Introduction to Biometrics

Peter T. Higgins

peter.higgins@thehhg.com

1-202-625-7780

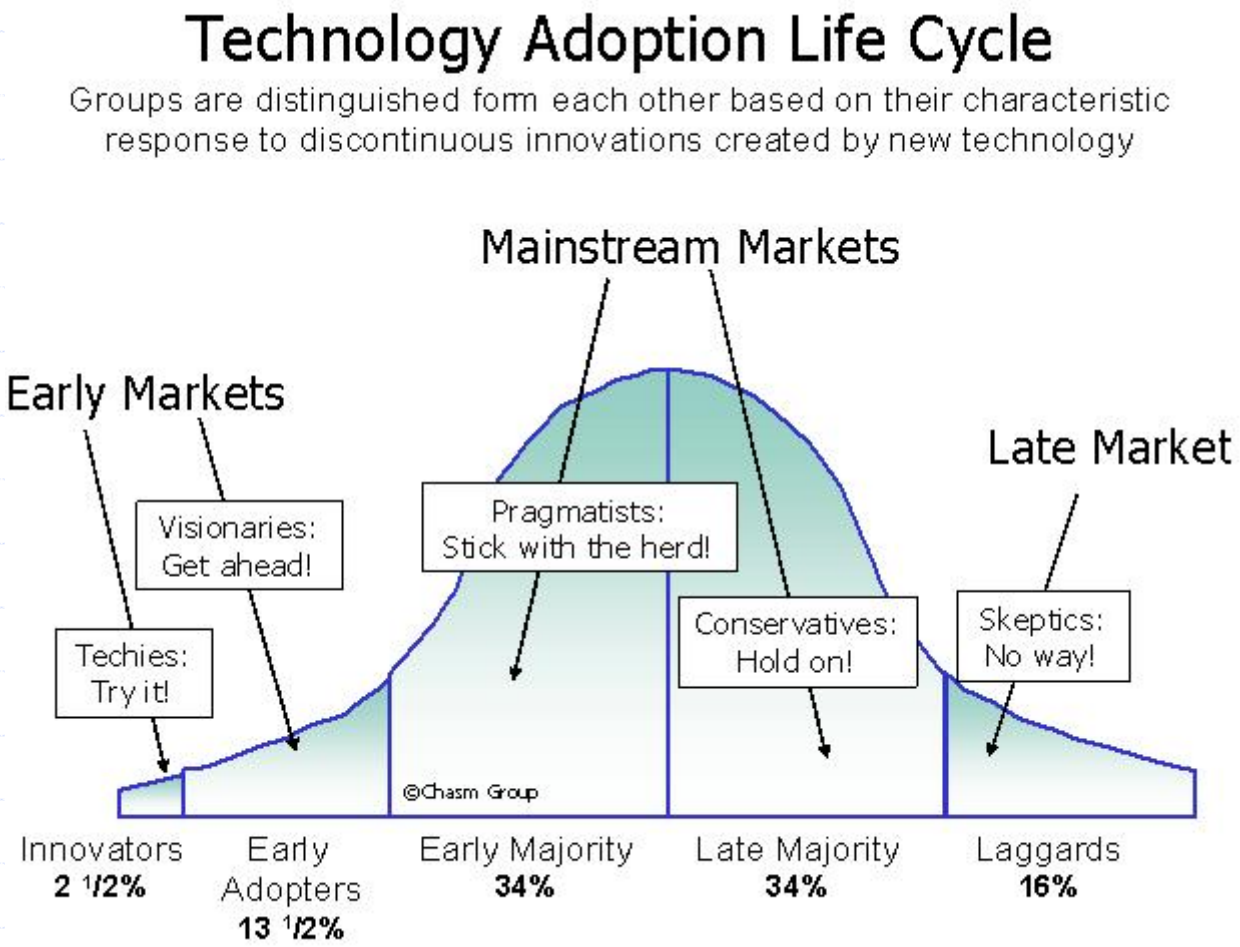
Outline of Presentation

- Biometrics - you are maturing
- Biometrics - your roots are showing
  - Vocabulary, performance metrics, etc.
- Basic Concept of Operations - models
- Vulnerabilities
- Standards
- Mandates

Biometrics - Still Maturing

- Technology - maturing quite nicely
  - Year-to-year performance tests show positive trends
- Industry - maturing
  - Consolidations and realism overcoming enthusiasm and marketing hype
  - Investors still seeking “the year of biometrics”
- Purchasers - broader base but governments still carrying the load

Biometrics - Still Maturing



Biometrics - Still Maturing

- Law enforcement - early adopters
  - Paved the cow paths
- Border crossing - a few visionaries and many pragmatists (really optimists?)
  - Follow the leader and then branch out
- Large Scale ID verification - pragmatists in the main
  - Building on the work of the techies and visionaries such as RAPIDS/DEERS

Biometrics - many roots

Vocabulary, metrics, uses, etc.

Biometrics Is …

- “Something you know, something you have, something you are.”
  - IBM InfoSec paper (G520-2169) - 1970
  - Ben Miller’s “Dynamic Model of Identification” - 1984
  - Everyone - 2005

Biometrics Is …

- The automated recognition of individuals based on biological and behavioral characteristics.

OR

- A measurable physical characteristic or personal behavioral trait used to recognize the identity of an enrollee or verify a claimed identity

Biometrics Is …

- Biometric is an adjective
- Biometrics is a noun
- Presentation of your “biometric sample” is strongly influenced by your behavior

Probabilistic

- Capture - extract features - store (enroll)
- Capture transaction time sample - extract features - compare to enrolled template - assign closeness score or ranked list of similar biometric samples - return signal
  - Every capture is an adventure

Degrees of Automation

- Fully: single finger logon or hand geometry gate
  - Right score - open file or gate
- Partially: US Visit
  - Fingerprint match results - a decision support tool
- Minimally: Latent fingerprints
  - AFIS - a search accelerator

Stepchild of Many Parents

- People working facial recognition in the 1980s had no perceived relationship with fingerprint people who had no inkling that speaker recognition systems were in the same field
  - Now an integrated (well sort of) field of study, application, and investment

Vocabulary Evolution

- Biometrics is …
  - SC37 WG4 is defining a set of standard definitions - 20 years into the discipline
- Collection of enrolled templates is …
- A search record is …

Collection of Templates is …

- Repository - fingerprint matching
- Gallery - facial recognition
- Corpus - speaker recognition
- Database - everyone

Search Record is …

- Search print (known print) or latent (unknown print) - fingerprints
- Probe - faces
- Utterance - voices
- Hand - hand geometry
- Sample - all

A Match is …

- Match
- Mate
- Hit
- Acceptance
- True positive
- Successful presentation
- …

Process Evolution

- Best Practices, UK Biometrics Working Group
- Best Practices V2, UK Biometrics Working Group
- ISO/IEC 19795-X Biometric Testing & Reporting

Error Types are …

- Failure to enroll
- Failure to acquire
- False match - False accept - False positive
- False non-match - False reject

