CS 5430

Authentication of Humans

Prof. Clarkson
Spring 2017

Review

- Course so far:
  - Introduction to security
  - Cryptography
- Rest of semester: Accountability, both for Prevention and Deterrance

Accountability

Hold principals responsible for their actions

- **Authorization:** mechanisms that govern whether actions are permitted

- **Authentication:** mechanisms that bind principals to actions

- **Audit:** mechanisms that record and review actions

Authentication of humans

Categories: [IBM, TR G520-2169, 1970]

- Something you know

  password, passphrase, PIN, answers to security questions

- Something you have

  physical key, ticket, {ATM,prox,credit} card, token

- Something you are

  fingerprint, retinal scan, hand silhouette, a pulse

Authentication of humans

- Two-factor authentication: authenticate based on two independent methods
  - password plus registered mobile phone
  - ATM card plus PIN
  - token plus PIN
  - combination lock codes plus gait analysis
- Multi-factor authentication: two or more independent methods
- Best to combine separate categories, not reuse categories
  - non-example: requiring two passwords from a single human: arguably not independent
  - non-example: requiring single password from each of two humans: authenticates two humans then makes *authorization* decision
- What is being authenticated...?

IDENTITY

Personal identity

- Major philosophical problem
  - People are not identical to themselves over time, but their identity persists throughout changes
  - cf. Ship of Theseus
- Intrinsic identity: continuation of consciousness
- Extrinsic identity: relationship to everything else
- Incarnated:
  - Personal identity is made present in a body
  - But is it confined to body?
- Control: individual's, others', no one's?

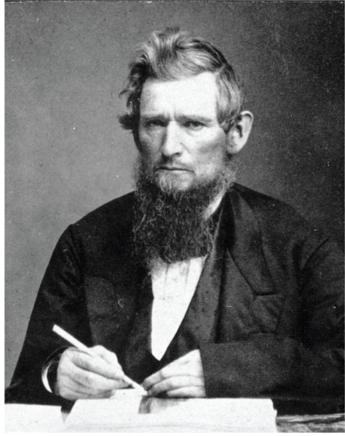
Digital identity

- Digital identity: data that describes a person and its relationship to others
  - not the person itself; not a personal identity
  - fictional people, dead people, virtual people (AIs?)
- A person could have many digital identities, some overlapping, some contradictory
- Data could be incorrect, outdated, incomplete

Aspects of digital identity

- Name
- NetID
- Email address
- URL
- IP address
- Citizenship
- Political party
- …

Identity



- Attribute: property of a principal
  - name is "Ezra Cornell", birthdate is 01/11/1807, mother's maiden name is Barnard
- Identity: set of attributes
  - each principal may have many identities of use in different scenarios (student, taxpayer, athlete)
- Identifier: an attribute that is unique within a population
- Verifier: an attribute that is hard to produce hence can be used as a basis for authentication

Identity

- Enrollment: establishing identity with a system
  - Create an account
  - Get an ID card, visa
  - Register a machine on a network
  - Get a signing key from a provider
- System might (not) verify claimed attributes during enrollment
  - Websites rarely do
  - Governments often do
  - Companies might, especially for a fee

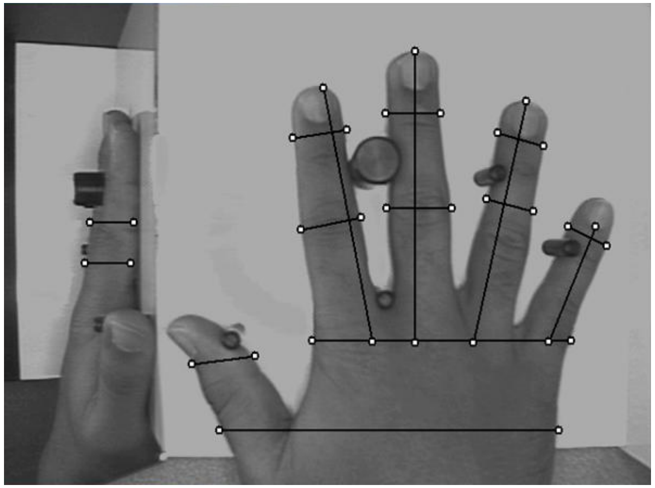
BIOMETRICS

Biometric

- Something you are
- Biometric: measurement of biological and behavioral attributes
  - fingerprint, iris, retina, face, voice, handwriting, hand shape, hand veins, hand print, (DNA?)
  - biological attributes can be confounded by behavior
  - biology and behavior is non-constant: variation from one measurement to the next

Example: Hand geometry

- Used in Olympic Games, Walt Disney World, nuclear facilities, data centers, …
- Camera images palm and side of hand (no texture information)
- Images reduced to (e.g.) 31000 points then 90 measurements then 9 bytes of data
  - Final data not directly related to any source measurements
  - Data stored as a template for later comparison



http://www.biometrics.gov/documents/handgeometry.pdf

Example: Hand geometry

- When user authenticates, another set of images taken
  - If data are close enough to stored template, user deemed authenticated
  - Can adjust threshold per-user, in case some users are difficult to authenticate
- Each time user is authenticated, template is updated to account for change over time

