Biometrics

Biometrics

- *Something you are*
- Measurement of biological and behavioral attributes
  - Fingerprint, iris, retina, face, voice, handwriting, hand shape, hand veins, DNA, …
- Biology and behavior is non-constant
  - Variation from one measurement to the next

Biometrics: Hand Geometry

- Used in Olympic Games, Walt Disney World, nuclear facilities, data centers, ...
- Camera images palm and side of hand (no texture information)
- Images reduced to (e.g.) 31000 points then 90 measurements then 9 bytes of data

Biometrics: Hand Geometry

- When user authenticates, another set of images taken
  - If data are close enough to stored template, user deemed authenticated
  - Can adjust threshold per-user, in case some users are difficult to authenticate
- Each time user is authenticated, template is updated to account for change over time

Biometrics: Apple Touch ID

Complete

Touch ID is ready. Your print can be used for unlocking your iPhone.

- Capacitive touch sensor (500 ppi)
- Reads ridges on your finger (fingerprint)
- Compares pattern to authorized users stored in *Secure Enclave*
  - Not online, not in the cloud, …
- Companion to passcode
  - Passcode required after 48 hours
  - Passcode required for some system operations

Biometrics: Apple Face ID

Biometrics: Apple Face ID

- Projects 30,000 infrared dots on face in random pattern
- Builds 3D model of face
- Compares 3D model to authorized user stored in *Secure Enclave*
  - Not online, not in the cloud, …
- Companion to passcode
  - Passcode required after 48 hours
  - Passcode required for some system operations

Biometrics

- Can we use biometrics as *verifiers*?
- Requirements
  - Identifier
  - Small variation over time and measurement
  - Easy to measure
  - Difficult to spoof
  - Acceptable to users

Biometrics

- Advantages
  - Can’t lose or forget biometric
  - Easy to use
- Disadvantages
  - Updating identifies after disclosure is hard
    - Get new fingerprint? Hand? Face?
  - Impossible to be application specific
    - Hand geometry is always the same
  - Physical process with *errors*
  - Fear of negative implications for *privacy*

Biometrics: Fraud

- How to spoof Touch ID?
  - Obtain physical device access
  - Obtain high resolution scan of fingerprint
    - From phone screen? From Starbucks cup? From your dead corpse?
  - Invert and print onto paper, cover with latex to get slight ridges, dusting of slight moisture
  - Profit!
- Watch YouTube videos

Biometrics: Fraud

- How to spoof Face ID?
  - "Under Development"
  - A mask formed from a 3D scan with printed photorealistic features may work – YMMV
  - Is it possible to create a sufficiently accurate 3D model from your Facebook photos?
    - Or celebrity / politician photos?

Virtual U: Defeating Face Liveness Detection by Building Virtual Models from Your Public Photos (2016)
https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/xu

Errors

- False accept: authenticate a principal with wrong identity (fraud)
- False reject: fail to authenticate a principal under right identity (insult)
- Tunable trade off of sensitivity between which error is more likely
  - False acceptance rate (**FAR**): percentage of attempts in which imposters are authenticated (with wrong identity)
  - False reject rate (**FRR**): percentage of attempts in which legitimate users are denied authentication

Errors

- Entry to military facility?
  - Letting imposters in might be worse than (temporarily) delaying entry of personnel
  - Prefer low false accept rate
- Entry to hotel lobby?
  - Letting non-guests in might be better than (temporarily) delaying entry of guests
  - Prefer low false reject rate
- Entry to your phone?
  - *Opinions will vary…*