security, face recognition for unlocking your phone right away, and defense-grade security that stands guard around the clock.

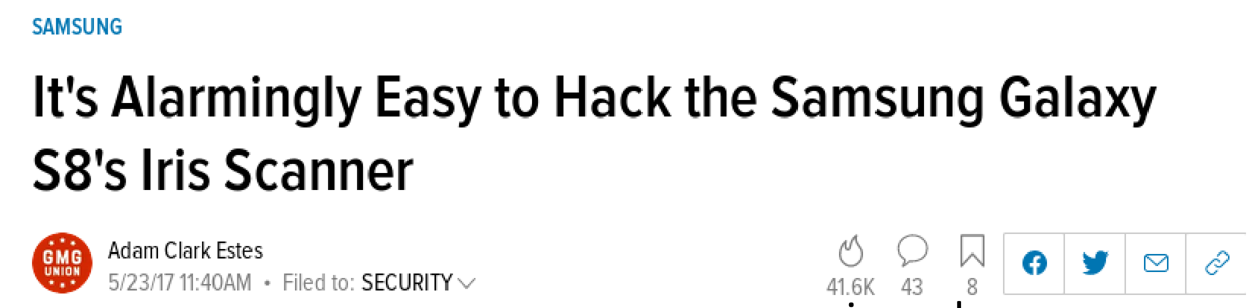
**Reality:**



Samsung Galaxy S8 Iris Scanner Hacked In Three Simple Steps

Ian Morris Contributor
Consumer Tech

Forbes.com



SAMSUNG

It's Alarmingly Easy to Hack the Samsung Galaxy S8's Iris Scanner

Adam Clark Estes
5/23/17 11:40AM • Filed to: SECURITY

gizmodo.com

# Is Mobile Biometric Security a Shattered Illusion?

- Researchers (including us) do not think so…just more is needed
- Remember?

  ***In theory strongest form of authentication***

  - *Faking biometrics is supposed to be difficult*
- **Let’s make it difficult!**

# Detect Spoofed Biometrics

- Researchers (including us) do not think so…just more is needed
- Anti-spoofing techniques to detect fake biometrics
  - **Hardware:** sensors that detect whether the biometrics are coming from a live human (pulse, skin galvanic response, ability to perform gestures, heat maps, depth sensing, internal skin structure, etc)
  - **Software:** detecting spoofing artifacts in images, analysis of sweat pores in fingerprints,  3D image analysis, color and motion analysis
  - Impressive array of techniques exist in literature…are they being applied to real-world mobile devices?

# Novel Biometric Modalities

- Develop other modalities that are naturally difficult to spoof?
  - Brainwaves?
  - DNA?
  - Behavioral biometrics?
  - Cardiac Characteristics?
- Emerging research area

# Multimodal Biometrics

- Combine the strengths of multiple biometrics!
- ECSCYBER researchers specialize in this area
- **Key approach:** combine features from multiple modalities to form a new modality with features from multiple:
  - Attacker needs to spoof multiple modalities (…but there are pitfalls)
  - More identifying information is required to prove identity
  - More robust verification accuracy in uncontrolled conditions (e.g., skewed camera angles, distorted images, noise interference…etc)

# Multimodal Biometrics

- What we have done?
  - – Novel techniques for combining features from face and voice on mobile and IoT devices (past 5 years)
    - Classical machine learning, ensemble, and deep learning techniques
  - – Deep learning techniques to combine features from face and ear
  - – Optimizing efficiency of mobile biometric system through integration of Field Programming Gate Arrays (FPGAs)

# Multimodal Biometrics

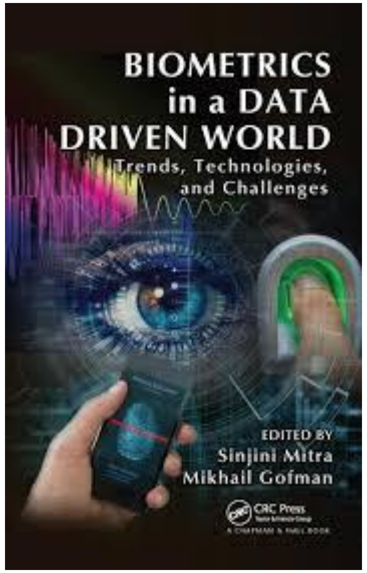
- What we found?
  - **Face in voice:** Combining features from face and voice using Discriminant Correlation Analysis (DCA) resulted in 52.45% and 81.62% improvement when compared to using only face or only voice in real-world uncontrolled conditions that significantly distort biometric image quality. See below for details:
    - https://ieeexplore.ieee.org/abstract/document/8666599
    - https://search.proquest.com/openview/59f183486cb11685988188170f4c28c4/1?pq-origsite=gscholar&cbl=1976342
    - https://m-cacm.acm.org/magazines/1816/4/180169-multimodal-biometrics-for-enhanced-mobile-device-security/abstract
  - **Face and Ear:** significant improvements attained (publication in progress)

# Multimodal Biometrics

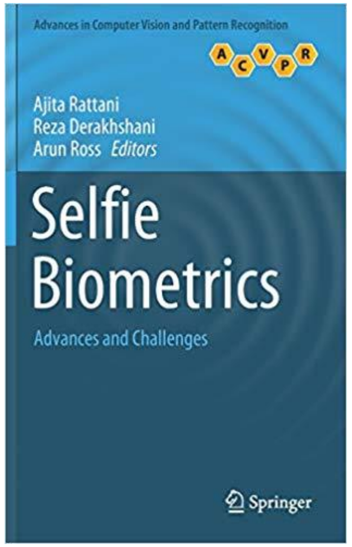
- **Future:**
  - Combining 3D face and ear features
  - IoT-specific techniques for multimodal biometrics
  - Mobile device multimodal biometrics for applications in education

# Multimodal Biometrics

- Our and publications for more information:


BIOMETRICS in a DATA DRIVEN WORLD
Trends, Technologies, and Challenges
EDITED BY
Sinjini Mitra
Mikhail Gofman
CRC Press

**Book:** Sinjini Mitra and Mikhail Gofman, eds. Biometrics in a Data Driven World: Trends, Technologies, and Challenges. CRC Press, 2016.



**Book chapter:** Mikhail Gofman, Sinjini Mitra, Yu Bai, and Yoonsuk Choi. "Security, Privacy, and Usability Challenges in Selfie Biometrics." In Selfie Biometrics, pp. 313-353. Springer, Cham, 2019.

# Multimodal Biometrics

- Conference and Journal Publications:
  - Please see http://www.fullerton.edu/cybersecurity/research/publications.php for a complete list

# Don’t Forget: Research Involvement is a HIP

- This work involved more than 25 graduate and undergraduate students!
- Experiences gained from research involvement resulted in students receiving jobs in:
  - Amazon
  - PayPal
  - MITRE
  - Raytheon
  - Pursuing Ph.Ds.

# Thank You! Questions?