CS G357: Computer Security, Privacy and Usability

Simson L. Garfinkel

Analysis of HW5: Good Reports

- Explains what tools were used
- Explains what was found.
- Gives specific details without compromising privacy

HW5: Things to avoid

- Spending more than a paragraph describing your tools
- Giving a few paragraphs of vague generalities talking about what was found.
- Listing filenames without any thought as to what might be in the files.

HW6: Comments?

Schedule Issues

- Option #1 - Class on July 5th: *****
- Option #2 - Class on July 8th: *****
- Option #3 - July 1 till 9pm : *******

Final Projects

- You will need to have groups of two. Justification:
  - Two people can do a better project than one person.
  - Group work ethic should prevent some people from leaving this to the last minute.
- You can write code, you can do policy, but the best projects will do both.

Biometrics and Privacy

Simson L. Garfinkel

Biometrics

- Something that you know
- Something that you have
- Something that you are

Uses of Biometrics:

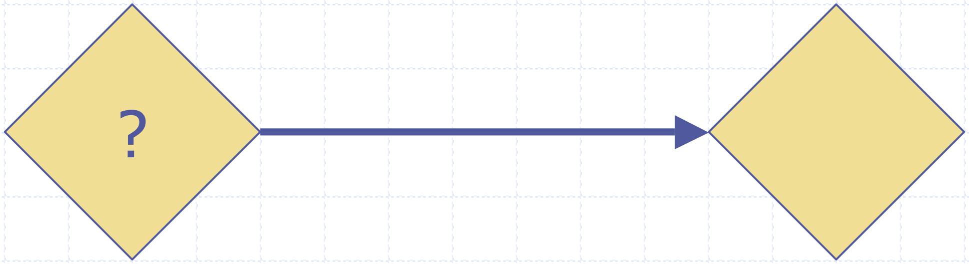
- Simple:
  - Verification – Is this who he claims to be?
  - Identification – who is this?
- Advanced:
  - Detecting multiple identities
  - Patrolling public spaces

Why the Interest in Biometrics?

- Convenient
- Passwords are not user-friendly
- Perceived as more secure
  - May actually be more secure
  - May be useful as a deterrent
- Passive identification

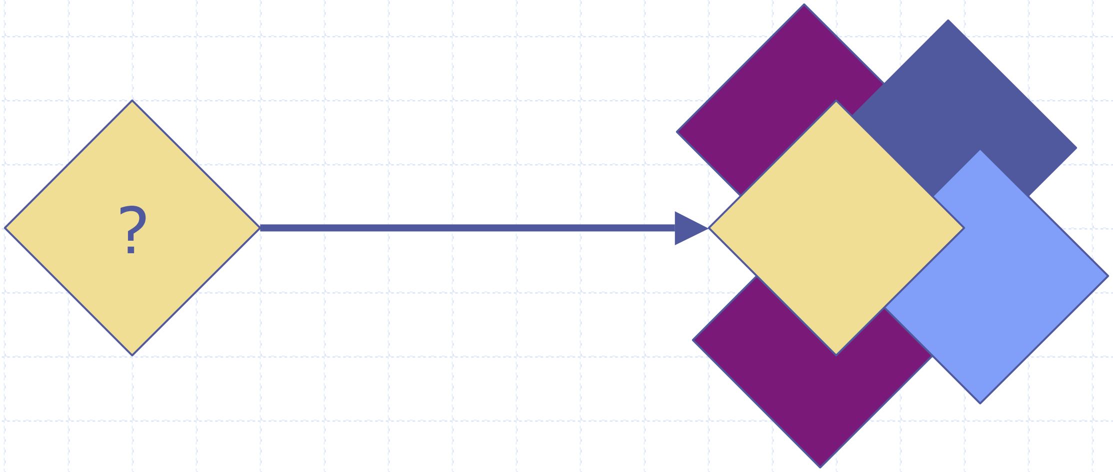
Verification

- Compare a sample against a single stored template
- Typical application: voice lock



