Lecture 12: Biometrics

CS 181W

Fall 2022

Recall: Authentication of humans

- Something you know

  secret information (e.g., a password)

- Something you are

  biometrics (e.g., fingerprints)

- Something you have

  possession of a physical device (e.g., a particular phone)

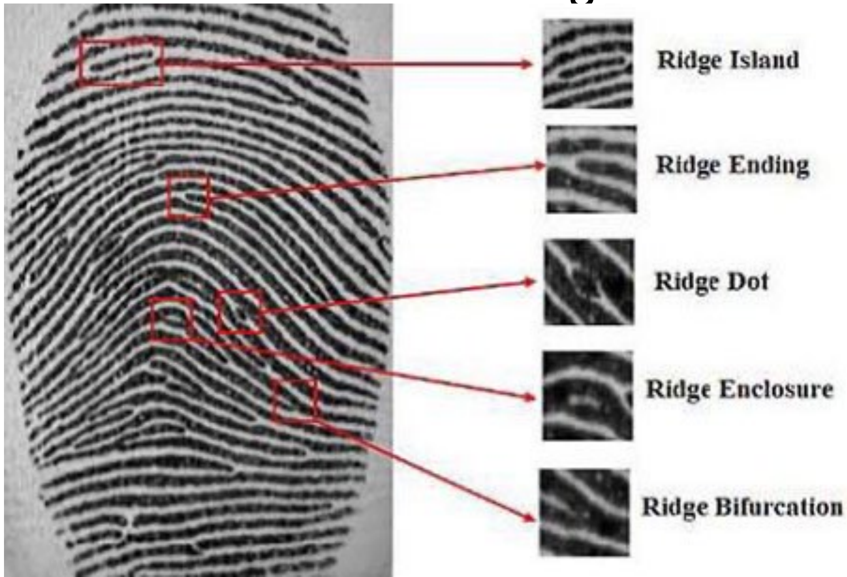
SOMETHING YOU ARE

Biometric

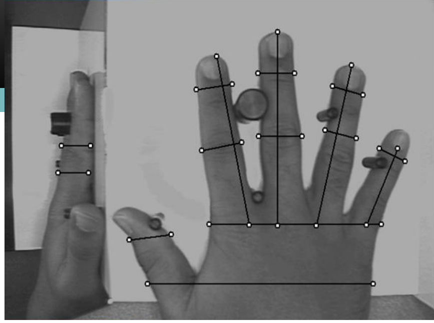
- **Biometric:** measurement of biological and behavioral attributes (something you are)
  - biological attributes can be confounded by behavior
  - biology and behavior is non-constant: variation from one measurement to the next

Example: Fingerprint

- Particular use: California social services
  - prevent applicants for welfare from defrauding state by receiving assistance under multiple identities
- Fingerprint stored as bitmap and as minutae
  - When user authenticates, computer compares minutiae
  - If they match, human additionally reviews bitmap images (about 15 out of 10000 authentications have minutiae match even though fingerprints do not)



