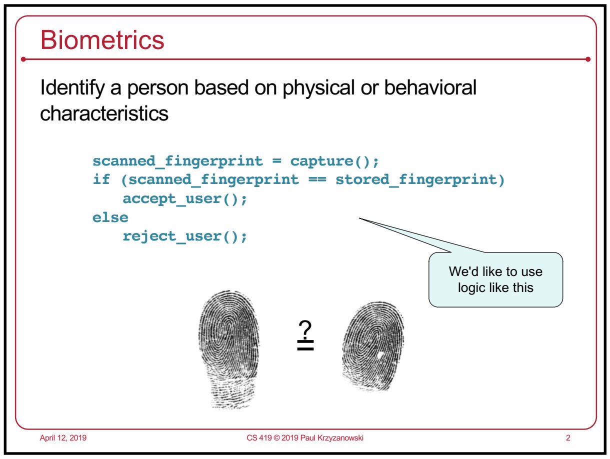
Computer Security

10. Biometric authentication

Paul Krzyzanowski

Rutgers University

Spring 2019

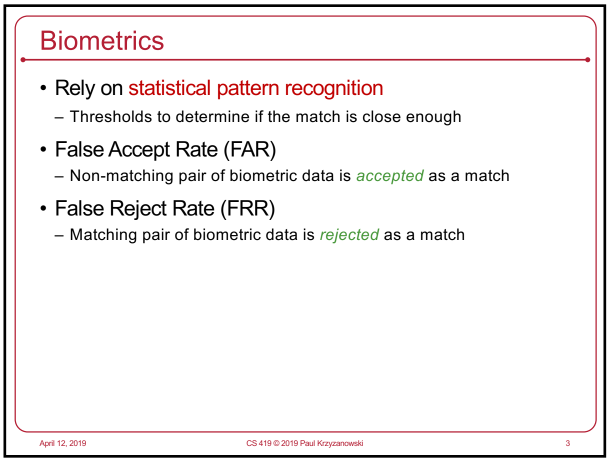


Biometrics

Identify a person based on physical or behavioral characteristics

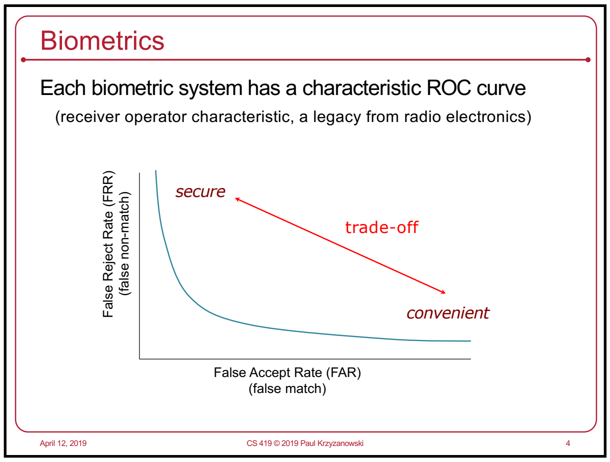
```
scanned_fingerprint = capture();
if (scanned_fingerprint == stored_fingerprint)
    accept_user();
else
    reject_user();
```

We'd like to use logic like this



Biometrics

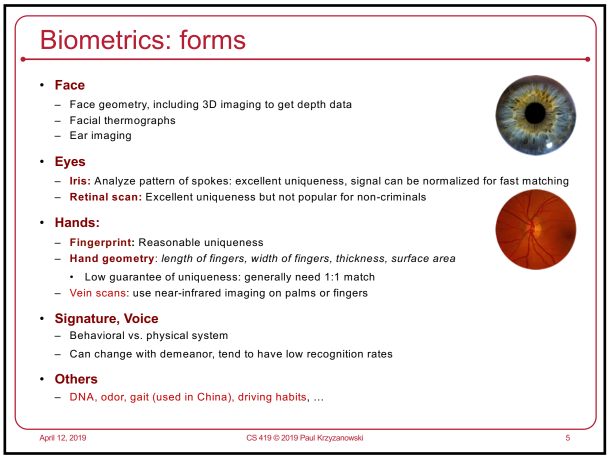
- Rely on statistical pattern recognition
  - – Thresholds to determine if the match is close enough
- False Accept Rate (FAR)
  - – Non-matching pair of biometric data is *accepted* as a match
- False Reject Rate (FRR)
  - – Matching pair of biometric data is *rejected* as a match



