Computer Systems Security

Lesson 04 - Authentication mechanisms

Authentication Mechanisms

- Token Based authentication
- Certificate based authentication
- Biometrics
- Authentication in DS
  - Single sign on
  - Trusted intermediaries

MD5 for Authentication

- Beyond encryption, MD5 can be used for authentication
- Each user has a file containing a set of keys:
  - Input into the MD5 hash
- Information being supplied to the authenticating server (e.g. passwords) has its MD5 checksum calculated using these keys then transferred to the authenticating server along with the MD5 hash result.

Remote User Authentication

- Authentication over network more complex
  - Problems of eavesdropping, replay
- Generally use challenge-response
  - user sends identity
  - host responds with random number *r*
  - user computes *f(r,h(P))* and sends back
  - host compares value from user with own computed value, if match user authenticated
- Protects against a number of attacks

Remote Authentication

- Student to read:
  - 1. Secure RPC Authentication
  - 2. Dial-in Authentication
  - 3. Remote Dial-in User Services (RADIUS) Authentication

Biometrics

- Identification by physical characteristics
- A two factor authentication:
  - Something you have is something that is part of you.

Biometrics

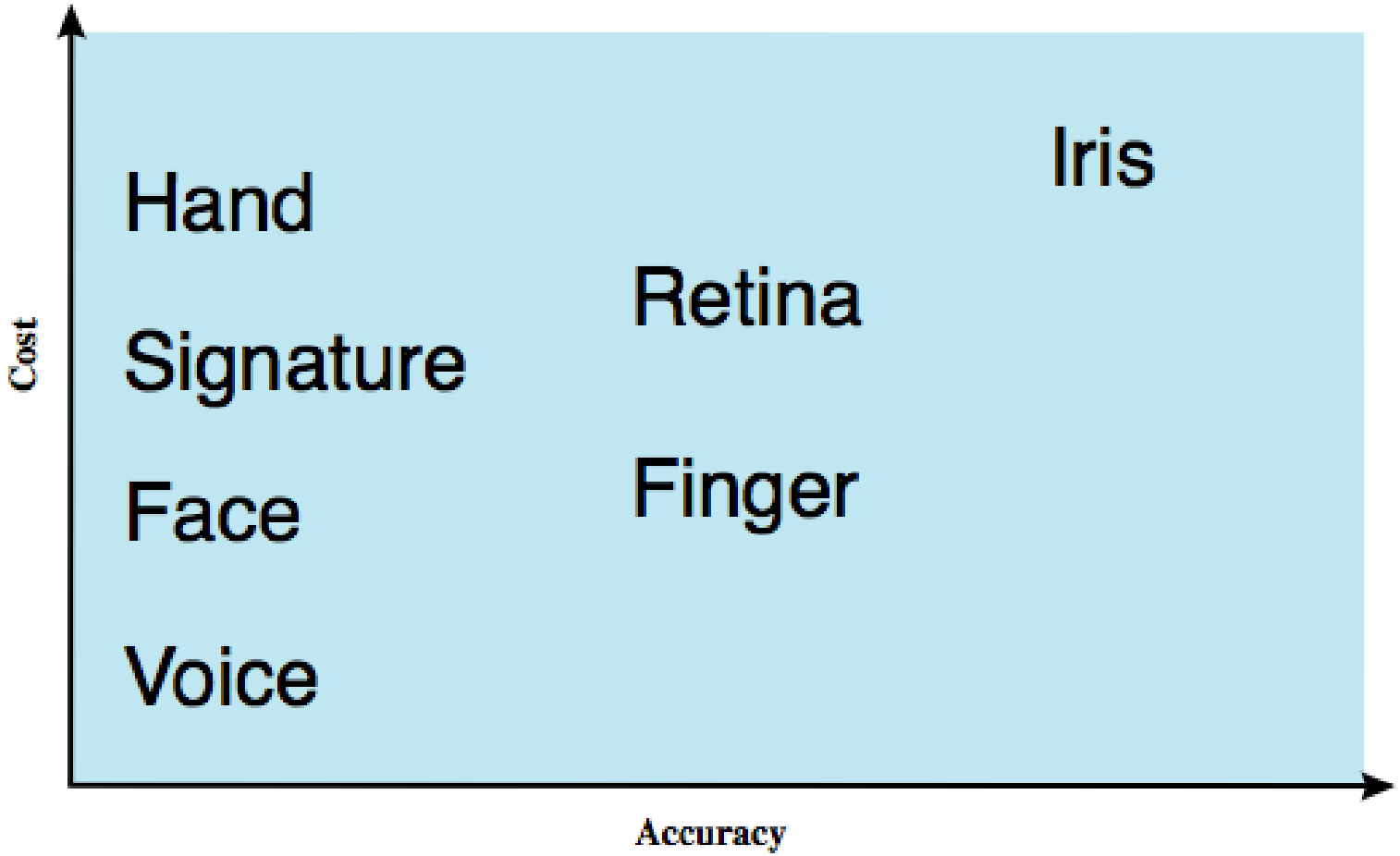
- Includes the use of:
  - Facial recognition and identification
  - Retinal scans
  - Iris scans
  - Fingerprints
  - Voice recognition
  - Lip movement and
  - Keystroke analysis