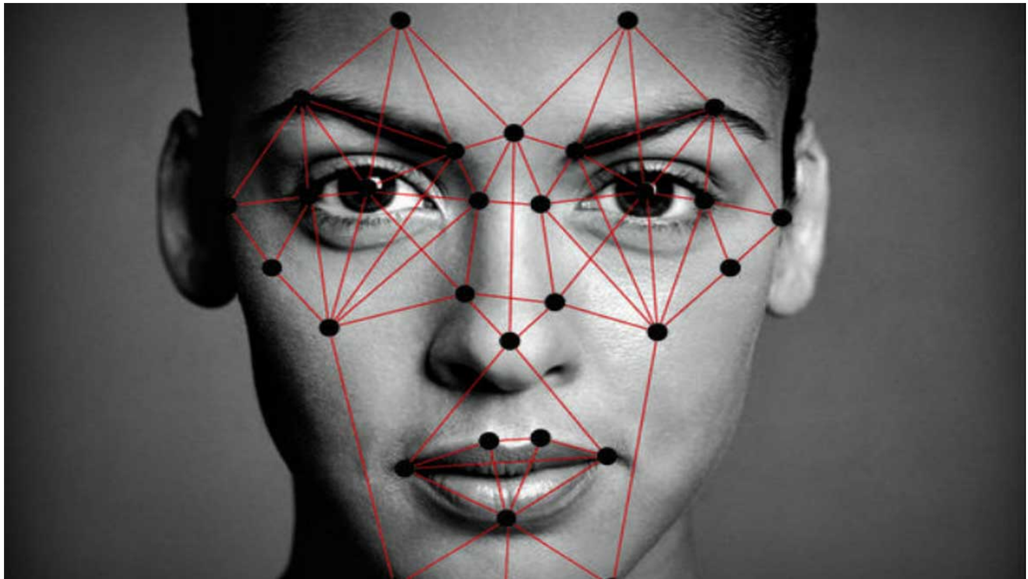
Example: Hand geometry



- Used in 2012 Olympic Games, Walt Disney World, nuclear facilities, data centers, ...
- Camera images palm and side of hand (no texture information)
- Images reduced to (e.g.) 31000 points then 90 measurements then 9 bytes of data
  - Final data not directly related to any source measurements
  - Data stored as a **template** for later comparison
- When user authenticates, another set of images taken
  - If data are close enough to stored template, user deemed authenticated
  - Can adjust threshold per-user, in case some users are difficult to authenticate
- Each time user is authenticated, template is updated to account for change over time

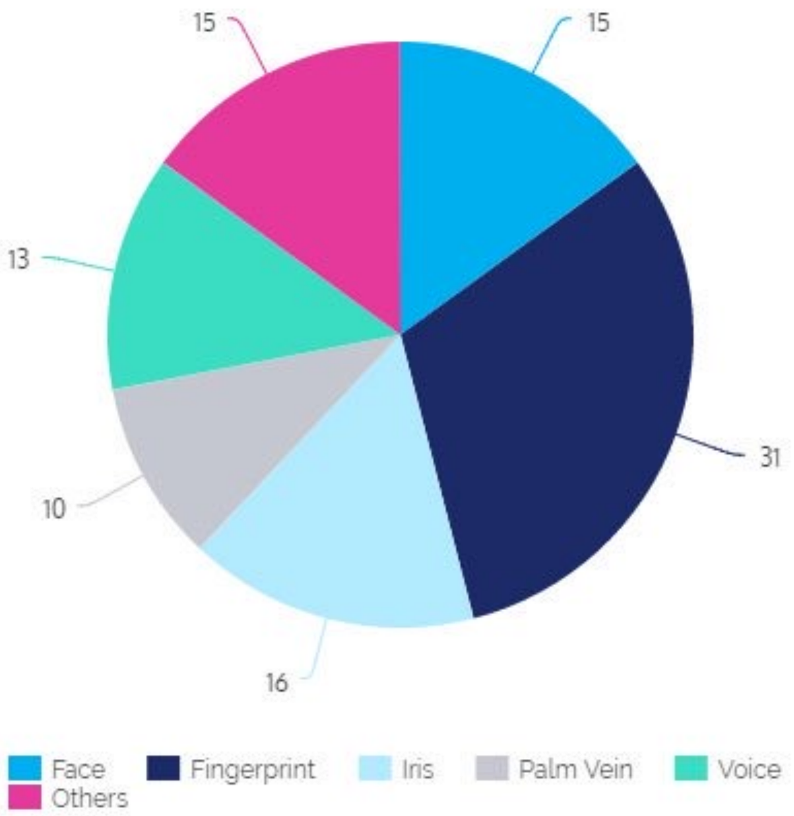
Example: Facial recognition

- Used in border control, Facebook, iPhones
- Operates on 2D image or depth map
- Modern systems use ML classifiers to identify matches
  - Most systems perform poorly on profiles, low-res images
  - Most systems perform less well on women and minorities