Biometrics

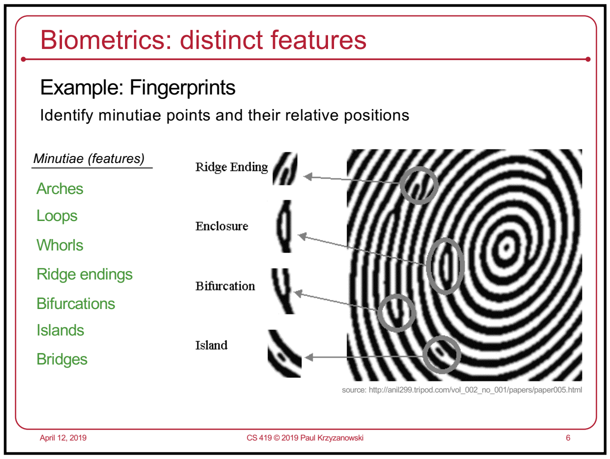
Each biometric system has a characteristic ROC curve

(receiver operator characteristic, a legacy from radio electronics)



Biometrics: forms

- **Face**
  - – Face geometry, including 3D imaging to get depth data
  - – Facial thermographs
  - – Ear imaging
- **Eyes**
  - – **Iris:** Analyze pattern of spokes: excellent uniqueness, signal can be normalized for fast matching
  - – **Retinal scan:** Excellent uniqueness but not popular for non-criminals
- **Hands:**
  - – **Fingerprint:** Reasonable uniqueness
  - – **Hand geometry**: *length of fingers, width of fingers, thickness, surface area*
    - Low guarantee of uniqueness: generally need 1:1 match
  - – Vein scans: use near-infrared imaging on palms or fingers
- **Signature, Voice**
  - – Behavioral vs. physical system
  - – Can change with demeanor, tend to have low recognition rates
- **Others**
  - – DNA, odor, gait (used in China), driving habits, …



Biometrics: distinct features

Example: Fingerprints

Identify minutiae points and their relative positions

Minutiae (features)

Arches

Loops

Whorls

Ridge endings

Bifurcations

Islands

Bridges

source: http://anil299.tripod.com/vol_002_no_001/papers/paper005.html

Biometrics: desirable characteristics

- Robustness
  - Repeatable, not subject to large changes over time
  - Fingerprints & iris patterns are more robust than voice
- Distinctiveness
  - Differences in the pattern among population
  - Fingerprints: typically 40-60 distinct features
  - Irises: typically >250 distinct features
  - Hand geometry: ~1 in 100 people may have a hand with measurements close to yours.

Biometrics: desirable characteristics

Biometric	Robustness	Distinctiveness
Fingerprint	Moderate	High
Hand Geometry	Moderate	Low
Voice	Moderate	Low
Iris	High	Ultra high
Retina	High	Ultra high
Signature	Low	Moderate

Irises vs. Fingerprints

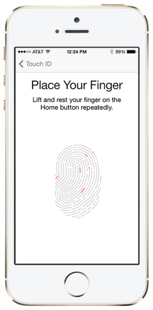
- Number of features measured:
  - High-end fingerprint systems: ~40-60 features
  - Iris systems: ~240 features
- False accept rates (FAR)
  - Fingerprints: ~ 1:100,000 (varies by vendor; may be ~1:500)
  - Irises: ~ 1:1.2 million
  - Retina scan ~1:10,000,000

