A Reference Framework for the Privacy Assessment of Keyless Biometric Template Protection Systems

Tom Kevenaar[1)], Ulrike Korte[2)], Johannes Merkle[3)], Matthias Niesing[3)], Heinrich Ihmor[2)], Christoph Busch[4)], Xuebing Zhou[5)]

[1)] priv-ID B.V.
High Tech Campus 9
5656 AE Eindhoven,
the Netherlands
tom.kevenaar@priv-id.com

[2)] BSI
Postfach 20 03 63
53133 Bonn, Germany
ulrike.korte@bsi.bund.de
heinrich.ihmor@bsi.bund.de

[3)] secunet
Kronprinzenstraße 30
45128 Essen, Germany
johannes.merkle@secunet.com
matthias.niesing@secunet.com

[4)] Hochschule Darmstadt-CASED
Mornewegstraße 2
64293 Darmstadt, Germany
christoph.busch@h-da.de

[5)] Fraunhofer IGD
Fraunhoferstraße 5
64283 Darmstadt, Germany
xuebing.zhou@igd.fraunhofer.de

Abstract[1]: Over the past decades, a number of methods have been reported in the scientific literature to protect the privacy of biometric information stored in biometric systems. Keyless Biometric Template Protection (KBTP) methods aim to protect biometric information without the use of long-term secrets by deploying one-way functions. These KBTP methods are currently developed to an extent that commercial products have become available. When assessing and comparing different KBTP methods it is important to have a common and generic approach. Therefore, in this paper we present a reference framework that can be used in assessing and comparing the privacy properties of KBTP systems.

1 Introduction

Biometric systems are becoming increasingly popular because they may offer more secure solutions than traditional means for authentication such as PIN codes, passwords and security badges because a biometric characteristic is tightly linked to an individual. For the same reason, biometrics can prevent the use of multiple identities by a single individual. Finally, in many applications biometric authentication is also considered to be more convenient.

Biometric technologies are, however, not without their challenges [JRP06]. Although accuracy, speed and interoperability remain important, this paper focuses on the security of biometric systems as well as privacy issues related to the biometric information stored

[1] This work is part of the BioKeyS project which is supported by the Bundesamt für Sicherheit in der Informationstechnik (BSI), Germany.

in these systems. Many of these challenges are related to the special properties of biometrics as compared to traditional means for authentication:

- Biometric characteristics are tightly coupled to an individual which makes revocation and re-issuing of authentication information unfeasible. In contrast, PIN codes, passwords, tokens, etc. can easily be revoked and re-issued;
- Biometric data is personal and in many cases contains sensitive information. For example, it might contain information on the health status of an individual [Pe65], gender, ethnicity, age, etc. Therefore, in contrast to PIN codes and passwords, in many countries biometric data are considered to be Personally Identifiable Information and use of biometrics is governed by privacy legislation (e.g. [Eu08]);
- Each individual has a limited number of instances for each biometric characteristic (e.g., one face, two irises, ten fingers) while the number of possible passwords or token identifiers is several orders of magnitude higher. As a consequence, an individual will have to re-use the same characteristic in different applications which can lead to cross-matching of applications;
- Biometric measurements are affected by noise and other forms of variability while authentication protocols based on passwords and the like rely on 'bit-exactness' of the authentication information. This variability limits the distinctiveness of biometric features. Although this limitation also applies to, say, 4-digit PIN codes, passwords and token identifiers allow for a higher level of distinctiveness than single biometric modalities.

These special properties of biometric characteristics and measurements have an impact on security and privacy considerations of biometric authentication systems. Keyless Biometric Template Protection (KBTP) technologies can make an important contribution in solving some of these vulnerabilities [CS07]. In this paper we define a framework to assess the privacy of KBTP methods. In Section 2 we will define security and privacy for biometric systems and define the objective of KBTP methods. In Section 3 an overview of practical KBTP methods will be given and an abstraction will be made to allow for a generic framework. Finally, in Section 4, the reference framework will be given illustrating how the privacy assessment of KBTP methods could be done.