- For large populations - all are non-zero - for all biometrics

Error Rate Factoid

- A 3% failure to enroll or failure to acquire does not mean 3% of the time each user will experience a problem
- It is far more likely that 3% of the enrolled population will experience problems nearly 100% of the time

Open vs. Closed Set Testing

- Open set - search samples from people not enrolled in the system can and will be used
  - Simulates the real world use of biometrics
- Closed set - search samples are from the same population as the enrollees
  - Only false claim of identity within the set can occur - not real world - avoid

Performance Metrics are …

- Reliability and Accuracy
  - ANSI/IAI 1985
- True / False accept rate
- Equal error rate
- Receiver operating characteristics (ROC) - DET
- Cumulative match characteristic curve (CMC)

Reliability & Accuracy

- Reliability is the probability that the system will find the matching record (I.e., a true match)
- Accuracy is the probability that the system will not return the wrong answers (I.e., return a false match)

ROC Definition

- Receiver operating characteristic (ROC) curves are an accepted method for summarizing the performance of imperfect pattern matching systems.
- An ROC curve plots, parametrically as a function of the decision threshold, the rate of “false positives” (i.e. impostor attempts accepted) on the x-axis, against the corresponding rate of “true positives” (i.e. genuine attempts accepted) on the y-axis.
- ROC curves are threshold independent, allowing performance comparison of different systems under similar conditions, or of single system under differing conditions.

ROC Example

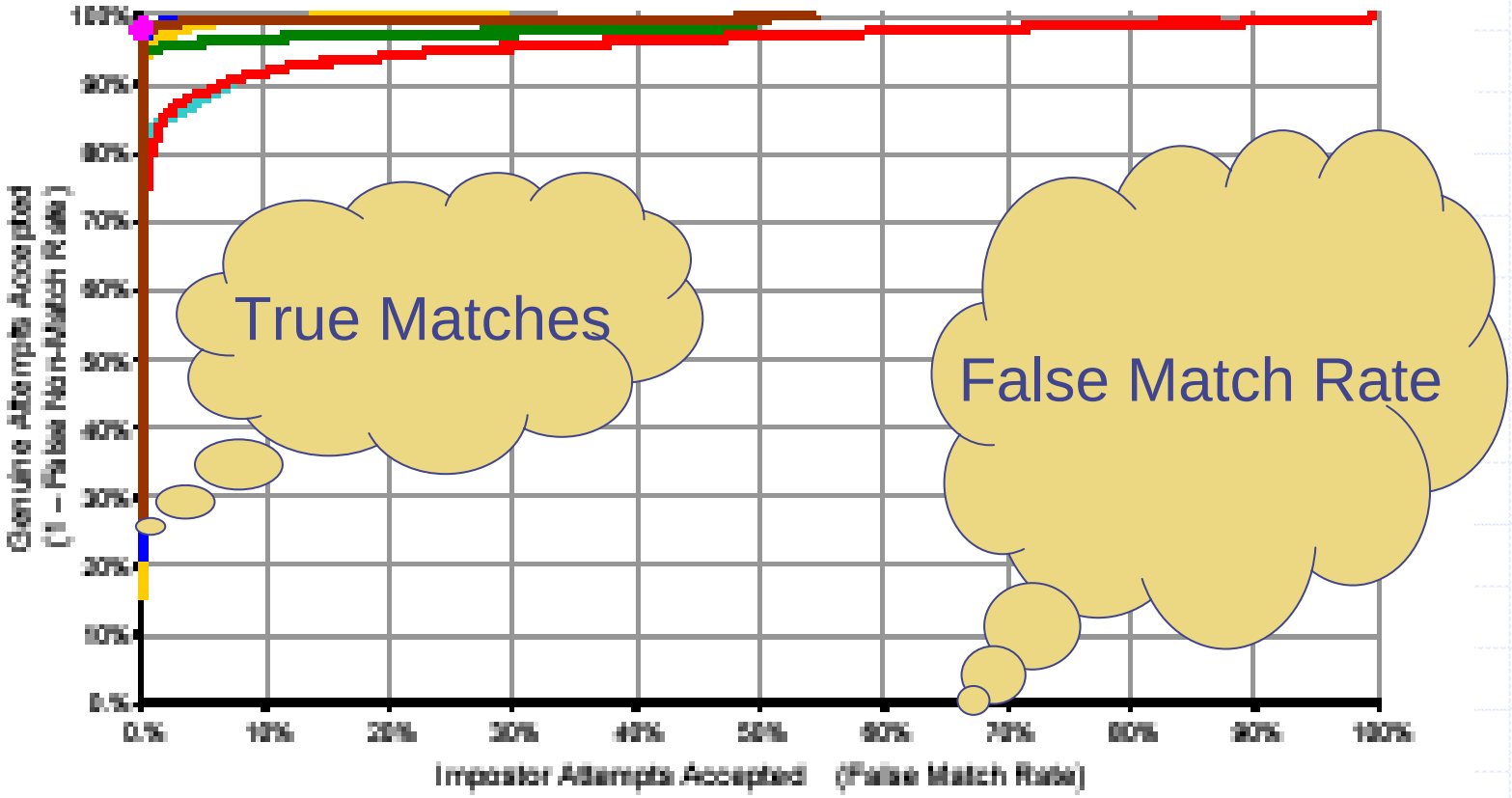


Figure 2 Example ROC curves

DET Definition

- **Detection error trade-off (DET) curves:** In the case of biometric systems, a modified ROC curve known as a “detection error trade-off” curve is preferred.
- A DET curve plots error rates on both axes, giving uniform treatment to both types of error. The graph can then be plotted using logarithmic axes. This spreads out the plot and distinguishes different well-performing systems more clearly. E.g., the DET curve [next chart] uses the same data as the ROC curve on the previous chart.