Irises vs. Fingerprints

- Ease of data capture
  - More difficult to damage an iris … but lighting is an issue
  - Feature capture more difficult for fingerprints:
    - Smudges, gloves, dryness, …
- Ease of searching
  - Fingerprints cannot be normalized
    1:many searches are difficult
  - Irises can be normalized to generate a unique IrisCode
    1:many searches much faster

Biometric: authentication process

0. Enrollment
   - The user's entry in a database of biometric signals must be populated.
   - Initial sensing and feature extraction
   - May be repeated to ensure good feature extraction



Touch ID

Place Your Finger

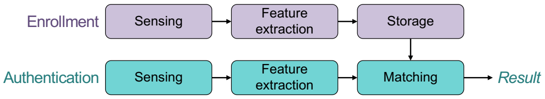
Lift and rest your finger on the Home button repeatedly.

Biometric: authentication process

1. Sensing
   - User's characteristic must be presented to a sensor
   - Output is a function of:
     - Biometric measure
     - The way it is presented
     - Technical characteristics of sensor
2. Feature Extraction
   - Signal processing
   - Extract the desired biometric pattern
     - remove noise and signal losses
     - discard qualities that are not distinctive/repeatable
     - Determine if feature is of "good quality"

Biometric: authentication process

3. Pattern matching
   - Sample compared to original signal in database
   - Closely matched patterns have "small distances" between them
   - Distances will hardly ever be 0 (perfect match)
4. Decision
   - Decide if the match is close enough
   - Trade-off:
     ↓ false non-matches leads to ↑false matches



Identification vs. Verification

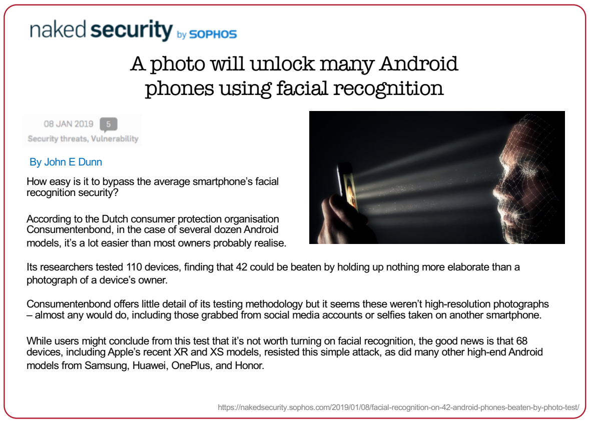
- Identification: *Who is this?*
  - *1:many* search
- Verification: *Is this Bob?*
  - Present a name, PIN, token
  - *1:1* (or 1:small #) search

Biometrics: Essential characteristics

- Trusted sensor
- Liveness testing
- Tamper resistance
- Secure communication
- Acceptable thresholds

Biometrics: other characteristics

- Cooperative systems (multi-factor)
  - User provides identity, such as name and/or PIN
- vs. Non-cooperative
  - Users cannot be relied on to identify themselves
  - Need to search large portion of database
- Overt vs. covert identification
- Habituated vs. non-habituated
  - Do users regularly use (train) the system



naked security by SOPHOS

A photo will unlock many Android phones using facial recognition

08 JAN 2019 5
Security threats, Vulnerability

By John E Dunn

How easy is it to bypass the average smartphone's facial recognition security?

According to the Dutch consumer protection organisation Consumentenbond, in the case of several dozen Android models, it's a lot easier than most owners probably realise.

Its researchers tested 110 devices, finding that 42 could be beaten by holding up nothing more elaborate than a photograph of a device's owner.