2 Security and privacy

Figure 1 gives a high-level overview of a biometric system where, without loss of generality, we consider a fingerprint verification system. During enrolment, a fingerprint sensor SENS generates the image sample of a fingerprint. After processing the image and extracting relevant features in the feature extraction block FE, a template representing the fingerprint is stored as reference in the biometric system (STOR). During verification, an individual claims an identity, and a so-called probe image from this individual is obtained. This image is transformed into a template and compared (COMP) with the template stored in the biometric system corresponding to the claimed identity. The comparison subsystem produces a similarity score and applying a threshold T to this score leads to an Accept or Reject message.

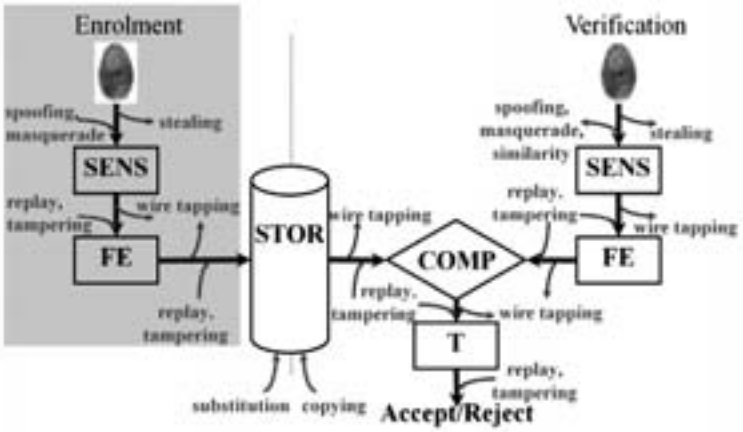

Figure 1 Security and privacy vulnerabilities in a biometric system

Figure 1 also depicts some important vulnerabilities of a biometric system [Bu08] [CS07] [RCB01]. Although in the literature a large number of potential attacks are mentioned, we propose to group them into the following two categories:

- **Insertion**, depicted with ingoing arrows in Figure 1,
- **Eavesdropping**, depicted with outgoing arrows in Figure 1.

As illustrated by the gray rectangle in Figure 1, in many cases the enrolment functionality can be assumed to operate in a secure environment such that the most important vulnerabilities are concerned with the storage and verification functionality.

In the context of biometric systems we associate the *security* of a biometric system with *insertion* vulnerabilities while the *privacy* of a biometric system is associated with *eavesdropping* vulnerabilities. Thus, the *security* of a biometric system defines how difficult it is to be illegitimately accepted by the system. In contrast, the *privacy* of a biometric system is related to the difficulty to obtain any relevant information from a provided biometric characteristic other than a verification decision.

2.1 A Perfectly Private Biometric system

If we assume that enrolment takes place in a trusted environment, a Perfectly Private Biometric (PPB) system can be defined as the gray rectangle in Figure 2 (see also [Br09] [ISO10]). A PPB system contains a sensor SENS, a feature extractor FE, a state-of-the-art comparator COMP, a threshold module T and storage STOR. When offering a fingerprint, possibly in combination with an identity claim, the system outputs an Accept or Reject decision. This PPB system is sealed and perfectly private in the sense that it outputs the minimal required amount of information in the form of a binary Accept/Reject decision. Furthermore, assuming a sensor leaving no latent prints (e.g. a touchless sensor or swipe sensor), the system has no eavesdropping vulnerabilities.

On the other hand, if the comparator COMP is not perfect, the system will occasionally incorrectly generate an Accept message due to a wrong decision of the comparator and in that sense the system is not perfectly secure.

