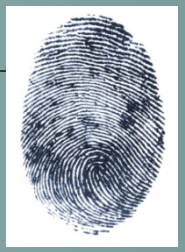
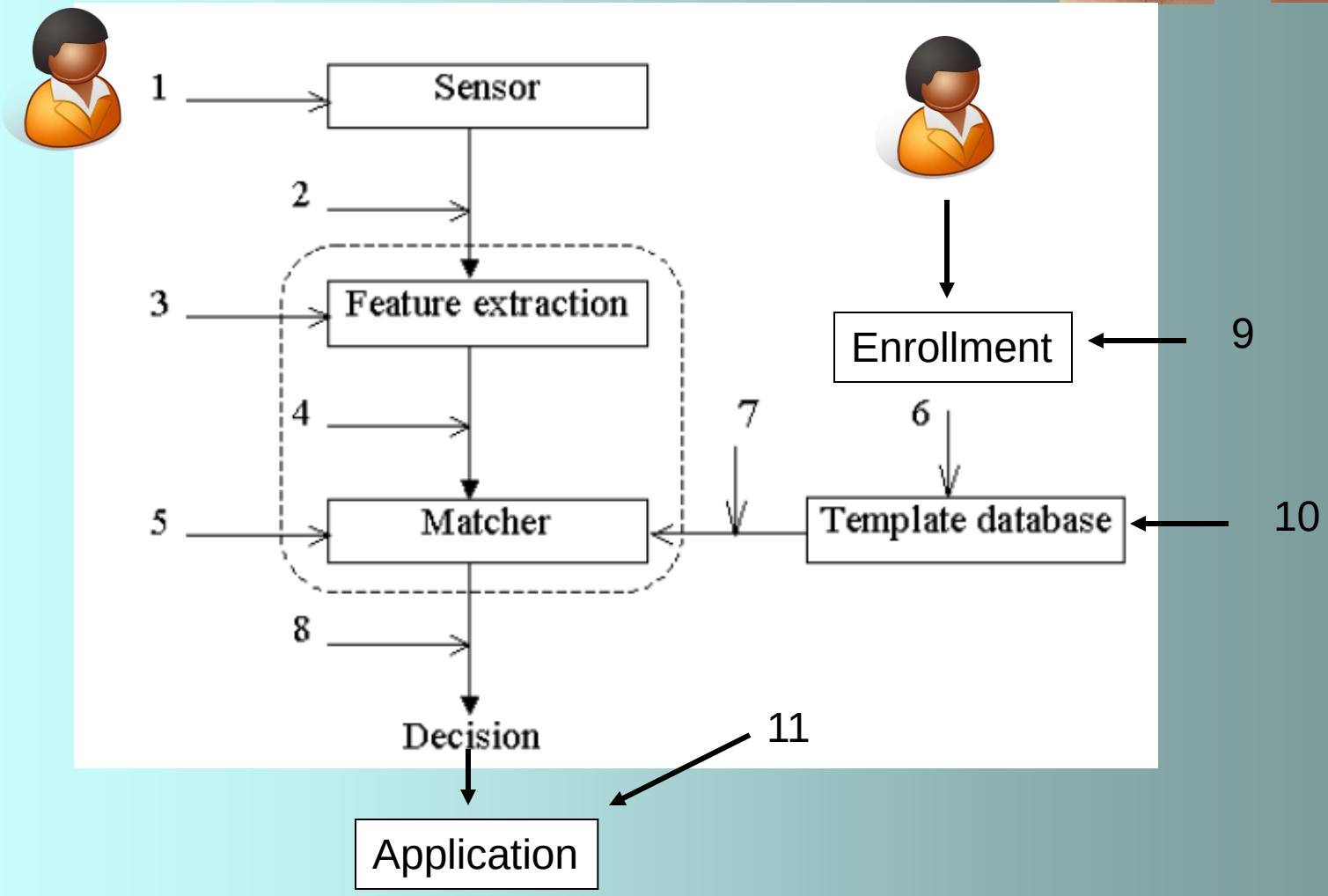
Understanding Biometrics



8. Defeating Biometrics

Dr. Terence Sim

Points of attack



Attacking biometric sample

- Point 1 in figure.
- Coercive attack
  - Force the legitimate user to authenticate
  - Counter: supervised authentication
- Impersonation attack
  - Changing one’s appearance so that the measured biometric matches that of a true user.
  - e.g. using a photograph to fool face recognition
  - e.g. gummy fingers

Gummy fingers

- http://news.bbc.co.uk/2/hi/science/nature/1991517.stm
- Latent prints can be lifted using fingerprint kit commonly sold as toy.
  - www.crimescene.com/store/index.php?main_page=product_info&zenid=8757c3f57cbe9a9502a059df56f3e325&products_id=36
- Mythbuster [episode 59, 2006]
  - shows how easy this is:

There’s an easier way!

