

Biometrics: The future is at our fingertips?

Prof. James L. Wayman,
FIET

JLWayman@aol.com

What's in a Name?

“Biometrics” -- the automated recognition of individuals based on their biological and behavioral characteristics --- ISO/IEC JTC1 SC37 Working Group 1

This use of the term dates to 1980. Between 1960 and 1980, “Automated Personal Identification” was used.

“Biometrics” – the application of statistical methods to biological data – Oxford English Dictionary, 10th Edition, 2002



Not Included in Definition

Deception

Intent

Identity/identification

Security

Most forensic human identification

Biometric technologies can be **part of** security and identity management system

Recognizing “Individuals” by Their Bodies



- Recognize “me” by inspecting my body
- Define “me” as my body
- Discomfort with equation articulated as “invading my privacy”
- Assumption of autonomous social function by bodies without agency

Beyond Access Control

- Two applications
 - Establishing I am known (recognized)
 - When I give you an identifier
 - When I don't give you an identifier
 - Establishing I am not known (recognized)
- But no biometric method guarantees the validity of the non-biometric data in the database
- Once you have determined who you think I am, biometrics can link me to that identity

Positive Claims

- To prove I am known to the system
- Prevent multiple users of a single identity
- Matching sample to single stored reference
- False match allows fraud
- False non-match is inconvenient
- Multiple alternatives
- Can be voluntary



Negative Claims

- To prove I am not known to the system
- Prevent multiple identities of a single user
- Matching sample to all stored references
- False non-match allows fraud
- False match is inconvenient
- No alternatives if recognition needs to be persistent over time
- Mandatory for all users

PINS and Passwords Do Not Compete With Biometrics

- In positive claim systems, if there exist data subjects with no interest in preventing multiple users of single identity
 - Disney
 - New York Times web site
- In negative claim systems, if there exist data subjects with no interest in preventing multiple identities and time period is extended
 - Social Service systems
 - National ID
 - Driver licensing
- If data subjects can be depended upon to protect system or recognition does not extend over time, biometrics may not be required
 - With credit/bank cards, data subjects need to prevent multiple users
 - In loyalty programs, data subjects need to prevent multiple identities
 - In voting or prison access, use indelible ink.

Key Issues

- Expense and complexity
 - Added hardware
 - Retained exception handling
- Is specialized enrollment necessary?
 - PINs and passwords can be assigned on-line or in the mail
 - For biometrics, bodily presence is generally necessary
 - National ID => one enrolment, multiple apps
- Usability by everyone
 - Effective to use (effectiveness)
 - Efficient to use (efficiency)
 - Enjoyable to use (satisfaction)
 - Easy to learn (learnability)
 - Easy to remember (memorability)

Summary

- Access control is only one application of biometrics and perhaps not the most important
- Biometric technology may be the only technology appropriate for some applications
- PINs and passwords do not compete with biometrics
- Establishing the business case has been difficult in nearly every deployment
- Applications have increased dramatically since the first deployments in the 1970s
- Applications will become even more ubiquitous over the next two decades