CSCE 201
Introduction to Computer Security
Biometrics
(Something You Are)

Professor Lisa Luo
Spring 2019
Previous Class

• Credentials
  – Something you know (Knowledge factors)
  – Something you have (Possession factors)
  – Something you are (Inherence factors)

• How to store passwords securely?

• Multi-factor authentication

• Time-based One Time Password (OTP)
  – RSA’s SecureID
  – Google Authenticator
When you go to an ATM machine to withdraw money, is it two-factor authentication?

Yes.

Something you know: PIN
Something you have: Debit Card
How to store user passwords?

- Adding “salts” when hashing
  - Prevent rainbow table attack
  - Store “salt1, hash(salt1, password1); salt2, hash(salt2, password2); …”
  - Now the pre-computed rainbow table is useless

- Using a slow hash algorithm
  - Slow down Brute Force or Dictionary Attack
Outline

• What are Biometrics?
• What are Biometrics used for?
• Advantages and Disadvantages
• How to evaluate its effectiveness?
• Framework of a Biometric System
• Case studies
  – Fingerprint
  – Iris
Biometrics

• Biometrics: the measurement and application of human characteristics
  – Bio-: life
  – -Metrics: to measure

• Applications:
  – Authentication: Something you are
  – Identification: To identify individuals
Identification vs. Authentication

• Identification (also known as One to Many)
  – A sample is effectively matched against all templates in the database
  – The user only provide her biometric as input

• Authentication (also known as Verification or One to One)
  – The sample is matched against one pre-selected template.
  – The pre-selected template is determined by the claimed identity in the form of, e.g., username
Biometrics Authentication

• Biometrics authentication is the process of extracting measurable biological or behavioral characteristics for the purpose of uniquely identifying or authenticating an individual.
Types of Biometrics

• Biological Biometrics
  – Fingerprint
  – Hand Geometry
  – Iris
  – Face
  – DNA

• Behavioral Biometrics
  – Signature
  – Typing Rhythm
  – Gait
Market share

Figure 1: Biometrics market share by system type
Biometrics are widely used

- Smartphones (Apple’s TouchID)
- FBI
- US Immigration department
- Airport
- …
Advantages and Disadvantages

• Advantages
  – You do not need to remember sth. (as with passwords)
  – You do not need to carry sth. (as with security tokens)
  – More convenient and quicker (e.g., compared to typing)
  – Recognition can be automated (critical for police and FBI)

• Disadvantages
  – Some biometrics may be easily stolen, e.g., signature
  – Accuracy
  – Users may not feel comfortable (e.g., scanning eyes)
  – Costly
Framework of Applying Biometrics for Authentication

**Enrollment**

- User Identity, $I$
  - Biometric Sensor
  - Quality Assessment Module
  - Feature Extractor
  - System Database

**Authentication**

- Claimed Identity, $I$
  - Biometric Sensor
  - Quality Assessment Module
  - Feature Extractor
  - Matcher
  - Decision Module
  - System Database

User
Framework of Applying Biometrics for Identification

Enrollment

User Identity, I

Biometric Sensor → Quality Assessment Module → Feature Extractor → System Database

Identification

Identification → Feature Extraction → Template Matching (1:1) → Multiple matches → Storage

Output Interface → True/False
Five important components

• Sensor
  – Scans the biometric trait of the user
• Feature extractor
  – Processes the scanned biometric data to extract the template
• Template database
  – For storage
• Matcher
  – Compares two templates and outputs a similarity score
• Decision module
  – Determines “Yes” (matched) or “No” (not-matched)
How to measure accuracy

- **False Rejection Rate (FRR)** as known as **False Non-Match Rate (FNMR)**
  - The percentage that the system fails to detect a match between a user’s input template and the user’s stored template.
- **False Acceptance Rate (FAR)** also know as **False Match Rate (FMR)**
  - The percentage that the system incorrectly matches the input pattern to a non-matching template in the database.
  - Apple’s TouchID: FAR is 1 in 50,000
FRR and FAR

![Graph showing False Acceptance Rate (FAR) and False Rejection Rate (FRR) as functions of a threshold. The Equal Error Rate (EER) is marked as the point where both rates are equal.](image-url)
Biometric Template

• A biometric template is a digital representation of an individual’s distinct characteristics
Fingerprint Characteristics

An example technology that extracts features from fingerprints

- A fingerprint is made of a series of ridges and valleys. Once a fingerprint is captured the system locates the minutia points where the lines of the ridges begin, end, branch off and merge.
  - The number of minutia points required to uniquely identify a person varies from 12 to 17
- These points are mapped and lines are drawn between points. This creates a map of how each point relates to the other points. The map is then stored as a data stream called a minutia template
Fingerprint System Shortcomings

1. Complexity is added to take into account cuts, dirt, wear, and tear that may be present on a finger.

2. It is difficult to distinguish between a real finger and a picture of a finger.

3. A small percentage of the population either does not have any minutiae or has less minutiae than average.

- Even though, fingerprint systems remain widely used around the world.
Iris Recognition

• The iris pattern is unique for a person, and is stable throughout a person’s life
• The processing power needs to be 10x faster than a fingerprint system, in order to produce results in the same timeframe
• The extra processing power increases the cost of iris systems
Iris Recognition

- Limbus boundary
- Ciliary zone
- Pupillary zone
- Contractile furrows
- Crypt
- Collarette
- Pupil
- Pupillary boundary
- Pupillary frill
- Stroma fibers
- Wolffian nodules
- Nevi

Source (eye image): Dr. Jan Drewes. www.jandrewes.de
1. Acquisition
- Camera
- Controlled illumination

2. Segmentation

3. Normalization

4. Encoding

5. Recognition
   - Enrollment
   - Authentication
   - Database
   - Matching
   - Decision
Unwrapping Iris
Some systems do not work well (yet)

• **Voice recognition** is hard because there are filters which can make a female voice seem male and makes you sound like another, etc.

• **Face recognition** currently has error rates that are too high.

• Typing patterns, walking patterns ("gait"), etc.
## Comparison

<table>
<thead>
<tr>
<th>Biometric Type</th>
<th>Accuracy</th>
<th>Easy to use</th>
<th>User Acceptance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Voice</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Retina</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Iris</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Signature</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Face</td>
<td>Low</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>
Summary

• Biometrics
  – Measurement and applications of human characteristics
• Applications
  – Identification
  – Authentication
• False rejection rate; false accept rate
• Fingerprint
• Iris