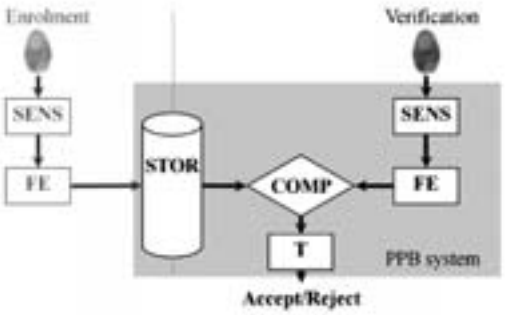

Figure 2 A Perfectly Private Biometric system

In practical systems, apart from the non-perfect comparator COMP, many security and privacy vulnerabilities can be prevented using standard cryptographic protocols. For example, replay and tampering attacks can be prevented by combining message uniqueness (by, for example, time stamps or sequence numbers) and verifying message authenticity using Message Authentication Codes (MACs) or digital signatures. A substitution attack can be foiled by adding a digital signature over a template and the wiretapping attack can be thwarted using secure channels which can be generated by the Diffie-Hellman key exchange protocol [DH76]. Although these methods require at least mid-term secret keys, management of these authentication keys is much easier than management of keys used to protect, for example, stored information.

The copying attack is very similar in nature to a wiretapping attack by interpreting storage as a communication channel and it can be prevented by a secure channel (encryption). In a (storage) communication channel the key must be retained for at least as long as the message is in storage. This means that in order to protect biometric information from a copying attack using standard cryptographic protocols, a long-term secret is required.

There are two approaches for storing and handling these long-term secret keys. The first is to keep the keys inside the biometric system under control of the biometric system owner. In a practical situation, this will lead to protocols and access rights that are limited to trusted operators only. An important drawback is that if these biometric systems scale up, the protocols become vulnerable to "incidents" by sloppy execution, change in regulations or legislation, human mistakes or intentional misuse.

The second method to handle long-term secrets is to store the keys outside the system. In many proposed systems the user will have control over the key. The key can be stored on a smartcard or token, or it can be derived from a password, PIN code, pass phrase, etc. An advantage of this method is that the user is in control of his biometric information, and the system owner does not have access to the decrypted biometric data. Drawbacks are that it reduces the convenience advantage of biometrics and it does not allow biometric identification (1-to-many), thus limiting the scope of biometric applications.

The purpose of Keyless Biometric Template Protection (KBTP) technology is to eliminate the drawbacks of both approaches by obviating long-term keys. This prevents

key abuse by the biometric system owner while simultaneously allowing higher convenience and biometric identification. Thus, the goal of (KBTP) technology can be formulated as to *prevent relevant biometric information to be obtained from storage facilities in biometric systems without the need for long-term secrets.*

Ongoing ISO standardization activities [ISO10] more specifically state that safeguarding the privacy of the data subject comprises i) preventing anyone to have access to biometric data or derived attributes thereof that are not required and agreed upon by the data subject and ii) ensuring that third parties and external observers have no access to the biometric references.

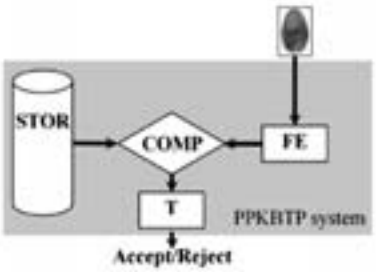

Figure 3 A Perfectly Private Keyless Biometric Template Protection system

2.2 Perfectly Private Keyless Biometric Template Protection

Based on the discussion above, a Perfectly Private Keyless Biometric Template Protection (PPKBTP) system can be depicted as in Figure 3 where, without loss of generality, it is assumed that feature extraction is part of the KBTP technology. It contains a feature extractor FE, a state-of-the-art comparator COMP, a threshold module T and storage STOR. It accepts the image of a fingerprint, possibly in combination with an identity claim, and outputs an Accept or Reject decision. This (conceptual) PPKBTP system does not need any secrets while at the same time, it does not leak any biometric information (other than the binary Accept/Reject decision) and in that sense is the highest achievable goal of any practical KBTP system. It is important to notice that vulnerabilities that are common between a PPKBTP system and a practical implementation thereof cannot be attributed to limitations of the implementation but must be attributed to the limitations of the use of biometrics. These intrinsic biometric vulnerabilities need to be addressed by proper system design.

