Privacy and Security Assessment of Biometric Systems

Mohamad El-Abed, Patrick Lacharme, Christophe Rosenberger

Privacy and Security Assessment of Biometric Systems

Mohamad El-Abed[1] and Patrick Lacharme[2] and Christophe Rosenberger[2]

[1] *Rafik Hariri University*
Meshref, Lebanon

[2] *Université de Caen Basse-Normandie, UMR 6072 GREYC, F-14032 Caen, France*
ENSICAEN, UMR 6072 GREYC, F-14050 Caen, France
CNRS, UMR 6072 GREYC, F-14032 Caen, France

Keywords: Biometrics, Evaluation, Threats and Vulnerabilities, Data Protection, Privacy and Security Assessment

1. Introduction

The increasing need for security leads to the involvement of biometrics in our daily life. It became part of many aspects of life such as border control, e-payment (Jain et al., 2004). Nowadays, many biometric authentication systems have been proposed going from morphological (such as fingerprint (Chen and Jain, 2009)), behavioral (such as keystroke dynamics (Giot et al., 2009a)) and even biological (such as DNA (Hashiyada, 2004)) modalities. Despite the advantages of such systems in providing better security comparing to traditional authentication systems based on "what we own" (such as a key) or "what we know" (such as a password), biometric systems introduce new threats and present limitations in terms of *privacy* and *security*. The International Organization for Standardization (ISO/IEC FCD 19792, 2008) presents a list of several threats and vulnerabilities of biometric systems. The standard also addresses privacy concerns when dealing with biometric systems. Similar concerns have been also raised by the Common Criteria Biometric Evaluation Working Group (CC, 1999). For example, personal biometric information could be tracked from one application to another by cross-matching between biometric databases, thus compromising privacy. Direct attacks illustrated by the presentation of a fake biometric data to the sensor has been also shown as a frequent attack on several biometric modalities such as face, fingerprint and iris. An example of such attack on an iris

recognition system is presented by Ruiz-Albacete et al. (2008). But the security of a biometric system concerns the entire system, not only the sensor. Therefore, it is important that biometric systems be designed to withstand these concerns when employed in security-critical applications and to achieve an end to end security. The goal of this chapter is then to present a privacy- and security-based assessment methodology to be used to evaluate and compare biometric systems.

The outline of the chapter is defined as follows. An introduction to the general concepts of biometric systems is given in Section 2. Section 3 presents an overview of the security and privacy concerns when dealing with biometric systems. We present in Section 4 the existing works regarding the security and privacy assessment of biometric systems. In Section 5, the *Security Evabio* tool which is an on-line tool for the security and privacy assessment of biometric systems is presented. Future trends of the chapter are then given in Section 7.

2. Biometric Technology

2.1. Biometric Modalities

Biometrics refers to the automatic verification or recognition of individuals by measuring their physical/behavioural characteristics. Any of such characteristic can be considered as a biometric information if it satisfies the following properties as detailed in El-Abed et al. (2012a): universality, uniqueness, permanency, collectability and acceptability. An example of the most commonly used biometric modalities is given in Figure 1.

Figure 1: An example of biometric modalities. From left to right, top to bottom, hand veins, face, hand geometry, keystroke dynamics, iris and fingerprint.

2.2. Biometric Process

Biometric systems are concerned by the following functionalities:

- **Enrolment** which constitutes the initial process of collecting biometric data samples from an individual to be used in order to create its reference (called also a biometric template). An example of a biometric template is the extracted minutiae from a fingerprint.
- **Verification** which provides a matching score between the biometric sample provided by the individual and the biometric template of the claimed identity.
- **Identification** which consists of determining the identity of an unknown individual by comparing the user's biometric sample with templates stored in a database.

3. Biometric Systems Limitations

Biometric systems suffer from several security and privacy concerns which may significantly decrease their widespread of use, by the introduction of new threats and vulnerabilities, that are specific to biometrics.

Ratha et al. (2001) have identified eight locations of possible attacks in a generic biometric system as depicted in Figure 2:

- **Point 1**: involves presenting a fake biometric data to the sensor such as a dummy finger.
- **Point 2**: in a replay attack, an intercepted biometric data is submitted to the feature extractor bypassing the sensor.
- **Point 3**: the feature extractor is replaced with a Trojan horse program that functions according to its designer specifications.
- **Point 4**: genuine extracted features are replaced with other features selected by the attacker.
- **Point 5**: the matcher is replaced with a Trojan horse program.
- **Point 6**: involves attacks on the template database.
- **Point 7**: the templates can be altered or stolen during the transmission between the template database and the matcher.

- **Point 8**: the matcher result (accept or reject) can be overridden by the attacker.