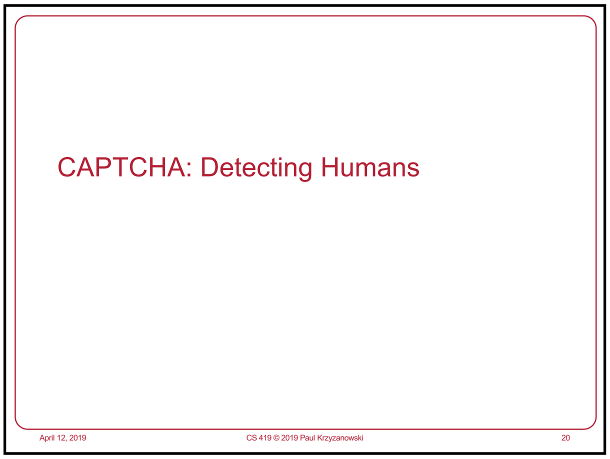
Consumentenbond offers little detail of its testing methodology but it seems these weren't high-resolution photographs – almost any would do, including those grabbed from social media accounts or selfies taken on another smartphone.

While users might conclude from this test that it's not worth turning on facial recognition, the good news is that 68 devices, including Apple's recent XR and XS models, resisted this simple attack, as did many other high-end Android models from Samsung, Huawei, OnePlus, and Honor.

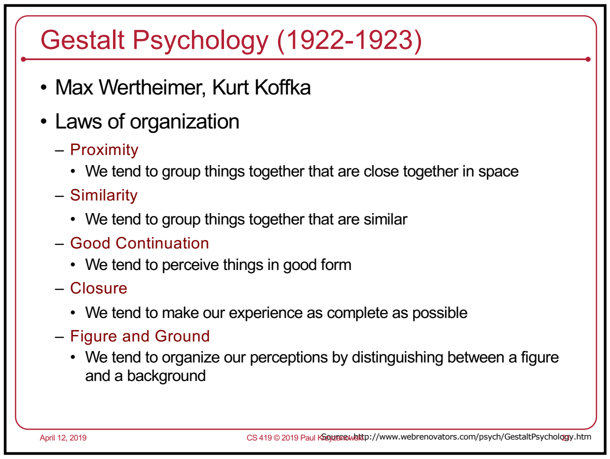
https://nakedsecurity.sophos.com/2019/01/08/facial-recognition-on-42-android-phones-beaten-by-photo-test/

Problems with biometric systems

- Requires a sensor
  - Camera works OK for iris scans & facial detection
    (but a good Iris scan will also take IR light into account)
- Tampering with device or device link
  - Replace sensed data– or just feed new data
- Tampering with stored data
- Biometric data cannot be compartmentalized
  - You cannot have different data for your Amazon & bank accounts
- Biometric data can be stolen
  - Photos, lifting fingerprints
  - Once biometric data is compromised, it remains compromised
    - You cannot change your iris or finger



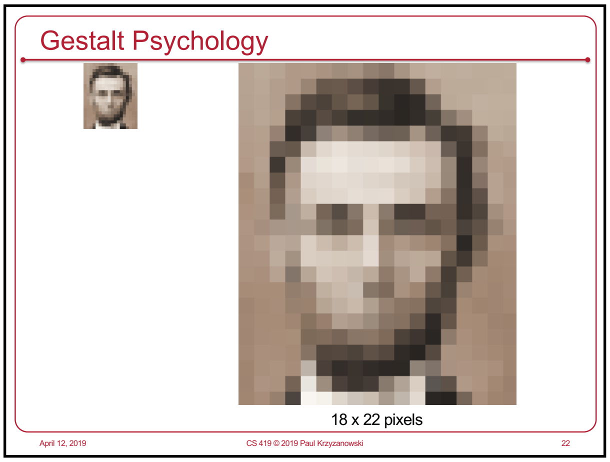
CAPTCHA: Detecting Humans



Gestalt Psychology (1922-1923)