3. Practical KBTP methods

Practical KBTP systems aim at implementing the PPKBTP system. In the scientific literature a number of methods are proposed to protect biometric information stored in a biometric system. In this section, a brief overview will be given and, following the reasoning in the previous chapter, we will only consider methods that do not require secret information to achieve this protection. Therefore methods as presented in, for example, [TNG04] [Br02][Ti02][SKK04] will not be considered.

The essence of all KBTP systems is that a biometric template, before it is stored in the biometric system, is first transformed into a representation from which it is impossible to retrieve any biometric information. On a high level of abstraction, all practical KBTP methods use the same format to represent the protected biometric information consisting of a Pseudonymous-Identifier (*PI*) and Auxiliary Data (*AD*) [ISO10]. The *PI* is generated using a (keyless) one-way function (e.g. a hash function $h(.)$) which forms the basis of the protection mechanism. The *AD* essentially contains variability information and/or randomization data. During verification *AD* is combined with a probe biometric measurement to generate a candidate Pseudonymous-Identifier *PI**. During verification, *PI** is compared with *PI* leading to an Accept or Reject message. Thus, practical KBTP protected templates consists of the pair (*AD*, *PI*) and KBTP methods differ in the way that the *PI* and *AD* are generated. Next, a brief overview of KBTP methods is given.

- Mytec [So98] was the first practical KBTP system. The method works directly on (fingerprint) images and protects the image by multiplying the phase part of the Fourier transform of a (fingerprint) image $F(\omega)$ with a random phase function $\varphi(\omega)$ and $H(\omega)=F(\omega)\varphi(\omega)$ is stored as auxiliary. A secret S is embedded by pointing to certain bits in $c(x)$, which is the inverse Fourier transform of the random phase function $\varphi(\omega)$ multiplied by the magnitude part of the (fingerprint) image "optimal" filter. *PI* is defined as $h(S)$ where h is a cryptographic hash function (e.g. SHA256).
- In [RCB01] the authors introduce an approach known as cancelable biometrics[2]. During enrolment, the image of a biometric is distorted using a parameterized one-way geometric distortion function before storing it in a biometric system. The parameter determining the distortion function is stored as *AD*. The function is made such that from the distorted image it is difficult to retrieve the original image. The distorted image is stored as *PI*.
- The fuzzy vault [JS02] is a general cryptographic construction that allows storing a secret S in a "vault" that can be locked using an unordered set X. The secret S can only be retrieved from the vault using a set Y if the sets X and Y have sufficient overlap. The "vault' is stored as *AD* while *PI* is set to $h(S)$. The use of unordered sets makes the method well suited to be used with minutiae fingerprints (see e.g. [UPJ05]).
- In the recently proposed Biotope™ scheme [Bo06], each component x of a feature vector is translated by t and scaled by s to obtain $v = (x-t)/s$. The resulting value v is separated into the integer $g = \lfloor v/E \rfloor$ and the residual $r = v \bmod E$ such that $v = g+r$ where E is a parameter. The entities t, s, r are stored as *AD*, while the integer part g is first passed through a one-way function to obtain *PI* which is then stored.
- The Norwegian company Genkey has developed an approach referred to as Biocryptics™ [LLO06]. The approach works directly on continuous features. In order to cope with noise and other variabilities, a correction vector, stored as *AD*, is used to shift a measured feature to the middle of a quantization interval that defines one bit of a binary string S to be embedded in the biometric template. *PI* is interpreted as a public key derived from S. The method resembles the so-called

[2] The term 'cancelable biometrics' is somewhat misleading because clearly the biometric itself cannot be cancelled. In the context of KBTP methods, the terms 'cancelable' and 'revocable' refer to the property that authentication information can be changed and revoked.

shielding functions as proposed in [LT03].