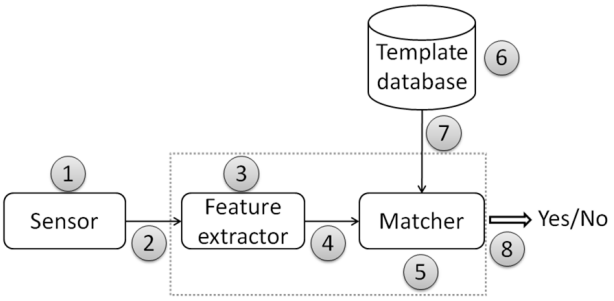

Figure 2: Possible attacks in a generic biometric system according to Ratha et al. (2001)

Direct attacks on biometric sensors (point 1) are the most known attacks in the literature. Several works show the feasibility of such attack on several modalities such as face (Kose and Dugelay, 2013), iris (Ruiz-Albacete et al., 2008) and on-line writer verification system (Yamazaki et al., 2005). A classical example is fake fingers that can be built with silicone, gelatin, wood glue or latex (van der Putte and Keuning, 2000; Matsumoto et al., 2002; Barral and Tria, 2009). Fake fingers constructed with all these technologies are used on different sensor technologies. An example of such attack is presented in Figure 3. It illustrates a successful attack using a fake finger created out of latex that we have created to evaluate several sensors of different technologies (optical and capacitive). Countermeasures including liveness detection are presented in Franco and Maltoni (2007); Galbally et al. (2012).

Several attacks are possible on other parts of the biometric system. Thus, an attacker can introduce a trojan horse in the system, or realize a denial of service attack and corrupts the authentication system so that legitimate users cannot use it. The attacker can also intercept and/or replay the biometric data in order to illegally access or modify the system. Thus, hill-climbing attacks construct iteralively biometric template, by observing the final score of the matcher (Soutar, 2002). It could be realized on several modalities as fingerprints (Uludag and Jain, 2004; Martinez-Diaz et al., 2006, 2011), signature Galbally et al. (2007), iris (Marta Gomez-Barrero and Fierrez, 2012) or face (Adler, 2003; Galbally et al., 2010b; Gomez-Barrero et al., 2012). The attempts are made, by injecting samples on the communication link, to the feature extractor input (image) or the matcher input (template).

Figure 3: Successful attack resulting from the comparison between a fake finger (on the left) and a genuine one stored in the database (right).

More precisely the changes on the synthetic templates are kept if the final score increases and otherwise the corresponding modifications are discarded. Transmission channels (points 2 and 4) are particularly vulnerable to these attacks.

The biometric database (point 6) is an other important target for attackers, particularly for centralized database and non-protected database. This point is directly related with user's privacy by the fact that a biometric trait cannot be replaced if it is compromised. Various attacks are possible, as the possibility to create fraudulently a new template or to modify existing templates without authorization. Galbally et al. (2010a) disproves the popular belief of minutiae templates non-reversibility using fake fingers generated from ISO templates, where the experiments grant access in over 75% of the attempts. Template protection schemes can be used to protect the biometric database (Cavoukian and Stoianov, 2009; ISO 24745, 2011). Nevertheless these techniques do not necessary protect the biometric template against reversibility or distinguishability (Simoens et al., 2009; Blanton and Aliasgari, 2001; Nagar et al., 2010; X.Zhou et al., 2012; Lacharme et al., 2013).

4. Privacy and Security Assessment of Biometric Systems

The privacy and security assessment of biometric systems is now carefully considered. Many platforms have been proposed (such as FVC-onGoing (Maio

et al., 2013) and BioSecure (Petrovska and Mayoue, 2007)) whose objective is mainly to compare biometric systems. However, these platforms are dedicated to quantify the performance technology (algorithms, processing time, *etc.*) without testing the robustness of the target system against fraud neither if it respects the privacy of end-users. This clearly shows that few works are dedicated toward the security and privacy assessment of biometric systems. We focus in this section in presenting an overview of these works.

The International Organization for Standardization ISO/IEC FCD 19792 (2008) has listed several threats and vulnerabilities of biometric systems. In addition to the threats addressed by Maltoni *et al.*, the ISO standard addresses other typical threats related to system performance and the quality of the acquired biometric raw data. It also addresses privacy concerns when dealing with biometric systems but does not propose a security evaluation method of biometric systems. Its aims is to guide the evaluators by giving suggestions and recommendations that should be taken into account during the evaluation process. Dimitriadis and Polemi (2004) present a security comparison study of several biometric technologies in order to be used as an access control system for stadiums. The presented method can easily be used for comparing biometric systems since it is a quantitative-based evaluation method. However, an extended research work should be done in order to take into account the recent vulnerabilities of biometric systems (especially those presented by the ISO/IEC FCD 19792 standard). Attack tree technique introduced by Schneier (1999), provides a structure tree to conduct security analysis of protocols, applications and networks. However, attack trees are dependent from the intended system and its context of use. Therefore, it is infeasible to be used as a generic evaluation purpose. Matyás and Ríha (2002) propose a security classification of biometric systems. Their proposal classifies biometric systems into four categories according to their security level. However, their model could not be considered as discriminative to compare the security level of biometric systems. *Security EvaBio* presented by El-Abed et al. (2012b) is a web-based automated evaluation platform toward the security and privacy evaluation of biometric authentication systems. The aim of the platform is twofold. First, it allows researchers in biometrics to easily evaluate their developed systems using the presented security assessment method. Second, its aims is to enhance the presented database of common threats and vulnerabilities of biometric systems based on researchers feedbacks. To the best to our knowledge, it is the only on-

line evaluation platform for the security and privacy assessment of biometric systems. We present this platform in the next section.