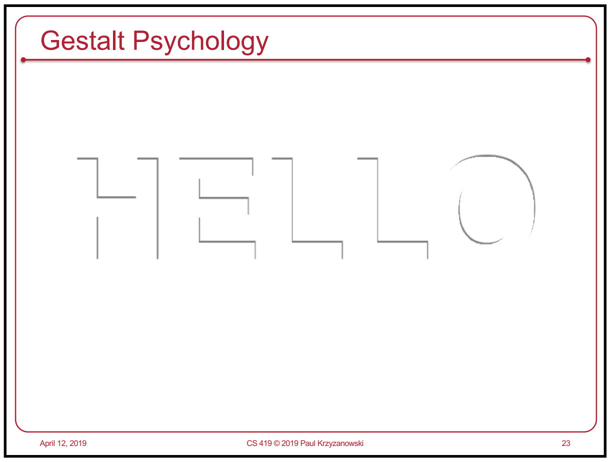
- Max Wertheimer, Kurt Koffka
- Laws of organization
  - Proximity
    - We tend to group things together that are close together in space
  - Similarity
    - We tend to group things together that are similar
  - Good Continuation
    - We tend to perceive things in good form
  - Closure
    - We tend to make our experience as complete as possible
  - Figure and Ground
    - We tend to organize our perceptions by distinguishing between a figure and a background

Source: http://www.webrenovators.com/psych/GestaltPsychology.htm



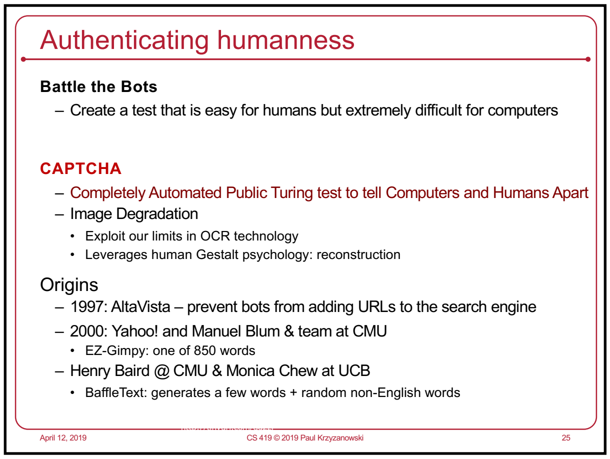
Gestalt Psychology

18 x 22 pixels



Gestalt Psychology

Gestalt Psychology



Authenticating humanness

Battle the Bots

- Create a test that is easy for humans but extremely difficult for computers

CAPTCHA

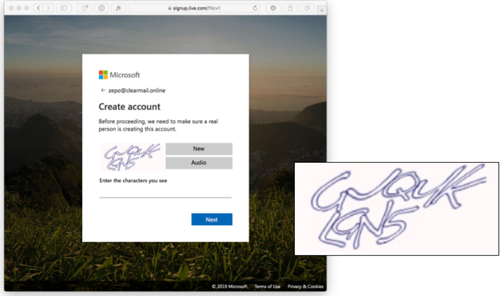
- Completely Automated Public Turing test to tell Computers and Humans Apart
- Image Degradation
  - Exploit our limits in OCR technology
  - Leverages human Gestalt psychology: reconstruction

Origins

- 1997: AltaVista – prevent bots from adding URLs to the search engine
- 2000: Yahoo! and Manuel Blum & team at CMU
  - EZ-Gimpy: one of 850 words
- Henry Baird @ CMU & Monica Chew at UCB
  - BaffleText: generates a few words + random non-English words

CAPTCHA Example (2019)

Microsoft



Microsoft

← zepo@clearmail.online

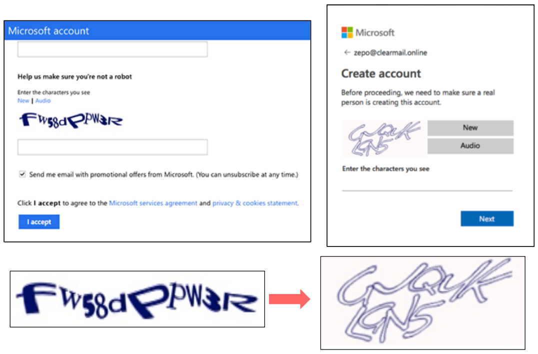
Create account

Before proceeding, we need to make sure a real person is creating this account.