- The Fuzzy Commitment scheme [JW99] is considered most suitable for biometrics that have a template in the form of an ordered string or fixed length feature vector. A biometric X represented as a binary string is XORed with a codeword C of an (arbitrary) error correcting code. $C \oplus X$ is stored as AD while PI is set to $h(C)$.

In this brief overview it was shown that all practical KBTP systems generate a private representation of a biometric in the form of the KBTP template (AD, PI) which is stored in the biometric system. In the following section a framework for the assessment of the privacy of such systems will be given.

4 Privacy of KBTP systems

4.1 Privacy requirements

In Section 2, a high level notion of privacy was introduced in terms of a (conceptual) PPB and PPKBTP system that leaks no information about biometric templates. The concept of a PPB system is also described in [Br09] which serves as a basis for a new ISO standard that is currently being developed [ISO10]. This ISO standard provides guidance for the protection of biometric information under various requirements for confidentiality, integrity, availability and renewability/revocability. More specifically the standard proposes the following privacy goals for biometric information:

- irreversibility: To prevent the use of biometric data for any other purpose than originally intended, biometric data shall be transformed in such a way that the biometric sample or a deductible attribute that does not serve the agreed purpose of the identity management system cannot be retrieved from the transformed representation;
- unlinkability: The stored biometric references shall not be linkable across applications or databases;
- confidentiality: To protect biometric references against access by external observers resulting in a privacy risk, biometric references shall be kept confidential;
- data minimization: minimizing irrelevant and/or undesired processing of personal data, including during the verification of a person's identity.

The standard does not prescribe the mechanisms of how to achieve these requirements but as a framework standard it is applicable to a much wider range of techniques than KBTP techniques including traditional encryption of the template. In the assessment of a KBTP method, it must be verified to what extent it obtains these privacy goals or how much effort an adversary should invest in order to thwart one of these goals. Clearly, whether or not an adversary can thwart one of the privacy goals depends on his capabilities. The adversary capabilities are formalised in the following section.

4.2 Adversary capabilities

In the assessment of security systems and KBTP systems, it is essential to define the capabilities of an adversary.

A first high level notion in adversary capabilities is to assume a black-box model or a white-box model [Wy09]. In the black-box model it is assumed that an adversary knows all the details of the algorithm. During operation, the adversary has access to the inputs and/or the outputs of the algorithm but not to the internal intermediate computation results. In contrast, the white-box model assumes that an adversary, besides all the black-box capabilities, also has access to the implementation of the algorithm and is able to observe and modify intermediate computation results.

The white-box assumption is a very strong. For example, most implementations of traditional ciphers (such as RSA, AES, etc.) and security systems are not secure under the white-box model and it is customary in the assessment of such systems to adopt the black-box model. Therefore it seems reasonable to also assess KBTP methods under the black-box model.

A second notion that is important in the assessment of security systems is the efficiency of an attack. If the (minimum) required effort to thwart a certain security goal of a system (e.g. secrecy, privacy, authenticity) is higher, then the system is considered to have a better security concerning this specific goal. The security is commonly expressed as a number of bits which is the logarithm (to the base 2) of the required effort. This notion of the efficiency of an attack for a certain security goal should also be used in the assessing the privacy properties of KBTP systems.

A third important notion in the assessment of security algorithms is that the best-known-attack against a certain security goal defines the security of the algorithm for this goal. For example, if the General Number Field Sieve (GNFS) is the best (i.e., in terms of required effort/resources) known algorithm to break RSA, then the security of the RSA algorithm is directly related to the required effort of the GNFS to factor the public RSA modulus in its two primes. The notion of best-known-attack should also be adopted in assessing KBTP solutions.

4.3 Possible attacks

In defining adversary capabilities one can distinguish between high level and low level attacks. High level attacks are independent of the algorithmic details of the underlying KBPT method while low level attacks target specific properties of the KBTP method.