DET Example

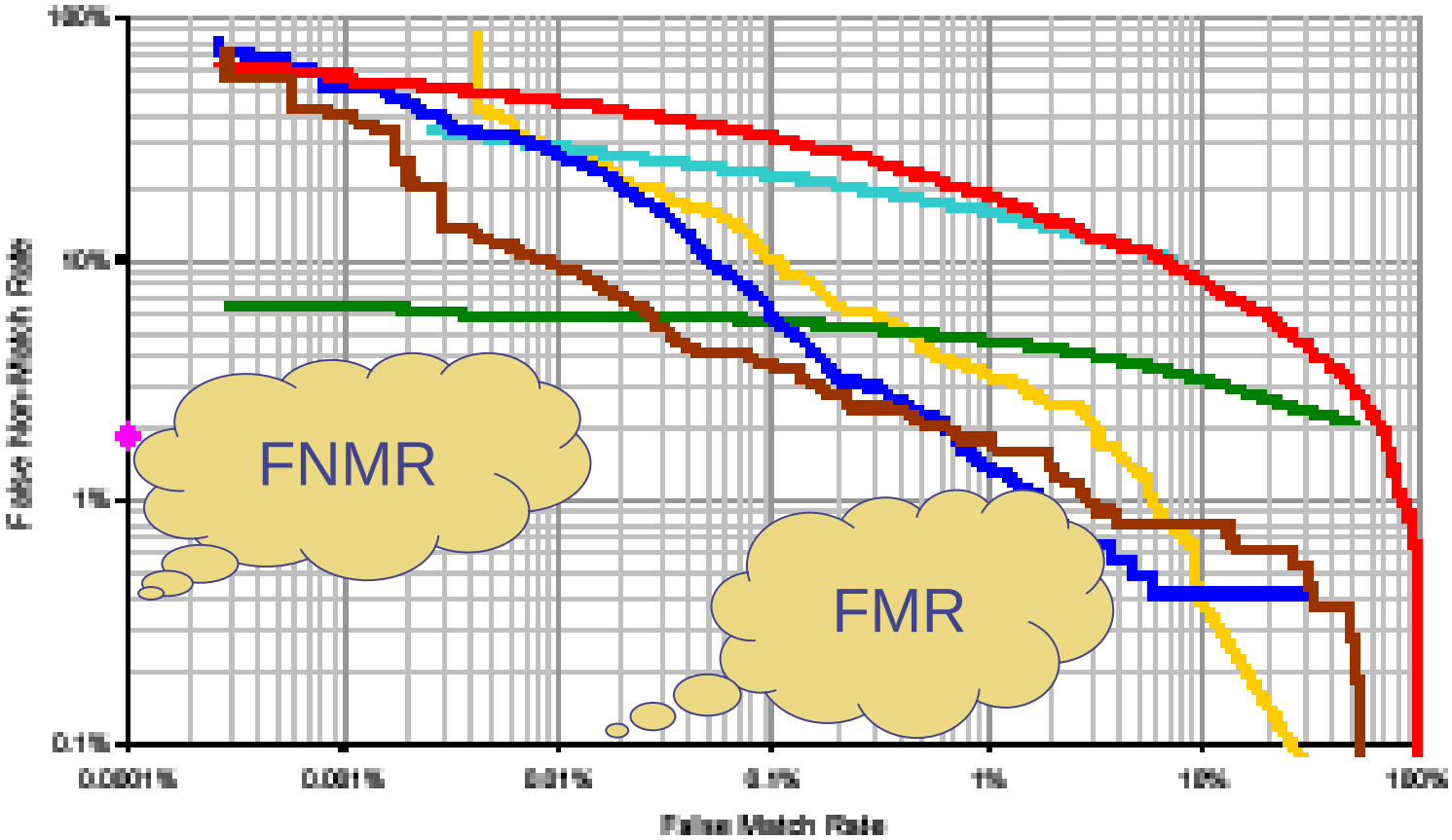


Figure 3 Example DET curves

CMC Definition

- A Cumulative Match Characteristic (CMC) curve plots the probability of identification against the returned 1:N candidate list size.
  - It shows the probability that a given user appears in different sized candidate lists. The faster the CMC curve approaches 1, indicating that the user always appears in the candidate list of specified size, the better the matching algorithm. (DAON)

Performance Metrics are …

- Throughput
  - Same as capacity?
- Response time
  - Same as transaction time?

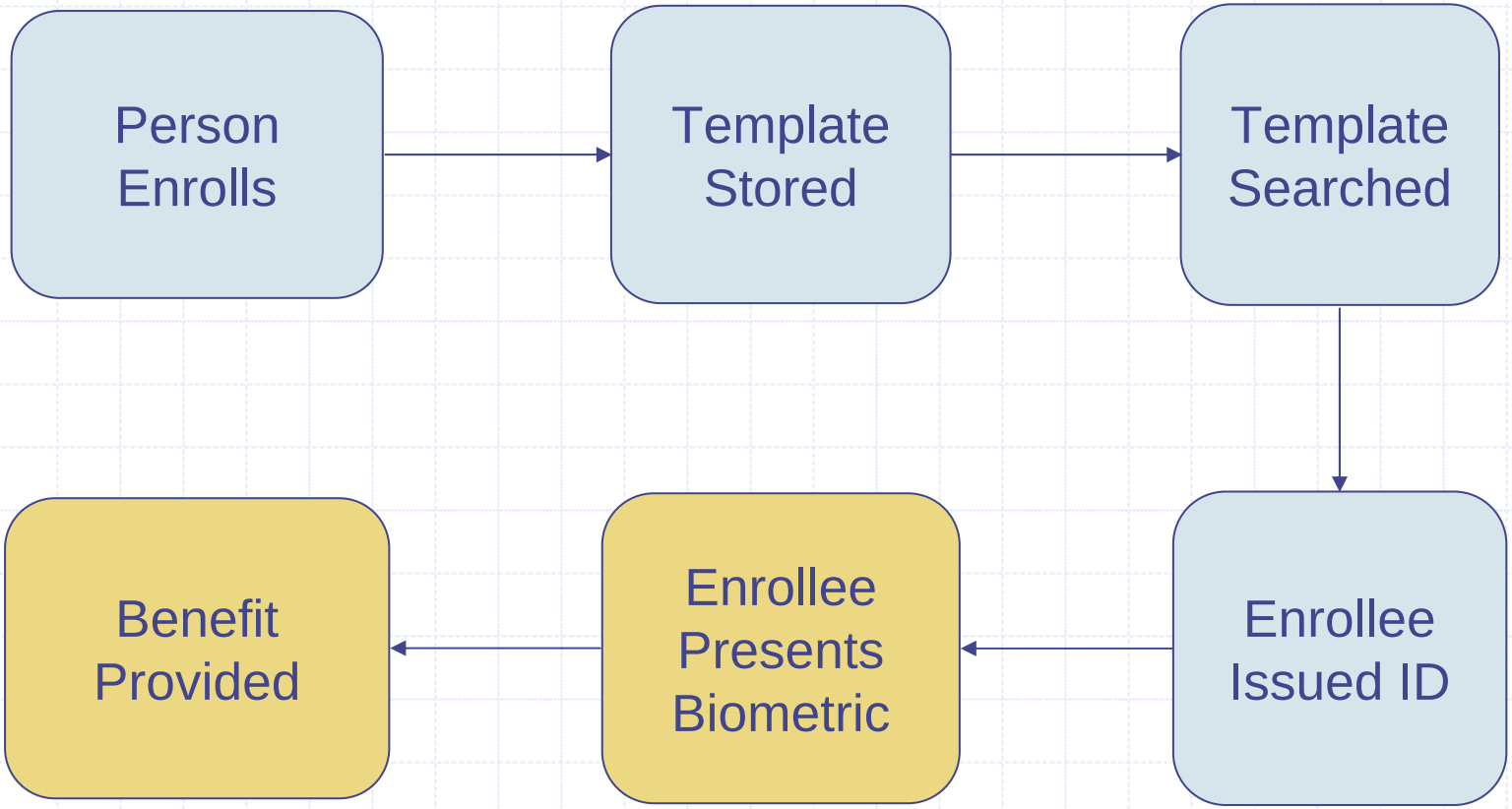
Basic Concept

Enroll, use, enjoy, …

Workflows

- Workflows vary all over the map
  - Think law enforcement vs. access to your own laptop
- Enrollment-through-use examples follow
  - End-to-end-processes for benefits, enforcement, convenience