- Latent prints can be re-activated simply by breathing on it!
  - Heat and humidity triggers capacitive sensors
  - Called *replay attack*

- Counter: “liveness” detection
  - Check for motion, 3D face, heat

Impersonation

- ExtremeTech article
  - www.extremetech.com/article2/0,1697,13919,00.asp
- Fake iris
  - Hole the in photograph to fool “liveness” detection

Replay attack

- Point 1 or 2 in figure.
- Record and playback biometric sample, or signal.
- e.g. face photograph, voice recording, fingerprint re-activation

- Counter: liveness test, or change text to be read

Front-end attacks

- Replay attack
  - Points 1, 2 and 4
- Trojan horse attack
  - Points 3 and 5
  - At pre-determined time (or conditions), produce a pre-selected feature, or high score

Circumvention

- Collusion:
  - Bypassing the biometrics authentication (Point 8 in figure)
  - Biometrics system may have override mode to handle exceptional situations
    - e.g. for handicap individuals
  - User colludes with operator to bypass authentication, or to fall back to non-biometrics authentication.

Circumvention

- Denial
  - Prevent legitimate user from successfully authenticating.

Back-end attacks

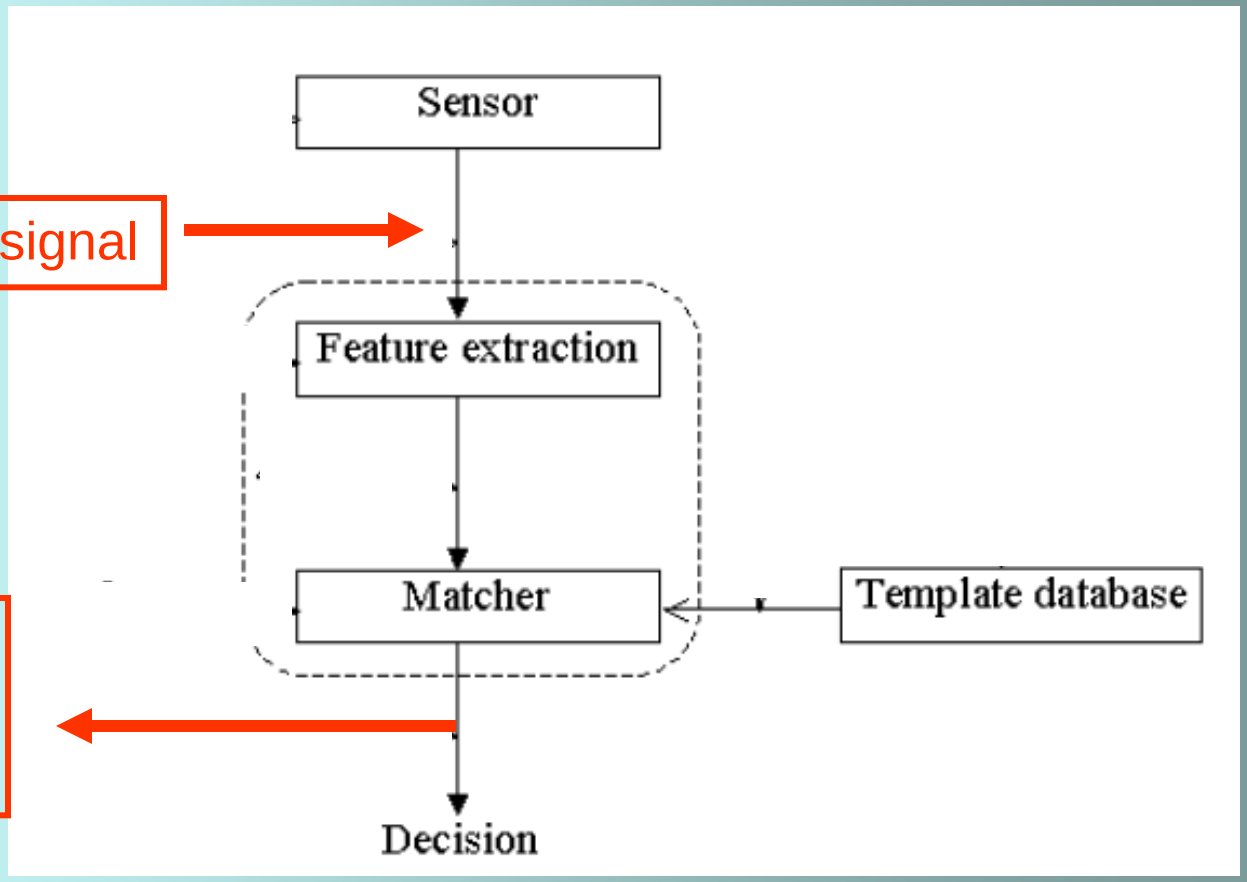
- Attacking the enrollment (Points 6 and 9).
- Attacking the database (Point 10).
- Attacking the communications channel between database and matcher (Point 7).
- Attacking the application (Point 11).

- Counter: Conventional security measures must be applied on the back-end too.

Hill-climbing attack

Generate biometric signal

Use score to modify generation



Any other ideas?

- Feel free to devise new ways to attack!

Conclusion

- It is easy to guard against common attacks.
  - e.g. liveness test, supervised authentication
- A very determined attacker will succeed!
  - Cost and sophistication not a barrier.
- The goal is to balance the value of the resource being protected vs. the cost of preventing attacks.
- Physical security should be used to complement biometrics.