Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Security evaluation of biometric keys

*Hisham Al-Assam**, *Sabah Jassim*

Department of Applied Computing, University of Buckingham, Hunter Street, Buckingham MK18 1EG, UK

ARTICLE INFO

Article history:
Received 4 July 2011
Received in revised form
6 January 2012
Accepted 7 January 2012

Keywords:
Biometric cryptosystems
Biometric keys
Biometric entropy
Security evaluation
Effective entropy
Face-based keys

ABSTRACT

Biometric cryptosystems combine biometrics with cryptography by producing Biometric Cryptographic Keys (BCKs) to provide stronger security mechanisms while protecting against identity theft. The process of generating/binding biometric keys consists of a number of steps starting with a feature extraction procedure, the complexity of which depends on the specific biometric trait/scheme, followed often by user selected transformation to allow for revocability, and an error correction scheme to tolerate reasonable amount of intra-class variation. Each of these steps has its own effect on the security of the generated/bound key. Proper security evaluation must include thorough analysis of the security effect of each of these steps. We propose a comprehensive approach to BCK's security evaluation that takes into consideration each of the steps involved in their construction. We first review existing BCKs and highlight that the analysis of their security is either insufficient or not provided. In addition to evaluating the correctness (i.e. error rates), and the generated/bound key size, we evaluate the randomness of biometric features employed in the process of key generation. Our proposal combines the Kullback–Leibler divergence and the discrimination entropy to formulate a new measure of the *Entropy of Biometric Features* (EBF), defined as the average number of bits that distinguishes a user from a given population. Then we rigorously evaluate the impact of using error correcting scheme on the security of BCKs to calculate the *Effective Entropy of Biometric Features* (EEBF). Finally, inherent individual differences of the EBFs will be discussed. Here, we focus on face-based BCKs, but this does not restrict the use of the proposed evaluation. This paper argues that current face-based BCKs are not secure enough for high level security applications, and demonstrates that the average EEBF of BCKs using PCA-based facial features is less than 20-bit even when applying a user-based randomization on biometric features.

1. Introduction

Communication over open networks, such as the internet, has serious security concerns. Cryptographic algorithms form a rich source of security mechanisms to ensure both confidentiality and integrity of sensitive information. A vital requirement of such algorithms is the protection of the decryption key. Generally speaking, cryptographic keys must satisfy two conflicting requirements: 1) be difficult to guess by imposters, and yet 2) be easy to reproduce by legitimate users. Typical keys are long and assumed to be random making them difficult to be memorised by human. Using easy to remember passwords to reproduce/release stored keys is the most common way (Uludag et al., 2004). Passwords may offer strong key protection but, in practice, they are often easy to guess by simple brute force dictionary attacks (Li, 2009). In contrast, biometrics cannot be lost or forgotten, expected to exhibit high entropy across population, and legitimate users can

* *Corresponding author.*
E-mail address: hisham.al-assam@buckingham.ac.uk (H. Al-Assam).
0167-4048/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2012.01.002

easily reproduce fresh samples. Biometrics is therefore more suitable for key generation/protection mechanisms.

Biometric-based authentication relies on the uniqueness of physical or behaviour characteristics of a person such as fingerprint, facial features, iris, and voice. However, the security of biometric systems can be undermined in a number of ways, e.g. a biometric template can be replaced by an impostor's template in a system database or it might be stolen and replayed (Nandakumar, 2008). Moreover, it has been shown that a physical spoof can be created starting from standard templates (Adler, 2005). Furthermore, biometric data on its own is not very secret. Individuals usually unintentionally leave (poor-quality) fingerprints everywhere, and a hidden camera can capture an image for a face or an iris (Hao et al., 2006). In fact, the level of secrecy varies among different biometric modalities e.g. covertly collecting of face images or voice samples is much easier compared to collecting retina and palm vein samples.