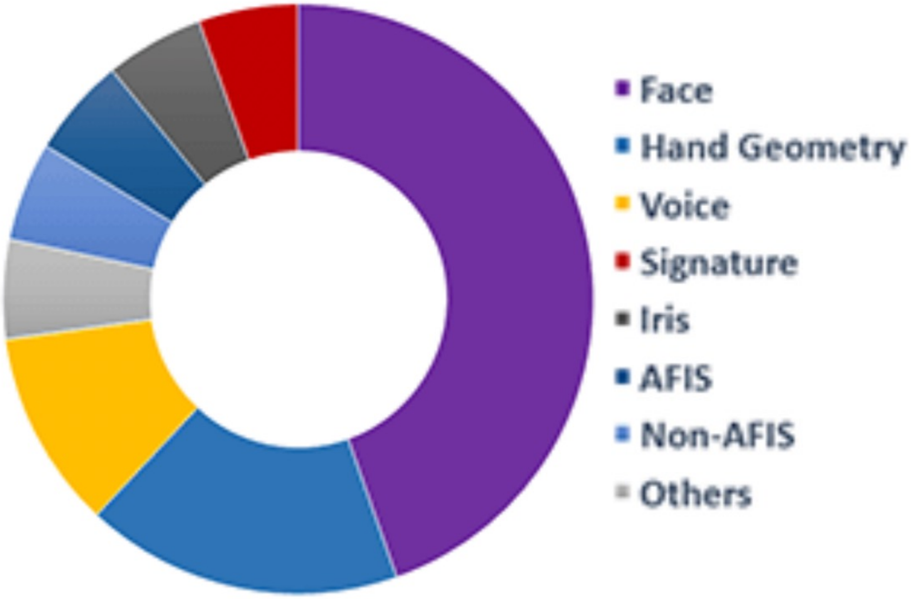


Other Biometrics

2018



2021



Biometric attributes as verifiers

- **Advantages:**
  - Can't lose or forget a biometric
  - Easy to use some biometrics (e.g., facial scan vs. PIN on iPhone)
- **Disadvantages:**
  - Physical process with errors...
  - Updating identities after disclosure is hard (new fingerprints? new retina?)
    - So enrolling a biometric identifier places **permanent trust** in receiver, even if they go bankrupt, retroactively change privacy policies, get taken over by new administration, ...
  - Impossible to be application specific (your hand geometry is the same regardless of what system you use)
  - Fear of negative implications for privacy...

EVALUATING BIOMETRICS

Biometric attributes as verifiers

Requirements:

- Easy to measure
- Identifier
- Small variation over time and measurement
- Acceptable to users
- Difficult to spoof

Biometric	Easy to Measure
Face	High
Voice	High
Fingerprint	Medium
Iris	Medium
Palm vein	High

