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

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 scan: 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
Furrows
Islands
Bridges

Minutiae points and their relative positions

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.

Biometric: authentication process

1. **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

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
- Habitudated vs. non-habitudated
  - Do users regularly use (train) the system

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—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

A photo will unlock many Android phones using facial recognition

By John E Dunn

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 nearly any would do, including those grabbed from social media accounts or selfies taken on another smartphone.

While some might conclude from this that biometric authentication is too weak to be relied upon, the good news is that 68 devices, including all recent iPhones and XS models, resisted the simple attack, as did many other high-end Android models from Samsung, Huawei, OnePlus, and Honor.

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.

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 – AEGIS – which is used by 5,700 organizations across 83 countries, including the UK Metropolitan Police.

CAPTCHA: Detecting Humans

- Laws of organization
  - Proximity
  - Similarity
  - Good Continuation
  - Closure
  - Figure and Ground

Gestalt Psychology (1922-1923)

- Max Wertheimer, Kurt Koffka
- Laws of organization
  - Proximity
  - Similarity
  - Good Continuation
  - Closure
  - Figure and Ground
Gestalt Psychology

Hello

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

See captchas.net

They’re getting harder

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

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

reCAPTCHA reCAPTCHA

- 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

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