Computer Security

9. Biometric authentication

Paul Krzyzanowski

Rutgers University

Fall 2019

1

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

2

Biometrics

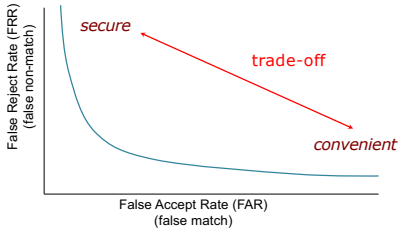
- Rely on statistical pattern recognition
  - Thresholds to determine if the match is close enough
- False Accept Rate (FAR)
  - Non-matching pair of biometric data is *accepted* as a match
- False Reject Rate (FRR)
  - Matching pair of biometric data is *rejected* as a match

3

Biometrics

Each biometric system has a characteristic ROC curve

(receiver operator characteristic, a legacy from radio electronics)



4

Galaxy S9 Intelligent Scan favors unlocking ease over security

An in-depth look at Samsung's new biometrics verification system -- and how it stacks up against the iPhone X's Face ID — shows it's not quite safe enough for mobile payments.

Shara Tibken, Alfred Ng March 1, 2018 5:00 AM PST

Unlocking the Galaxy S9 might be faster -- but that doesn't mean it's more secure.

Samsung's newest smartphones, the Galaxy S9 and S9 Plus, include a new feature the company calls Intelligent Scan. The technology combines Samsung's secure iris scanner with its less-secure facial recognition unlock technology.

When unlocking your phone, it first will scan your face. If that fails to unlock the phone, the device then will check your irises. If both fail, Intelligent Scan will try to authenticate your identity using a combination of the two. And it all happens almost instantaneously.

https://www.cnet.com/news/samsung-galaxy-s9-intelligent-scan-unlock-favors-ease-over-security/

5

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, …

6

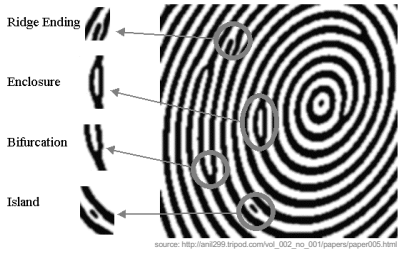
Biometrics: distinct features

Example: Fingerprints

Identify minutiae points and their relative positions

Minutiae (features)

- Arches
- Loops
- Whorls
- Ridge endings
- Bifurcations
- Islands
- Bridges



source: http://ani299.tripod.com/vol_002_no_001/papers/paper005.html

November 11, 2019 CS 419 © 2019 Paul Krzyzanowski 7

7

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.

November 11, 2019 CS 419 © 2019 Paul Krzyzanowski 8

8

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

November 11, 2019 CS 419 © 2019 Paul Krzyzanowski 9

9

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

November 11, 2019 CS 419 © 2019 Paul Krzyzanowski 10

10

Irises vs. Fingerprints

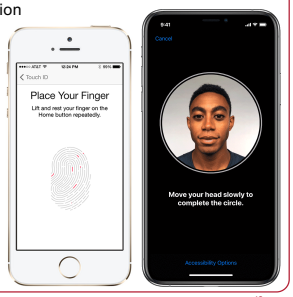
- Ease of data capture
  - More difficult to damage an iris … but lighting is an issue
  - Feature capture more difficult for fingerprints:
    - Smudges, gloves, dryness, …
- Ease of searching
  - Fingerprints cannot be normalized
    1:many searches are difficult
  - Irises can be normalized to generate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

November 11, 2019 CS 419 © 2019 Paul Krzyzanowski 11

11

Biometric: authentication process

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



12

12

Biometric: authentication process

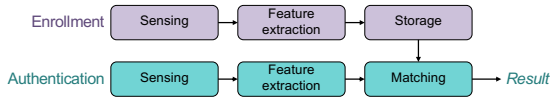
1. Sensing
   - User's characteristic must be presented to a sensor
   - Output is a function of:
     - Biometric measure
     - The way it is presented
     - Technical characteristics of sensor
2. Feature Extraction
   - Signal processing
   - Extract the desired biometric pattern
     - remove noise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

November 11, 2019 CS 419 © 2019 Paul Krzyzanowski 13

13

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



November 11, 2019 CS 419 © 2019 Paul Krzyzanowski 14

14

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

November 11, 2019 CS 419 © 2019 Paul Krzyzanowski 15

15

Biometrics: Essential characteristics

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

November 11, 2019 CS 419 © 2019 Paul Krzyzanowski 17

17

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

November 11, 2019 CS 419 © 2019 Paul Krzyzanowski 18

18

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/

November 11, 2019 CS 419 © 2019 Paul Krzyzanowski 19

19

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

20

BBC NEWS

Google Pixel 4 Face Unlock works if eyes are shut

Chris Fox • Technology reporter • 17 October 2019

Google has confirmed the Pixel 4 smartphone's Face Unlock system can allow access to a person's device even if they have their eyes closed. One security expert said it was a significant problem that could allow unauthorised access to the device.

By comparison, Apple's Face ID system checks the user is "alert" and looking at the phone before unlocking.