Idealized Model



Enrollment

- Definition
  - 1. vti to enter your own or somebody else's name on an official register or list of members
  - 2. vt to make sure that something, especially somebody's help, will definitely be available

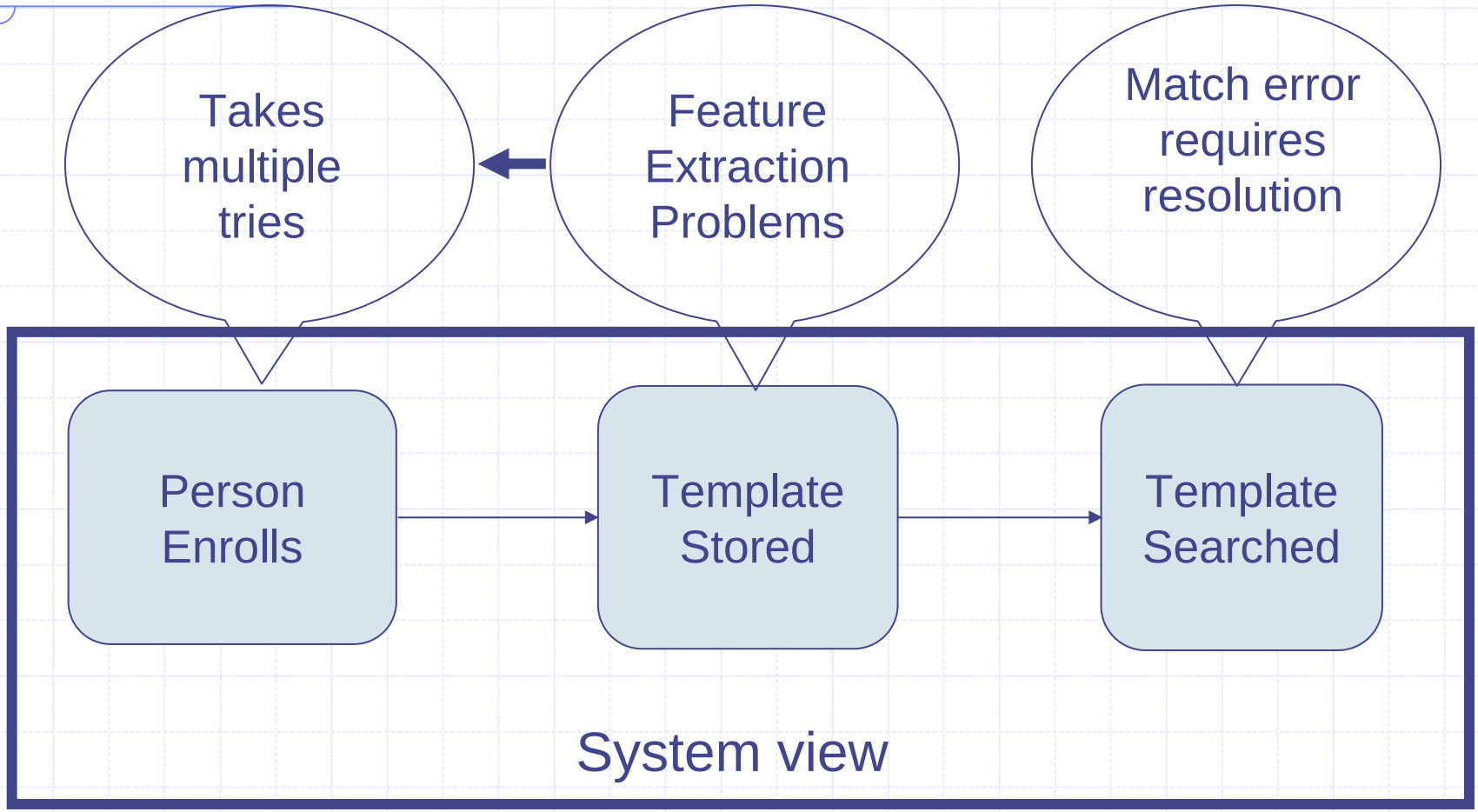
School

AAA

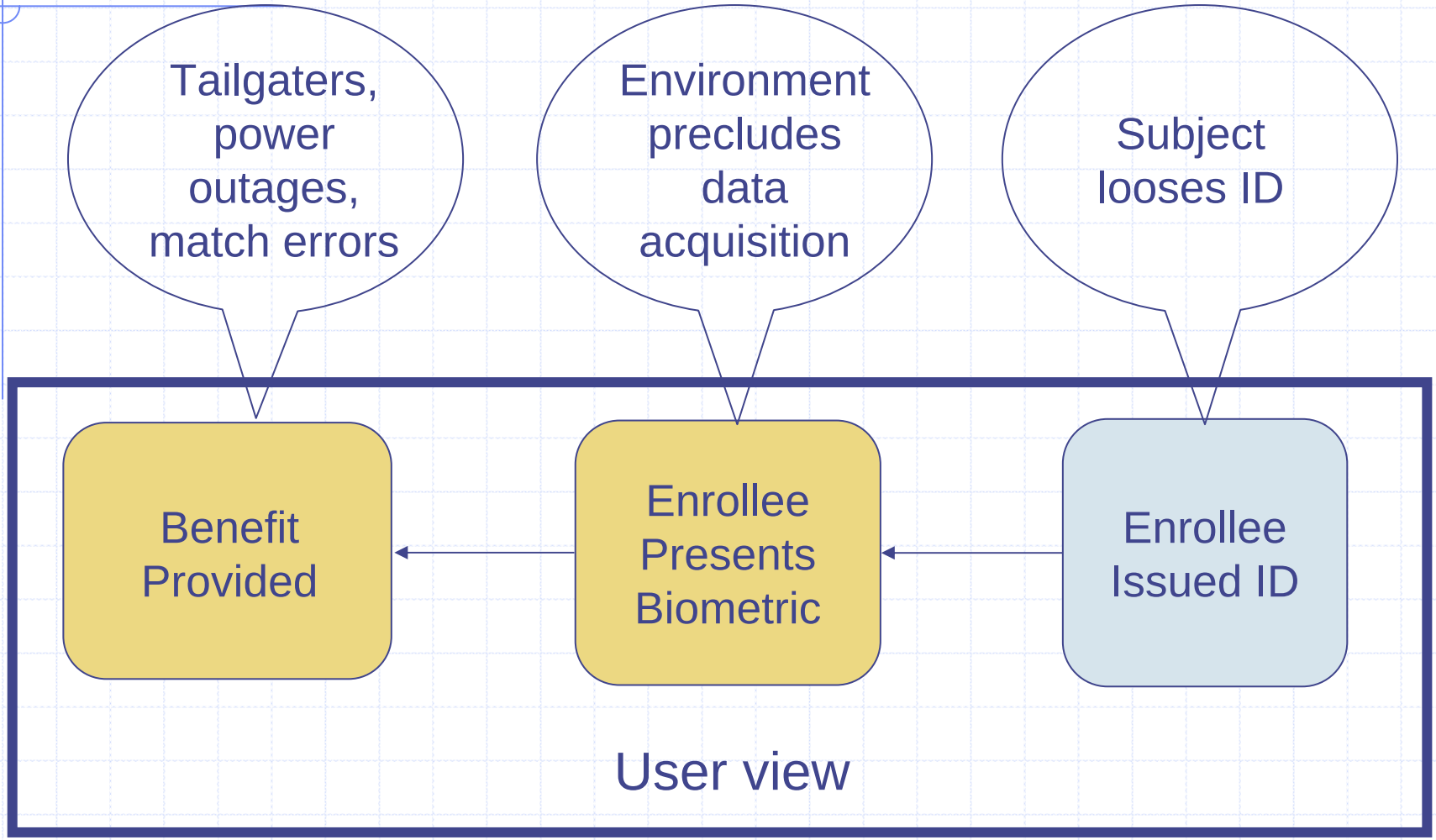
Capture: at Enrollment & Use

- Variables include
  - Presentation
  - Environment (light - noise - objects)
  - Person (age - time of day - time since last use - illness/injuries)
  - Collection device (calibration, quality, similarity to original enrollment device)