5. Security EvaBio Platform

Security Evabio (El-Abed et al., 2012b) is an online evaluation tool for the security and privacy assessment of biometric systems. A snapshot of this tool is given in Figure 4. It implements a quantitative-based assessment method based on a database of common threats and vulnerabilities of biometric systems, and the notion of risk factors. The principle of the proposed approach contains four steps as detailed below: study of the context, expression of security needs, risk analysis and security index. We present in Sections 5.1, 5.2, 5.3 and 5.4 the four mentioned steps followed by the database of common threats and vulnerabilities of biometric systems in Section 5.5. A comparison study of two different biometric systems is presented in Section 6 to clarify the relevance of *Security Evabio* assessment tool.

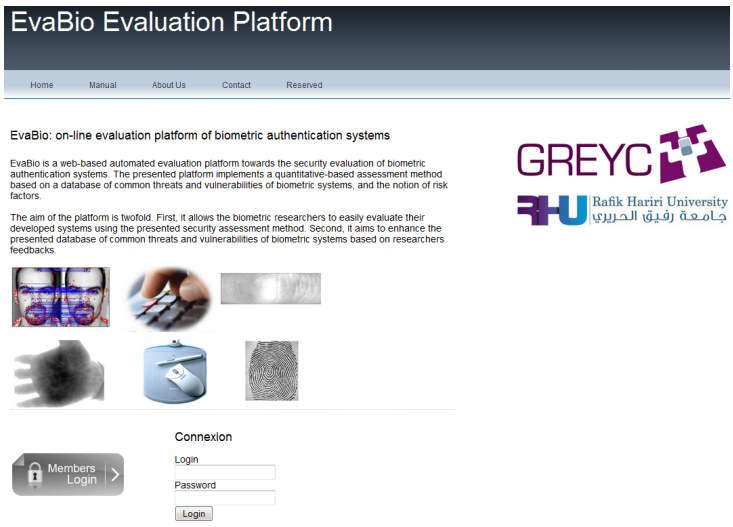

Figure 4: Security EvaBio on-line evaluation tool accessible through the following link: `http://www.epaymentbiometrics.ensicaen.fr/securityEvaBio/index.php`.

5.1. Study of the Context

The first step consists of identifying the utility and the characteristics of the target system. This step consists also of detailing its different components

and essential elements (known by assets). Using the generic architecture of biometric systems as illustrated in Figure 2 by Ratha *et al.*, the identified assets to be protected are divided into three types as presented in Table 1: an information (I_), a function (F_) and a material (M_).

Reference	**Description**
I_DATA_BIO	Acquired biometric raw data
I_TEMPLATE	User template
I_DECISION	System decision (yes or no)
F_EXTRACTION	Processing data function implemented on the feature extractor component
F_MATCHER	Matcher function between the acquired biometric data and its corresponding template
M_SENSOR	Biometric sensor
M_COMPONENT	Materials in which the F_EXTRACTION and F_MATCHER are implemented
M_BD	Storage medium of the biometric templates
M_CHANNELS	Transmission channels connecting the different components of the target system

Table 1: The identified assets of a generic biometric system

5.2. Expression of Security Needs

After describing the target system, the next step consists of identifying the security requirements that will contribute to the risk assessment process. As any IT system, these requirements should include confidentiality (C), integrity (I), availability (D) and authenticity (A). In the context of biometric systems, confidentiality ensures the privacy and civil liberties of its intended users, whereas authentication is the main functionality of biometric systems.

Security needs of biometric systems include the confidentiality and the integrity of the biometric data I_DATA_BIO and I_TEMPLATE (the confidentiality of I_DATA_BIO and I_TEMPLATE are particularly important in a privacy context). Security needs also include the availability on M_SENSOR, M_CHANNELS, I_TEMPLATE and F_EXTRACTION. Finally, the authenticity on I_DECISION is directly related to the functionality of a biometric system. These security requirements are necessary in order to ensure the security of the biometric system.

5.3. Risk Analysis

Risk analysis is essential to ensure the proper functionality of any IT system. It is generally realized within two approaches: quantitative or qual-

itative approaches. A comparative study of both approaches (advantages and limitations) is presented by Rot (2008). *Security Evabio* implements a quantitative approach based on the notion of risk factors. The choice of the quantitative approach is mainly retained to its easiness when evaluating and comparing biometric systems. It is also more exploitable lately during the risk reduction process. A risk factor, for each identified threat and vulnerability, is considered as an indicator of its importance. The computation of risk factors in the presented method is given in both Sections 5.3.1 (identified threats) and 5.3.2 (retained vulnerabilities).

