Enhancing Information Security and Privacy by Combining Biometrics with Cryptography

Synthesis Lectures on Information Security, Privacy, and Trust

Synthesis Lectures on Information Security, Privacy and Trust is composed of 50- to 100-page publications on topics pertaining to all aspects of the theory and practice of Information Security, Privacy and Trust. The scope will largely follow the purview of premier computer security research journals such as ACM Transactions on Information and System Security, IEEE Transactions on Dependable and Secure Computing and Journal of Cryptology, and premier research conferences, such as ACM CCS, ACM SACMAT, ACM AsiaCCS, IEEE Security and Privacy, IEEE Computer Security Foundations, ACSAC, ESORICS, Crypto, EuroCrypt and AsiaCrypt. In addition to the research topics typically covered in such journals and conferences the series also solicits lectures on legal, policy, social, business and economic issues addressed to a technical audience of scientists and engineers. Lectures on significant industry developments by leading practitioners are also solicited.

Enhancing Information Security and Privacy by Combining Biometrics with Cryptography
Sanjay G. Kanade, Dijana Petrovska-Delacrétaz, and Bernadette Dorizzi
2012

Analysis Techniques for Information Security
Anupam Datta, Somesh Jha, Ninghui Li, David Melski, and Thomas Reps
2010

Operating System Security
Trent Jaeger
2008

Enhancing Information Security and Privacy by Combining Biometrics with Cryptography
Sanjay G. Kanade, Dijana Petrovska-Delacrétaz, and Bernadette Dorizzi

ISBN: 978-3-031-01207-5 paperback
ISBN: 978-3-031-02335-4 ebook

DOI 10.1007/978-3-031-02335-4

A Publication in the Springer series
SYNTHESIS LECTURES ON INFORMATION SECURITY, PRIVACY, AND TRUST

Lecture #3
Series ISSN
Synthesis Lectures on Information Security, Privacy, and Trust
Print 1945-9742 Electronic 1945-9750

Enhancing Information Security and Privacy by Combining Biometrics with Cryptography

Sanjay G. Kanade, Dijana Petrovska-Delacrétaz, and Bernadette Dorizzi
Institut TELECOM: TELECOM SudParis

SYNTHESIS LECTURES ON INFORMATION SECURITY, PRIVACY, AND TRUST #3

ABSTRACT

This book deals with 'crypto-biometrics', a relatively new and multi-disciplinary area of research (started in 1998). Combining biometrics and cryptography provides multiple advantages, such as, revocability, template diversity, better verification accuracy, and generation of cryptographically usable keys that are strongly linked to the user identity. In this text, a thorough review of the subject is provided and then some of the main categories are illustrated with recently proposed systems by the authors.

Beginning with the basics, this text deals with various aspects of crypto-biometrics, including review, cancelable biometrics, cryptographic key generation from biometrics, and crypto-biometric key sharing protocols. Because of the thorough treatment of the topic, this text will be highly beneficial to researchers and industry professionals in information security and privacy.

KEYWORDS

biometrics, cryptography, crypto-biometrics, cancelable biometrics, revocability, cancelability, diversity, template protection, key generation, key regeneration, key sharing, session key generation and sharing, protocols

Contents

Preface

Securing information during its storage and transmission is an important and widely addressed issue. Generally, cryptographic techniques are used for information security. In cryptography, the general idea is to transform the information during a phase called encryption, before being stored or transmitted, based on a secret key. This secret key is required in order to retrieve the information from the transformed data during decryption. These secret keys are generally too long for a user to remember, and therefore, need to be stored somewhere. The drawback of cryptography is that these keys are not strongly linked to the user identity. In order to strengthen the link between the user identity and his cryptographic keys, biometrics is combined with cryptography.

Unfortunately, biometric systems possess problems of their own such as nonrevocability, non-template diversity, and possibility of privacy compromise which should be taken into consideration. Combining biometrics with cryptography in a secure way can eliminate these drawbacks. Thus, biometrics and cryptography can complement each other. The systems, in which, techniques from biometrics and cryptography are combined are called as crypto-biometric systems. The combined system can inherit the positive aspects of the two while eliminating their limitations.