Biometrics

- NOTE:
  - Biometrics currently in use have been chosen because they represent characteristics that are unique to individuals.
  - Relative accuracy of each system is judged by the number of false negatives and false positives that it generates.

Biometric authentication

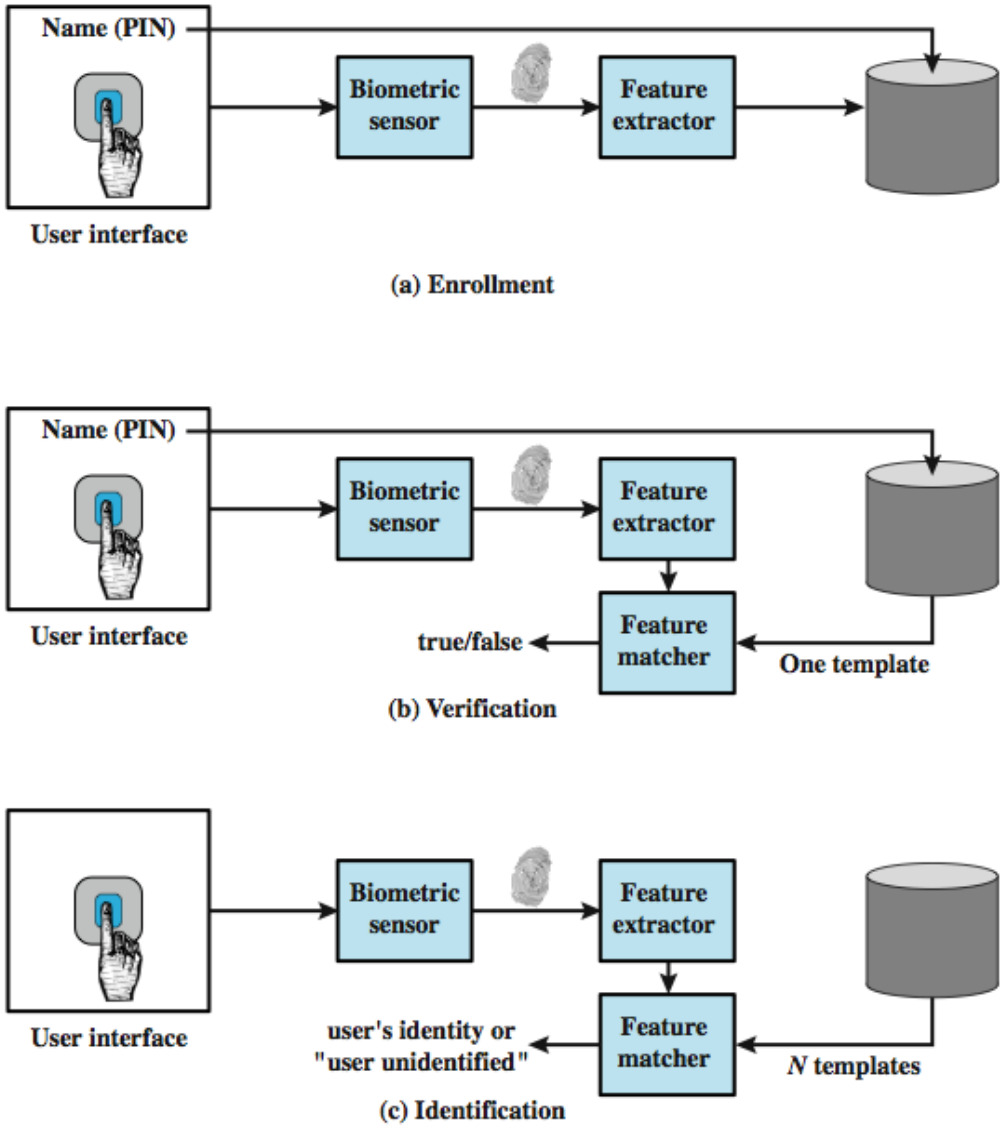
- Cost against Accuracy



Operation of a biometric system

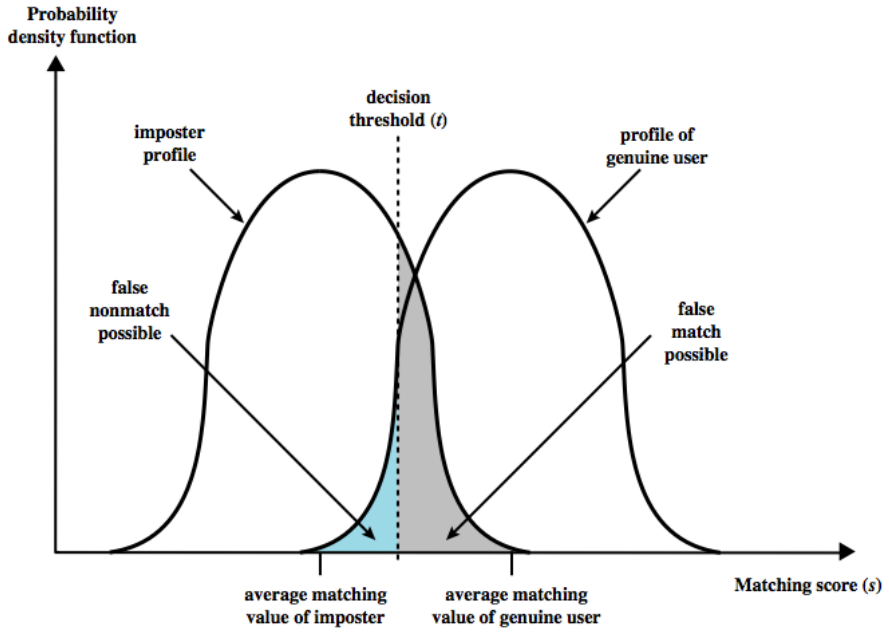
Verification *is analogous to user login via a smart card and a PIN*

Identification *is biometric info but no IDs; system compares with stored templates*



Biometric Accuracy

- The system generates a matching score (a number) that quantifies similarity between the input and the stored template
- Concerns: sensor noise and detection inaccuracy
- Problems of false match/false non-match



Biometrics

- Vulnerabilities:
  - Gummy finger attack (May 2002)
    - http://cryptome.org/gummy.htm
  - **Theorized**: Malicious attackers cutting body parts from the real person and using them to authenticate (terrorism).

Biometrics

- Advantages
  - Cannot be disclosed, lost, forgotten
- Disadvantages
  - Cost, installation, maintenance
  - Reliability of comparison algorithms
    - False positive: Allow access to unauthorized person
    - False negative: Disallow access to authorized person
  - Privacy?
  - If forged, how do you revoke?

Biometrics

- Common uses
  - Specialized situations, physical security
  - Combine
    - Multiple biometrics
    - Biometric and PIN
    - Biometric and token

Authentication Security Issues

- **Client attacks**: attacker attempts to achieve user authentication without access to the remote host
  - Masquerade as a legitimate user (e.g., guess the password or try all passwords)
  - Countermeasure: strong passwords; limit number of attempts

Authentication Security Issues

- **Host attacks**: attacker attacks the host where passwords/passcodes are stored
  - Countermeasure: hashing, protect password databases

Authentication Security Issues

- **Eavesdropping**: attacker attempts to learn passwords by observing the user, finding written passwords, keylogging
  - Countermeasures
    - diligence to keep passwords
    - multifactor authentication
    - admin revoke compromised passwords

Authentication Security Issues

- **Replay**: attacker repeats a previously captured user response
  - Countermeasure
    - Challenge-response
    - 1-time passcodes

Authentication Security Issues

- eavesdropping
- replay
- trojan horse

Authentication Security Issues

- **Trojan horse**: an application or physical device masquerades as an authentic application or device
  - Countermeasure: authentication of the client within a trusted security environment
- **Denial of service**: attacker attempts to disable a user authentication service (via flooding)
  - Countermeasure: a multifactor authentication with a token