5.3.1. Risk factor computation of the identified threats

The risk factor computation of each identified threat uses a quantitative approach based on the multi-criteria analysis (MCA, 2009). More generally speaking, two criteria are used for the risk factor computation of each identified threat ($risk\ factor = f_1 \times f_2$):

- **Impact (f_1):** represents the impact of the threat in terms of criticality. It is defined between 0 and 10 (the highest score 10 corresponds to a critical attack). This factor is arbitrary fixed according to the four security requirements (confidentiality, integrity, availability and authenticity) presented in Section 5.2. The impact (f_1) of threats affecting the confidentiality property is penalized more since such kind of threats affect the privacy and civil liberties of legitimate users.

- **Easiness (f_2):** represents the easiness to make a successful attack. It is defined between 0 and 10 (the lowest score 0 corresponds to an impossible attack, while the highest score 10 corresponds to an easy attack). This factor is arbitrary fixed using two types of informations: first, the weakness of the target system (*e.g.*, weakness related to its architecture), second, the cost in terms of specific equipments and required expertise to implement the attack.

5.3.2. Risk factor computation of the vulnerabilities

For the three retained system overall vulnerabilities (see Section 5.5.2), the tool uses a set of rules for the risk factors computation process as depicted in Table 2. For the system performance vulnerability, it is multiplied by 2 since a biometric system providing a performance measure (such as the Equal Error Rate EER) more than or equal to 50% is not usable. For such systems,

the risk factor is rated to the highest score 100. For the quality aspect, there is four rules according to whether the system implements quality checking during the enrollment step. For the templates database protection, there is also a set of rules according to whether the system implements protection mechanisms (such as encryption schemes, cancelable techniques, *etc.*).

Point	Rules	Risk factor
9	Sufficient panel of users	$2 \times$ EER
10	- Multiple captures with quality assessment	0
	- One capture with quality assessment	40
	- Multiple captures without quality assessment	60
	- One capture without quality assessment	100
11	- Secure database and local storage	0
	- Secure database and central storage	40
	- Unsecure database and local storage	60
	- Unsecure database and central storage	100

Table 2: General scheme of risk computation for the system overall vulnerabilities

5.4. Security Index

Security EvaBio uses the notion of the area under curve of the curve resulting from the retained risk factors to compute the security index of the target system. It is calculated using the trapezoid rule. The main benefit of using this approach is that it permits to take into account all the risks of a biometric system and their relationships in the processing chain. The security index of the target system is then defined as follows:

$$\text{Index} \;=\; \alpha \;\left(1 - \frac{AUC(f(x))}{AUC(g(x))}\right) = \alpha \;\left(1 - \frac{\int_1^n f(x)\,\mathrm{d}x}{\int_1^n g(x)\,\mathrm{d}x}\right) \tag{1}$$

where α =100, $n = r + s$ with r the number of locations of possible attacks in a generic biometric system and s the number of the retained system overall vulnerabilities (in the presented method, $r = 8$ and $s = 3$); f(x) is the curve resulting from the set of risk factors retained from the n points (the maximal risk factor is retained from each point); and g(x) is the curve resulting from a set of the highest risk factors we can have from each point (according to our model, they are equal to 100). The use of the security index for comparing and evaluating biometric systems is used as follows: the more the index is near 100%, the better is the robustness of the target system against attacks.

5.5. Database of Common threats and Vulnerabilities

The database of common threats and vulnerabilities used by *Security EvaBio* is presented in this section. The presented database is collected due to the results of desk research at the GREYC research laboratory, and take into account the known threats presented in previous works (such as those presented in (Maltoni et al., 2003; Roberts, 2007)). The database followed also the concerns and the recommendations presented by the International Organization for Standardization (ISO/IEC FCD 19792, 2008). It is mainly divided into two categories: system threats (Section 5.5.1) and system overall vulnerabilities (Section 5.5.2).

5.5.1. System Threats

The presented threats are related to the locations of possible attacks in a generic biometric system as illustrated in Figure 2. Each threat is presented as the following form: "Description" which defines the threat, and "Affect" describes which couples (*security requirement* on *asset*) will be affected in the case of a successful attack. This representation allows automatically *Security EvaBio* to compute the risk factor of each identified threat during the evaluation process.