Example: Fingerprint

- Particular use: California social services
  - prevent applicants for welfare from defrauding state by receiving assistance under multiple identities
- Fingerprint stored as bitmap and as minutae
  - When user authenticates, computer compares minutiae
  - If they match, human additionally reviews bitmap images (about 15 out of 10000 authentications have minutiae match even though fingerprints do not)

Biometric attributes as verifiers

Requirements:

- Identifier
- Small variation over time and measurement
- Easy to measure
- Difficult to spoof
- Acceptable to users

Biometric attributes as verifiers

- **Advantages:**
  - Can't lose or forget a biometric
  - Easy to use some biometrics (e.g., fingerprint scan vs. PIN on iPhone)
- **Disadvantages:**
  - Updating identities after disclosure is hard (new fingerprints? new retina?)
    - So enrolling a biometric identifier places **permanent trust** in receiver, even if they go bankrupt, retroactively change privacy policies, get taken over by new administration, ...
  - Impossible to be application specific (your hand geometry is the same regardless of what system you use)
  - Physical process with errors...
  - Fear of negative implications for privacy...

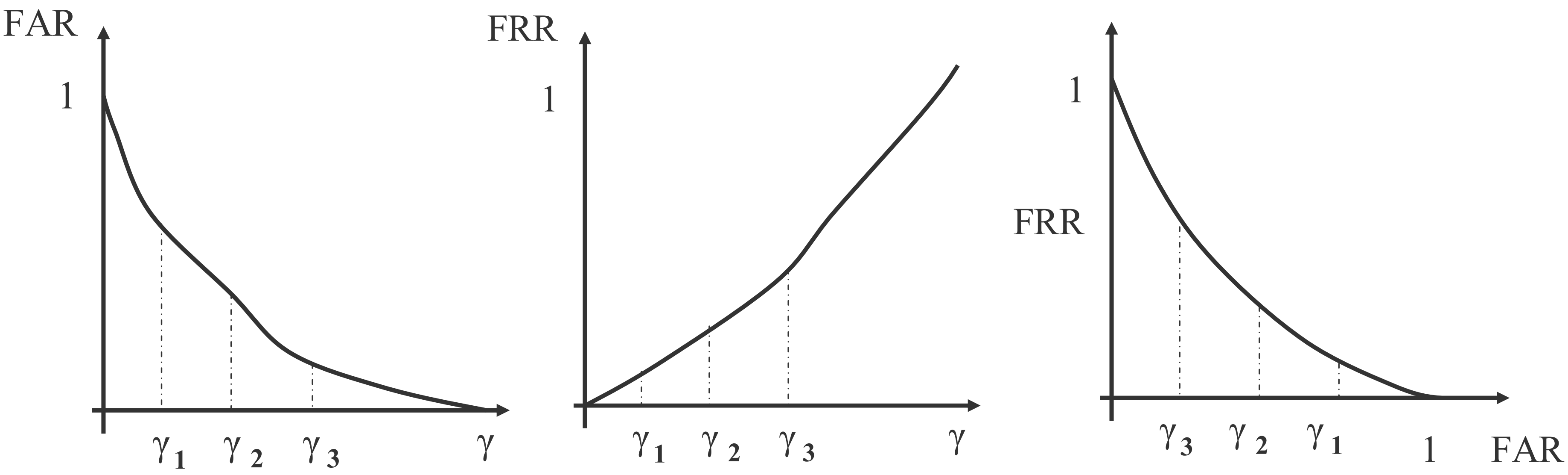
ERRORS

Accuracy

- False accept: authenticate a principal with wrong identity (fraud)
- False reject: fail to authenticate a principal under right identity (insult)
- Hypothesis testing:
  - null hypothesis: human being authenticated has claimed identity
  - false accept = type II error
  - false reject = type I error
- Tunable trade off of sensitivity between which error is more likely
  - False acceptance rate (FAR): percentage of attempts in which imposters are authenticated (with wrong identity)
  - False reject rate (FRR): percentage of attempts in which legitimate users are denied authentication

Sensitivity

Receiver operating characteristics (ROC) curve: graph of FRR vs. FAR (or perhaps 1-FAR, perhaps nonlinear axes)