Google said in a statement: "Pixel 4 Face Unlock meets the security requirements as a strong biometric."

https://www.bbc.com/news/technology-50085630

21

c|net

Samsung Galaxy S8 iris scanner tricked by photo, contact lens

Turns out the sophisticated tech can't tell the difference between your eye and a picture with a contact lens over the iris, a hacking club says.

Alfred NG. May 24, 2017 8:34 AM PDT

You won't believe your eyes. But maybe the Samsung Galaxy S8 will.

In the month since Samsung released its flagship device, hackers in Germany have figured how to break the phone's iris recognition lock. Samsung has touted the biometric technology as "one of the safest ways to keep your phone locked," claiming that a person's iris patterns are "virtually impossible to replicate."

But that's exactly what the hackers from the Chaos Computer Club say they did. The hackers used a photo shot in night mode and from a medium distance, about the same range that would pop up in a Facebook profile picture or a selfie. They then printed out a closeup of the person's eye and put a contact lens over the iris on the paper.

The lens is there to replicate the eye's curvature, the Chaos Computer Club said in a blog post this week. Someone then held up the piece of paper to the Samsung Galaxy S8's iris scanner, and it unlocked as if a real person had looked at it. https://www.cnet.com/news/samsung-galaxy-s8-iris-scanner-tricked-photo-contact-lens/

22

THE WALL STREET JOURNAL.

Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case

Scams using artificial intelligence are a new challenge for companies

By Catherine Stupp • August 30, 2019

Criminals used artificial intelligence-based software to impersonate a chief executive's voice and demand a fraudulent transfer of €220,000 ($243,000) in March in what cybercrime experts described as an unusual case of artificial intelligence being used in hacking.

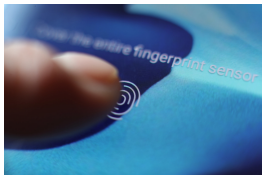
The CEO of a U.K.-based energy firm thought he was speaking on the phone with his boss, the chief executive of the firm's German parent company, who asked him to send the funds to a Hungarian supplier. The caller said the request was urgent, directing the executive to pay within an hour, according to the company's insurance firm, Euler Hermes Group SA.

https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

23

engadget

Massive biometric security flaw exposed more than one million fingerprints



The system is used by banks, police and defence companies.

August 14, 2019 – Rachel England, @rachel_england

A biometrics system used by banks, UK police and defence companies has suffered a major data breach, revealing the fingerprints of more than one million people as well as unencrypted passwords, facial recognition information and other personal data.

Biostar 2, the biometrics lock system managed by security company Suprema, uses fingerprints and facial recognition technology to give authorised individuals access to buildings. Last month the platform was integrated into another access system -- AEOS -- which is used by 5,700 organizations across 83 countries, including the UK Metropolitan Police.

https://www.engadget.com/2019/08/14/biometric-security-flaw-fingerprints

24

THE VERGE

Samsung's Galaxy S10 fingerprint sensor fooled by 3D printed fingerprint

It took 13 minutes to print up the fake

By Andrew Liptak • April 7 2019

… user darkshark outlined his project: he took a picture of his fingerprint on a wineglass, processed it in Photoshop, and made a model using 3ds Max that allowed him to extrude the lines in the picture into a 3D version. After a 13-minute print (and three attempts with some tweaks), he was able to print out a version of his fingerprint that fooled the phone's sensor.

https://www.theverge.com/2019/4/7/18299366/samsung-galaxy-s10-fingerprint-sensor-fooled-3d-printed-fingerprint

Video: https://imgur.com/gallery/8aGqsSu

25

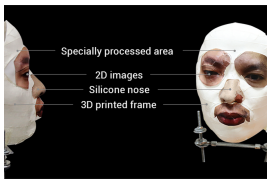
THE VERGE

This $150 mask beat Face ID on the iPhone X

It's just a proof of concept at the moment

By Thuy Ong • Nov 13 2017

Vietnamese cybersecurity firm Bkav claims it's been able to bypass the iPhone X's Face ID feature using a mask. The mask is made to trick Apple's depth mapping and the result is a kind of creepy hybrid monster head with realistic cutouts for the eyes, nose and mouth.



Bkav says the mask is crafted through a combination of 3D printing, makeup, and 2D images.

https://www.theverge.com/2017/11/13/16642690/bkav-iphone-x-faceid-mask

26

CAPTCHA: Detecting Humans

27

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

28

Gestalt Psychology

18 x 22 pixels

29

Gestalt Psychology

30

Gestalt Psychology

31

Authenticating humanness

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

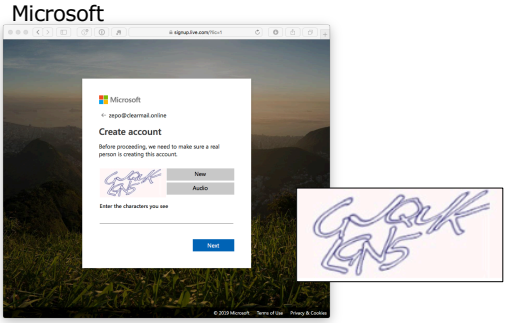
CAPTCHA
- Completely Automated Public Turing test to tell Computers and Humans Apart
- Image Degradation
  - Exploit our limits in OCR technology
  - Leverages human Gestalt psychology: reconstruction