Attack	Details
A_{11}	Description: Attacker presents a fake biometric data to the sensor (*e.g.*, prosthetic fingers created out of latex). Such kind of attack is called spoofing Affect: Authenticity on I_DECISION
A_{12}	Description: Attacker exploits the similarity due to blood relationship to gain access (*e.g.*, case of identical twins and biometric systems using specific modalities such as face) Affect: Authenticity on I_DECISION
A_{13}	Description: Authorized users willingly provide their biometric sample to attacker Affect: Authenticity on I_DECISION
A_{14}	Description: Attacker provides own biometric sample as a zero-effort attempt to impersonate an authorized user Affect: Authenticity on I_DECISION
A_{15}	Description: Attacker exploits a residual biometric image left on the sensor to impersonate the last authorized user Affect: Confidentiality on I_DATA_BIO; Authenticity on I_DECISION
A_{16}	Description: Attacker physically destroy the biometric sensor to turn it out of service Affect: Availability on M_SENSOR

Table 3: Attacks on point 1. Sensor

Attack	Details
A_{241}	Description: The attacker intercepts an authorized biometric sample from a communication channel in order to be replayed (replay attack), bypassing the biometric sensor, at another time for gaining access Affect: Confidentiality on I_DATA_BIO; Authenticity on I_DECISION
A_{242}	Description: The attacker cuts the communication link in order to make the system unavailable to its intended authorized users (Denial of Service attack) Affect: Availability on M_CHANNELS
A_{243}	Description: The attacker alters the transported information from a communication channel in order to deny legitimate users to be authenticated (Denial of Service attack) Affect: Integrity on I_DATA_BIO; Integrity on M_CHANNELS
A_{244}	Description: The attacker attempts continuously to enter the system (known as hill-climbing attack), the input image/template is conveniently modified until a desired matching score is attained. The attempts are made, by injecting samples on the communication link, to the feature extractor input (image) or the matcher input (template) Affect: Authenticity on I_DECISION
A_{245}	Description: The attacker injects continuously samples in order to deny the legitimate users to access the system (Denial of Service attack) Affect: Availability on M_CHANNELS

Table 4: Attacks on points 2 and 4. Transmission channels

Attack	Details
A_{351}	Description: Biometric system components may be replaced with a Trojan horse program that functions according to its designers' specifications Affect: Confidentiality on I_DATA_BIO; Confidentiality on I_TEMPLATE; Availability on F_EXTRACTION; Availability on F_MATCHER

Table 5: Attacks on points 3 and 5. Software components

Attack	Details
A_{61}	Description: The attacker illegally reads the biometric templates Affect: Confidentiality on I_TEMPLATE; Authenticity on I_DECISION
A_{62}	Description: The attacker modifies (adding, replacing or suppressing) biometric templates from storage Affect: Availability on I_TEMPLATE; Integrity on I_TEMPLATE

Table 6: Attacks on points 6. Template database

5.5.2. System Overall Vulnerabilities

- **Point 9. Performance limitations**
  By contrast to traditional authentication methods based on "what we

Attack	Details
A_{71}	Description: The attacker reads biometric templates from a communication channel in order to be replayed (replay attack) Affect: Confidentiality on I_TEMPLATE; Authenticity on I_DECISION
A_{72}	Description: The attacker alters the transported information from a communication channel in order to deny the legitimate users to access the system (Denial of Service attack) Affect: Integrity on I_TEMPLATE; Integrity on M_CHANNELS
A_{73}	Description: The attacker cuts the communication link in order to make the system unavailable to its intended authorized users (Denial of Service attack) Affect: Availability on M_CHANNELS

Table 7: Attacks on points 7. Transmission channel

Attack	Details
A_{81}	Description: The attacker alters the transported information (yes or no) in order to deny access of a legitimate user, or even allow access to an impostor Affect: Integrity on I_DECISION; Authenticity on I_DECISION
A_{82}	Description: The attacker cuts the communication link in order to make the system unavailable to its intended authorized users (Denial of Service attack) Affect: Availability on M_CHANNELS

Table 8: Attacks on points 8. Transmission channel

know" or "what we own" (0% comparison error), biometric systems are subject to errors such as False Acceptance Rate (FAR) and False Rejection Rate (FRR). This inaccuracy illustrated by statistical rates has potential implications regarding the level of security provided by a biometric system. Doddington et al. (1998) assigns users into four categories: sheep, lambs, goats and wolves. The sheep correspond to users who are easily recognized (contribute to a low FRR). The lambs correspond to users who are easy to imitate (contribute to a high FAR). The goats represent users who are difficult to recognize (contribute to a high FRR). The wolves represent users who have the capability to spoof the biometric characteristics of other users (contribute to a high FAR). Thus, a poor biometric in terms of performance, may be easily attacked by lambs and wolves users.

- **Point 10. Quality limitations during the enrollment process**
  The quality of the acquired biometric samples is considered as an important factor during the enrollment process. It is a generic organizational point of view in the deployment of the biometric system. The

absence of a quality test increases the possibility of enrolling authorized users with weak templates. Such templates increase the probability of success of zero-effort impostor, hill-climbing and brute force attempts.

- **Point 11. Protection schemes of the biometric templates**
  The use of biometric systems presents concerns in terms of privacy. The fact of storing biometric data in a central database is considered as a violation of civil liberties. Biometric template security is becoming a major concern in biometrics field since, because compromised templates cannot be revoked and reissued.

6. Security EvaBio Assessment

The security and privacy assessment of two different biometric systems is presented in this section to clarify the relevance of the *Security EvaBio* platform. The first one is a keystroke dynamics application developed in the GREYC research laboratory (Giot et al., 2009b) while the second one is a commercial fingerprint lock to manage physical access.

