Biometric Authentication Model

- **Biometric Registration**
- **Biometric Capture Device**
- **Feature Extraction**
- **Feature Matching**
- **Authentication Request**
- **Authenticated**
  - Yes / No
Attacks on Biometrics

- Attack the database
- Attack the network – Replay
- Attack the sensor or other part of the trusted computing base
- Attack the registration process
  - Dummy finger
  - Contact lenses
  - Disguises
- Collusion
Security Considerations

- Biometrics are not secrets and are therefore susceptible to modified or spoofed measurements
- There is no recourse for revoking a compromised identifier
- Threatens individual right to anonymity
  ✦ Cultural concerns
  ✦ Religious concerns
  ✦ Violates civil liberties
Types of Biometrics

- Physiological
  - Fingerprints
  - Retinal patterns
  - Face
  - Hand geometry
  - DNA (not yet used for authentication)

- Behavioral
  - Keystroke dynamics
  - Voice
Fingerprints for Biometric Authentication

**MAIN SHAPES:**
- ARCH
- WHORL
- LOOP

**MINUTIAE:**
- END
- BIFURCATION
- ISLAND
- LAKE
- DOT

**EACH PERSON HAS A UNIQUE ARRANGEMENT OF MINUTIAE:**
Fingerprint Capture

**Biometric Authentication**

- **ST-Micro TouchChip** (Capacitative)
- **American Biometric Company BioMouse** (Optical)
- **Biometric Partners Touchless Sensor**
- **Thompson-CSF FingerChip** (Thermal-sensed swipe)

Dr. Indrajit Ray, Computer Science Department
Discussion

- Very low false acceptance rate
  - Typically 95–98% accurate
  - Accuracy varies depending on gender, racial characteristics
- Relatively high false rejection rate
  - Chemical residues may cause rejection
- Easy to use
- Fast, small storage requirement
- People handling rough materials, children require updating the database
Retinal Patterns for Biometric Authentication

- Match retinal vascular pattern
- Extremely low false acceptance rate
  - Ethnicity and eye color can affect accuracy
- High rejection rate
- Fast, very small storage needed
- Very stable biometric
  - Affected by certain diseases like blindness and cataract
Retinal Scan
Other Biometrics

- Keystroke timing for typing a password
  - Affected by network properties
  - Timing can be used to make guessing passwords easier
- Finger geometry, hand vein patterns
- Face recognition
  - Perspective, lighting
  - Disguises, quality of original source