More Realistic Model



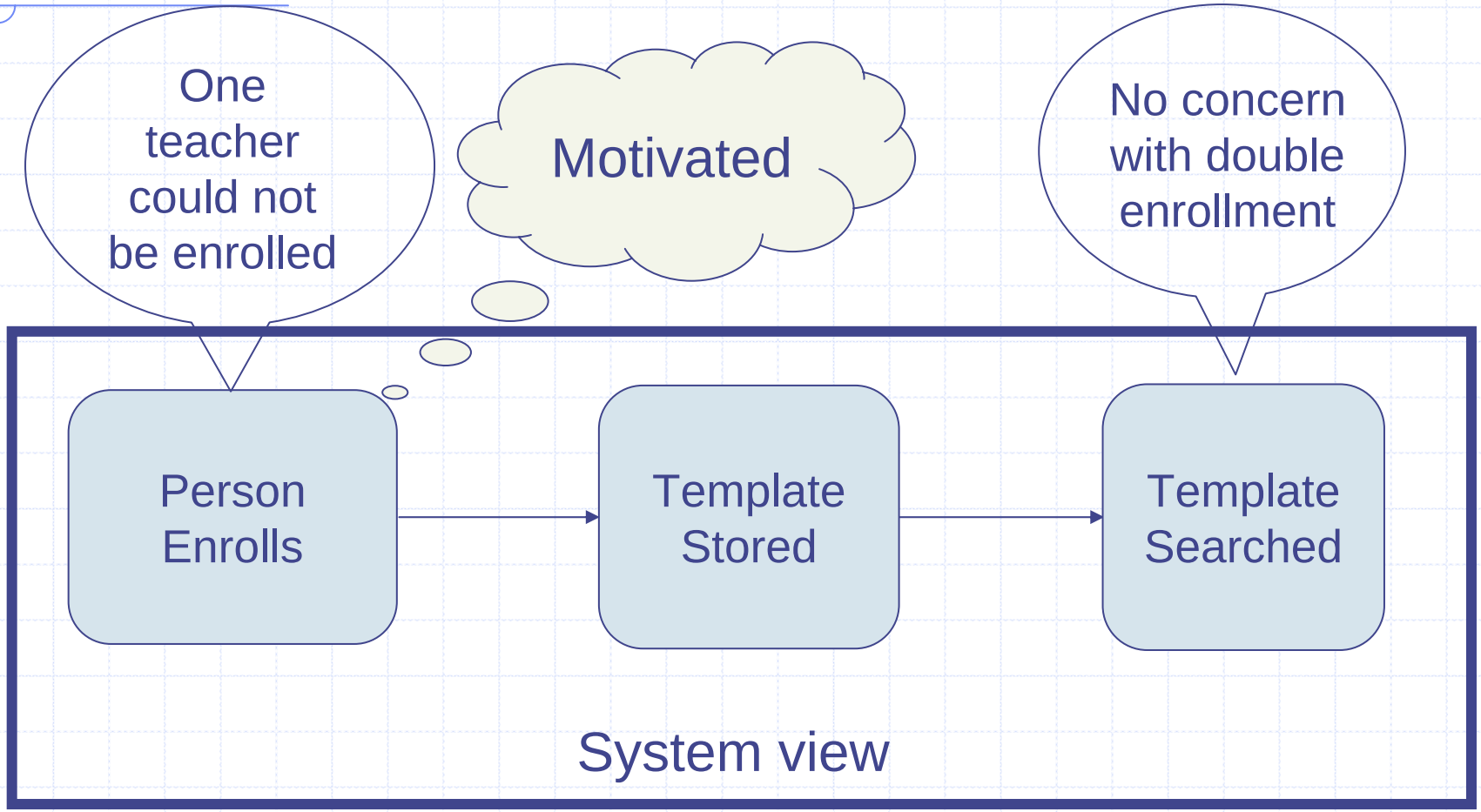
More Realistic Model



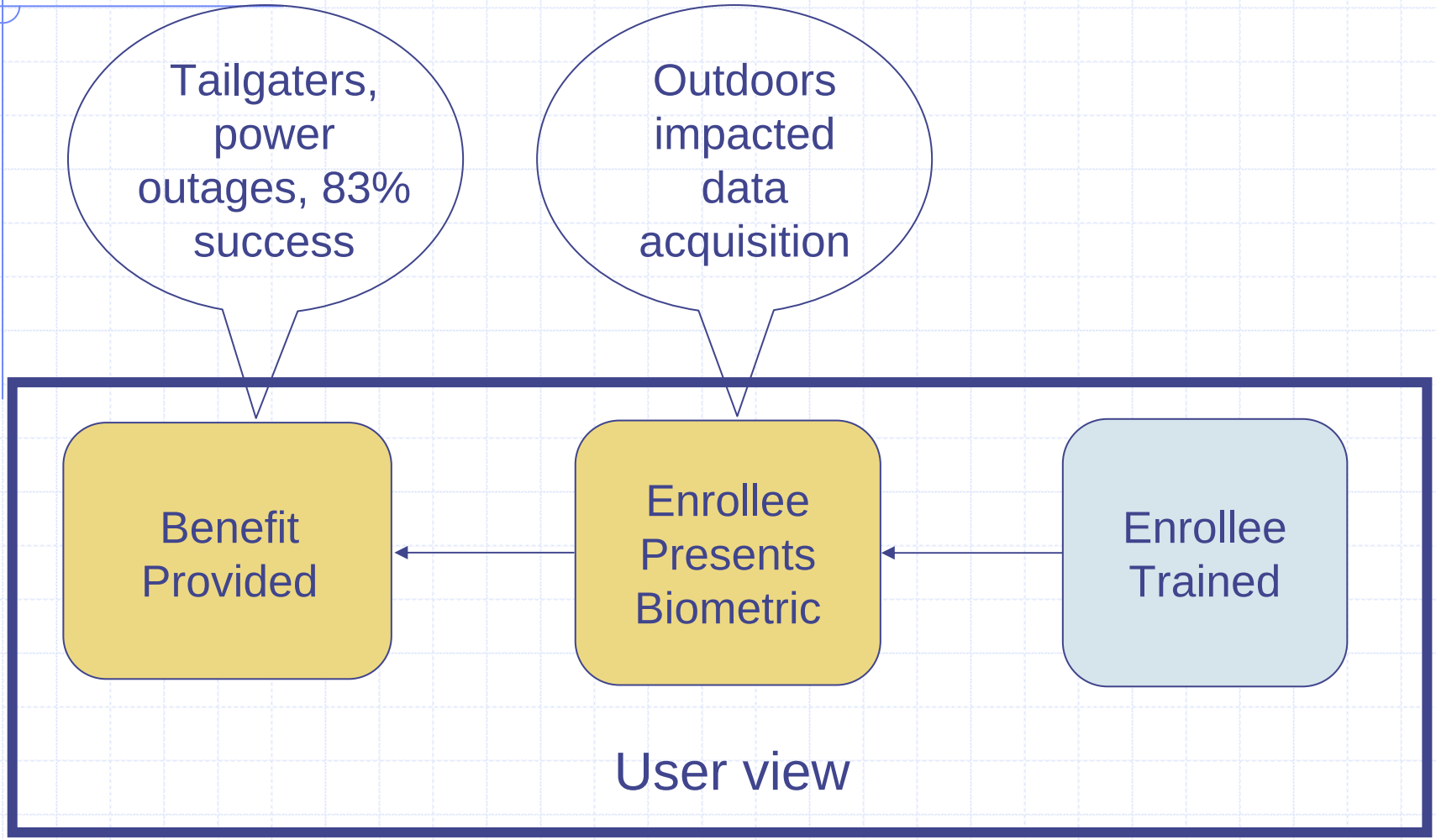
Benefit Model

- In September 2002, the Plumsted Township (NJ) School District received a federal grant to install iris recognition technology in its three schools:
  - New Egypt Elementary School,
  - New Egypt Middle School, and
  - New Egypt High School.
- The project was named T-PASS: Teacher-Parent Authorization Security System.