The architecture and the main characteristics of the keystroke dynamics system are:

- The system implements a score-based method and provides an EER of 17.51%.
- System architecture is not distributed (all system components including the template database are implemented within the same PC).
- There is no data protection neither encryption schemes applied on the template database.
- There is no quality check during the enrollment phase.
- The used PC is connected to the Internet.

For the fingerprint lock system:

- The system provides an EER of 0.1%.
- There is no data protection neither encryption schemes applied on the template database, but it is physically protected.

- System architecture is not distributed (all system components including template database are implemented within the same material).
- The material is not connected to the Internet and there is no USB port.
- There is no quality check during enrolment phase.
- The material power supply is 4 * 1.5V AA batteries with a life span of 1-2 years.

Tables 9 and 10 present the risk analysis of both target systems presented in the previous section. For the "Impact" and "Easiness" criteria (f_1 and f_2, respectively), we have put the symbol "-" in the last three lines since the corresponding risk factors are computed according to the set of rules presented in Table 2. From Table 9, we have identified three threats on the sensor such as A_{16} threat. For this threat, the "Impact" criterion ($\mathbf{f}_1$) is automatically rated by the platform to the value 2 since such kind of threat does not affect the "confidentiality" property. For the "Easiness" criterion ($\mathbf{f}_2$), we have rated (using the ten-point Likert-type scale) at 10, since there is no physical protection of the keyboard.

Figure 5 illustrates a comparative study (of the maximal value of risk factor at each location) between both systems. From this figure, we can conclude several results such as: fingerprint lock system is much more vulnerable at location 1 than the keystroke dynamics system, keystroke dynamics system is much more vulnerable at locations 2, 3, 5, 6, 7, 8 and 9 than fingerprint lock system, both systems are not vulnerable at location 4.

Using Equation 1, the security index (total risk) of keystroke dynamics system is equal to (56.7%), while for the fingerprint lock system it is equal to (86%). These indexes show clearly that the overall security of keystroke system is less important than the fingerprint lock system against attacks. Because the fingerprint lock system is a black box, we cannot say a lot of things for different locations. Even if we have not presented security problems for these locations, an attacker could be able to find them, thanks to reverse engineering (hardware and software). However, the use of the commercial system in this study was taken as an illustration case for the comparison. More generally speaking, during the security evaluation process of an IT system, system designers should provide all the details/characteristics of the intended system for the evaluators.

Point	Attack	C	I	D	A	f_1	f_2	Risk
1	A_{14}				×	6	2	12
	A_{16}			×		2	10	20
	A_{15}	×			×	8	3	24
2	A_{245}			×		2	6	12
	A_{243}		×			2	6	12
	A_{242}			×		2	10	20
	A_{244}				×	6	4	24
	A_{241}	×			×	8	6	48
3	A_{351}	×		×		8	6	48
5	A_{351}	×		×		8	6	48
6	A_{62}		×	×		8	4	32
	A_{61}	×			×	8	6	48
7	A_{72}		×			2	6	12
	A_{73}			×		2	10	20
	A_{71}	×			×	8	6	48
8	A_{82}			×		2	10	20
	A_{81}		×		×	6	6	36
9	Performance				×	-	-	35.02
10	Multiple captures without quality assessment				×	-	-	60
11	Unsecure database and central storage	×	×	×	×	-	-	100

Table 9: Security analysis of GREYC-Keystroke (C: Confidentiality, I: Integrity, D: Availability, A: Authenticity).

Point	Attack	C	I	D	A	f_1	f_2	Risk
1	A_{16}			×		2	10	20
	A_{11}				×	6	8	48
	A_{13}				×	6	8	48
	A_{15}	×			×	10	6	60
9	Performance				×	-	-	0.1
10	Multiple captures without quality assessment				×	-	-	60
11	Unsecure database and central storage	×	×	×	×	-	-	100

Table 10: Security analysis of the fingerprint lock system (C: Confidentiality, I: Integrity, D: Availability, A: Authenticity).

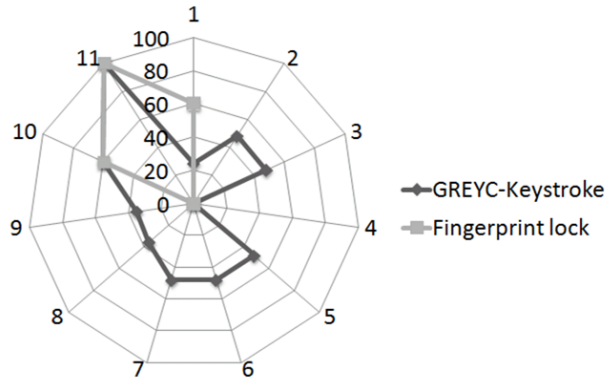

Figure 5: A comparative illustration of both systems among the 11 tested points

7. Future Trends

7.1. Multibiometric

Multibiometric authentication systems use multiple biometric sources in order to recognize a person. These systems are gaining popularity since they provide better performance and larger population coverage comparing to classical biometric systems (Ross et al., 2006). Besides enhancing matching performance, these systems are considered to be promising against spoof attacks that are commonly encountered in classical biometric systems as shown in this chapter.