This is a relatively new domain in which the research started in 1998 and lacks a uniform nomenclature/classification. Therefore, first we present a through and systematic review of crypto-biometric systems. The primary criterion for the classification is the main goal of the system. There can be two principal goals: (i) protecting biometric data, and (ii) obtaining cryptographic keys from biometrics. The systems in these two categories are further divided according to their working methodology. We illustrate each of these categories with our recently proposed crypto-biometric systems. We also study the crypto-biometric systems from the application point of view and their actual usability in information security. We present a review of protocols found in literature which deal with crypto-biometric systems. One such protocol, recently proposed by the authors is discussed in details.

The first system we describe is a shuffling based cancelable biometric system. This is a simple shuffling scheme which randomizes the biometric data with the help of a shuffling key. This shuffling scheme: (a) adds revocability to the biometric systems, (b) improves the verification performance (nearly 80% decrease in equal error rate) because it increases the impostor Hamming distance without changing the genuine Hamming distance, (c) adds template diversity, and (d) makes cross-matching impossible and thus protects privacy.

The second system is for obtaining cryptographic keys using biometrics. The shuffling scheme described above is first applied on the biometric data to make it revocable. This data is then used in a fuzzy commitment based key regeneration scheme. The generic scheme is then adapted to two biometric modalities: iris and face. The amount of errors (variability) in the biometric data for these two modalities is different. Therefore, different sets of error correcting codes are used for these modalities in order to cope with the variability of biometric data. The entropy of keys obtained using the iris and face based key regeneration systems are 83 and 112 bits, respectively.

Finally, we address the issue of sharing crypto-bio keys. We describe a protocol to share the crypto-bio keys generated using our key regeneration scheme. The same crypto-bio key is shared in every run of the protocol. In order to have better security, we proposed another novel protocol to generate and share biometrics based session keys. This protocol allows mutual authentication between the two parties - client and the server - without the need of trusted third party certificates. This protocol has a potential to replace existing key sharing protocols. Moreover, it can easily be integrated into existing key sharing protocols in order to have an additional layer of security.

Sanjay G. Kanade, Dijana Petrovska-Delacrétaz, and Bernadette Dorizzi
May 2012

Acknowledgments

Most of the work included in this book was carried out as part of the project BIOTYFUL (BIOmetrics and crypTographY for Fair aUthentication Licensing) which was supported by the French "Agence Nationale de la Recherche" (ANR) (BIOTYFUL project number ANR-06-TCOM-018).

We would like to thank Diane Cerra, the Executive editor at Morgan & Claypool publishers for her help during the initial phase of this book proposal. We also thank Mr. Michael Morgan for his continuous support throughout the publication process. We would also like to thank Dr. C. L. Tondo and his team for suggesting numerous improvements in the text.

Sanjay Kanade would personally like to thank his parents, Ganesh and Mangala, and his wife Kirti, for their constant encouragement and support during the development of this work. He also acknowledges the help of various past and present members of the Intermedia group at the Electronics and Physics Department, Institut Mines-TELECOM, TELECOM SudParis.

Sanjay Ganesh Kanade, Institut Mines-TELECOM, TELECOM SudParis Dijana Petrovska-Delacrétaz, Institut Mines-TELECOM, TELECOM SudParis Bernadette Dorizzi, Institut Mines-TELECOM, TELECOM SudParis