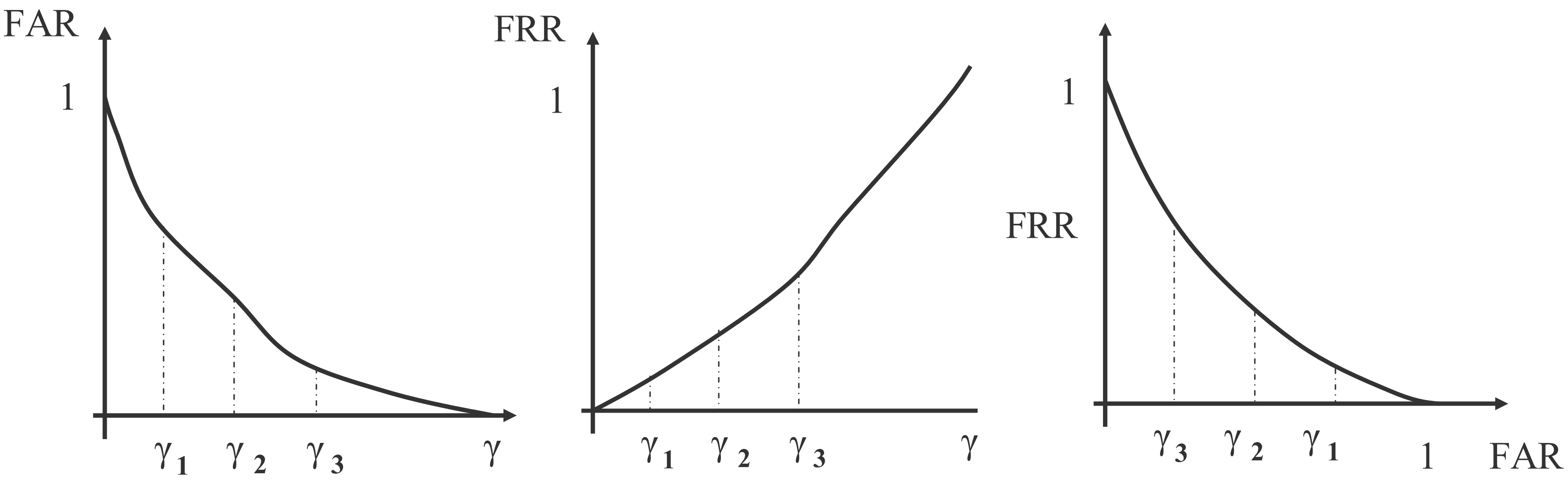
Accuracy

- **False accept:** authenticate a principal with wrong identity
- **False reject:** fail to authenticate a principal under right identity

- Tunable trade off of **sensitivity** between which error is more likely
  - **False acceptance rate (FAR):** percentage of attempts in which imposters are authenticated (with wrong identity)
  - **False reject rate (FRR):** percentage of attempts in which legitimate users are denied authentication

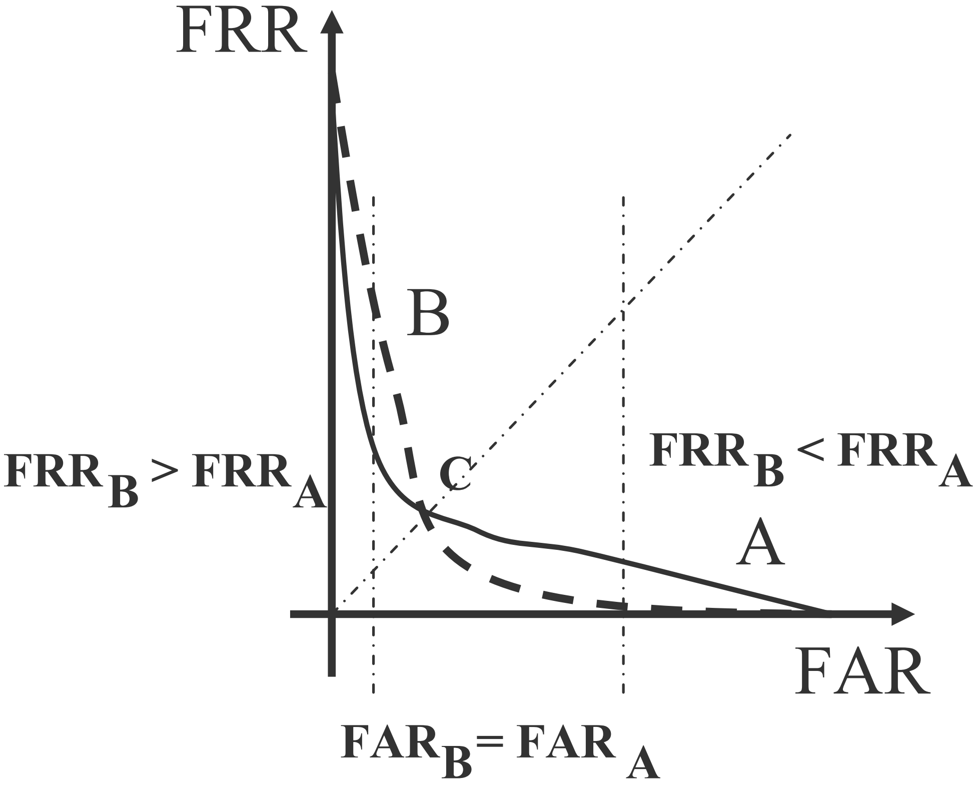
Sensitivity

Receiver operating characteristics (ROC) curve: graph of FRR vs. FAR (or perhaps 1-FAR, perhaps nonlinear axes)



γ = sensitivity

ROC comparison



- Two matchers (A=solid; B=dashed)
- At point C, matchers have same FAR and FRR
- To the left of C, matcher A has lower FRR for same FAR
- To the right, matcher B has lower FRR for same FAR