4.3.1 High Level Attacks

FAR attack Being a high level attack, the FAR attack does not exploit algorithm-specific knowledge. Instead it uses the fact that practical biometric systems have a non-zero False Accept Rate (FAR). The FAR is the probability that the biometric system will incorrectly accept an unauthorized user in a verification setting. Thus, given a KBTP private template, the attack consists of trying sufficient biometric images until an Accept

message is obtained. If the comparator is operating at FAR=α and the required effort for a single comparison is N_{FAR} then the expected required effort for a successful FAR attack is N_{FAR}/α.

It is important to note that the FAR attack is applicable also to the PPKBTP system introduced in Section 2.2 and therefore, it does not exploit a vulnerability of the KBTP implementation per se. Still, it allows the adversary to obtain information about the protected biometric information in the sense that a successful trial image is in some sense similar to the image that was used to generate the KBTP template. Thus, the FAR attack has an impact on the privacy goal of 'irreversibility'. If different applications use a PPKBTP system, the FAR attack can also be exploited to link templates across applications. Thus, the FAR attack also puts a limit on the 'unlinkability' goal of [ISO10]. Therefore it is essential that the system design incorporates a strategy to prevent the FAR attack.

Hill climbing In traditional biometric systems, hill climbing exploits the continuity of a similarity score as a function of changes in the input image [Ma06]. Regarding the ISO privacy goals, this threat is similar to the FAR attack: the adversary obtains an image that is in some sense close to the image that was used to generate the KBTP template.

Referring to Section 3 it can be seen that KBTP systems are traditionally implemented such that they do not output a similarity score but just a one-bit Accept/Reject decision (or a hashed version of some stable value *S*) which thwarts the high level hill climbing threat. For KBTP systems, hill climbing allows obtaining a working image using the FAR attack but it does not allow increasing the image quality.

4.3.2 Low Level Attacks

Hash inversion In most KBTP systems, the *PI* is computed from a secret bit string *S* using a strong one-way hash function (see Section 3). In this case, a first low level threat is inverting the hash in the *PI* of a private template. For good hash functions, the best-known-attack for hash inversion is to perform an exhaustive search (dictionary attack) which means that the required effort for inversion is proportional to $2^{|S|}$. For example, in case of the FCS, the adversary would have to try all possible codewords *C* of the applied error correcting code. Since the one-wayness of the hash function in KBTP systems is an essential part of the privacy mechanism, a successful inversion of the hash function will at least leak some information on the biometric that was used to generate the KBTP template (*AD*, *PI*) and will affect the 'irreversibility' and 'unlinkability' goals of [ISO10]. In view of the notion of the best-known-attack, hash inversion should be significantly more difficult than the FAR attack where is should be noted that hash inversion does not necessarily brings the adversary the same information (a ‘working’ biometric characteristic) as a FAR attack.

Using AD In a KBTP protected template (*AD*, *PI*), the auxiliary data *AD* contains user-specific information. Therefore, in information theoretical sense it is expected that *AD* will leak information on the biometric that was used to generate the KBTP template. On the other hand, it can be shown that if robustness against variability is required, some

privacy leakage cannot be avoided [DRS04]. If and how this privacy leakage can be exploited depends on the specific KBTP system. For example, in case of the FCS, if the code word C is chosen from an (n,k) error correcting code, then k information bits of the biometric are protected and, in an information theoretic sense, AD leaks n-k bits of information about the biometric. However, this information theoretic representation does not indicate how this leakage can be exploited by an adversary to learn dedicated information about the biometric or to thwart the 'irreversibility' and 'unlinkability' goals.

4.4 Information theoretic treatment

As opposed to the assessment of a KBTP method by known attacks, many scientific publications use information theoretic measures of privacy. Although these measures do not always point towards a practical attack, they are useful in assessing the required effort for certain attacks.

In terms of the unified KBTP template format (AD, PI), while assuming that PI leaks no information because it is protected by a hash function, it is interesting to consider $H(X|AD)$ which is the remaining entropy in the biometric information X after observation of AD. Two definitions of entropy have been considered for measuring the information leakage of a KBTP system.

