Biometrics

Biometrics

- Something you are
- A characteristic of the body
- Presumed unique and invariant over time

Metanote: biometrics is an area of rapid progress; some of the limitations I describe here are likely to change in the near future. Exercise: which of the problems are likely to remain difficult issues for system designers?

Common Biometrics

- Fingerprint
- Iris scan
- Retinal scan
- Hand geometry
- Facial recognition

Fingerprints

- Uniqueness well-established (not an idle issue; Bertillon measurement were once thought unique)

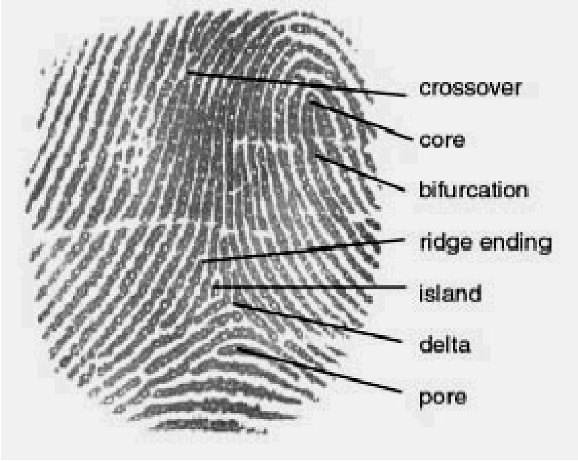
  ☞Fingerprints are *congenital*, not genetic

- Lots of backup fingers

- Commodity hardware available; built into many phones

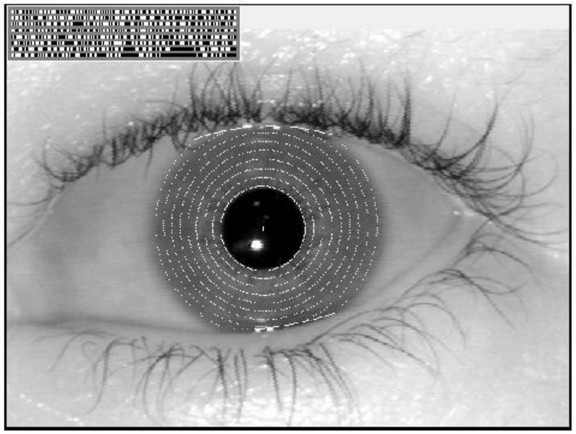
Fingerprint Recognition

- Image recognition technology
- Find significant features
- Does *not* match entire image
- Matching isn't as easy as you see on television
- New automated systems have improved scanning speed, but there can still be accuracy issues



Iris Scans

- Considered one of the most accurate biometrics
- Uses patterns in the iris of the eye that form after birth
- Hard part in some applications: finding the eye
- People do not like to stare into scanners

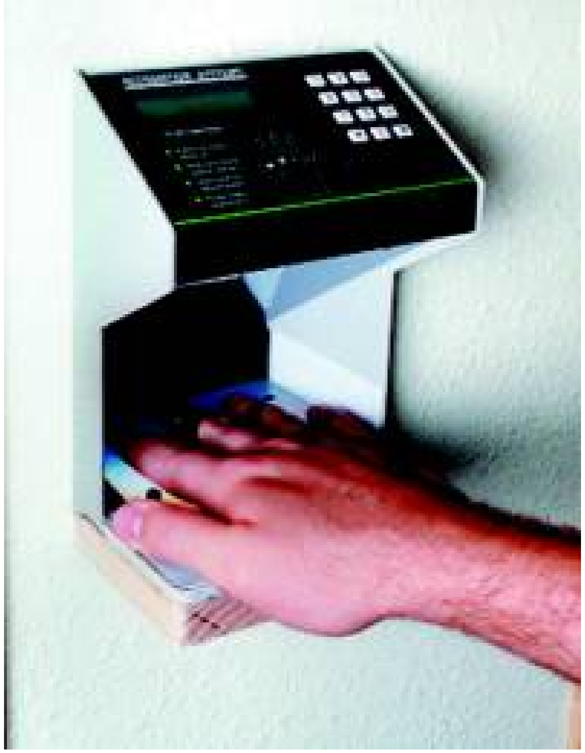


Retinal Scan

- Looks at pattern of blood vessels inside the eye
- Must put eye up to laser scanner
- Most people *really* dislike scanners that shine things into their eyes. “You’re going to shine a *what* into my eye?!”
- Falling out of favor compared to iris scans

Hand Geometry

- Requires somewhat fussy hand-positioning
- Relatively easy to use; few acceptability issues
- Formerly used at Disney World and by U.S. Immigration. Disney has switched to finger geometry; Immigration has switched to fingerprints



Facial Recognition

- Reasonably accurate under the right circumstanes
- Relies on geometry of key features—eye spacing, ears, etc.
- One major market: phones
- Another: walk-through authentication, e.g., airplane boarding

☞ Also: finding suspects in a crowd. (Gov. Cuomo wanted to deploy it at toll plazas—but it didn't work. And the MTA says its version is fake.)