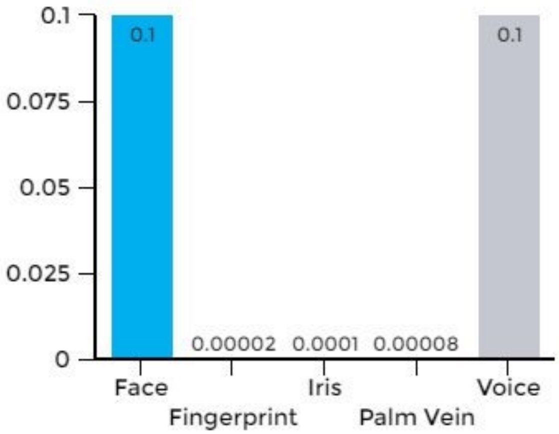
ROC comparison

- **Crossover error rate (CER):** value on ROC at which FAR=FRR (aka *equal error rate, ERR)*
- Many other statistics for comparison possible
  - Anytime a graph is reduced to a single number, we lose information
- *What matters most for biometrics is the use case/threat model*

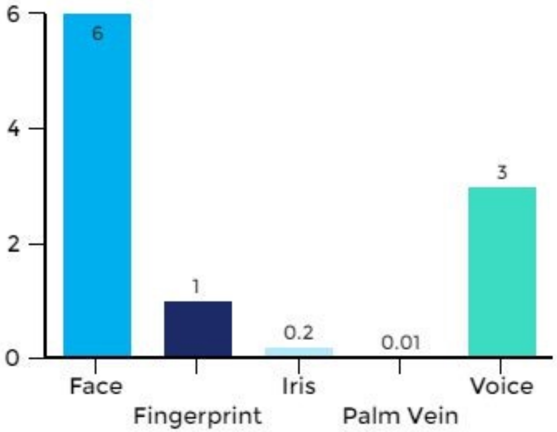
Use cases

- **Entry to military facility:**
  - letting imposters in might be worse than (temporarily) delaying entry of personnel
  - so prefer low false accept rate
- **Entry to hotel lobby:**
  - letting non-guests in might be better than (temporarily) delaying entry of guests
  - so prefer low false reject rate

