



**Biometric
Technology**



Features:

- Biometrics are automated methods of recognizing an individual based on physiological or behavioral characteristics (fingerprints, retina, iris, face, wrist veins, hand geometry, speech and handwritten signatures)
- Biometric recognition can be used in *identification mode*, where the system identifies a person from the entire enrolled population by searching a database for a match
- Can also be used in *verification mode*, where the system authenticates a person's claimed identity from his/her previously enrolled pattern
- Data can reside on a web-server (requires fingerprint reader to be connected to a computer that is connected to the internet), or on a smart-card (user inserts his credit-card sized smart-card into device, and puts finger on reader)

Terms to know:

- False-Acceptance rate (percentage of impostors accepted)
- False-Rejection rate (percentage of authorized users rejected)
- Equal-Error rate (the decision threshold is adjusted so that the false-acceptance rate equals the false-rejection rate)

Benefits:

- Cost is low for initial hardware and lifetime support
- Biometric systems are very accurate
- Systems are quite user-friendly
- Cannot be lost, stolen, duplicated, forgotten, shared, observed or left at home
- NOTE: newer methods, even those with a great deal of scientific support such as DNA-based matching, sometimes do not hold up in courts of law

Applications in Agricultural Security:

- Verifying a purchaser of products (i.e. PCO to ensure that he is licensed to buy and use restricted use products)
- Background checks (i.e. making sure that a potential applicator or PCO is not a child molester or terrorist)
- Access to web-sites with sensitive information
- Physical access to a building can be validated through the use of various biometric devices

The way to achieve fast, user-friendly authentication with a high level of accuracy.