- Some countries (US, UK, Germany, probably others) now prohibit smiling for passport pictures, to aid (future) automated recognizers

☞ But: some jurisdictions are prohibiting use by law enforcement

Other Biometrics

- Voiceprint
- Gait
- Heart rhythm
- Typing rhythm

Human Voice Recognition

- Press the red button to "go secure"
- Crypto magic happens, followed by the display of some hex digits
- Each party reads the hex digits to the other
- You must recognize the other party's voice speaking those digits

☞ Computers can fake that now. . .

(Photo courtesy Matt Blaze)

Advantages of Biometrics

- You can't forget your fingers
- You can't lend your eyes to a friend
- You can't fake a fingerprint
- Why aren't they used more?
- Maybe they're not that secure. . .

Some Problems with Biometrics

- False accept rate
- False reject rate
- Fake (or “detached”) body parts
- Computer-synthesized voices
- “Bit replay”
- Non-reproducibility
- Many biometrics are *public*

False Accept Rate

- No biometric system is perfect
- Reducing false accept rate increases false reject rate
- Usual metric: what is the true accept rate for a given false accept rate?
- Substantial difference between different products
- Dramatic improvements in facial recognition over the last several years, as hard-coded algorithms were replaced by machine learning
- All systems work much better for one-to-one match than “does this biometric match something in the database?”

Why is One-to-One Match Better?

- Suppose that the false positive on a 1-1 match is F
- Assume that the database has N entries
- False positive probability on one-to-many match is $1-(1-F)^N$
- For $F=10^{-6}, N=1000000$, that's 63%

False Reject Rate

- People change, including aging
- Cuts, scars, glasses, colds, bandages, etc.
- Problems in original image acquisition

Capture Quality

- Quality of the captured data, for both initial enrollment and checking, is crucial
- Facial recognition *can* work well, but only under good circumstances, including lighting, angle, obscuring details (e.g., a hat or sunglasses), etc.

Fake Body Parts

- Thieves cut off someone's finger to steal his fingerprint-protected car (`http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm`)
- Biometric sensors have been fooled by "Gummi Bear" fingerprints, close-up pictures of face
- One solution: use "liveness" detectors—temperature, blood flow, etc.
- Another solution: use biometrics only when under observation

Demographic Differences

- Facial recognition algorithms are sensitive to subjects' demographics
- Algorithms generally perform much worse on darker-skinned faces and on women
- It's probably a problem with training data

NIST’s Results

1. “For one-to-one matching, the team saw higher rates of false positives for Asian and African American faces relative to images of Caucasians.
2. “Among U.S.-developed algorithms, there were similar high rates of false positives in one-to-one matching for Asians, African Americans and native groups
3. “However, a notable exception was for some algorithms developed in Asian countries.
4. “For one-to-many matching, the team saw higher rates of false positives for African American females.
5. “However, not all algorithms give this high rate of false positives across demographics in one-to-many matching”

Non-Reproducibility

- Biometric matching compares an image to a template or set of templates
- It is hard (but not impossible) to reduce a biometric to a reproducible set of bits, suitable for use as a cryptographic key
- This makes it difficult to use a biometric to protect locally-stored keys; you're really relying on the operating system

Hardware Security Features

- More and more computers and phones have some sort of hardware security mechanism
- On PCs, it's the TPM: Trusted Platform Module
- iPhones use the Secure Enclave
- Android phones have the TEE: Trusted Execution Environment
- Intel CPUs have SGX
- All of these store keys and do cryptographic operations, and are isolated from the main operating system
- But: security issues have been reported with several of these. . .

iPhone Fingerprint Recognition

- Some iPhones have a fingerprint recognizer in the Home button: replace the PIN to unlock the phone
- Uses advanced technology; claimed to be immune to fake fingerprints, detached body parts, etc.
- Apple says the odds on a random finger matching are 1 in 50,000—and only five tries are allowed

☞ $1 - (1 - 50,000)^5 \approx \frac{1}{10,000}$ — the same as one guess at a 4-digit PIN

- But—users will notice false negatives more than false positives
- The Chaos Computer Club has already shown that those claims are incorrect: use a high-resolution camera, a suitable printer, and some white glue. . .

Is That Secure?

- Lossy mapping of fingerprint images to template; cannot reconstruct fingerprint from it
- Templates stored in physically and logically secure coprocessor; communications from sensor to coprocessor are encrypted
- You can’t even replace the sensor without the phone noticing and refusing to listen to it
- Data is *not* backed up in cleartext to iCloud
- The PIN is used to encrypt sensitive data on the phone (more detail on that later)
- PIN reentry is required periodically, after several failed authentication attempts, or after rebooting

Apple's Facial Recognition

- Uses an infrared light source and camera
- Forms a 3D map of your face, using 30,000 points
- Supposedly odds on a false match are 1 in 1,000,000
- All processing is done in the phone's "Secure Enclave"; no data is ever sent to Apple's iCloud
- Only works if you are looking at the phone and have your eyes open

Biometrics in Public

- Many biometrics are visible or retrievable
- Example: high-resolution photos show irises, fingerprints
- Collect fingerprints from items someone has touched
- ☞ Often possible to create fake fingerprints!
- Not practical to change one's biometrics if compromised. . .