Enter the characters you see

See captchas.net

They're getting harder



Microsoft account

Help us make sure you're not a robot

Enter the characters you see

☑ Send me email with promotional offers from Microsoft. (You can unsubscribe at any time.)

Click **I accept** to agree to the Microsoft services agreement and privacy & cookies statement.

Microsoft

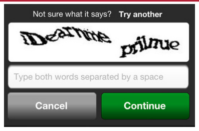
← zepo@clearmail.online

Create account

Before proceeding, we need to make sure a real person is creating this account.

Enter the characters you see

Problems

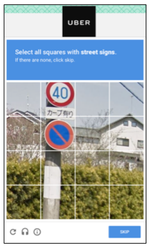


Type both words separated by a space

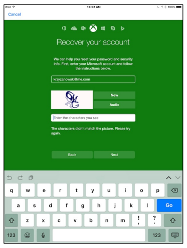
- **Accessibility**
  - Visual impairment → audio CAPTCHAs
  - Deaf-blind users suffer
- **Frustration**
  - OCR & computer vision has improved a lot!
  - Challenges that are difficult for computers may be difficult for humans
- **Attacks**
  - Man in the middle (sort of)
    - Use human labor – CAPTCHA farms
  - Automated CAPTCHA solvers
    - Initially, educated guesses over a small vocabulary

Alternate approaches

- MAPTCHAs = math CAPTCHAs
  - Solve a simple math problem
- Puzzles, scene recognition



Select all squares with **street signs**.
If there are none, click skip.



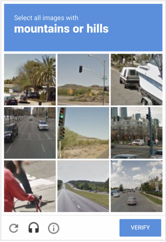
Recover your account

We can help you reset your password and security info. First, enter your Microsoft account and follow the instructions below.

krzyzanowski@me.com

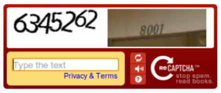
Enter the characters you see

The characters didn't match the picture. Please try again.



Select all images with
mountains or hills

reCAPTCHA

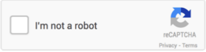


- Ask users to translate images of real words & numbers from archival texts
  - Human labor fixed up the archives of the New York Times
- Two sections
  - (1) known text
  - (2) image text
  - Assume that if you get one right then you get the next one correct
    - Try it again on a few other people to ensure identical answers before marking it correct
- Google bought reCAPTCHA 2009
  - Used free human labor to improve transcription of old books & street data

2014: Google found that AI could crack CAPTCHA & reCAPTCHA images with 99.8% accuracy

NoCAPTCHA reCAPTCHA

Ask users if they are robots



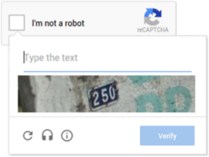
□ I'm not a robot

- Reputation management
  - "Advanced Risk Analysis backend"
  - Check IP addresses of known bots
  - Check Google cookies from your browser
  - Considers user's entire engagement with the CAPTCHA: before, during, and after
    - Mouse movements & acceleration, precise location of clicks
- Newest version: invisible reCAPTCHA
  - Don't even present a checkbox

NoCAPTCHA fallback

If risk analysis fails,

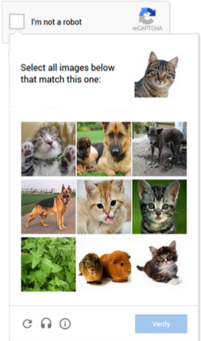
- Present a CAPTCHA
- For mobile users, present a image labeling problem



□ I'm not a robot

reCAPTCHA

Type the text



□ I'm not a robot

reCAPTCHA

Select all images below that match this one:

Alternative: Text/email verification

- Text/email verification
  - Ask users for a phone # or email address
  - Service sends a message containing a verification code
    - Still susceptible to spamming
    - Makes it a bit more difficult … and slower
- Measure form completion times
  - Users take longer than bots to fill out and submit forms
  - Measure completion times
    - Bots can program delays if they realize this is being done

The End