7.2. Biometric Information Protection

Secure biometric information storage is critical since once revealed, they would allow am attacker to obtain sufficient information to impersonate a genuine user. This is considered as a challenging issue because it is difficult to guarantee that a storage device (such as server or smart card) can never be compromised, and once compromised, users' templates cannot be revoked like passwords. The International Standard (ISO 24745, 2011) aims to present the potential threats and requirements with respect to confidentiality, integrity, availability and renewability of biometric templates during storage and transmission. In addition, several works exist that deal with biometric data protection such as applying a biohashing scheme (Belguechi et al., 2013).

Biography

Mohamad El-Abed is an assistant professor at Rafik Hariri University, Lebanon. His research interests biometrics, especially the evaluation of biometric systems.

Patrick Lacharme is an associate professor at the school of engineering of Caen ENSICAEN, France. His research interests include cryptography and biometrics. He is particularly interested in authentication methods respecting the privacy of end users.

Christophe Rosenberger is a full professor at the school of engineering of Caen ENSICAEN, France. His research interests include computer security and biometrics. He is particularly interested in authentication methods for e-transactions applications.

References

Adler, A., 2003. Sample images can be independently restored from face recognition templates. Electrical and Computer Engineering 2, 1163–1166.

Barral, C., Tria, A., 2009. Fake fingers in fingerprint recognition: Glycerin supersedes gelatin. In: Formal to Practical Security, LNCS 5458. pp. 57–69.

Belguechi, R., Cherrier, E., Rosenberger, C., Ait-Aoudia, S., 2013. An integrated framework combining bio-hashed minutiae template and pkcs15 compliant card for a better secure management of fingerprint cancelable templates. Computers & Security 39, 325–339.

Blanton, M., Aliasgari, M., 2001. On the (non)-reusability of fuzzy scketches and extractors and security in the computational setting. In: Secrypt.

Cavoukian, A., Stoianov, A., 2009. Biometric encryption chapter from the encyclopedia of biometrics.

CC, 1999. Common Criteria for Information Technology Security Evaluation.

Chen, Y., Jain, A., 2009. Beyond minutiae: A fingerprint individuality model with pattern, ridge and pore features. In: International Conference on Biometrics (ICB). pp. 523–533.

Dimitriadis, C., Polemi, D., 2004. Application of multi-criteria analysis for the creation of a risk assessment knowledgebase for biometric systems. In: international conference on biometric authentication (ICB). Vol. 3072. pp. 724–730.

Doddington, G., Liggett, W., Martin, A., Przybocki, M., Reynolds, D., 1998. Sheep, goats, lambs and wolves: A statistical analysis of speaker performance in the NIST 1998 speaker recognition evaluation. In: International Conference on Spoken Language Processing (ICSLP). pp. 1–4.

El-Abed, M., Charrier, C., Rosenberger, C., 2012a. New Trends and Developments in Biometrics. InTech, Ch. Evaluation of Biometric Systems, pp. 149–169.

El-Abed, M., Lacharme, P., Rosenberger, C., 2012b. Security evabio: An analysis tool for the security evaluation of biometric authentication systems. In: the 5th IAPR/IEEE International Conference on Biometrics (ICB). pp. 1–6.

Franco, A., Maltoni, D., 2007. Advances in Biometrics: Sensors, Systems and Algorithms, Ch. Fingerprint Synthesis and Spoof Detection.

Galbally, J., Alonso-Fernandez, F., Fierrez, J., Ortega-Garcia, J., 2012. A high performance fingerprint liveness detection method based on quality related features. Elsevier Future Generation Computer Systems.

Galbally, J., Cappelli, R., Lumini, A., Gonzalez-de Rivera, G., Maltoni, D., Fierrez, J., Ortega-Garcia, J., Maio, D., 2010a. An evaluation of direct attacks using fake fingers generated from iso templates. Pattern Recognition Letters 31, 725–732.

Galbally, J., Fierrez, J., Ortega-Garcia, J., 2007. Bayesian hill-climbing attack and its application to signature verification. In: International Conference on Biometrics (ICB), LNCS 4642. pp. 386–395.

Galbally, J., McCool, C., Fierreza, J., Marcel, S., Ortega-Garcia, J., 2010b. On the vulnerability of face verification systems to hill-climbing attacks. Pattern Recognition, Elsevier.

Giot, R., Abed, M. E., Rosenberger, C., 2009a. Keystroke dynamics with low constraints SVM based passphrase enrollment. In: IEEE Third International Conference on Biometrics : Theory, Applications and Systems (BTAS). pp. 425–430.

Giot, R., El-Abed, M., Rosenberger, C., 2009b. Greyc keystroke : a benchmark for keystroke dynamics biometric systems. In: IEEE Third International Conference on Biometrics : Theory, Applications and Systems (BTAS). pp. 1–6.