Identification

- Search a sample against a database of templates.
- Typical application: identifying fingerprints



Bertillion System of Anthropomorphic Measurement

- Alphonse Bertillion Appointed to Prefecture of Police in 1877 as Records Clerk
- Biometrics to give harsher sentences to repeat offenders
- Measurements:
  - Head size
  - Fingers
  - Distance between eyes
  - Scars
  - Etc…
- Key advance: Classification System
- Discredited in 1903: Will West was not William West
- http://www.cmsu.edu/cj/alphonse.htm

Fingerprints (ca. 1880-)

- Henry Faulds letter to Nature (1880)
  - Fingerprints might be useful for crime scene investigations
- W. J. Herschel letter to Nature (1880)
  - Had been using fingerprints in India for 20 years; suggested a universal registration system to establish identity and prevent impersonations

Fingerprints after Faulds…

- *Pudd'nhead Wilson*, Mark Twain (Century Magazine, 1893)
- Prints quickly become tool of police.
- Manual card systems:
  - 10 point classification
  - Scaling problems in the mid 1970s.
- AFIS introduced in the 1980s
  - Solves back murder cases
  - Cuts burglary rates in San Francisco, other cities.

VoiceKey (ca. 1989)

- Access Control System
  - Z80 Microprocessor
  - PLC coding
  - 40 stored templates
  - 4-digit PINs
- False negative rate: 0-25%
- False positive rate: 0%*
- “Airplane”

Biometrics Today

- Fingerprints
- Retina Prints
- Face Prints
- DNA Identification
- Voice Prints
- Palm Prints
- Handwriting Analysis
- Etc…

Biometrics In Practice…

- Inherently not democratic
- Always have a back door
- Discrimination function tradeoffs:
  - Low false negatives => high false positives
  - Low false positives => high false negatives

Policy Issues That Effect Biometrics:

- Strong identification may not be necessary or appropriate in many circumstances
  - Voters may be scared off if forced to give a fingerprint
- Authorization can be granted to the *individual* or to the *template*.
  - It is frequently *not necessary* to identify an individual with a name.

Biometrics and Privacy

- Long association of biometrics with crime-fighting
- Biometrics collected for one purpose can be used for another

Accuracy Rates:

- False Match Rate (FMR)
- Single False Match Rate vs. System False Match Rate
  - If the FMR is 1/10,000 but you have 10,000 templates on file — odds of a match are very high
- False Nonmatch Rate (FNR)
- Failure-to-Enroll (FTE) rate
- Ability to Verify (ATV) rate:
  - % of user population that can be verified
  - ATV = (1-FTE)(1-FNMR)

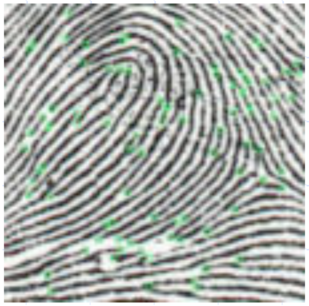
Other Issues:

- Stability of Characteristic ofver Lifetime
- Suitability for Logical and Physical Access
- Difficulty of Usage

Biometrics in Detail

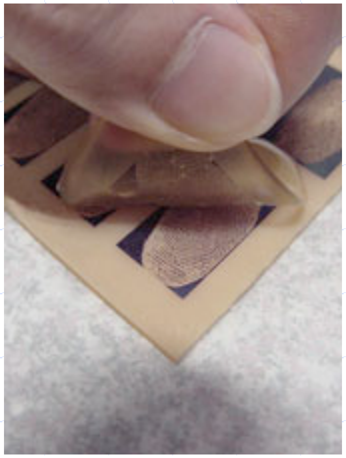
Finger-scan

- A live acquisition of a person’s fingerprint.
- Image Acquisition → Image Processing → Template Creation → Template Matching
- Acquisition Devices:
  - Glass plate
  - Electronic
  - Ultrasound