Comparing Biometric Accuracy



False Acceptance Rate



False Rejection Rate

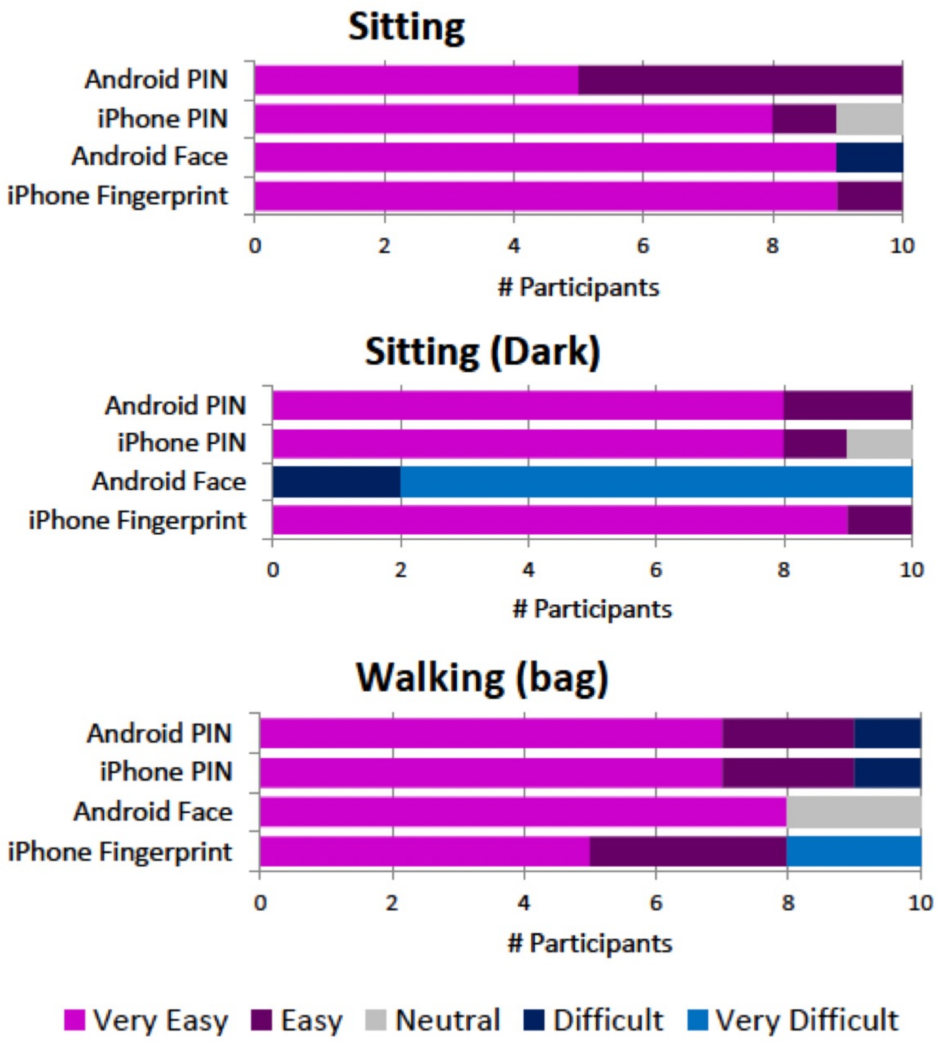
Phone Authentication

- Fingerprints (introduced to iPhone 5S in 2013)
- Facial Recognition (introduced to Android 4.0 in 2011, to iPhone X in 2017)
- PIN

In-person
Within subjects
n = 10

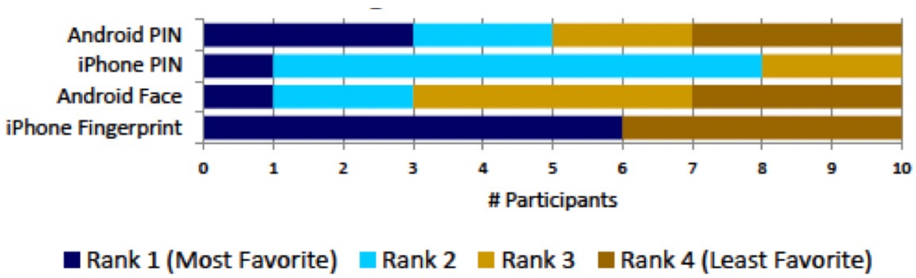
Online study
Survey
n = 198

Perceived Ease of Use


Sitting

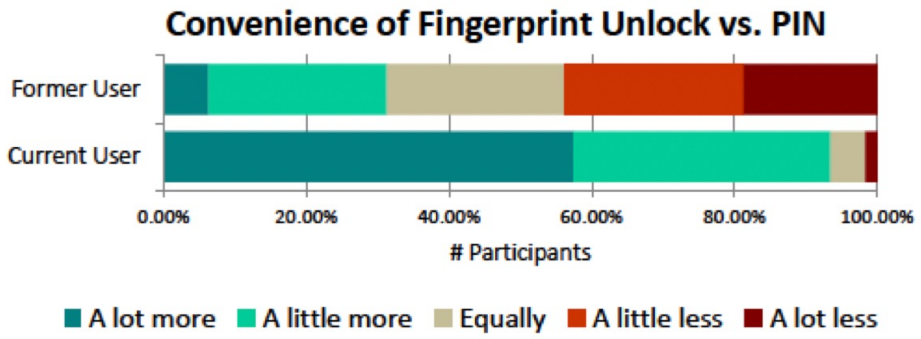
Sitting (Dark)

