Biometric Solutions as Privacy Enhancing Technologies

Amsterdam Privacy Conference (APC) 2015

Sunday 25/10/2015

Christina-Angeliki Toli
PhD Researcher in Biometrics Security
Questions

• Can a biometric trait keep its source secret?

• Are biometrics a protection mechanism of individual privacy?

• Can really biometrics be characterized as PETs?

• Under which conditions can biometrics be considered as private friendly?
Setting Goals

- The design of a biometric system that respects privacy standards and security principals.
- Clarify the terms of *security* and *privacy*.
- How to develop and ensure crypto-biometric techniques.
- Addressing the societal impacts of that modern technological issue.
Outline

• Quick Introduction
• Debate: Biometric versus Privacy
• The Role of Cryptography
• Privacy & Security Principles for Biometric Systems
• Biometrics as Privacy Enhancing Technologies
• Privacy Friendly Biometric eFinance Application
• Conclusion
• Discussion & Future Research
Facts about Biometrics

- They are the modern key to authentication and identification models.
- Efforts are either insufficient for laws or too legally restrictive.
- Becoming common, popular and compulsive.
- By nature may reveal more information than necessary.
- Carry the term: “Bring yourself with you”.
- They cannot be lost and hardly changed.
- A society with pervasive biometric systems would make anonymity a virtual impossibility.
Debate: Biometrics VS Privacy

• Applications may require storing datasets for human authentication.

• Facial recognition technology is a part of everyday life.

• RFID and on-line transactions expose the template so to become not a secret.

• Carry sensitive personal information

• Lack of user’s permission can lead to gathering, correlating and sharing data.

• From fraud and spoofing to hacking devices or even border’s control safety.

• Soft biometrics are the perfect way to pinpoint, track and control people.
Debate: The Role of Security

• Biometric Template Protection models

• Attacks prevention after evaluation and putting the system into test.

• Government agency applications are follow the privacy laws strictly to ensure privacy of citizens.

• Commercial applications save digits instead of images.

• There is no generation of the original template if the initial was compromised.

• Beyond cryptography and ISO standards are privacy principles in terms of limitation, data minimization, accuracy, transparency, confidentiality...
Hotspots in a Generic Biometric System

Sensor
- Coercive attack
- Spoofing attack
- Mimicry attack
- Device Substitution
- Denial of Service

Feature Extraction
- Insertion of imposter data
- Component replacement

Matching
- Insertion of imposter data
- Component replacement
- Hill climbing
- Manipulation of score
- Guessing attack

Decisor
- Component replacement
- Hill climbing
- Manipulation of threshold
- Manipulation of match decision

Reading template
- Replacing template
- Changing bindings ID

Eavesdropping attack
- Replay attack
- Man in the middle
- Brute force attack

Manipulation
- Yes/No
Privacy & Security Principles for Biometric Systems

International biometric standards, development activities.
Approaches towards Security of Biometric Technologies

• Features Transformation for Template Protection
  - The functions are not accessible
  - Low false acceptance rates (FAR)
  - Non-invertible mechanisms
  - Possible use to single or multiple biometrics

• Cancelable Biometrics and Renewability
  - Compose unusable any quotation to biometric template
  - Multiple transformed templates associated with biometrics
  - Collaboration of the involved parties (user-designer)
  - They are the basis for other suggestions
Approaches towards Security of Biometric Technologies

• Crypto-biometrics: Key Management
  - Cryptographic encryption and decryption algorithms
  - Two schemes: Randomly key generation and binding
  - Non-biometric database
  - Disadvantage: Low accuracy

• Multiple pseudo-identities from biometrics samples
  - One way functions
  - Serve the principal of revocability
  - Delete the biometric data trait after identity’s generation
  - Minimal biometric data are not yet supported
Pseudonymous Biometric Identities (1)

- Template Protection
  - Absolute ONE-WAY Link

- Create PI
  - Irreversible Bit String 1
    - Pseudo-Identities 1

- Verify PI

- Expire PI

- Revocate PI
  - Irreversible Bit String n
    - Pseudo-Identities n
Pseudonymous Biometric Identities (2)

Architecture for renewable biometric pseudo-identities.

Privacy Friendly Biometric Application for Access Control

Private Sector Bank

Client Device

Mobile Applications

Minutiae Fingerprint

Customer

Biometric Key Encryption Algorithm

Supplementary Data

PIN or Passcode

Protected Template

Protected Template

10100010
10111011

Internet

Distant Database System

Database

Non-biometric

Accounts

Yes

No

Key Verification

Reconstruction of encrypted keys

Algorithm

Database Keys
Conclusion

• Invasive actions strengthen the critique about biometrics inability.

• Law determines the limits of any system allows an interaction between man and machine.

• Pseudonymous biometric identities prove that privacy technology can offer a solution to handle privacy-friendly identity verification.

• Putting research security suggestions into the context of privacy for reducing the leeway for misuse and mismanagement of biometric data.

• The requirements for template protection combined with the technical standards related to applications may satisfy the demands.

• The implementation in large scale applications and final overall evaluation are important tasks.
What’s Next?

- Security and Privacy aren’t a double edged sword.
- Public key infrastructures (PKI) and protocols for certificate repository and distribution manner can benefit from improvements.
- Biometric key commitments can extend the protocols to provide non-transferability, but they lack tools for a generic architecture.
- Pseudo-identities cannot yet extend the schemes to continuous biometric sources, where the quantization is used as a pattern of error correction.
- Multi-modalities should be exploited in a more systematic way for obtaining keys.
- Unordered sets (minutiae points) deserve better analysis.
- Cloud computing environments suffer from inability of samples reconstruction.
Instead of an Epilogue

- **1st truth:** There is no such thing as a perfectly secured system!
- **2nd truth:** We do not have another choice instead of keeping pace with technological changes.
- **Question:** Do the current and aimed applications of biometrics serve their primary objectives?
- **Admission:** Privacy-preserved biometric secure services, under specific conditions could be considered as a confidential mean of a safe infrastructure.
18

To know more...


• C. Diaz and S. Grses. Understanding the landscape of privacy technologies, Extended abstract of invited talk in proceedings.


Acknowledgments

COSIC
Computer Security
and
Industrial Cryptography
Contact:  http://www.esat.kuleuven.be/cosic/
  ctoli@esat.kuleuven.be

Time for questions...