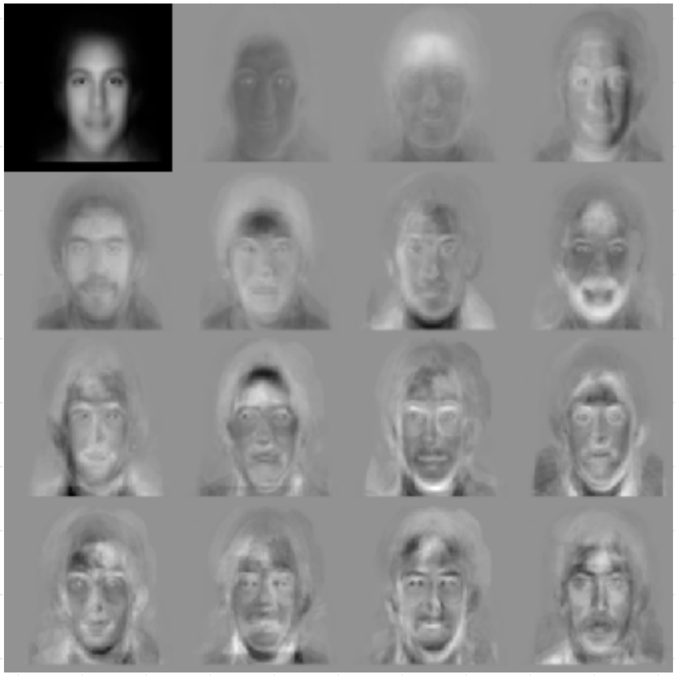
Fingerprint SWAD

- Strengths:
  - Fingerprints don't change over time
  - Widely believed fingerprints are unique
- Weaknesses:
  - Scars
- Attacks:
  - Surgery to alter or remove prints
  - Finger Decapitation
  - "Gummy fingers"
  - Corruption of the database
- Defenses:
  - Measure physical properties of a live finger (pulse)



Facial Scan

- Based on video Images
- Templates can be based on previously-recorded images
- Technologies:
  - Eigenface Approach
  - Feature Analysis (Visionics)
  - Neural Network

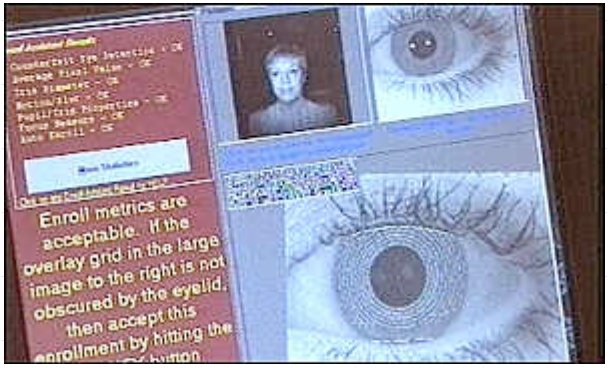


Facial Scan: SWAD

- Strengths:
  - Database can be built from driver’s license records, visas, etc.
  - Can be applied covertly (surveillance photos). (Super Bowl 2001)
  - Few people object to having their photo taken
- Weaknesses:
  - No real scientific validation
- Attacks:
  - Surgery
  - Facial Hair
  - Hats
  - Turning away from the camera
- Defenses:
  - Scanning stations with mandated poses

Iris Scan

- Image Acquisition → Image Processing → Template Creation → Template Matching
- Uses to date:
  - Physical access control
  - Computer authentication



Assistant Results

Contact/Eye Detection - OK
Average Pixel Value - OK
Iris Diameter - OK
Motion/Blur - OK
Pupil/Iris Properties - OK
Focus Measure - OK
Auto Enroll - OK

Enroll metrics are acceptable. If the overlay grid in the large image to the right is not obscured by the eyelid, then accept this enrollment by hitting the button

Iris Scan: SWAD

- Strengths:
  - 300+ characteristics; 200 required for match
- Weaknesses:
  - Fear
  - Discomfort
  - Proprietary acquisition device
  - Algorithms may not work on all individuals
  - No large databases
- Attacks:
  - Surgery (*Minority Report*)
- Defenses:

Voice Identification

- Scripted vs. non-scripted

Voice: SWAD

- Strengths:
  - Most systems have audio hardware
  - Works over the telephone
  - Can be done covertly
  - Lack of negative perception
- Weaknesses:
  - Background noise (airplanes)
  - No large database of voice samples
- Attacks:
  - Tape recordings
  - Identical twins / soundalikes
- Defenses:

Hand Scan

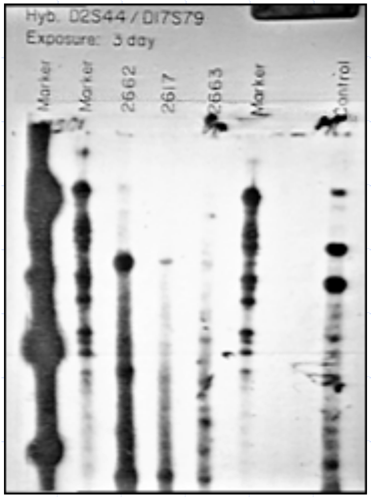
- Typical systems measure 90 different features:
  - Overall hand and finger width
  - Distance between joints
  - Bone structure
- Primarily for access control:
  - Machine rooms
  - Olympics
- Strengths:
  - No negative connotations – non-intrusive
  - Reasonably robust systems
- Weaknesses:
  - Accuracy is limited; can only be used for 1-to-1 verification
  - Bulky scanner

Oddballs

- Retina Scan
  - Very popular in the 1980s military; not used much anymore.
- Facial Thermograms
- Vein identification
- Scent Detection
- Gait recognition

DNA Identification

- RFLP - Restriction Fragment Length Polymorphism
- Widely accepted for crime scenes
- Twin problem



Behavior Biometrics:

- Handwriting (static & dynamic)
- Keystroke dynamics

Classifying Biometrics

Template Size

Biometric	Approx Template Size
Voice	70k – 80k
Face	84 bytes – 2k
Signature	500 bytes – 1000 bytes
Fingerprint	256 bytes – 1.2k
Hand Geometry	9 bytes
Iris	256 bytes – 512 bytes
Retina	96 bytes

Passive vs. Active

- Passive:
  - Latent fingerprints
  - Face recognition
  - DNA identification

- Active
  - Fingerprint reader
  - Voice recognition (?)
  - Iris identification (?)

Knowing vs. Unknowing

- Knowing:
  - Fingerprint reader
  - Hand geometry
  - Voice prints*
  - Iris prints (?)

- Unknowing:
  - Latent fingerprints

Body Present vs. Body Absent

- Performance-based biometrics
- Voice print
- Hand Geometry
- Facial Thermograms
- Iris Prints

- Fingerprint
- DNA Identification

Template: Copy or Summary

- Copy
  - Original fingerprint
  - Original DNA sample

- Summary
  - Iris Prints
  - Voice Prints
  - DNA RFLPs

Racial Clustering? Inherited?

- Racial Clustering
  - DNA fingerprints

- No Racial Clustering
  - Fingerprints?
  - Iris prints

Racial Clustering? Inherited?

- Racial Clustering
  - DNA fingerprints

- No Racial Clustering
  - Fingerprints?
  - Iris prints

System Design and Civil Liberties

- Biometric Verification
  - Is biometric verified locally or sent over a network?
- Biometric Template:
  - Matches a name?
    - “Simson L. Garfinkel”
  - Matches a right?
    - “May open the door.”

Identity Card

- Card has:
  - Biometric
  - Digital Signature?
  - Database Identifier?

- Central Database has:
  - Biometric?
  - Biometric Template?

Biometric Encryption

- Big problems:
  - Biometrics are noisy
  - Need for “error correction”
- Potential Problems:
  - Encryption with a 10-bit key?
  - Are some “corrected” values more likely than others?
  - What happens when the person changes --- you *still* need a back door.