γ = sensitivity

Graph source: http://www.csee.wvu.edu/~natalias/biom426/performance_fall09.pdf

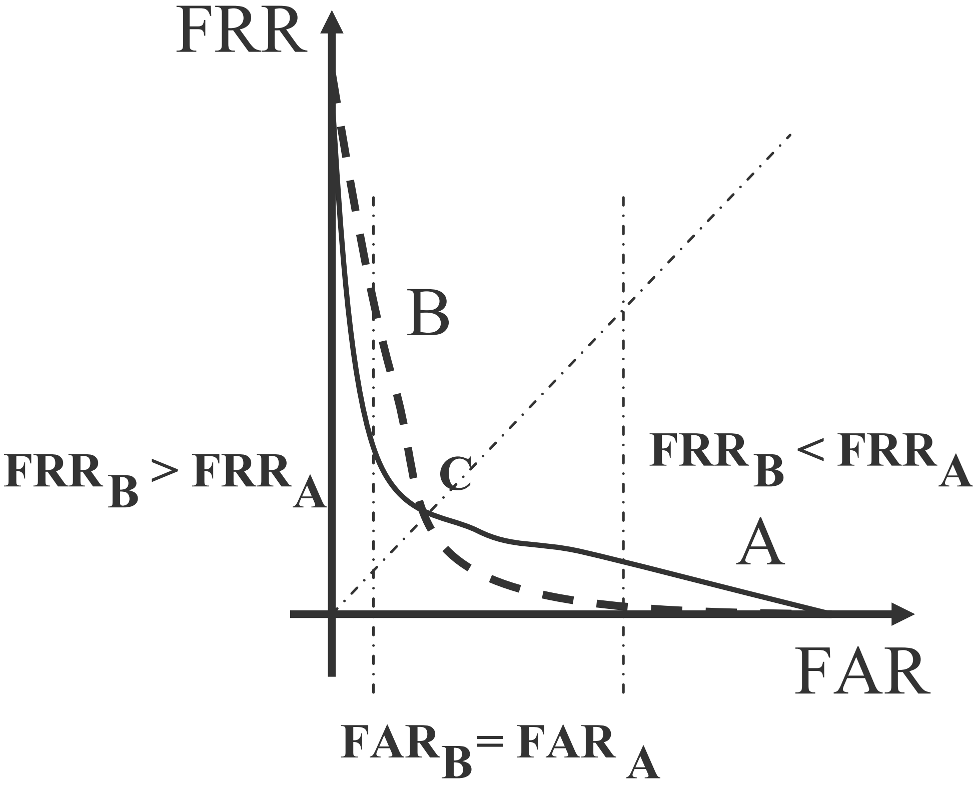
ROC comparison

- Crossover error rate (CER): value on ROC at which FAR=FRR (aka *equal error rate, ERR)*
- Many other statistics for comparison possible
  - Anytime a graph is reduced to a single number, we lose information
  - Maybe what matters most for biometrics is the use case

Use cases

- **Entry to military facility:**
  - letting imposters in might be worse than (temporarily) delaying entry of personnel
  - so prefer low false accept rate
- **Entry to hotel lobby:**
  - letting non-guests in might be better than (temporarily) delaying entry of guests
  - so prefer low false reject rate

ROC comparison



- Two matchers (A=solid; B=dashed)
- At point C, matchers have same FAR and FRR
- To the left of C, matcher A has lower FRR for same FAR
- To the right, matcher B has lower FRR for same FAR

Graph source: http://www.csee.wvu.edu/~natalias/biom426/performance_fall09.pdf

PRIVACY

Privacy concerns

- Governments/businesses and individuals are sometimes at odds over how identity is used
- Intrinsic privacy: the individual's right to be left alone
- Informational privacy: the individual's right to determine for itself when, how, and to what extent information about it is communicated to others

Privacy concerns

- Humans might not want to disclose attributes during enrollment (SSN, political party)
- Humans might have concerns about measurements (have photo taken, parts of body scanned)
- Humans might not want action bound to their identity (buying medication)
- Requiring authentication may inadvertently become a discouraging form of authorization (those who don't want to be authenticated opt out)
- Widespread use of identifiers links identities across systems, exposing humans to inference about what they thought were unrelated activities...

Standard Universal Identifier (SUI)

[US Department of Health and Welfare (HEW), 1973]

- **Uniqueness:** no more than one person can have same SUI; each person must have no more than one SUI (injectivity)
- **Permanence:** SUI must not change during person's life
- **Ubiquity:** entire population must be issued SUIs
- **Availability:** SUI must be readily obtainable and verifiable
- **Indispensability:** Each person must remember SUI and be able to report it correctly
- **Arbitrariness:** SUI must not contain any information
- **Brevity:** SUI must be as short as possible
- **Reliability:** Must be possible to detect errors in SUI

Standard Universal Identifier (SUI)

US HEW report:

- *"A permanent SUI issued at birth could create an incentive for institutions to pool or link their records, thereby making it possible to bring a lifetime of information to bear on any decision about a given individual"*
- *"A universally identified [person] might become a prisoner of [the] recorded past."*
- *"Fear of a SUI is justified... The dangers inherent...far outweigh any of its practical benefits."*

Principles for privacy

When building authentication systems...

- **Seek consent:** get permission to authenticate and store identity
- **Select minimal identity:** use the smallest possible set of attributes
- **Limit storage:** don't save information about identity or authentication without need, and delete when no longer needed
- **Avoid linking:** don't reuse identifiers across systems

Privacy and biometrics

- Biometrics can violate intrinsic privacy by requiring submission to bodily contact or measurement
  - Fear of germs
  - Religious prohibitions
- Biometrics can violate informational privacy
  - Biometric identifiers might effectively become a SUI, enabling linking

Privacy and mobile phones

- Mobile phones broadcast their identity and location at frequent intervals
- GPS receiver on phone can track and report location to provider
- But mobile phones aren't permanently bound to a person

Upcoming events

- [next Wed] A3 due

Be yourself; everyone else is already taken.
– Oscar Wilde