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

32

CAPTCHA Example (2019)

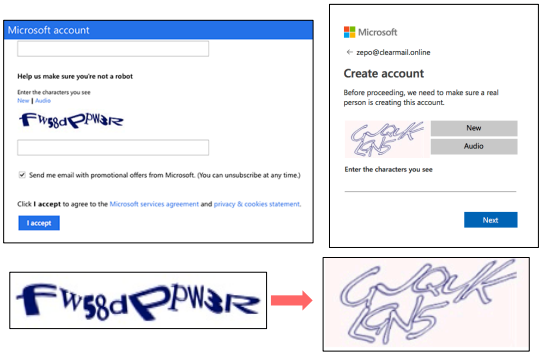
Microsoft



See captchas.net

33

They're getting harder



34

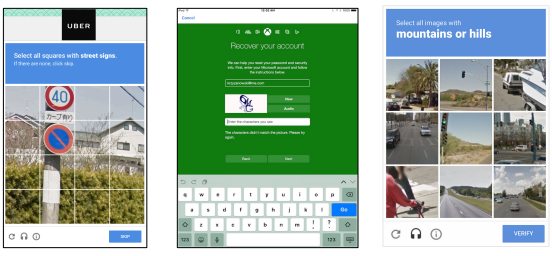
Problems

- **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

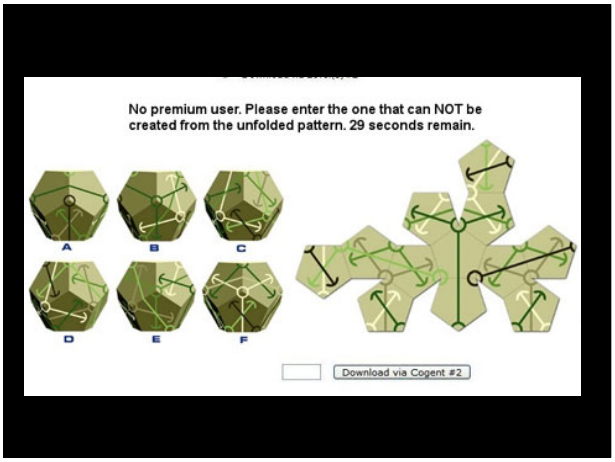
35

Alternate approaches

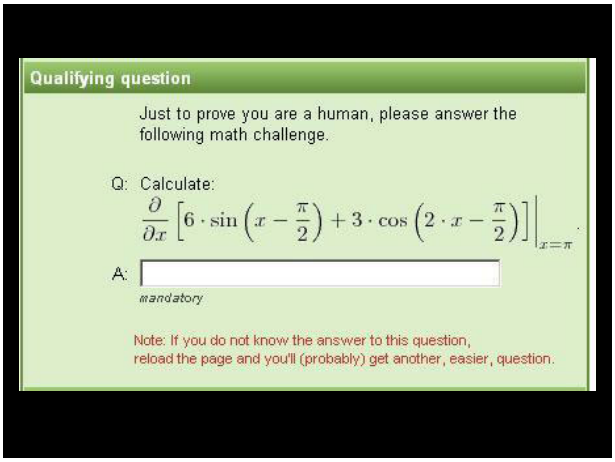
- MAPTCHAs = math CAPTCHAs
  - Solve a simple math problem
- Puzzles, scene recognition



36



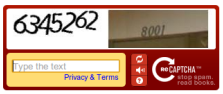
37



38

reCAPTCHA

- Ask users to translate images of real words & numbers from archival texts
  - Human labor fixed up the archives of the New York Times



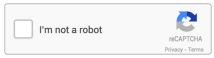
- Two sections
  - (1) known text
  - (2) image text
  - Assume that if you get one right then you get the next one correct
    - Try it again on a few other people to ensure identical answers before marking it correct
- Google bought reCAPTCHA 2009
  - Used free human labor to improve transcription of old books & street data

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

39

NoCAPTCHA reCAPTCHA

Ask users if they are robots

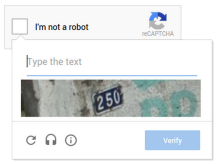


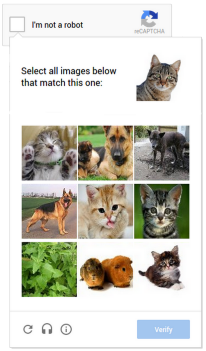
- Reputation management
  - "Advanced Risk Analysis backend"
  - Check IP addresses of known bots
  - Check Google cookies from your browser
  - Considers user's entire engagement with the CAPTCHA: before, during, and after
    - Mouse movements & acceleration, precise location of clicks
- Newest version: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

40

NoCAPTCHA fallback

If risk analysis fails,
- Present a CAPTCHA
- For mobile users, present a image labeling problem





41

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

42

The End

43