Sanjay G. Kanade, Dijana Petrovska-Delacrétaz, and Bernadette Dorizzi
May 2012

Abbreviations

AES	Advanced Encryption Standard
ANR	Agence Nationale de la Recherche
BCH codes	Bose, Ray-Chaudhuri and Hocquenghem codes
BIOTYFUL	BIOmetrics and crypTographY for Fair aUthentication Licensing
CBS	Casia BioSecure Database
ECC	Error Correcting Codes
EER	Equal Error Rate
FAR	False Acceptance Rate
FeaLingECc	*Fea*ture *L*evel Fus*ion* through Weighted *E*rror *C*orre*c*tion
FRGC	Face Recognition Grand Challenge
FRGC-Exp1*	FRGC Experiment-1 (controlled vs controlled) on our subset
FRGC-Exp4*	FRGC Experiment-4 (controlled vs uncontrolled) on our subset
FRR	False Rejection Rate
GAR	Genuine Acceptance Rate
HTTPS	Hypertext Transfer Protocol Secure
ICE	Iris Challenge Evaluation
ICE-Exp1	ICE Experiment-1 (right eye experiment)
ICE-Exp2	ICE Experiment-2 (left eye experiment)
NIST	National Institute of Standards and Technology
OSIRIS	Open Source Iris Recognition System
RS	Reed-Solomon
SudFROG	SudParis Face Recognition System
TLS	Transport Layer Security

Glossary

The most common terms used in crypto-biometrics are defined below:

1. Biometric template – Set of stored biometric features comparable directly to probe biometric features. It is a special case of a biometric reference, where biometric features are stored for the purpose of a comparison.
2. Identifier/authenticator/credential – Information provided by a user which is required to confirm his identity, e.g., password, token, and biometric characteristics.
3. Verification – One to one comparison of the captured biometric sample with a stored biometric template to verify that the individual is who he claims to be. The result of verification is a Yes/No response.
4. Identification – One to many comparison of the captured biometric sample against a biometric database in an attempt to identify an unknown individual. The result of identification is the identity of a user.
5. Authentication – A term generally used synonymously to verification. In this thesis, we make a distinction between verification and authentication. In addition to verifying the identity of a person based on his credentials, a secure session is opened between the two parties (generally a client and a server).
6. Repudiation – A user can willfully share his credentials and later claim that they were stolen.
7. Crypto-biometric system – A system that combines biometrics with cryptography in order to remove one or more drawbacks of either of the two techniques.
8. Crypto-biometrics – The field of study covering the design, development, evaluation, and analysis of crypto-biometric systems. The research in this field can be dated back since 1998.
9. Cancelable biometric template – The transformed data obtained by applying the cancelable transformation on the reference biometric data.
10. Crypto-biometric template – The template stored in a crypto-biometric system.
11. Helper data – A term used for the data stored in a crypto-biometric system which is required for key (re)generation during verification (e.g., locked code, information for binarization, etc).
12. Crypto-bio key – A key obtained from or with the help of biometric data.

13. Session key – A cryptographic key valid only during a single communication session.

14. BioHash – Quantized multiple projections of a biometric feature vector over a randomly generated ortho-normal matrix. The binary string obtained after quantization is denoted as BioHash. The BioHash may contain variability (i.e., Hamming distance ≥ 0).

15. BioHashing – The process of generating BioHash.

16. Hash key – A user specific key assigned to the user which is required to generate the random ortho-normal matrix for BioHashing.

17. Biometric Hash – Similar to a cryptographic hash. The Biometric Hash does not contain variability (i.e., Hamming distance $= 0$).

18. Stolen biometric scenario – Many crypto-biometric systems involve a secret parameter along with the biometric data (e.g., a Hash key in BioHashing). The stolen biometric scenario is a special case when it is assumed that the biometric data for all the subjects is compromised.

19. Stolen key scenario – Many crypto-biometric systems involve a secret parameter along with the biometric data (e.g., a Hash key in BioHashing). The stolen key scenario is a special case when it is assumed that the secret parameter for all the subjects is compromised.

20. Biometric bottle-neck problem – The result of biometric comparison is one-bit (yes/no). When integrating them in secure authentication systems, this can result in a weak link. attackers can replace the biometric recognition module with a Trojan horse which can provide the required result. We define this situation as biometric bottle-neck problem.

21. Verification string – This is a bit-string stored in crypto-biometric systems. At the time of key (re)generation, another verification string is obtained and compared with the stored one. This comparison is with zero tolerance (i.e., Hamming distance = 0). Note that, this string is not used in the key (re)generation process.

22. Systematic error correcting code – An error correcting code is said to be systematic in nature if the input to the code is present in its original form in the output.