Biometric cryptosystems have been developed to provide stronger security mechanisms and to create revocable representations of individuals by combining biometrics with cryptography. Typical biometric cryptosystems employ additional authentication factor(s) such as a password, a PIN or a token to mitigate some security concerns surrounding the use of biometrics as a standalone component. One potential benefit of additional factors is enhanced revocability and diversity of biometric keys (Section 3.3 provides detailed discussion on this point). In fact, it can be argued that compromising two authentication factors is more difficult than compromising one. However, involving traditional authentication factors (e.g. a password/PIN or a token) in biometric cryptosystems, seem to undermine the claims about the security benefits of using biometrics. This disparity can be addressed by the observation that adding a secret password/PIN helps not only revocability but also reduces possibility of playback attacks.

In general, there are three approaches to biometrics cryptosystems: (i) key release (ii) key generation and (iii) key binding. In key release schemes, both the cryptographic key and the biometric data are stored as two separate entities and the key is released only when the client is biometrically authenticated. This method is straightforward and easy to implement but it has two major drawbacks (Nandakumar et al., 2007): biometric templates are not secure and biometric matcher can be overridden. In key generation schemes, a cryptographic key is directly derived from the biometric data without storing it anywhere. Such methods suffer from unacceptably high False Rejection Rate (FRR) (Hao et al., 2006). Lastly, in key binding schemes, the biometric template and the key are coupled to form what is known as *biometric lock* (Juels and Wattenberg, 1999) in a way that makes it computationally infeasible to retrieve the key without previous knowledge of client's biometric data. While biometric data are fuzzy due to intra-class variations, cryptographic keys have to be repeatable every time. To bridge the gap, key binding schemes typically rely on error correction techniques such as Error Correcting Codes (ECC) (Further discussion is provided in Section 2.1). Although this paper is primarily concerned with security evaluation of key binding schemes, the discussion can be equally applied to other schemes.

Proper security evaluation of Biometric-based Cryptographic Keys (BCKs) schemes is a crucial factor in their viability. Typically, biometric features (in binary/real data type) are input to the process of BCKs binding/generation to produce/release a repeatable cryptographic key. Evaluating the security of the output key without evaluating the source of input biometric features is only a partial evaluation (see Section 2.2). Binding/generating a cryptographic key of considerable length whose Shannon entropy is high with high accuracy is not sufficient to conclude that the BCK system is secure unless it is proved that it is computationally infeasible for an attacker to guess the input biometric feature vector. In this paper, we argue that security evaluation of BCK schemes that relies solely on estimating the size of the key space/entropy is not sufficient due to: 1) availability of Auxiliary information such as population distribution of biometric features and biometric lock/template, 2) correlation between the attributes of biometric feature vectors may introduce redundancy into the generated biometric key, and 3) the impact of error correction codes may not be negligible. Herein, we propose a new BCK security evaluation approach that considers these three issues and covers every step in the process from feature extractions, user-based secret transformation, to error correction codes. To deal with the first two issues, we use a hybrid entropy-based scheme that is based on a combination of the Kullback–Leibler divergence and the discrimination entropy to evaluate the *Biometric Entropy* (BE) of Biometric Features (BFs), which can be defined as the average number of bits that distinguishes a user from the population. Furthermore, we provide a detail analysis of the effect of employing an error correction technique on the security of BCKs and evaluate the Effective Entropy of BFs. Herein, we use the term Effective Biometric Entropy (EBE) to refer to BE of BFs after evaluating the effect of error correction. Finally, inherent individual differences of the entropy of BFs will be discussed. The rest of this paper is organized as follows: Section 2 reviews BCK binding schemes, evaluates the literature on how key security has been evaluated, and introduces the concept of Discrimination Entropy (DE). In Section 3, we describe our proposed security evaluation scheme. Experimental results will be presented and discussed in Section 4. Section 5 includes conclusions and future work.

2. Background

2.1. Biometric-based cryptographic key binding

In key binding schemes, a cryptographic key is randomly generated during the enrolment stage but independent of the biometric template(s) and can be changed when needed. The Fuzzy Commitment scheme proposed in Juels and Wattenberg (1999) is one of the earliest methods of binding biometrics and user keys. To commit (bind) a binary key K, a codeword C is generated based on K using a predefined error correcting code. The ultimate commitment will be (h(C), BC), where B is a biometric binary template and h is a cryptographic hash function. To decommit a commitment, an individual has to provide a fresh biometric sample B′ which is close enough to B and then h(C) is used to verify that the right