- The Shannon entropy $\mathbf{H}$. Due to its rich mathematical theory, this measure allows a very comprehensive analysis of information leakage in a KBTP system [Ig09]. The conditional Shannon entropy $\mathbf{H}(X|AD)$ can be used to measure the average information content of X after observation of AD.
- The min-entropy $\mathbf{H}_\infty$. This defines an upper bound for the success probability of an attacker who tries to guess X from AD. The average min-entropy $\hat{\mathbf{H}}_\infty(X|AD)$ provides an upper bound for an attacker's success probability for average AD [DRS04].

If the entropy is a measure for the required effort for certain attacks, one could be interested in the relation between $\mathbf{H}(X|AD)$ or $\mathbf{H}(S|AD)$ and the FAR of the system (where S is the embedded key). Some publications state that $\mathbf{H}(S|AD) \leq -\log_2(\mathrm{FAR})$ which bound is derived assuming the Fuzzy Commitment scheme [JW99] where X is a perfectly random independent and identically distributed (i.i.d.) binary string [Pl07]. For some special choices of the entropy function (e.g. the average min-entropy $\hat{\mathbf{H}}_\infty$ [Ko08]), it has been shown that $\hat{\mathbf{H}}_\infty(S|AD)=\hat{\mathbf{H}}_\infty(X|AD)$ and $\hat{\mathbf{H}}_\infty(X|AD) \leq -\log_2(\mathrm{FAR})$ which holds for arbitrary distributions of the biometric strings X. Moreover, it is expected that similar bounds will hold for any KBTP system. The details of using entropy measures to estimate the required effort of a practical attack are a point of further research.

5 Summary

In this paper we presented a reference framework that can be used in assessing and comparing the privacy properties of KBTP systems. KBTP methods are a building block

in larger biometric systems and in the privacy assessment of KBTP systems it is important to differentiate between, on one hand, threats against the system and, on the other hand, specific threats against the KBTP method. This has lead to the concept of a Perfectly Private KBTP system and to the goal of KBTP systems to protect biometric information without the use of long-term secrets. In order to set up a generic framework, an abstraction of KBTP templates was taken from [ISO10] in the form (*AD*, *PI*). Based on this uniform format, after defining the adversary capabilities, attacks can be defined that affect the privacy goals as defined in [ISO10]. High level attacks are independent of the algorithmic details of the underlying KBPT method while low level attacks must be targeted at a specific KBTP method. The presented reference framework can be used as a first step to set up practical methods assess and compare the privacy properties of commercial KBTP systems.

Bibliography

[Bo06] T. Boult: Robust distance measures for face recognition supporting revocable biometric tokens, Proc. 7th Int. Conf. on Automatic Face and Gesture Recognition (FGR), IEEE Computer Society, Washington, DC, pp560-566, 2006.

[Br02] M. Braithwaite, U.C. von Seelen, J. Cambier, J. Daugman , R. Glass, R. Moore, and I. Scott: Application-specific biometric templates, IEEE Workshop on Automatic Identification Advanced Technologies, Tarrytown, NY, March 14-15, pp167-171, 2002.

[Br09] Jeroen Breebaart, Bian Yang, Ileana Buhan-Dulman, Christoph Busch: Biometric template protection, the need for open standards. Datenschutz und Datensicherheit - DuD, Vol. 33, No 5, May 2009, Vieweg Verlag, pp299-304.

[Bu08] Ileana Buhan: Cryptographic keys from noisy data, theory and applications, PhD Thesis, University of Twente, the Netherlands, 2008.

[CS07] Ann Cavoukian, Alex Stoianov: Biometric Encryption, A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy, 2007, see http://www.ipc.on.ca/images/Resources/bio-encryp.pdf.

[DH76] W.Diffie, M.E.Hellman: New directions in cryptography. IEEE Trans. Inform. Theory, IT-22, 6, 1976, pp644-654.

[DRS04] Y. Dodis, M. Reyzin, and A. Smith: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data, Proc. Eurocrypt 2004, Lecture Notes in Computer Science, Vol. 3027, pp523-540, Springer-Verlag, New York, 2004.