Benefits Experience



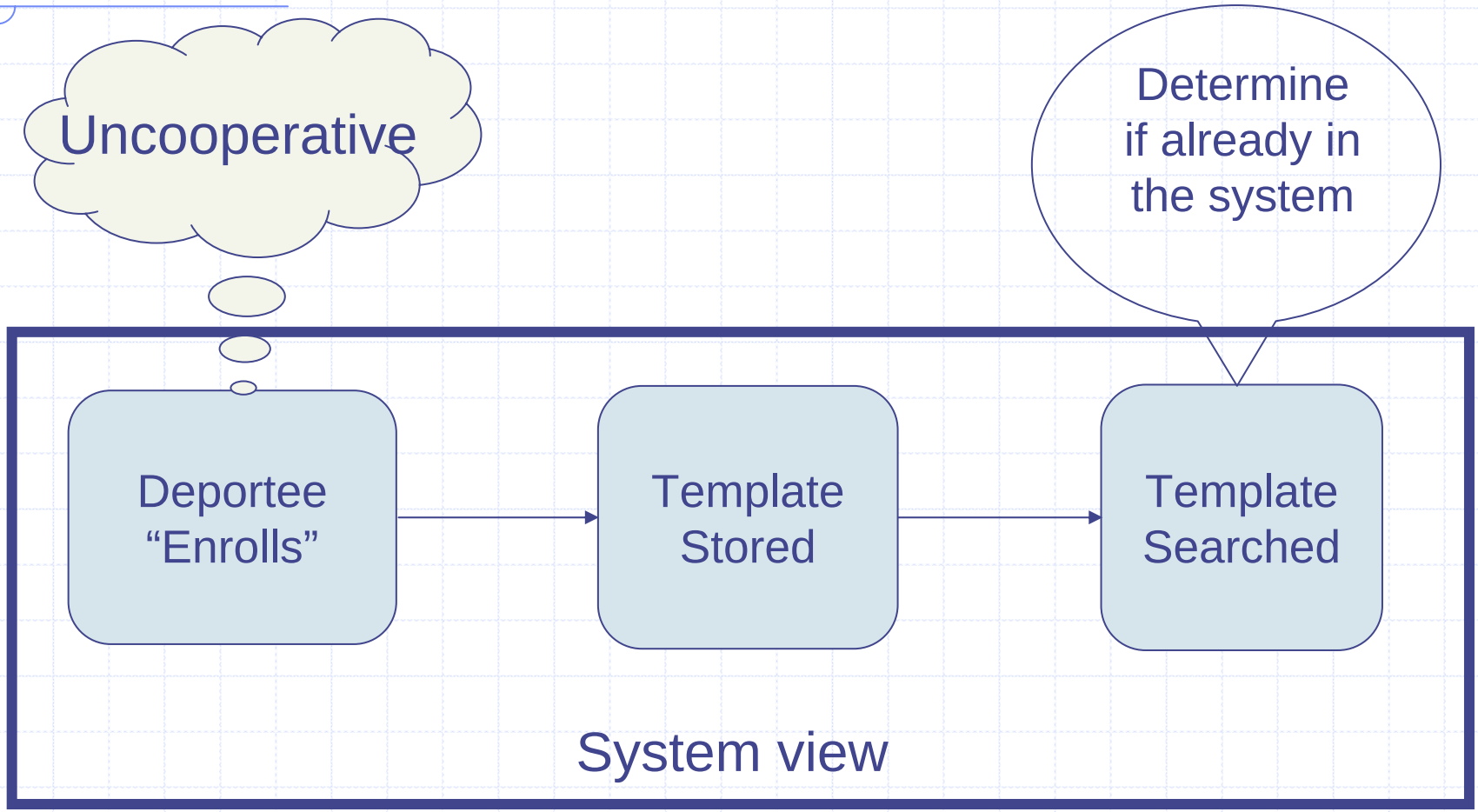
Benefits Experience



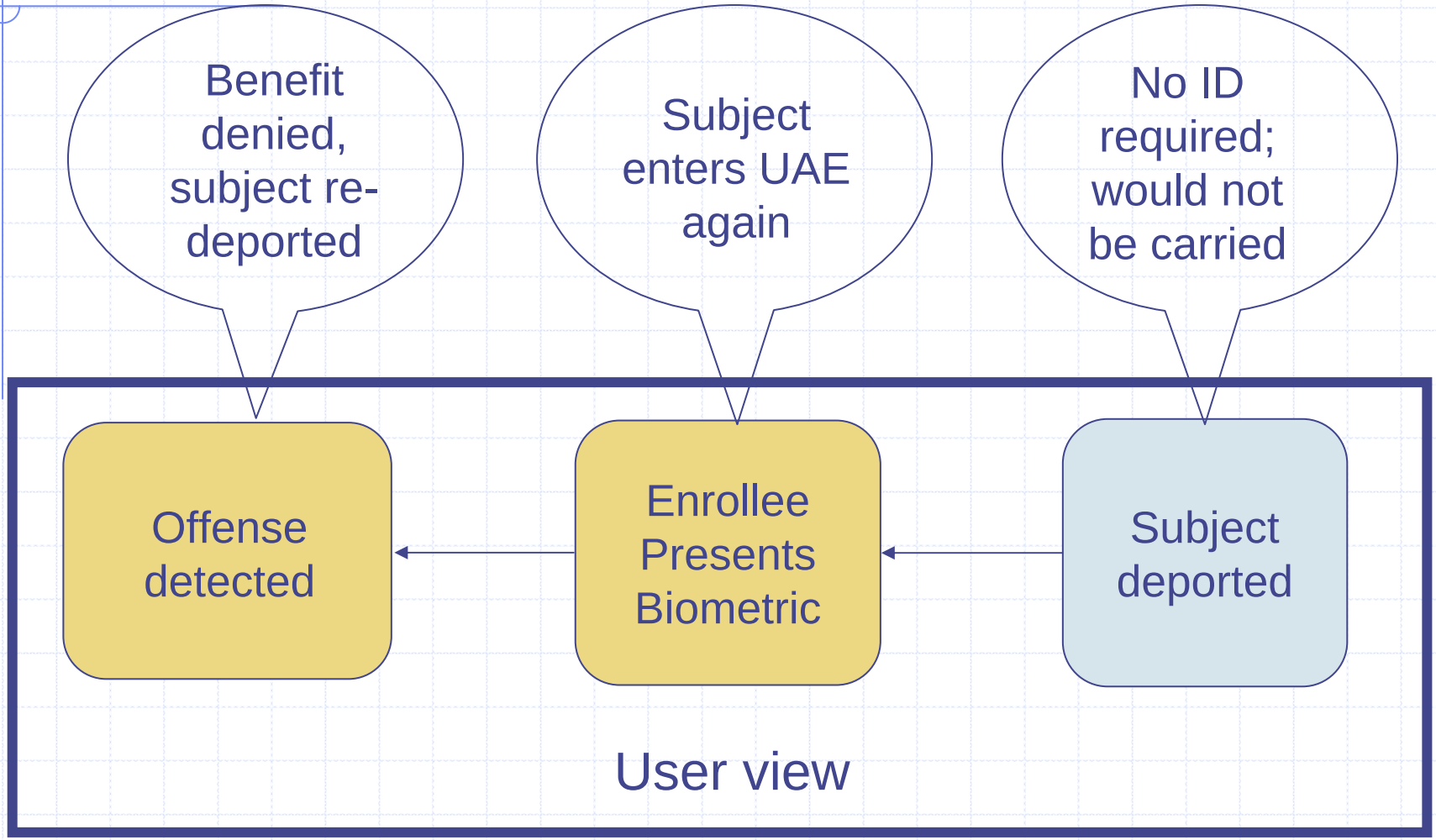
Enforcement Model

- The UAE started the “Eye Scan Project” in 2000 by installing systems at three major jails. The project was expanded to ports and airports in 2002.
  - At the Dubai airport all arriving passengers have to wait in line to have their eyes scanned.
  - By early 2004 the UAE Expellee Tracking System
    - Over two million transactions
    - 420,000 deported persons enrolled
    - Identified over 9,500 people attempting to re-enter the UAE with fraudulent travel documents