Gomez-Barrero, M., Galbally, J., Fierrez, J., Ortega-Garcia, J., 2012. Face verification put to test: A hill-climbing attack based on the uphill-simplex algorithm. In: International Conference on Biometrics (ICB).

Hashiyada, M., 2004. Development of biometric dna ink for authentication security. Tohoku Journal of Experimental Medicine, 109–117.

ISO 24745, 2011. Information technology – security techniques – biometric information protection.

ISO/IEC FCD 19792, 2008. Information technology – security techniques – security evaluation of biometrics.

Jain, A. K., Pankanti, S., Prabhakar, S., Hong, L., Ross, A., 2004. Biometrics: A grand challenge. International Conference on Pattern Recognition (ICPR) 2, 935–942.

Kose, N., Dugelay, J.-L., 2013. On the vulnerability of face recognition systems to spoofing mask attacks. In: ICASSP 2013, IEEE International Conference on Acoustics, Speech, and Signal Processing.

Lacharme, P., Cherrier, E., Rosenberger, C., 2013. Preimage attack on biohashing. In: Secrypt.

Maio, D., Maltoni, D., Capelli, R., Franco, A., Ferrara, M., Turroni, F., 2013. FVC-onGoing: on-line evaluation of fingerprint recognition algorithms. URL `https://biolab.csr.unibo.it/fvcongoing/UI/Form/Home.aspx`

Maltoni, D., Maio, D., Jain, A. K., Prabhakar, S., 2003. Handbook of Fingerprint Recognition. Springer-Verlag.

Marta Gomez-Barrero, Javier Galbally, P. T., Fierrez, J., 2012. On the vulnerability of iris-based systems to a software attack based on a genetic algorithm. In: CVIARP.

Martinez-Diaz, M., Fierrez, J., Galbally, J., Ortega-Garcia, J., 2011. An evaluation of indirect attacks and countermeasures in fingerprint verification systems. Pattern Recognition Letters 32, 1643–165.

Martinez-Diaz, M., Fierrez-Aguilar, J., Alonso-Fernandez, F., Ortega-Garcia, J., Siguenza, J., 2006. Hill-climbing and brute-force attacks on biometric systems: A case study in match-on-card fingerprint verification. In: In Carnahan Conferences Security Technology. pp. 151–159.

Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S., 2002. Impact of Artificial Gummy Fingers on Fingerprint Systems. In: SPIE, Optical Security and Counterfeit Deterrence Techniques.

Matyás, V., Ríha, Z., 2002. Biometric authentication - security and usability. In: Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security. pp. 227–239.

MCA, 2009. Multi-criteria analysis: a manual. Department for Communities and Local Government: London.

Nagar, A., Nandakumar, K., Jain, A., 2010. Biometric template transformation: A security analysis. In: Proceedings of SPIE, Electronic Imaging, Media Forensics and Security XII.

Petrovska, D., Mayoue, A., 2007. Description and documentation of the BioSecure software library. Tech. rep., BioSecure.

Ratha, N. K., Connell, J. H., Bolle, R. M., 2001. An analysis of minutiae matching strength. In: Audio- and Video-Based Biometric Person Authentication. pp. 223–228.

Roberts, C., 2007. Biometric attack vectors and defences. Computers & Security.

Ross, A., Jain, A., Nandakumar, K., 2006. Handbook of Multibiometrics. Springer.

Rot, A., 2008. IT risk assessment: Quantitative and qualitative approach. In: the World Congress on Engineering and Computer Science (WCECS). pp. 1–6.

Ruiz-Albacete, V., Tome-Gonzalez, P., Alonso-Fernandez, F., Galbally, J., Fierrez, J., Ortega-Garcia, J., 2008. Direct attacks using fake images in iris verification. In: Biometrics and Identity Management. pp. 181–190.

Schneier, B., 1999. Attack trees. Dr. Dobb's Journ. of Softw. Tools.

Simoens, K., Tuyls, P., Preneel, B., 2009. Privacy weaknesses in biometric sketches. In: IEEE symposium on Security and Privacy.

Soutar, C., 2002. Biometric system security.

Uludag, U., Jain, A. K., 2004. Attacks on biometric systems: A case study in fingerprints. In: Proc. SPIE-EI 2004, Security, Seganography and Watermarking of Multimedia Contents VI. Vol. 5306. pp. 622–633.

van der Putte, T., Keuning, J., 2000. Biometrical fingerprint recognition: Don't get your fingers burned. In: Proceedings of CARDIS, vol 180. pp. 289–306.

X.Zhou, Kuijper, A., Busch, C., 2012. Cracking iris fuzzy commitment. In: International Conference on Biometrics (ICB).

Yamazaki, Y., Nakashima, A., Tasaka, K., Komatsu, N., 2005. A Study on Vulnerability in On-line Writer Verification System. In: Eighth International Conference on Document Analysis and Recognition.