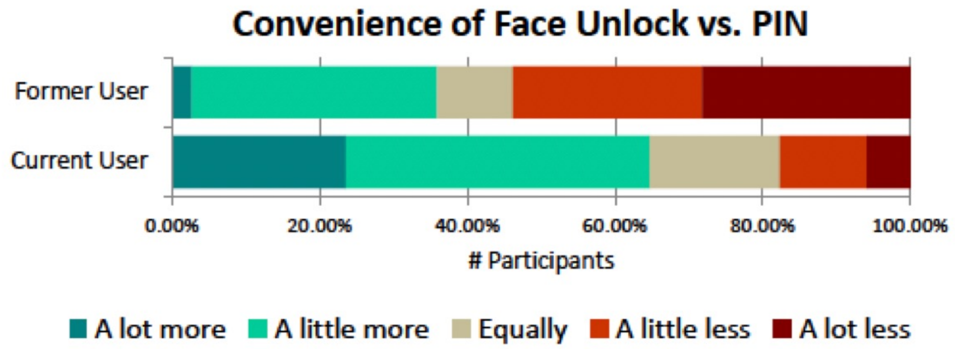
Walking (bag)

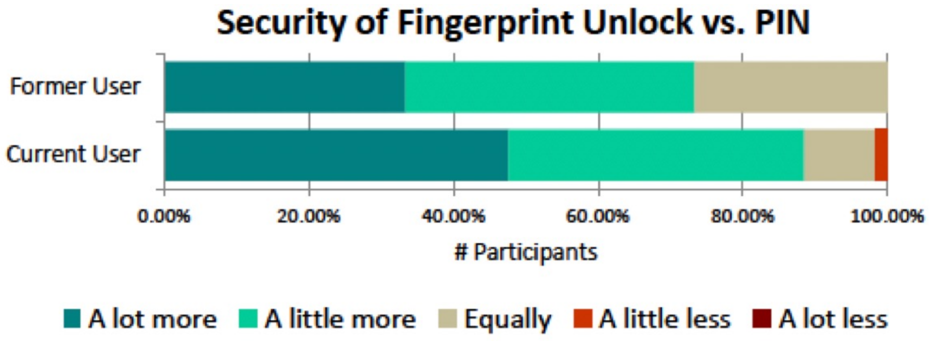


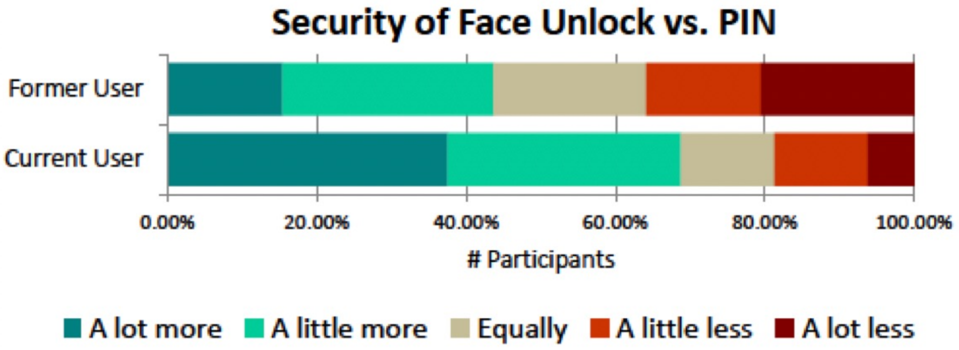
In-person
Within subjects
n = 10

Comparing Biometrics


Convenience of Fingerprint Unlock vs. PIN


Convenience of Face Unlock vs. PIN


Security of Fingerprint Unlock vs. PIN


Security of Face Unlock vs. PIN

Online study
Survey
n = 198

Biometric attributes as verifiers

Requirements:

- Easy to measure
- Identifier
- Small variation over time and measurement
- Acceptable to users
- Difficult to spoof

Biometric	Accuracy
Face	Low
Voice	Medium
Fingerprint	High
Iris	High
Palm vein	High

Privacy concerns

- Humans might have concerns about **measurements** (have photo taken, parts of body scanned)
- Humans might not want to **disclose attributes** during enrollment (SSN, political party)
- Humans might not want action bound to their **identity** (buying medication)
- Humans might not want their actions **linked** to other actions, exposing them to inference about what they thought were unrelated activities.