Enforcement Model



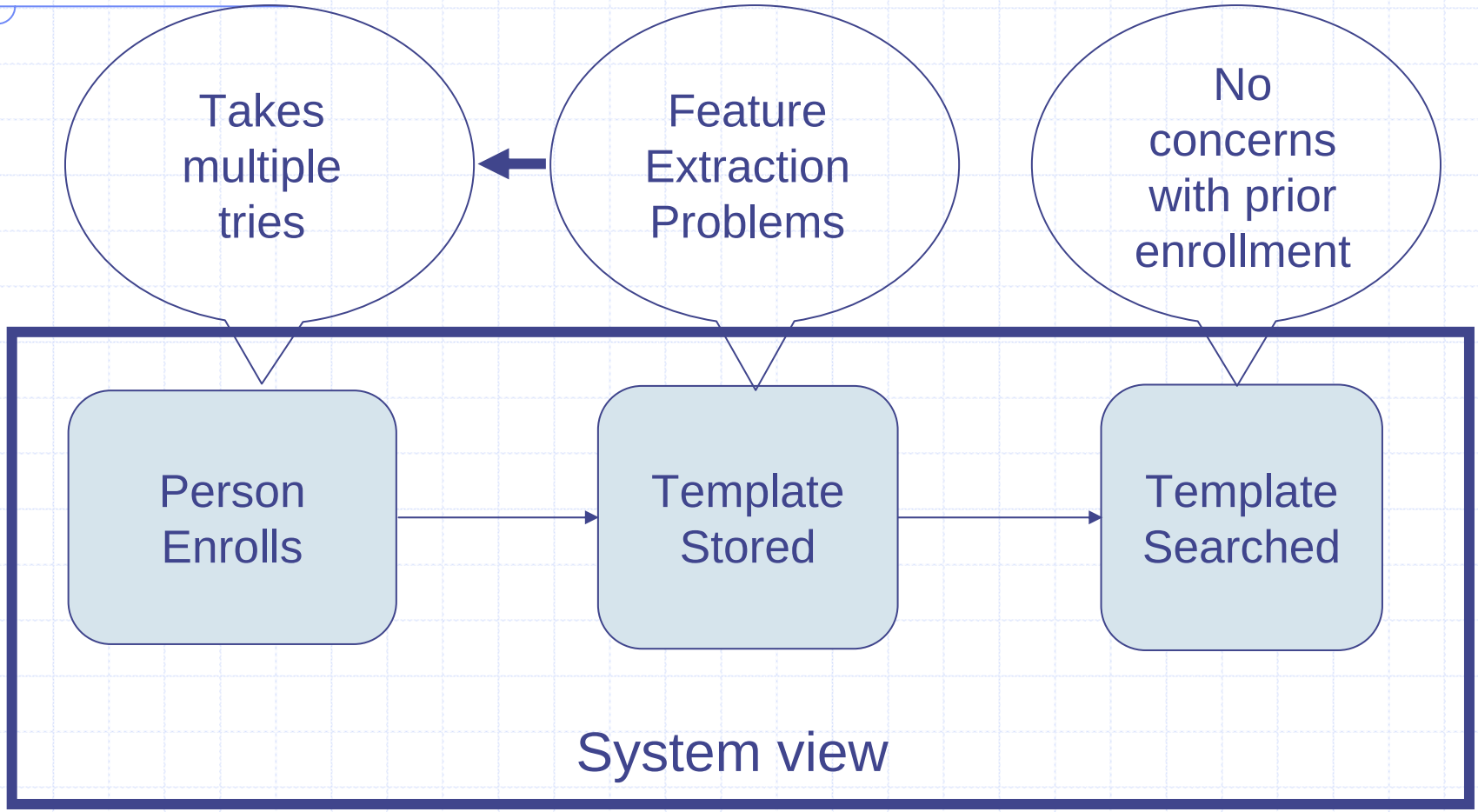
Enforcement Model



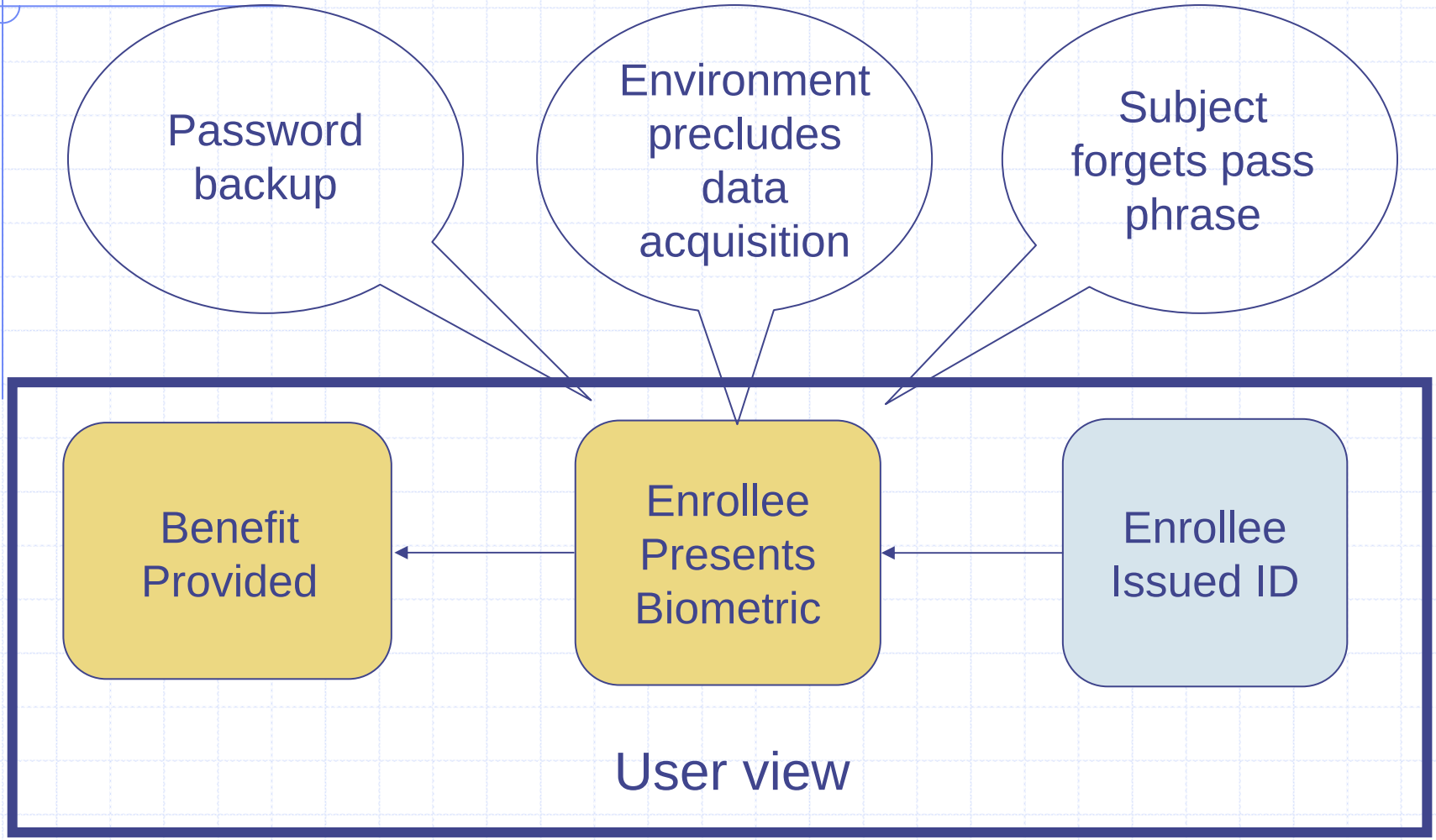
Convenience Model

- Apple put speaker verification in the Mac Operating System (OS 9)
  - Used built in microphone
  - User enrolled their own phrase
  - User prompted with a clue
    - Had to match the spoken phrase
  - Two challenges: ambient noise and public use of phrase

Convenience Model



Convenience Model



Vulnerability

The unspoken danger

Vulnerability Evolution

- Silicon finger spoofs noted as early as 1984 by Sandia National Labs
- Academic papers
- Government and journalist experiments
- Attack points are everywhere
  - Data collection, transmission, signal processing, data storage, and decision logic

Attacks

- “I am not known to the system”, even though I am enrolled
- “I am a known person”, other than myself

Defense

- Common Criteria Protection Profile
- Supervision

Standards

Key to interoperability

Standards Evolution

- Multiple committees
- Extreme sensitivity to possibility of leaving a biometric or a company behind
- Logically standards require vocabulary harmonization

Most Mature Standard

- Fingerprint image exchange
  - IAFIS was the driving force
  - NIST has held workshops in 1992/3; 1997; 2000; and 2005
  - Covers fingerprints, faces, palms, etc.
  - Domains of interest have specified their implementations: US, Canada, Interpol, etc.

Mandates for Biometrics

Biometrics writ large

Mandates

- 9/11 has led to numerous mandates for biometrics (or something that looks like biometrics)
  - US VISIT
  - Biometric Passports
  - Biometric VISAs
  - PIV Card
  - P.L. 109-13 Real ID

