CSE 40537 / 60537: Biometrics

Template Protection 1
The Course Instructor Feedback (CIF) survey window for biometrics opens tomorrow

December 1st - 13th
https://cif.nd.edu/
Course Roadmap

Basics

3 Core Modalities

Multi-Biometric Fusion

Privacy & Security
Privacy and Biometrics
Security and Privacy

An Inherent Trade-Off?

Security

Privacy

Deterrence, Accuracy, Efficiency, Usefulness

Identity protection, Attribute protection, Limit inference, Limit abuse
Security ≠ Privacy

“…the right to exercise control over your personal information.”

Ann Cavoukian

“…the right to be let alone” Warren & Brandeis

“Privacy is at the heart of liberty in the modern state.” Alan Westin
Privacy = choice & control over use and disclosure of our identity and our information

...including our biometrics
Unfortunate Privacy Truisms

1. Most people don’t value their privacy until it is threatened or lost

2. Once invalidated or lost, you will need to regain your privacy over and over again...
Security vs. Privacy

- Accountable to Commander, President or Board of Directors

- Accountable to the subject of the data

- Access and use controls defined by the system owner

- Access and use controls defined by design, use limitation, subject consent and legislation
Security vs. Privacy

- Generally focused on protecting against outsiders
- Requires protecting against outsiders, insiders, and system owners
- Short-term risk based assessment. (How likely is it?)
  - 6 months
- Long-term capabilities based assessment (Is it possible?)
  - 30 years
Privacy and Biometrics (as sold today)

- Claims of “privacy” since it is not possible to recover fingerprints from a template
- Government officials stating that biometrics are public information
- Border/Passports and National ID
  ± Biometric access control to facilities
  ± Biometrics for computer / file access and data encryption
  ± Commercial biometric systems for private use
Relationships Between Privacy and Security

- In theory, privacy and security may be completely different elements of a system
- In practice, security is a facilitator of privacy and an important foundation to it
- Not protecting privacy often impacts security
- Security is never, in and of itself, sufficient to ensure privacy
Security is a Foundation to Privacy

- data protection
- authentication
- data-integrity
- confidentiality
- non-repudiation

Security

Privacy
How do we measure privacy?

**Identity:** measures the degree to which information is personally identifiable

**Linkability:** measures the degree to which data tuples or transactions are linked to each other

**Observability:** measures the degree to which identity or linkability may be impacted from the use of a system
Privacy risks determined by:

- Use of technology
- Collection methods (covert or intrusive)
- System model — storage and security of data
- Unique identifiers
- Function creep
- Capturing and linking extra data — healthy, ethnicity, disability, emotional…
- Inaccuracy — false acceptances or rejections
- Ability to validate / challenge data
Fair information practices

1. Accountability
2. Identifying purpose
3. Consent
4. Limiting collection
5. Limiting use, disclosure, retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual access
10. Challenging compliance
Biometric privacy problems

- Unique identifier
- Infrastructure for surveillance
- Consent / Control
  - Infrastructure
  - Template Storage
  - Biometric Acquisition
  - Usage

Image credit: Newsweek
Different Approaches to Privacy

- Central repository / decision model (Fort Knox syndrome)
- Divide and Conquer — strategic pseudonymisation / anonymisation
- Build in elements of personal consent and control
- Smart hardware
  - privacy rules embedded in hardware
- Smart data
  - encapsulate methods inside the data
Vendor “Hardened” Biometrics Systems

- End-to-end encryption of transactions
- “Customized” (i.e., weakly encrypted) template format and security
  - Some can export to standard formats

Crossmatch product offerings

TCS4H Swipe Sensor
including image data signing, encryption and anti-spoofing. Key Features Superior Technology Advanced ... Anti-spoofing protection
User navigation features Image data encryption/signing Sensor to host authentication ...

TouchChip Module Developer Kit
functions including fingerprint image capture, template enrollment, template matching, image encryption ...

TCS4K Chipset
processor. Power-On Authentication (POA), One-Time Passwords (OTP) and encrypted host communications ...

Software Development Kits
extraction, template matching, identification, data encryption and more. They support multiple platforms ...

U.are.U 4500 Module
and automatically captures and encrypts the fingerprint image before sending it to the FingerJet matching engine ...
How do we measure privacy?

• **Nymity or Identifiably**
  ‣ Measures the degree to which information is personally identifiable.

• **Linkability**
  ‣ Measures the degree to which data tuples or transactions are linked to each other.

• **Observability**
  ‣ Measures the degree to which identity or linkability may be impacted from the use of a system.
Privacy Dimensions

- Nymity
- Linkability
- Observability
Nymity (Identifiability)

Measures the degree to which information is personally identifiable or recoverable.

- **Anonymity**
- **Non-Reversible Pseudonymity or polynymity**
- **Reversible Polynymity**
- **Reversible Pseudonymity**
- **Verinymity**

The quality or state of being unknown. *without name*

from Greek pseudonunon, neuter of pseudonumos, *falsely named*
And poly meaning many, with polynymity meaning *many named*

from Latin verus, true, *truly named*

- DeDuplication only requires system unique pseudonymity within system
- Non-repudiation requires reversible polynymity, where some (trusted) party controls the reversibility
- Some researchers talk about $k$-identifiability if an action can be tracked to one of $k$ identities, where $k$ then measures level of de-identification
Linkability

This metric requires \( n \) data elements.
Where \( n > 1 \).

Measures the degree to which data elements are linked to each other.

**Non-linkability**

It cannot be determined which set of transactions belong with each other.

**Full Linkability**

It may be fully determined which set of transactions belong with each other.

Linkability relations can be directional, given A can link to B does not mean that B can link to A.

Example: Transactions belonging to the same individual.
Unlinkability

The requirements for unlinkability are intended to protect the user against the use of profiling of operations.

For example…

• When a telephone SIM card is employed with a unique number, the telephone company can determine the behavior of the user of this card.

• Hiding the relationship between different invocations of a service or access of a resource will prevent this kind of information gathering.