Privacy and biometrics

- Biometrics can **violate intrinsic privacy** by requiring submission to bodily contact or measurement
  - Fear of germs
  - Religious prohibitions
- Biometrics can **violate informational privacy**
  - Biometric identifiers might effectively become a standard, universal identifier, enabling linking

Biometric Phone Authentication

- Fingerprints (introduced to iPhone 5S in 2013)
- Facial Recognition (introduced to Android 4.0 in 2011, to iPhone X in 2017)

Online study
Survey
n = 383

Why people (don't) use biometrics

	Touch ID	Face Unlock
Reason Activated	Usability (70%)	Security (44%)
	Security (39%)	Curiosity (22%)
	Emotion (13%)	Usability (17%)
Reason Deactivated	Usability (47%)	Usability (36%)
	Emotion (18%)	Reliability (29%)
	Reliability (18%)	External (29%)
Reason Never Activated	Usability (38%)	Ignorance (27%)
	Misconception (38%)	No need (24%)
	Trust (2 people)	Reliability (23%)

Privacy and Trust were rarely mentioned

Biometric attributes as verifiers

Requirements:

- Easy to measure
- Identifier
- Small variation over time and measurement
- Acceptable to users
- Difficult to spoof

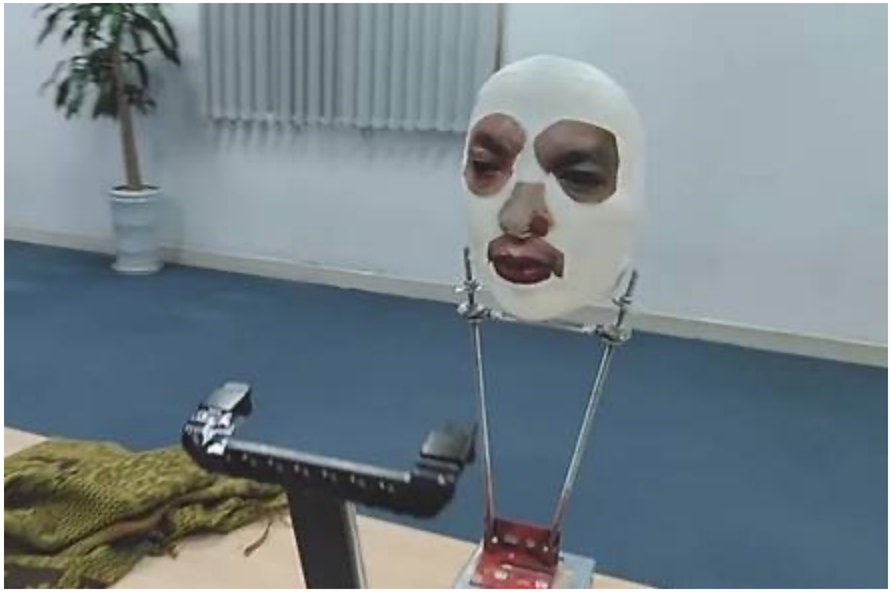
Biometric	Easy to Measure	Accuracy	User Acceptance
Face	High	Low	High
Voice	High	Medium	High
Fingerprint	Medium	High	Low(?)
Iris	Medium	High	Medium
Palm vein	High	High	Medium

Spoofing

- Active adversary fools sensor with artificial object
- Solution:
  - better sensors
  - better biometrics
  - multi-factor authentication

Gummy Bear Attack

Face ID Attack



Exercise: Evaluating Biometrics

Consider the use of voice authentication as a biometric. With voice authentication, the human is asked to say a specific passphrase and their response compared to a recorded voice print by a machine learning system.

1. What are potential advantages of this biometric?
2. What are potential disadvantages of this biometric?
3. Would you recommend this biometric for unlocking phones?

Biometrics

WHY ARE YOU STEPPING ON YOUR NEW PHONE?
I'M SETTING UP THE FINGERPRINT RECOGNITION THINGY.
AREN'T YOU SUPPOSED TO USE YOUR FINGER FOR THAT, NOT YOUR TOE?
I FIGURE A TOE PRINT IS EVEN MORE SECURE THAN A FINGERPRINT.
© 2017 Brian Crane, dist. by Washington Post Writers Group
11/10
BRIAN CRANE
picklescomic@gmail.com

© Brian Crane.