US Visit

- Excellent program that uses biometrics for several things:
  - Enforcement
    - Link foreigners to past criminal activities, international warrants, latent fingerprints, etc.
  - Benefits
    - Screen VISA applicants, refugee claimants, etc.

Biometric Passport

- Implementation of ICAO Standards:
  - Face
    - Digital JPEG Facial Image initially - no template
    - Facial recognition features could be added in the future - ANSI/INCITS 385-2004
  - Finger and irises
    - Future options under ICAO

Biometric VISA

- Prescreened through fingerprint and facial image checks
- No biometric on VISA
  - Pointers to stored facial image and fingerprints in various files
    - Fingerprint verified through US Visit when VISA is presented to DHS immigration officer

PIV Card

- Personal Identity Verification Card
- Think Common Access Card for the rest of the government
  - Employees and certain contractors
- Uses
    - Verify ID through facial image on face of card
    - Verify card integrity through PKI
    - Biometrically verify ID through fingerprints
- Issue
    - Standard calls for fingerprint images
    - Push is for tokens

Real ID

- Compliments The Intelligence Reform and Terrorism Prevention Act of 2004
  - Delegates authority to the Secretary of Transportation, in consultation with the Secretary of Homeland Security, to issue regulations on minimum standards for federal acceptance of drivers' licenses and personal ID cards
- Requires facial images but no biometric tokens or use
  - Privacy risks: Bar codes with lots of personal data and potential for biometric use of images

Questions?

peter.higgins@thehhg.com