Is Biometric Authentication Secure?

What is “Secure”?

- What is being protected?
- What is the threat model?
- We can’t answer “is it secure?” without defining what we’re trying to protect!

System Elements

- User, e.g., a person with some biometric attribute
- (Generically called the *prover*)
- The captured biometric data
- The verifier

Possible Weak Points

- Is the biometric actually doing its job?
- The data
- The verifier
- The links between the elements

Most assertions about biometric security begin and end with the first point—and they rarely get even that right

What Are We Trying To Do?

- One-to-one verification? For what value resource?
- One-to-many? For access control? Identifying a suspect? Tracking people?

Error Types

- What is the acceptable risk of a false positive?
- What is the acceptable risk of a false negative?
- What is the system's response to such issues?

Data Source

- Where does the initial data come from?
- How is it authenticated?
- How is it updated?

Example: Unlocking a Phone

- One-to-one verification
- Data supplied by owner at setup time, or after previous unlock
- No communications links
- Apple, at least, updates facial images on each use—can account for aging (in the lifetime of a phone??) and other gradual changes
- Does biometric unlock really work properly?

Issues

- What is the false positive rate?
- False negatives: just request a PIN—not a serious problem
- How do we protect the data internally?
- What about the the wires—the communications link!—inside the phone between the sensor and the CPU?

But. . .

- What about involuntary unlocking?
- A 7-year-old used his sleeping father's finger to unlock his iPhone
- The father is a well-known computer security prof! (And I confirmed the story with him. . .)
- A 6-year-old girl unlocked her mother's phone and bought $250 of Pokémon stuff from Amazon
- What about phone thieves and facial recognition?
- Abusive partners?
- Scanners that don't work well, e.g., a Samsung Galaxy S10 with a screen protector
- What are the appropriate defenses?

How About Banking?

- Assumption: there's a camera in your laptop that is used for facial recognition for login
- Is that secure?

Not Really

- Can the bank authenticate the remote app?
- Can the bank authenticate the camera?
- What if malware is running on the computer?
- How does the bank get the proper face originally? (Where is the image stored?)
- But we use our phones for banking. . .

Phone App Banking

- The biometric is used to unlock the phone, *not* to authenticate to the bank
- The phone stores the actual authentication data
- (Most) phones are considerably more secure than laptop computers
- There is (generally) strong isolation between apps on today's phones
- And remember that security isn't binary, nor does it have to be perfect

Boarding Airplanes

- Face images come from government databases
- False negatives can be dealt with by checking a boarding pass
- False positives are *presumed* to be low enough
- But: there are serious concerns about privacy

Law Enforcement: Finding Suspects

- Take a surveillance photo; run it through a database
- Use this as a *hint*—a human confirms the match, it's just one more data point, etc.
- But: there are privacy issues
- But: most surveillance camera images are pretty poor quality
- But: remember the issues about race and gender?
- The consequences of a false positive can land someone in jail or worse

Legal Issues

- Biometrics are seen as a serious privacy matter
- Many jurisdictions restrict or ban some uses of biometrics—Facebook just paid $550 million to settle charges under Illinois law
- The GDPR is also very strict

Accessibility Issues

- What about people who are missing fingers? (Btw, about 5% of people don’t have readily scannable fingerprints)
- Not everyone can open their eyes for iPhone face scans
- Injuries can distort biometrics, temporarily or permanently
- *System* designs have to cope

Bit Replay

- Ultimately, a biometric translates to a string of bits
- If the biometric sensor is remote from the accepting device, someone can inject a replayed bit stream
- What if someone hacks a server and steals a biometric? You can't change your fingerprints. . .

☞ Note: this happened with the OPM database breach

- Encryption helps; so does tamper-resistance
- Relying on human observation may help even more

Using Biometrics

- Biometrics work best in public places or under observation
- Remote verification is difficult, because verifier doesn't know if it's really a biometric or a bit stream replay
- Local verification is often problematic, because of the difficulty of passing the match template around
- Users don't want to rely on remote databases, because of the risk of compromise and the difficulty of changing one's body
- Best solution: use a biometric to unlock a local tamper-resistant token or chip; store keys there

☞ This is what the iPhone does

- Another solution: put the template on a mag stripe card in the user's possession; that supplies it to a local verification station. But how is the template authenticated?

Signed Templates

- Can digitally sign a biometric template
- Medium doesn’t matter; signed template is self-authenticating
- Verifier can operate offline
- But—which digital signatures should it trust?
- How do you revoke *authorization*?

Systems Considerations

- Authentication doesn’t stand by itself
- Whether or not biometrics are suitable depends on the situation
- How you set up your biometric authentication matters, too
- In fact, all authentication schemes are situation-dependent
- Authentication is a *systems problem*