[Eu08] European Parliament and European Council: Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[Ig09] T. Ignatenko: Secret-Key Rates and Privacy Leakage in Biometric Systems, PhD thesis, Technical University of Eindhoven, 2009.

[ISO10] ISO/IEC JTC1 SC27 2nd CD 24745 – Information technology- Security techniques- Biometric template protection.

[JRP06] A.K. Jain, A.Ross, S. Pankanti: Biometrics: A Tool for Information Security. IEEE Trans. Information Forensics And Security, v.1, No.2, pp125-143, 2006.

[JW99] A. Juels and M. Wattenberg: A fuzzy commitment scheme, Sixth ACM Conf. on Computer and Communications Security, p28-36. ACM Press, N, 1999.

[JS02] A. Juels, M. Sudan: A fuzzy vault scheme. Proc. IEEE Int. Symp. on Information Theory, p408. IEEE Press, Lausanne, Switzerland, 2002.

[Ko08] Ulrike Korte, Michael Krawczak, Ullrich Martini, Johannes Merkle, Rainer Plaga, Matthias Niesing, Carsten Tiemann, Han Vinck: A cryptographic biometric authentication system based on genetic fingerprints, Proc. Sicherheit 2008, in Lecture Notes of Informatics, pp263-276, LNI P-128, Springer-Verlag, 2008.

[LT03] J.-P. Linnartz and P. Tuyls: New shielding functions to enhance privacy and prevent misuse of biometric templates. In Proc. of the 4th Int. Conf. on Audio and Video Based Biometric Person Authentication, pp393-402, Guildford, UK, 2003.

[LLO06] J. Lyseggen, R. A. Lauritzsen, and K. G. S. Oyhus: System, Portable device and method for digital authenticating, crypting and signing by generating short-lived cryptokeys, US Patent Application 2006/0198514 A1, Sep. 7, 2006.

[Ma06] M. Martinez-Diaz, J. Fierrez-Aguilar, F. Alonso-Fernandez, J. Ortega-Garcia and J. A. Siguenza, Hill-climbing and brute-force attacks on biometric systems: A case study in Match-on-Card fingerprint verification", Proc. IEEE Intl. Carnahan Conf. on Security Technology, ICCST, pp151-159, Lexington, USA, October 2006

[Pe65] L. Penrose: Dermatoglyphic topology. Nature, 205:545–546, 1965.

[Pl07] R. Plaga: Biometrics and cryptography - On biometric keys, their information content and proper use, Conference on Biometric Feature Identification and Analysis, Göttingen,7 September 2007.

[RCB01] N. K. Ratha, J. H. Connell, R. M. Bolle: Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40(3):614–634, 2001.

[SKK04] M. Savvides, B.V.K.Vijaya Kumar and P.K.Khosla: Cancelable biometric filters for face recognition, Proceedings of the 17th International Conference on Pattern Recognition (ICPR'04), Cambridge, England. v.3,pp922-925, 2004.

[So98] C. Soutar, D. Roberge, A.V. Stoianov, R. Gilroy, and B. V. K. Vijaya Kumar: Biometric Encryption using image processing, in Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques II, v. 3314, pp178-188, 1998.

[TNG04] A. Teoh , D. Ngo, and A. Goh: Biohashing: two factor authentication featuring fingerprint data and tokenised random number, Pattern Recognition, v. 37, pp2245-2255, 2004.

[Ti02] M. Tiberg:A Method and a System for Biometric Identification or Verification, Swedish patent 0202147-5, PCT patent appl. WO 2004/006495, PCT/SE2003/001181. US Patent Application US2005/0210269 A1, Sep. 22, 2005.

[UPJ05] U. Uludag, S. Pankanti, A. K. Jain: Fuzzy vault for fingerprints, in Lecture Notes in Computer Science. Vol. 3546, pp270-319, Springer-Verlag, 2005.

[Wy09] B. Wyseur: White-Box Cryptography, PhD thesis, Catholic University of Leuven.